Cisco IPICS Troubleshooting Guide

Release 2.0(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-8362-02

Cisco IPICS Troubleshooting Guide

Preface

The *Cisco IPICS Troubleshooting Guide, Release 2.0(1)* provides you with the information that you need to troubleshoot problems that you may encounter when you install, configure, or use the Cisco IP Interoperability and Collaboration System (hereafter referred to as *Cisco IPICS*) solution. System administrators should review this document to aid in their troubleshooting efforts for problems that they may encounter when they use Cisco IPICS.

Audience

The *Cisco IPICS Troubleshooting Guide, Release 2.0(1)* targets system administrators who install, configure, operate, and manage tasks on the Cisco IPICS system. This document also targets end users who communicate with other users by using a PMC or Cisco IP Phone.

Organization

This document is organized as follows:

Chapter 1, "Finding Troubleshooting Information for Cisco IPICS"	This chapter provides information about how to find troubleshooting information for Cisco IPICS.
Chapter 2, "Troubleshooting Cisco IPICS Network Processes"	This chapter includes troubleshooting tips for the network processes that the Cisco IPICS server uses, such as the tomcat service, the database server, the license manager, the dial engine, and the Cisco Security Agent (CSA).
Chapter 3, "Troubleshooting the Cisco IPICS Server"	This chapter includes information about troubleshooting the Cisco IPICS server and Cisco IPICS policy engine (hereafter known as policy engine). It also includes information about components that work with Cisco IPICS, such as Cisco Unified IP Phones and the router media service (RMS).
Chapter 4, "Troubleshooting Tips for the PMC Application"	This chapter includes troubleshooting information for the Cisco IPICS Push-to-Talk Management Center (PMC).
Chapter 5, "Using the Cisco IPICS CLI Tools and Service Commands"	This chapter includes information about the command line interface (CLI) tools and service commands that you can use with Cisco IPICS.
Chapter 6, "Understanding the Cisco IPICS Logs"	This chapter includes information about the activity and error logs that Cisco IPICS generates, along with information about how to interpret the data in the logs.

Related Documentation

For more information about Cisco IPICS components, refer to the following documentation:

- *Cisco IPICS PMC Installation and User Guide, Release 2.0(1)*—This document describes how to install, configure, manage, and operate the Cisco IPICS PMC application.
- *Cisco IPICS PMC Quick Start Reference Card, Release 2.0(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 2.0(1)*—This document provides a quick reference for troubleshooting and debugging the Cisco IPICS PMC.
- *Cisco IPICS PMC Command Line Interface, Release 2.0(1)*—Describes the commands that you can use from the command line interface (CLI) to obtain information or to change settings for the Cisco IPICS PMC.
- *Cisco IPICS Server Administration Guide, Release 2.0(1)*—This document contains information about the key configuration, operation, and management tasks for the Cisco IPICS server.
- *Cisco IPICS Server Quick Start Guide, Release 2.0(1)*—This document is a condensed version of the *Cisco IPICS Server Administration Guide* to help the administrator to quickly get started with Cisco IPICS.
- *Cisco IPICS Server Quick Start Reference Card, Release 2.0(1)*—This document provides tips, quick references, and usage guidelines for the Cisco IPICS server.
- *Cisco IPICS Server Installation and Upgrade Guide, Release 2.0(1)*—Describes how to install, configure, and upgrade the Cisco IPICS server software and Cisco IPICS operating system.
- *Cisco IPICS Server Quick Start Installation Reference Card, Release 2.0(1)*—This document provides tips and quick references for installing and upgrading the Cisco IPICS server.
- *Release Notes for Cisco IPICS Release 2.0(1)*—This document contains a description of the new and changed features, important notes, caveats, and documentation updates for this release of Cisco IPICS.

- *Cisco IPICS 2.0(1) Resources Card (Documentation Locator)*—This document provides a summary of the documentation that is available for this release of Cisco IPICS.
- *Solution Reference Network Design (SRND) for Cisco IPICS Release 2.0(1)*— This document provides information about design considerations and guidelines for deploying the Cisco IPICS solution.
- *Cisco IPICS Compatibility Matrix*—This document contains information about compatible hardware and software that is supported for use with Cisco IPICS.

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

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

Cisco Unified CallManager Documentation

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

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

Cisco Unified CallManager Express Documentation

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

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

Cisco 7800 Series Media Convergence Servers Documentation

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

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

Cisco Unified IP Phone Documentation

For information about Cisco Unified IP Phones, refer to 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 Documentation

For information about Cisco Land Mobile Radio (LMR) over IP, refer to 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 Documentation

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

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

Voice Quality Documentation

For 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

IP Multicast Documentation

For a description of common problems and solutions that relate to using IP multicast communications, refer to 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/en/US/products/ps6552/products_ios_technology_home.html

Session Initiation Protocol Documentation

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

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

Document Notes and Conventions

This document uses the following conventions for instructions and information:

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

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

Table 1 Conventions

Convention	Description
boldface font	Commands and keywords appear in **boldface**.
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. This section explains the product documentation resources that Cisco offers.

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

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

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

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

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

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

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

If you do not have a user ID or password, you can register at this URL:

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

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Technical Support & Documentation site area by entering your comments in the feedback form available in every online document.

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 will find information about how to do the following:

- 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, security notices, and security responses for Cisco products is available at this URL:

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

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at 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 have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only—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.

- For 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 (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked encryption key 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.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive Cisco Product Alerts and Cisco Field Notices by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. (To register as a Cisco.com user, go to this URL: http://tools.cisco.com/RPF/register/register.do) Registered users can access the tool at this URL: http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

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 Tool** to locate your product serial number before submitting a request for service online or by phone. You can access this tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This 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.

Tip Displaying and Searching on Cisco.com

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing F5.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. On the Cisco.com home page, click the **Advanced Search** link under the Search box and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

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)—An existing network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations 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 the network is impaired while 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.

- The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

  http://www.cisco.com/offer/subscribe

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:

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

- 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

- *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 where networking professionals 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

- "What's New in Cisco Documentation" is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of "What's New in Cisco Documentation" at this URL:

  http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

- 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

Finding Troubleshooting Information for Cisco IPICS

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

Table 1-1 Locating Troubleshooting Information

Source of Problem	Where to Find Help
Issues with Cisco IPICS installation	To troubleshoot problems related to installing Cisco IPICS, refer to the "Troubleshooting the Installation" chapter of the *Cisco IPICS Server Installation and Upgrade Guide, Release 2.0(1)*.
Issues with one of the following areas: • The Cisco IPICS server • Policy engine • Communication between Cisco IPICS end-user devices • Equipment, such as Cisco Unified IP Phones • RMS configuration • General operation	For problems that are related to the server, the policy engine, and the devices that communicate with the server, see Chapter 3, "Troubleshooting the Cisco IPICS Server." For help in gathering log information to enhance your problem determination and resolution process, see Chapter 6, "Understanding the Cisco IPICS Logs."

Table 1-1 Locating Troubleshooting Information (continued)

Source of Problem	Where to Find Help
PMC issues	To troubleshoot problems that you may encounter when you install or use the PMC application, see Chapter 4, "Troubleshooting Tips for the PMC Application." For help in gathering PMC log information to enhance your problem determination and resolution process, see the "Generating and Modifying the PMC Log Levels" section on page 6-6.
Backup and restore issues	To obtain information about backing up or restoring the Cisco IPICS database, or to troubleshoot problems that you encounter in the backup or restore process, refer to the "Performing Cisco IPICS Database Backup and Restore Operations" chapter of the *Cisco IPICS Server Administration Guide, Release 2.0(1)*.
Licensing issues	For information about problems that are related to the installation and usage of licenses, refer to the "Troubleshooting the Installation" chapter of the *Cisco IPICS Server Installation and Upgrade Guide, Release 2.0(1)*.

CHAPTER 2

Troubleshooting Cisco IPICS Network Processes

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

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

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

Note This chapter provides you with procedures that require you to check the network processes by accessing the server via a terminal console session, logging in with the root user ID, and entering command-line interface (CLI) commands. If the tomcat service and database server are both running, you can check their status

without using CLI by logging in to the Administration Console, navigating to the **Serviceability > Diagnostics** window, and viewing the information in the Diagnostic Summary pane.

Performing Tomcat Service Procedures

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

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

This section includes the following topics:

Checking the Status of the Tomcat Service

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

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

Procedure

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

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

[root]# **service ipics_tomcat status**

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

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

If the tomcat service is not running, the response to the **status** command is similar to the following example:

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

If the **status** command shows that the tomcat service is not running, you can start it manually by entering the **service ipics_tomcat start** CLI command. For more information, see the "Starting the Tomcat Service" section on page 2-4.

Stopping the Tomcat Service

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

To stop the tomcat service, perform the following procedure:

Procedure

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

The console terminal displays.

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

[root]# **service ipics_tomcat stop**

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

If the tomcat service does not stop, Cisco IPICS displays an error message. If you cannot stop the tomcat service, continue to Step 3.

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

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

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

b. Note the Process IDs, which display in the second column of the grep results.

c. To stop the tomcat processes that are still running, enter the following command:

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

where:

<*process-id*> specifies the Process IDs that you noted in Step b.

d. Repeat Step c for every tomcat process that is running.

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

[root]# **service ipics_tomcat status**

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

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

Step 5 If a message displays that indicates that the tomcat service is running on the system, contact your Cisco technical support representative for further assistance.

Starting the Tomcat Service

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

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

Procedure

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

A terminal window displays.

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

[root]# **service ipics_tomcat start**

If you successfully started the tomcat service, Cisco IPICS 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 3 If the tomcat service does not successfully start, check the following files to gather information on the nature of the problem:

- **/root/tomcat/current/logs/catalina.out**
- **/root/tomcat/current/logs/catalina.***yyyy-mm-dd***.log**

  where:

  yyyy-mm-dd is the date on which the file was created.

Note The catalina logs contain information about the Cisco IPICS web-based processes, including the tomcat service.

Step 4 Attempt to fix the problem based on the information that you obtained in the log files. The logs can provide you with information to find the root cause of a process that could not start, or that terminated unexpectedly.

Step 5 If you cannot resolve the problem with the information in the log files, contact your Cisco technical support representative for further assistance.

Restarting the Tomcat Service

To restart the tomcat service, while it is already running, execute the **restart** command.

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

To restart the tomcat service, perform the following procedure:

Procedure

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

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

[root]# **service ipics_tomcat restart**

After restarting the tomcat service, Cisco IPICS 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 Database Server Procedures

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

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

- Checking the Status of the Database Server, page 2-6
- Restarting the Database Server, page 2-7
- Starting the Database Server, page 2-8

Checking the Status of the Database Server

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

Note If the database server is stopped, you cannot log in to the Administration Console to check its status.

If you cannot log in to the Administration Console, you can manually check the status of the database server by performing the following procedure:

Procedure

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

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

[root]# **service ipics_db status**

If the database server is running properly, the **status** command returns a process that is similar to the following example:

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

If the database server is not running, the response to the **status** command is similar to the following example:

```
Ipics Database is stopped.
```

If the **status** command indicates that the database server is not running, start the database server. For more information, see the "Starting the Database Server" section on page 2-8l.

Restarting the Database Server

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

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

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

To restart the database server, perform the following procedure:

Procedure

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

Step 2 To restart the database server, enter the following command:

[root]# **service ipics_db restart**

Cisco IPICS displays the message `[OK]` when the database server successfully stops, and displays the message `[OK]` again when the database server successfully restarts.

Step 3 If you receive an error message after you attempt to restart the database server, contact your Cisco technical support representative for further assistance.

Starting the Database Server

Cisco IPICS starts the database server when the server boots up. You can also start the database server manually, if you determine that the database has stopped. To check whether the database is running, see the "Checking the Status of the Database Server" section on page 2-6.

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

Procedure

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

Step 2 To start the database server, enter the following command:

[root]# **service ipics_db start**

If you successfully started the database server, Cisco IPICS displays the message `[OK]`.

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

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

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

Step 5 If you cannot resolve the problem with the information in the log file, contact your Cisco technical support representative for further assistance.

Performing License Manager Procedures

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

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

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

- Checking the Status of the License Manager, page 2-9
- Restarting the License Manager, page 2-10
- Starting the License Manager, page 2-11

Checking the Status of the License Manager

To check the status of the license manager from the Cisco IPICS Administration Console, navigate to the **Serviceability > Diagnostics** window and view the Diagnostic Summary area. The database server status is listed in the Cisco IPICS Tomcat Web Server Status field.

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

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

Procedure

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

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

[root]# **service ipics_lm status**

If the license manager is running, the **status** command displays text that is similar to the following example:

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

If the license manager is not running, the **status** command displays text that is similar to the following example:

```
ipics_lm is not running.
```

If the **status** command indicates that the license manager is not running, start the database. For more information, see the "Starting the Database Server" section on page 2-8l.

Restarting the License Manager

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

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

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

Procedure

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

Step 2 To restart the license manager, enter the following command:

[root]# **service ipics_lm restart**

Cisco IPICS displays the message `[OK]` when the license manager successfully stops, and displays the message `[OK]` again when the license manager successfully restarts.

Step 3 If you receive an error message after you attempt to restart the license manager, contact your Cisco technical support representative for further assistance.

Starting the License Manager

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

Procedure

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

Step 2 To start the license manager, enter the following command:

[root]# **service ipics_lm start**

If you successfully started the license manager, Cisco IPICS displays the message `[OK]`.

Step 3 If the license manager does not start, check the status by performing the actions that are documented in the "Checking the Status of the License Manager" section on page 2-9.

Step 4 If you cannot start the license manager, contact your Cisco technical support representative for further assistance.

Performing Dial Engine Procedures

The dial engine controls the dial-in and dial-out functionality for the policy engine. For more information about the policy engine and dial engine, refer to the "Using the Cisco IPICS Policy Engine" chapter in the *Cisco IPICS Server Administration Guide, Release 2.0(1)*.

Note Your Cisco IPICS system must be licensed for the policy engine before you can perform dial engine procedures. To check whether you are licensed for the policy engine, navigate to the **Administration > License Management > Summary** tab in the Administration Console and check the Policy Engine Base License field. If your system is licensed for the policy engine, the field displays a status of Licensed. For more information about licenses, refer to the "Performing Cisco IPICS System Administrator Tasks" chapter in the *Cisco IPICS Server Administration Guide, Release 2.0(1)*.

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

Checking the Status of the Dial Engine

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

Procedure

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

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

[root]# **service ippe_dial_engine status**

If the dial engine is running properly, the **status** command returns a process similar to the following example:

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

If the dial engine processes are not running, the response to the **status** command is similar to the following example:

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

If the **status** command indicates that the dial engine is not running, start the database. For more information, see the "Starting the Dial Engine" section on page 2-14.

Stopping the Dial Engine

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

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

Procedure

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

Step 2 To stop the dial engine, enter the following command:

[root]# **service ippe_dial_engine stop**

Cisco IPICS displays the message `[OK]` when the dial engine processes successfully stop.

Restarting the Dial Engine

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

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

Procedure

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

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

[root]# **service ippe_dial_engine restart**

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

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

a. Check that the policy engine is licensed by navigating to the **Administration > License Management > Summary** tab.

b. Check the status of your license in the Policy Engine Base License field.

The status displays as Licensed or Not Licensed.

c. If the Policy Engine Base License field shows a status of Licensed, contact your Cisco technical support representative for further assistance.

Starting the Dial Engine

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

Procedure

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

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

[root]# **service ippe_dial_engine start**

If you successfully started the dial engine processes, Cisco IPICS displays the message `[OK]`.

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

a. Check that the policy engine is licensed by navigating to the **Administration > License Management > Summary** tab.

b. Check the status of your license in the Policy Engine Base License field.

The status displays as Licensed or Not Licensed.

c. If the Policy Engine Base License field shows a status of Licensed, contact your Cisco technical support representative for further assistance.

Performing CSA Procedures

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

This section includes the following topics:

Viewing CSA Log Messages

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

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

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

Procedure

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

Step 2 Navigate to the **/var/log** directory on the Cisco IPICS server by entering the following command:

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

Step 3 To list the files that start with the **csalog** name in the directory, enter the following command:

[root]# **ls -l csalog***

All files that begin with **csalog** display.

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

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

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

where:

x is the numeric extension of the file (if applicable).

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

Stopping CSA

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

Procedure

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

Step 2 To stop CSA, enter the following command:

[root]# **service ciscosec stop**

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

Starting CSA

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

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

Procedure

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

Step 2 To start CSA, enter the following command:

[root]# **service ciscosec start**

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

Troubleshooting the Cisco IPICS Server

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

Troubleshooting Cisco IPICS Installation and License Issues

For information about troubleshooting problems that you may experience when you install Cisco IPICS, including license problems, refer to the "Troubleshooting the Installation" chapter in the *Cisco IPICS Server Installation and Upgrade Guide, Release 2.0(1)*.

Troubleshooting Cisco IPICS Administration Console Issues

The issues that are described in this section describe problems that you may encounter with the Cisco IPICS Administration Console. These problems range from login issues to issues with viewing the information in the Administration Console.

This section includes the following topics:

- Recovering a Deleted System Administrator User, page 3-22
- Host Name Mismatch or Problems Installing the License After Changing the Server IP Address, page 3-23

Browser Guidelines

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

- The Administration Console times out after 30 minutes of non use. When a timeout occurs, you are prompted to log back in.
- As a best practice, make sure that you update your browser window often and before you perform any server administration tasks to ensure that you are working with the most current information. If you attempt to perform administration updates in a window that does not display the most current data, the update will not succeed and Cisco IPICS will display an error. If this situation occurs, update your browser window and retry the operation.
- To ensure that a current browser window displays the most current information, refresh it by clicking the button or tab that you used to display it. Cisco IPICS does not support the use of the browser Refresh button to refresh a window in the Administration Console.
- The Cisco IPICS Administration Console uses browser pop-up windows for certain functionality. If you have any browser pop-up blocker software installed on your machine, you may be prevented from performing certain actions. To ensure that you are not blocked from performing administration tasks, disable any pop-up blocker software that is installed on your machine before you use the Administration Console.
- Cisco IPICS does not support accessing the Administration Console in more than one browser session at the same time on the same machine. If you use multiple browser sessions to access the Administration Console, you may experience unexpected results. To ensure proper server operational behavior, do not open more than one browser session at a time on the same machine for Administration Console functions.
- To avoid browser-related memory issues, exit your browser and then restart it after prolonged use of the Cisco IPICS Administration Console.

You Cannot Connect to the Administration Console via Your Browser

Problem After you install Cisco IPICS, you enter the IP address or the host name for the Cisco IPICS server into a supported 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 or DNS name for the Cisco IPICS server
- The tomcat service is not running
- The database server is not running

To diagnose the problem, perform the following procedure:

Procedure

Step 1 Make sure that the URL that you entered is correct by performing the following actions:

- Ensure that you are using the secure HTTP URL, **https://** in the URL.
- If you entered the IP address for the server, check that you entered the correct IP address for Cisco IPICS into the browser.
- If you entered the DNS name for the server, ensure that the DNS name is correct and that your network is able to resolve the DNS name. If you conclude that your network is not resolving the server DNS name correctly, enter the IP address in the URL.

Step 2 If you still cannot access the Administration Console, access the Cisco IPICS server by using a terminal console.

Step 3 Enter **root** in the *hostname* **login:** field and press **Enter**.

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

Step 4 Enter the password for the root user ID and press **Enter**.

Step 5 Ensure that the tomcat service is running by entering the following command:

[root]# **service ipics_tomcat status**

Step 6 Perform one of the following actions, depending on the output that you receive:

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

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

  If you receive output that indicates that the tomcat service is running, continue to Step 10.

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

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

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

  [root]# **service ipics restart**

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

Step 7 If the tomcat service does not run after you restart it manually, perform the following actions:

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

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

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

b. If the **crontab** command returns a message that is similar to the following message, the tomcatcron file already exists. Continue to Step 10.

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

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

c. If the **crontab** command returned a message such as **no crontab for ipicsadmin**, install the crontab file by entering the following command:

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

Cisco IPICS installs the crontab file.

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

For information about checking and, if necessary, editing the tomcatcron file, see the "Performing Tomcat Service Procedures" section on page 2-2.

Step 8 To check the status of the database, enter the following command:

[root]# **onstat -**

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

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

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

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

If the command output indicates that the database is not running, continue to Step 9.

Step 9 If the database is not running, manually start the database server by entering the following command:

[root]# **service ipics_db start**

Step 10 To verify that the static IP address, subnet mask, and default gateway are properly configured, enter the following command:

ping <*default gateway IP address*>

where:

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

Step 11 If the ping command is not successful, unplug the network cable from interface 1 of the server, and connect it to interface 2.

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

Step 12 Retry Step 10 to attempt to verify server network connectivity.

Step 13 If the ping command is successful, log in to another server on the network and attempt to ping the Cisco IPICS server.

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

Step 14 Retry accessing the server by entering the following URL in the supported browser:

https://<*ipaddress*> | <*dnsname*>

where:

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

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

Enlarging the Text in the Administration Console

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

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

Procedure

Step 1 Open a supported version of the Internet Explorer browser.

Step 2 From the menu bar of the browser, select **View > Text Size**.

Step 3 Select **Medium** or **Larger** from the list of options to enlarge the text size.

The text in the browser window displays in a larger font.

Reducing Text in the Administration Console

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

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

Procedure

Step 1 Open a supported version of the Internet Explorer browser.

Step 2 From the menu bar of the browser, select **View > Text Size**.

Step 3 Select **Medium** or **Smaller** from the list of options to make the text size smaller.

The text in the browser window displays in a smaller font.

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

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

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


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

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

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

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

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

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

Procedure

Step 1 Connect to the Cisco IPICS server by using SSH Secure Shell client software (or similar software).

Step 2 Log in to the server with root user privileges.

Step 3 Change the directory by entering the following command:

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

Step 4 Read the last 25 lines of the ipics.log file by entering the following command:

Step 5 [root]# **tail -25 ipics.log**

Step 6 Search the log for errors that indicate a problem with the web applications. These messages might contain the domain name (yourdomain.com). Messages relating to a 404 or 500 error also include phrases such as “Incompatible magic value” or “Class not found.”

Step 7 If you determine that the Cisco IPICS web applications have become corrupted, delete one or more copies of the ipics_server folder in the webapps location by entering the following command:

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

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

Step 8 Delete the ipics_server folder in the work location by entering the following command:

[root]# **rm –rf /opt/cisco/ipics/tomcat/current/work/Catalina/localhost/ipics_server**

Step 9 Restart the tomcat service by entering the following command:

[root]# **service ipics_tomcat restart**

The system displays a message to indicate whether the service has been restarted.

When the tomcat service restarts, the system creates new ipics_server folders.

Step 10 Open a supported version of the Internet Explorer browser.

Step 11 In the Location or Address field, enter the following URL, replacing <*ipaddress*> with the IP address of the Cisco IPICS server:

https://<*ipaddress*>

You should be able to access the Administration Console.

Browser Timeout Problems When Configuring an RMS with Twelve or More Loopback Interfaces

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

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

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

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

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

Procedure

Step 1 On the PC that you use to access the Administration Console, choose **Start > Run**.

Step 2 In the Open dialog box, enter **regedit**.

The Registry Editor displays.

Step 3 Click the **+** sign that displays next to the **HKEY_CURRENT_USER** entry.

The folders that contain root configuration information for the user who is currently logged in display.

Step 4 Click the **+** signs that display next to each of the folder names to navigate to the **Software\Microsoft\Windows\CurrentVersion** folder.

Step 5 Click the **+** sign that displays next to the **Internet Settings** folder.

At this point, you have navigated to the following folder: **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings**.

Step 6 In the Internet Settings folder, look for the **ReceiveTimeout** name.

Step 7 To modify this setting, right-click the **ReceiveTimeout** name; then, click **Modify**.

The Edit DWORD Value dialog box displays. The current DWORD value displays in hexadecimal format.

Alternatively, you can choose to delete the ReceiveTimeout name altogether by clicking **Delete**. If you choose to take this action, be aware that you could wait indefinitely for the server to respond.

Step 8 Click the **Decimal** radio button to display this value in decimal format.

Step 9 To configure this value to the recommended setting to accommodate high latency, low bandwidth links, enter **480000** in the Value data field.

This modification configures the timeout value to 8 minutes.

Step 10 Click **OK** to save your change.

Step 11 To exit the Registry Editor, choose **Registry > Exit**.

Step 12 Restart your PC for the change to become effective.

Users Cannot Complete Tasks in the Administration Console and New Users Cannot Log In

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

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

To troubleshoot this issue, perform the following procedure:

Procedure

Step 1 Check to make sure that the database is running by following these steps:

a. Connect to the Cisco IPICS server by using SSH Secure Shell client software (or similar software).

b. Log in to the server with the root user ID.

c. Check to see if the database is running by entering the following command:

[root]# **onstat -**

– If the database is online and running, the command returns the following response; continue to Step 5.

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

– If the database is in quiescent mode, the command returns the following response; continue to Step d.

```
IBM Informix Dynamic Server Version 10.00.UC1     -- Quiescent
-- Up 00:00:42 -- 124036 Kbytes
```

- If the database is not running, the command returns the following response; continue to Step 2.

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

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

e. If you are not currently restoring the database, move the database from maintenance mode to online mode by entering the following command:

[root]# **onmode –m**

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

[root]# **service ipics_db start**

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

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

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

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

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

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

VTG Activates Without Dispatcher Action

Problem From the VTG Workspace, the dispatcher sees that a VTG is active, even though the dispatcher did not activate it.

Solution One of the following instances may have occurred:

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

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

Policy Activates but VTG Does Not Activate

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

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

Procedure

Step 1 Navigate to the **Policy Management > Execution Status > Executing/Executed Policy** tab.

Step 2 Locate the policy that you activated.

Step 3 Click **+** next to the policy name to expand it.

Step 4 Check the Status field in any rows that contain **ActivateVTG** in the Action Type field.

Step 5 If the status displays as Failed, check the details of the failure in the Message field.

Step 6 Perform any actions based on the information in the Message field to fix the problem.

If a message that is similar to the following message displays in the Message field, one of the possible reasons for the failure is a lack of available multicast addresses:

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

VTG Does Not Appear on User PMC

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

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

Check the **User Management > Users** window for duplicate user IDs and delete any unused IDs.

Cisco Unified IP Phone Cannot Access Channel

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

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

only the associated channels that are assigned to their default location. If the configured default location is the ALL location, IP Phone users can access only the channels that are assigned to the ALL location.

For more information about managing locations, refer to the "Performing Cisco IPICS System Administrator Tasks" chapter in the *Cisco IPICS Server Administration Guide, Release 2.0(1)*.

Cannot Save an Ops View

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

```
Cisco IPICS could not save ops view opsview
```

where:

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

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

Procedure

Step 1 Log in to the Cisco IPICS Administration Console as the ipics user.

Step 2 Navigate to the **Serviceability > System Logs** window.

Step 3 Review the logs in the **Recent System Log Entries** pane. Check for any errors that display in red or blue text and which appear to be related to ops views.

Step 4 If you cannot find any errors related to ops views in the Recent System Log Entries window, click **Download** to download the activity logs to your computer.

Step 5 Unzip the ipics.zip file and save the ipics.log file to your computer.

Step 6 Open the ipics.log as a text file.

Step 7 Search for the word "ERROR" in the ipics.log file.

The ipics.log may help you to determine the cause of the failure so that you can resolve the problem.

If you are not able to determine the specific error that has occurred or find information in the ipics.log that may help you to isolate the problem, proceed to Step 8.

Step 8 Check to make sure that you can successfully view other Cisco IPICS Administration Console windows, such as the **User Management > Users** window or **Configuration > Channels** window. If you can view these windows without receiving an error, proceed to step 2.

Step 9 Check to see if the database is running by entering the following command:

[root]# **onstat -**

Step 10 Perform one of the following actions, depending on the output that displays:

- If the database is not running, the command displays text that is similar to the following example.

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

  If you determine that the database is not running, proceed to Step 11.

- If the database is online and running, the command displays text that is similar to the following example.

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

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

Step 11 If the database has stopped, you can start it by entering the following command:

[root]# **service ipics_db start**

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

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

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

Step 12 Press the **Spacebar** to view all the messages in the log file. To close the message log file, press **q**.

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

Browser Displays an Undefined Error

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

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

Commands Fail Intermittently

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

Solution Retry the command or action. For more information about the nature of the error, navigate to the **Serviceability > System Logs** window in the Administration Console and view the logs in the **Recent System Log Entries** window.

Some Language Characters Display Incorrectly

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

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

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

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

Procedure

Step 1 Open a supported version of the Internet Explorer browser.

Step 2 From the Internet Explorer menu, choose **Tools > Internet Options**.

The Internet Options window displays.

Step 3 Click **Fonts**.

The Fonts dialog box displays.

Step 4 From the Web page font pane, select Arial Unicode MS.

Step 5 To accept the font choice, click **OK**.

Step 6 Click **OK** to save your changes and close the Internet Options window.

Internet Explorer now displays the languages correctly.

PMC Users Receive Error Message After Database Restore

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

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

To resolve this problem, perform the following procedure:

Procedure

Step 1 Ensure that the tomcat service is running by entering the following command:

[root]# **service ipics_tomcat status**

Step 2 Perform one of the following actions, depending on the output that you receive:

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

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

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

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

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

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

[root]# **service ipics restart**

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

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

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

Problem Multiple users are configuring Cisco IPICS by using different Administration Consoles. One user changes a configuration. At a later time, the user notices that their changes were overwritten.

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

Recovering a Deleted System Administrator User

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

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

Note You must be assigned the operator role and have an operator user ID and password to recover a deleted system administrator user. For more information about operators, refer to the "Performing Cisco IPICS Operator Tasks" chapter in the *Cisco IPICS Server Administration Guide, Release 2.0(1)*.

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

Procedure

Step 1 Log in to the server by using the operator user ID and password.

Step 2 From the User Management drawer in the Cisco IPICS Administration Console, click **Users**.

Step 3 Click **Add**.

Step 4 In the required fields, which are indicated by an asterisk, enter the user information.

Step 5 From the Roles drop-down list box, choose **System Administrator** or **All** for the user role.

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

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

Problem You changed the IP address of your Cisco IPICS server. After you reboot the server, you open the Administration Console and upload the license. When you click **Apply** to apply the license to the server, the following message persists in the Administration Console and you cannot navigate to any area in the Administration Console except the **Administration > License Management** window:

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

Changing the IP address might cause problems when you install Cisco IPICS, or cause other **host mismatch** error messages.

Solution Some IP address changes do not update the /etc/hosts file, which can cause host mismatch and other IP connectivity problems. To change the IP address, use the **modify_ip** tool by performing the following procedure:

Procedure

Step 1 Connect to the Cisco IPICS server via a terminal console by using the root user ID.

Step 2 To change your IP address, enter the following command:

[root]# **modify_ip**

The system displays the following text:

```
Please enter new settings or press Enter to accept existing values:
ip address for interface eth0[]:
```

Step 3 Enter the IP address for your server; then, press **Enter**.

Note If you have an existing value for this field, or for any other field that follows, the information in the square brackets displays the current value. Press **Enter** without entering any value to retain the existing value.

The system displays the following text:

```
Subnet mask for interface eth0[]:
```

Step 4 Enter the subnet mask for your IP address; then, press **Enter**.

Step 5 The system displays the following text:

```
default gateway[]:
```

Step 6 Enter the default gateway for your network and press **Enter**.

The system displays the other fields that you configure to ensure network connectivity.

Step 7 Enter the host name, domain name, primary DNS server and (optional) any secondary DNS servers at the command line when you are prompted. Press **Enter** after each entry.

The system displays the following text:

```
Enter Y to confirm the new settings[No]:
```

Step 8 Press **Y**; then, press **Enter** to confirm the entries.

Note If you press **No**, or press **Enter** with no text, the system returns you to the beginning of the configuration steps, starting with Step 3.

The system displays the following text:

```
The tool is now ready to modify your system configuration.
After changing the configuration files, the tool will initiate a
system shutdown and restart the server.
If you are using a network connection, your session will be
interrupted and you will need to
reconnect by using the new settings:
    IP Address: 10.1.1.1       Hostname: myhostname

Enter Y to proceed with these values or N to cancel[N]:
```

Step 9 Press **Y**; then, press **Enter** to confirm your choices and reboot the server.

The server reboots and returns you to Login screen.

Troubleshooting User ID and Password Issues

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

This section includes the following topics:

Resetting a Forgotten or Missing ipics User Password

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

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

To resolve this problem, perform the following procedure:

Procedure

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

Step 2 To reset the root user password, enter the following command:

[root]# **reset_pw -u ipics**

The system prompts you to enter a new password for the ipics user.

Step 3 Enter a new password for the ipics user; then, press **Enter**.

Cisco IPICS requires that you use strong passwords that contain at least eight characters and include the following elements:

- At least one lower case letter
- At least one upper case letter

- At least one number
- At least one of the following special characters:

  @ [ ] ^ _ ` ! " # $ % & ' ( ) * + , - . / : ; { < | = } > ~ ?

The system prompts you to reenter the new password.

Step 4 Reenter the new password for the ipics user; then, press **Enter**.

Cisco IPICS changes the ipics user password. To test the new password, log in to the server by using the ipics user ID.

Login Problems With the ipicsadmin or informix User IDs

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

Solution By default, the installation program for Cisco IPICS does not create a password for the ipicsadmin or informix user. You can log in with the ipicsadmin or informix user ID by either logging in as the root user and entering the **su** command, or creating a password by entering the **reset_pw** command.

To log in as the ipicsadmin or informix user without creating a password, perform the following procedure:

Procedure

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

Step 2 Log in as the ipicsadmin or informix user by performing one of the following actions:

- To log in as the ipicsadmin user, enter the following command:

  [root]# **su - ipicsadmin**

- To log in as the informix user, enter the following command:

  [root]# **su - informix**

Step 3 After you have completed your tasks as the ipicsadmin or informix user, enter **exit** to log out as that user and return as the root user.

To create a password for the ipicsadmin or informix user, perform the following procedure:

Procedure

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

Step 2 Create a password for the ipicsadmin or informix user by entering the following command:

[root]# **reset_pw**

The system displays the following text:

```
Select the user name for password reset:

1) ipics
2) ipicsadmin
3) informix
4) root
5) quit
```

Step 3 Perform one of the following actions to create a password for the ipicsadmin or informix user:

- Enter **2** to change the password for the ipicsadmin user.
- Enter **3** to change the password for the informix user.

The system prompts you to enter a new password for the user.

Step 4 Enter a new password for the ipicsadmin or informix user; then, press **Enter**.

Cisco IPICS requires that you use strong passwords that contain at least eight characters and include the following elements:

- At least one lower case letter
- At least one upper case letter
- At least one number
- At least one of the following special characters:

  @ [ ] ^ _ ` ! " # $ % & ' ( ) * + , - . / : ; { < | = } > ~ ?

The system prompts you to reenter the new password.

Step 5 Reenter the new password for the ipicsadmin or informix user; then, press **Enter**.

Cisco IPICS changes the ipicsadmin or informix user password.

Step 6 To test the new password, log in to the server by using the ipicsadmin or informix user ID.

Changing the root User Password

Problem You need to change the root user password.

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

Procedure

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

Step 2 To reset the password for the root user ID, enter the following command:

[root]# **reset_pw -u root**

The system prompts you to enter a new password for the root user.

Step 3 Enter a new password for the root user; then, press **Enter**.

Cisco IPICS requires that you use strong passwords that contain at least eight characters and include the following elements:

- At least one lower case letter
- At least one upper case letter
- At least one number
- At least one of the following special characters:

  @ [ ] ^ _ ` ! " # $ % & ' ( ) * + , - . / : ; { < | = } > ~ ?

The system prompts you to reenter the new password.

Step 4 Reenter the new password for the root user; then, press **Enter**.

Cisco IPICS changes the password for the root user to the password that you specified.

Resetting a User Who Is Locked Out or Disabled

Problem A user cannot log in to the Cisco IPICS system with the correct user ID and password combination.

Solution The user may be locked out or disabled. A user can be locked out or disabled in the following ways:

- The number of invalid login attempts exceeded the number of maximum attempts, and Cisco IPICS automatically locked out the user. For more information, refer to the "Performing Cisco IPICS System Administrator Tasks" chapter in the *Cisco IPICS Server Administration Guide, Release 2.0(1)*.
- A user with Operator or All privileges manually locked out or disabled the user. For more information about locking out or disabling a user, refer to the "Performing Cisco IPICS Operator Tasks" chapter in the *Cisco IPICS Server Administration Guide, Release 2.0(1)*.

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

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

Perform the following procedure to unlock or enable a user:

Procedure

Step 1 To unlock or enable a user, perform one of the following actions:

- If you are able to access the Administration Console with a user ID that has Operator or All privileges, perform the following actions to unlock or enable the user:

- Follow the procedure in the "Locking or Unlocking a User" section in the "Performing Cisco IPICS Operator Tasks" chapter in the *Cisco IPICS Server Administration Guide, Release 2.0(1)* to unlock the user.
- Follow the procedure in the "Changing User Status" section in the "Performing Cisco IPICS Operator Tasks" chapter in the *Cisco IPICS Server Administration Guide, Release 2.0(1)* to enable the user.

- If you have access to the root user ID, perform the following steps to unlock or enable the user:

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

  b. To log in as the informix user, enter the following command:

     [root]# **su - informix**

  c. To unlock or enable the user, enter the following command:

     [informix]# **enableuser** <*user-id*>

     where:

     <*user-id*> represents the user ID that you would like to unlock or enable.

Note Enter the user ID in all lower case letters.

Step 2 To make sure that the user is unlocked or enabled, log in with the user ID and password of the user who was locked out or disabled.

Troubleshooting Policy Engine Issues

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

Error Occurs After You Upload a Large Zipped File That Contains Prompts

Problem You attempt to upload a large zipped file that contains dial engine prompts from the **Dial Engine > Prompt Management > Standard Script Prompts** or the **Dial Engine > Prompt Management > Customized Script Prompts** window of the Administration Console, and see the following error message:

```
The form could not be properly constructed.
```

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

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

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

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

Policy Engine Unable to Communicate With the Prompt Manager

Problem You are experiencing problems with the policy engine. Messages similar to the following messages display in the **Serviceability > System Logs** window or in the ipics.log file:

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

Solution This situation indicates that Cisco IPICS did not start the policy engine. Perform the following procedure to start the policy engine:

Procedure

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

Step 2 To start the policy engine processes, enter the following command:

[root]# **service ippe_dial_engine start**

If the policy engine starts, Cisco IPICS displays the message `[OK]` as it starts each process.

Dial-In Call Cannot Reconnect to Channel After Using Hold or Call Waiting Feature

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

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

To successfully reconnect with a dial-in call, either add MTP resources to your SIP provider, or configure your SIP provider so that it can allocate MTP resources from another source.

Dial-In Calls Do Not Connect

Problem Dial-in calls to a channel or VTG do not connect successfully. Dial-in calls receive a fast busy tone or a message that indicates that the call cannot be completed.

Solution Your dial engine or ops view configuration might be incorrect, or you did not restart the policy engine. Perform the following procedure to check your configuration and restart the policy engine:

Procedure

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

The Ops Views window displays.

Step 2 Determine if any ops views exist by checking the information that displays in the Ops Views pane.

Step 3 If an ops view does not exist, create an ops view by following the steps that are described in the "Creating New Ops Views" section in the "Configuring and Managing Cisco IPICS Operational Views" chapter in the *Cisco IPICS Server Administration Guide, Release 2.0(1)*.

Step 4 Navigate to the **Configuration > Ops Views** window.

Step 5 Determine if a dial-in number exists in the ops view by checking the Dial Number column in the Ops Views pane. If a dial-in number does not exist, create one.

Step 6 Determine if dial ports exist in the ops view by checking the Dial Ports Limit column in the Ops View pane. If dial ports do not exist, create one or more dial ports for the ops view.

For information about creating a dial-in number and dial ports for an ops view, refer to the "Configuring and Managing Cisco IPICS Operational Views" chapter in the *Cisco IPICS Server Administration Guide, Release 2.0(1)*.

Step 7 Make sure that a sufficient number of ports exist for dial-in calls in the ops view, and create ports if necessary, by performing the following steps:

a. Click the name of the ops view.

The Ops Views > <*opsviewname*> window displays.

b. View the following fields in the window to check if dial ports exist:

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

c. If the number in both fields is equal to zero, decrease the number of ports in the **Dial ports reserved for notifications** field; then, perform one of the following actions:

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

Step 8 If you make any changes to the SIP configuration in the **Dial Engine > SIP Configuration** window of the Administration Console, restart the policy engine and the tomcat service from the CLI by performing the following procedure:

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

b. To restart the policy engine and the tomcat service, enter the following command:

[root]# **service ipics restart**

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

For more information about configuring SIP, refer to the "Configuring SIP" and "Configuring the SIP Provider" sections of the "Configuring and Managing the Cisco IPICS Policy Engine" chapter in the *Cisco IPICS Server Administration Guide, Release 2.0(1)*.

Dial-Out Invitations Do Not Complete

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

Solution The Cisco IPICS configuration for dial-out invitations might be incorrect. Perform the following procedure to check your configuration and fix any problems that you find:

Procedure

Step 1 Make sure that you have configured an outbound dial number by performing the following steps:

a. Navigate to the **Dial Engine > Dial Engine Parameters** window from the Policy Engine tab.

b. Check the Outbound Dial Number field to determine if you have configured an outbound dial number.

c. If a valid number does not exist in the Outbound Dial Number field, create an outbound dial number by following the procedure that is in the "Configuring Dial Engine Parameters" section of the "Configuring and Managing the Cisco IPICS Policy Engine" chapter in the *Cisco IPICS Server Administration Guide, Release 2.0(1)*.

Step 2 Check to see if you have ports that are configured for dial-out invitations by navigating to the **Configuration > Ops Views >** <*opsviewname*> window in the Server tab.

Step 3 Determine if ports exist for dial-out invitations by checking the following fields in the window:

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

Step 4 If the number in both fields is equal to zero, perform the following steps to add ports for dial-in/invite feature:

a. Decrease the number of ports in the **Dial ports reserved for notifications** field.

b. Perform one of the following actions:

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

Dial-Out Notifications Do Not Complete

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

Solution It is possible that the configuration for dial-out notifications is incorrect. Perform the following procedure to check your configuration and fix any problems that you find:

Note If you are performing dial-out notifications from one ops view to another, see the "Dial-Out Notifications Do Not Complete Between Users in Different Ops Views" section on page 3-38.

Procedure

Step 1 If the notification is a dial-out notification, make sure that you have configured an outbound dial number by performing the following steps:

a. Navigate to the **Dial Engine > Dial Engine Parameters** window from the Policy Engine tab.

b. Determine that you have configured an outbound dial number by checking the Outbound Dial Number field.

c. If a valid number does not exist in the Outbound Dial Number field, create an outbound dial number by following the procedure in the "Configuring Dial Engine Parameters" section in the "Configuring and Managing the Cisco IPICS Policy Engine" chapter in the *Cisco IPICS Server Administration Guide, Release 2.0(1)*.

Step 2 If the notification is an e-mail, SMS or text-based pager notification, make sure that you have configured an SMTP server and a sender e-mail address by performing the following steps:

a. Navigate to the **Dial Engine > Dial Engine Parameters** window from the Policy Engine tab.

b. Determine if you have configured an SMTP server for e-mail notifications by checking the Outbound Dial Number field.

c. Determine if you have configured an e-mail address for your server by checking the Sender Email Address field.

d. Add the SMTP server or sender e-mail address, as required, by following the procedure in the "Configuring Dial Engine Parameters" section in the "Configuring and Managing the Cisco IPICS Policy Engine" chapter in the *Cisco IPICS Server Administration Guide, Release 2.0(1)*.

Step 3 Check that ports are configured for dial-out notifications by navigating to the **Configuration > Ops Views >** *<opsviewname>* window in the Server tab.

Step 4 Check that ports are configured for dial-out notifications by checking the following fields in the window:

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

Step 5 If the number of dial ports that are reserved for notifications (specified in the **Dial ports reserved for notifications** and **Dial ports reserved for dial-in/invite or notifications** fields) is equal to zero, perform the following steps to add ports for notifications:

a. Decrease the number of ports in the **Dial ports reserved for dial-in/invite feature** field.

b. Perform one of the following actions:

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

Dial-Out Notifications Do Not Complete Between Users in Different Ops Views

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

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

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

Note This policy-to-ops-view association information does not apply to the SYSTEM ops view, to which all users belong.

SIP Subsystem Displays PARTIAL_SERVICE or OUT_OF_SERVICE Status

Problem After you updated your SIP configuration, the SIP subsystem displays a PARTIAL_SERVICE or OUT_OF _SERVICE status.

Solution This situation may be caused by a SIP misconfiguration or a problem with the SIP subsystem. Perform the following procedure to check and fix your SIP configuration:

Procedure

Step 1 Restart the policy engine and the tomcat service from the CLI by performing the following steps:

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

b. To restart the policy engine and the tomcat service, enter the following command:

[root]# **service ipics restart**

Step 2 Recheck the status of your SIP configuration by navigating to **Dial Engine > Control Center > Status** window.

Step 3 If the SIP subsystem continues to show a status of PARTIAL_SERVICE or OUT_OF_SERVICE, check the log files for additional information to troubleshoot your problem by performing the following steps:

a. Navigate to the **Dial Engine > Control Center > Status > Subsystem Manager > SIP Subsystem** window.

b. Click the name of the Cisco001MIVR log file to select it.

Your host system prompts you to open or save the file.

c. To view the content of the log file, open the file with any software program that allows you to view text files.

d. If there are any successive log files (for example, Cisco002MIVR and Cisco003MIVR) open and view them.

e. Read the error messages in the log file(s), and attempt to fix the problem based on the information that you have gathered.

Note Messages that are related to SIP Subsystem debugging begin with MIVR-SS_SIP or MIVR-JASMIN-7.

Step 4 If you cannot determine the nature of the problem, contact your Cisco technical support representative for assistance.

For more information about the logs that are using with the dial engine and policy engine, see the "Understanding and Locating the Cisco IPICS Log Files" section on page 6-1.

IppeAgentImpl ERROR Messages Display in the ipics.log File

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

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

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

Note INFO messages (denoted by having **INFO** instead of **ERROR** in the message text) are informational messages and do not indicate a problem with the policy engine.

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

Procedure

Step 1 Check that you are licensed for the policy engine by navigating to the **Administration > License Management > Summary** window in the Server tab of the Administration Console.

Step 2 Check the status of your license in the Policy Engine Base License field.

If the field shows a status of Not Licensed, IppeAgentImpl messages are normal and no action is required.

Step 3 If the field shows a status of Licensed, perform the following steps to check if the policy engine processes are running and start them if necessary:

a. Open a terminal window and log in to the server by using the root user ID.

b. To check the status of the policy engine processes, enter the following command:

c. [root]# **service ippe_dial_engine status**

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

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

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

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

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

[root]# **service ippe_dial_engine start**

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

e. Check the status of the policy engine by reentering the **service ippe_dial_engine status** command.

f. If the policy engine processes are not running, contact your Cisco technical support representative for assistance.

Troubleshooting Communication Issues

This section provides information about troubleshooting communications issues and includes the following topics:

All Locations Cannot Communicate in a Channel

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

Solution Although the multicast address for the channel is set to All, the address may not be configured to reach everyone in the domain. The network administrator should reconfigure the router to include Location A. Some examples of this problem may be an IP access list blocking that channel, a firewall setting, or a multicast address that is not properly configured.

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

http://cisco.com/en/US/tech/tk828/technologies_tech_note09186a0080094b55.shtml

VTG Participants Cannot Communicate

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

Solution If Protocol Independent Multicast (PIM) on your router is set to sparse mode, this situation might indicate that you have not configured a rendezvous point (RP), or that all RPs are unreachable. If you set the PIM of the router to sparse mode and do not configure an RP, the router drops the packets and your VTG participants do not hear any audio. To ensure that this problem does not occur, make sure that you configure an RP, or set the router to sparse-dense mode.

For more information about configuring the router, refer to the "Configuring the Cisco IPICS RMS Component" appendix in the *Cisco IPICS Server Administration Guide, Release 2.0(1)*. For more information about multicast troubleshooting, refer to the *IP Multicast Troubleshooting Guide* at the following URL:

http://cisco.com/en/US/tech/tk828/technologies_tech_note09186a0080094b55.shtml

PMC Users Cannot Communicate In a Channel

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

Solution The router that the channel uses does not have sufficient digital signal processor (DSP) resources. 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.

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

http://www.cisco.com/en/US/products/hw/modules/ps3115/products_qanda_item0900aecd8016c6ad.shtml

For more information about configuring the RMS, refer to the "Configuring the Cisco IPICS RMS Component" appendix in the *Cisco IPICS Server Administration Guide, Release 2.0(1)*.

Logged-Out PMC Users Do Not Get Removed from the Active Users List

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

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

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

Procedure

Step 1 From the Administration Console, navigate to the **Administration > Active Users > PMC** window.

The PMC Users pane displays the list of active PMC users.

Step 2 Locate the user ID of the logged-out PMC user.

Step 3 To manually log out this user, check the check box next to the PMC user ID.

Step 4 Click **Logout**.

The PMC user status changes from **Logged-in** to **Logging-out**.

Step 5 To update the status, click **Refresh**.

Cisco IPICS removes the user from the list of active users.

PMC Users Can Listen to Channels But Cannot Listen to VTGs

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

Solution In Cisco IPICS, an RMS provides support for only one Cisco IPICS location (a Cisco IPICS location is defined as a multicast domain). All of the locations and routers that are configured in the Cisco IPICS system must be able to communicate by using the multicast addresses that have been defined in the global multicast address pool. All addresses in the multicast pool must be able to reach any RMS, PMC, or Cisco Unified IP Phone that is part of the Cisco IPICS system.

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

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

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

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

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

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

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

Router(config) **#gateway**

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

For more information about the correct router configuration for Cisco IPICS, refer to the "Configuring the Cisco IPICS RMS Component" appendix in the *Cisco IPICS Server Administration Guide, Release 2.0(1)*.

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

Feedback Noise on VTG

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

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

One-Way Audio Between PMCs and Cisco Unified IP Phones

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

Solution This situation could occur if the multicast address for a channel is assigned to another resource in your network. Make sure that you assign a unique multicast address to each channel and VTG and that no other resource in your network uses that multicast address.

Troubleshooting Equipment Issues

The issues that are detailed in this section describe problems that you may encounter with the Cisco IPICS hardware. For issues that relate to communication difficulties, see the "Troubleshooting Communication Issues" section on page 3-42.

This section includes the following topics:

No Power to Cisco Unified IP Phones

Problem Cisco Unified IP Phones are not receiving power.

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

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

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

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

[router] # **show power**

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

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

Interconnectivity Problems With Cisco Unified Wireless IP Phone 7920

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

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

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

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

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

If you encounter this problem, make sure that you preserve your data by backing up your database before you reboot the server. For more information about backing up your database, see the "Performing Cisco IPICS Database Backup and Restore Operations" chapter in the *Cisco IPICS Server Administration Guide, Release 2.0(1)*.

Troubleshooting Voice Quality Issues

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

Voice Quality Degrades for PMC

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

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

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

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

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

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

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

If the DS0 resources cannot support simultaneous G.729 connections, limit the number of G.729 channels that you use. When it is possible, use G.711 rather than G.729, because G.711 uses fewer DSP resources.

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

Dial Engine Calls Experience Degraded Voice Quality

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

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

For detailed information about configuring a transcoder in Cisco Unified CallManager, release 5.0(4), refer to the "Transcoder Configuration" chapter of the *Cisco Unified CallManager Administration Guide, Release 5.0(4)* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/5_0/sys_ad/5_0_4/ccmcfg/b04trans.htm

For more information about Cisco IOS gateway-related features and functionality, refer to the *Cisco Multiservice IP-to-IP Gateway Application Guide, Cisco IOS Release 12.4(11)T* at the following URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps5640/products_configuration_guide_book09186a0080409b6d.html

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

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

Problem Voice communications are interrupted when you use VTGs and SIP-connected PMCs. 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 by entering the following command in privileged EXEC mode:

Router# **configure terminal**

Step 2 Enter interface controller mode for one of the T1 controllers in the loopback by entering the following command in global configuration mode:

Router(config)# **controller t1** *x*/*x*/*x*

where:

x/*x*/*x* represents the shelf, slot and port of the interface controller.

Step 3 To configure the cable length, enter the following command in controller configuration mode:

Router(config-controller)# **cablelength short 133**

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

Step 4 To configure the clock source on this T1 controller in the loopback, enter the following command:

Router(config-controller)# **clock source internal**

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

Step 5 Return to privileged EXEC mode by entering the following command:

Router(config-controller)# **end**

Step 6 Enter interface controller mode for the second T1 controller in the loopback by repeating Step 1 and Step 2, specifying the shelf, slot and port number of the other T1 controller in the loopback.

Step 7 To make sure that clocking is not configured on the second T1 controller, enter the following command:

Router(config-controller)# **no clock source**

Note You must configure clocking for only one of the two T1 controllers in the loopback.

Step 8 Return to privileged EXEC mode by entering the following command:

Router(config-controller)# **end**

Step 9 Clear the error counters by entering the following command:

Router# **clear counters**

Step 10 To display information about the T1 controllers, enter the following command:

Router# **show controllers t1**

Note Make sure that you check the T1 controller configuration on a regular basis.

The following configuration example configures the first controller in the loopback pair:

```
Router(config)# controller T1 1/0
Router(config-controller)# framing esf
Router(config-controller)# clock source internal
Router(config-controller)# linecode b8zs
Router(config-controller)# cablelength short 133
Router(config-controller)# ds0-group 0 timeslots 24 type e&m-lmr
Router(config-controller)# ds0-group 1 timeslots 1 type e&m-lmr
Router(config-controller)# ds0-group 2 timeslots 2 type e&m-lmr
Router(config-controller)# ds0-group 3 timeslots 3 type e&m-lmr
Router(config-controller)# ds0-group 4 timeslots 4 type e&m-lmr
Router(config-controller)# ds0-group 5 timeslots 5 type e&m-lmr
```

```
Router(config-controller)# ds0-group 6 timeslots 6 type e&m-lmr
Router(config-controller)# ds0-group 7 timeslots 7 type e&m-lmr
Router(config-controller)# ds0-group 8 timeslots 8 type e&m-lmr
Router(config-controller)# ds0-group 9 timeslots 9 type e&m-lmr
Router(config-controller)# ds0-group 10 timeslots 10 type e&m-lmr
Router(config-controller)# ds0-group 11 timeslots 11 type e&m-lmr
Router(config-controller)# ds0-group 12 timeslots 12 type e&m-lmr
Router(config-controller)# ds0-group 13 timeslots 13 type e&m-lmr
Router(config-controller)# ds0-group 14 timeslots 14 type e&m-lmr
Router(config-controller)# ds0-group 15 timeslots 15 type e&m-lmr
Router(config-controller)# ds0-group 16 timeslots 16 type e&m-lmr
Router(config-controller)# ds0-group 17 timeslots 17 type e&m-lmr
Router(config-controller)# ds0-group 18 timeslots 18 type e&m-lmr
Router(config-controller)# ds0-group 19 timeslots 19 type e&m-lmr
Router(config-controller)# ds0-group 20 timeslots 20 type e&m-lmr
Router(config-controller)# ds0-group 21 timeslots 21 type e&m-lmr
Router(config-controller)# ds0-group 22 timeslots 22 type e&m-lmr
Router(config-controller)# ds0-group 23 timeslots 23 type e&m-lmr
Router(config-controller)# no shutdown
```

where:

ds0-group *ds0-group-number* identifies the ds0 group and must be a value from 0 to 23; ds0 groups must start with 0 and must be sequential.

timeslots *timeslot-list* specifies a single time-slot number; for T1 connectivity, allowable values range from 1 to 24.

The following configuration example configures the second controller in the loopback pair:

```
Router(config)# controller T1 1/1
Router(config-controller)# framing esf
Router(config-controller)# linecode b8zs
Router(config-controller)# cablelength short 133
Router(config-controller)# ds0-group 0 timeslots 24 type e&m-lmr
Router(config-controller)# ds0-group 1 timeslots 1 type e&m-lmr
Router(config-controller)# ds0-group 2 timeslots 2 type e&m-lmr
Router(config-controller)# ds0-group 3 timeslots 3 type e&m-lmr
Router(config-controller)# ds0-group 4 timeslots 4 type e&m-lmr
Router(config-controller)# ds0-group 5 timeslots 5 type e&m-lmr
Router(config-controller)# ds0-group 6 timeslots 6 type e&m-lmr
Router(config-controller)# ds0-group 7 timeslots 7 type e&m-lmr
Router(config-controller)# ds0-group 8 timeslots 8 type e&m-lmr
Router(config-controller)# ds0-group 9 timeslots 9 type e&m-lmr
Router(config-controller)# ds0-group 10 timeslots 10 type e&m-lmr
Router(config-controller)# ds0-group 11 timeslots 11 type e&m-lmr
Router(config-controller)# ds0-group 12 timeslots 12 type e&m-lmr
Router(config-controller)# ds0-group 13 timeslots 13 type e&m-lmr
```

```
Router(config-controller)# ds0-group 14 timeslots 14 type e&m-lmr
Router(config-controller)# ds0-group 15 timeslots 15 type e&m-lmr
Router(config-controller)# ds0-group 16 timeslots 16 type e&m-lmr
Router(config-controller)# ds0-group 17 timeslots 17 type e&m-lmr
Router(config-controller)# ds0-group 18 timeslots 18 type e&m-lmr
Router(config-controller)# ds0-group 19 timeslots 19 type e&m-lmr
Router(config-controller)# ds0-group 20 timeslots 20 type e&m-lmr
Router(config-controller)# ds0-group 21 timeslots 21 type e&m-lmr
Router(config-controller)# ds0-group 22 timeslots 22 type e&m-lmr
Router(config-controller)# ds0-group 23 timeslots 23 type e&m-lmr
Router(config-controller)# no shutdown
```

where:

ds0-group *ds0-group-number* identifies the ds0 group and must be a value from 0 to 23; ds0 groups must start with 0 and must be sequential.

timeslots *timeslot-list* specifies a single time-slot number; for T1 connectivity, allowable values range from 1 to 24.

The following example displays the output from the **show controllers** command:

```
Router#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
  Soaking time: 3, Clearance time: 10
  AIS State:Clear  LOS State:Clear  LOF State:Clear
  Version info Firmware: 20050620, FPGA: 16, spm_count = 0
  Framing is ESF, Line Code is B8ZS, Clock Source is Internal.
  Current port master clock:recovered from backplane
  Data in current interval (4 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,
     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
T1 1/0/1 is up.
  Applique type is Channelized T1
  Cablelength is short 133
  No alarms detected.
  alarm-trigger is not set
  Soaking time: 3, Clearance time: 10
```

```
  AIS State:Clear  LOS State:Clear  LOF State:Clear
  Version info Firmware: 20050620, FPGA: 16, spm_count = 0
  Framing is ESF, Line Code is B8ZS, Clock Source is Line.
  Current port master clock:recovered from backplane
  Data in current interval (7 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,
     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
```

For more information about RMS configuration, refer to "Configuring the Cisco IPICS RMS Component" appendix in the *Cisco IPICS Server Administration Guide, Release 2.0(1)*.

Troubleshooting 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 Delays Between Pressing the PMC PTT Button and Media Establishment, page 3-65

Server Reboots Slowly Following RMS Configuration

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

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

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

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

- Use a higher performing router for the RMS
- Do not load the RMS with an excessive number of controllers and DS0s.

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

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

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

Procedure

Step 1 From the Administration Console, navigate to the **VTG Management > Virtual Talk Groups** window to check the status of the VTGs.

Step 2 In the Virtual Talk Groups window, read the Status column to check the status of your VTGs.

The status of this column displays as inactive or active.

Step 3 For any VTG that displays with an active status, perform the following steps to deactivate the VTG(s):

a. Click the link for the VTG name to display the VTG details.

b. Click **Deactivate VTG** to deactivate the VTG.

c. Click **Save**.

Step 4 After you deactivate all of the active VTGs, check the status of the RMS by navigating to the **Configuration > RMS** window.

The status of the RMS should display as Deactivated.

Step 5 If the status of the RMS still displays as Stopping, perform the following steps to activate and deactivate the RMS:

a. Navigate to the **Configuration > RMS** window.

b. Click the name of the RMS to select it.

c. Click the **General** tab.

d. To activate the RMS, click **Activate**.

e. To deactivate the RMS, click **Deactivate**.

f. Click **Save**.

The status of the RMS should now display as Deactivated.

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

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

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

Cisco IPICS only supports the default prompts.

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

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

RMS Fails or Remains in Unreachable State

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

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

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

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

Router# **show users**

To clear a VTY line, enter the following command:

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

where:

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

Newly-Added RMS Does Not Display Loopbacks

Problem The RMS that you added to Cisco IPICS does not display loopbacks in the 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 "Configuring the Cisco IPICS RMS Component" appendix in the *Cisco IPICS Server Administration Guide, Release 2.0(1)* for information about connecting and configuring the T1/E1 controllers.

Router Remains in Unreachable State

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

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

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

To resolve the problem, perform the following procedure:

Procedure

Step 1 Navigate to the **Configuration > RMS** window in the Administration Console.

The RMS window displays.

Step 2 Select the router by checking the check box next to the router name in the Routers pane.

Step 3 Delete the router configuration from the server by clicking **Delete**.

Cisco IPICS removes the router from the system.

Step 4 Re-add the router to the configuration by following the procedure in the "Adding an RMS" section in the "Performing Cisco IPICS System Administrator Tasks" chapter in the *Cisco IPICS Server Administration Guide, Release 2.0(1)*.

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

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

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

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

Example 3-1 Out of Sequence Configuration

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

```
Router(config-controller)#DS0-group 5 timeslots 5 type e&m-lmr
Router(config-controller)#DS0-group 6 timeslots 6 type e&m-lmr
...
```

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

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

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

Procedure

Step 1 Navigate to **Configuration > RMS** on the Administration Console.

The **Configuration > RMS** window displays.

Step 2 Check the check box next to the router to select it.

Step 3 Click **Configuration > Merge** to merge the configuration.

Step 4 Click the name of the router to select it.

The **Configuration > RMS >** <*rms-name*> window displays.

Step 5 Click **Save** to update the Cisco IPICS RMS configuration with the changes.

For additional details about configuring the RMS, refer to the "Configuring the Cisco IPICS RMS Component" appendix in the *Cisco IPICS Server Administration Guide, Release 2.0(1)*.

Router Indicator Lights for the Loopback Are Not Green

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

Solution Each set of ports on the router has the following indicator lights. Check the loopbacks on your router to see if any of the following indicator lights are on, and perform the following actions to correct the problem:

- CD—This green light indicates that there are no problems with the loopback

- 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 AL and CD lights are on
  - The interface is shut down—Enable the interface by entering the following command in interface configuration mode on both ends of the T1 loopback interface:

    Router(config-if)# **no shutdown**
  - The framing is incorrect—Cisco recommends that you use the Extended Super Frame (ESF) framing method on both ends of the loopback.
  - The line code is incorrect—Cisco recommends the B8ZS encoding standard on both ends of the loopback

Voice Loops in Conferences and Router Configuration Shows Incorrect Information

Problem Users experience voice loops (continuous echoes) in conferences. When you view the configuration by clicking **Configuration > Show** in the **Configuration > RMS** window of the Administration Console, settings for voice ports or dial peers display that are not currently in use.

Solution When you add an RMS to a Cisco IPICS system, particularly an RMS that was previously associated with another Cisco IPICS system, you may observe differences between the output that displays with the router **show configuration** command and the configuration that displays when you click **Configuration > Show** in the **Configuration > RMS** window of the

Administration Console. 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 synchronized, perform the following procedure:

Procedure

Step 1 Navigate to **Configuration > RMS** on the Administration Console.

The **Configuration > RMS** window displays.

Step 2 Check the check box next to the router to select it.

Step 3 Click **Configuration > Update** to update the configuration.

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

Cisco IPICS automatically updates the router configuration every 10 minutes. An alternative to the preceding procedure is to wait until Cisco IPICS automatically updates the router configuration.

Long Delays Between Pressing the PMC PTT Button and Media Establishment

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

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

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

For detailed information about how to configure the RMS, “Configuring the Cisco IPICS RMS Component” appendix in the *Cisco IPICS Server Administration Guide, Release 2.0(1)*.

Troubleshooting Tips for the PMC Application

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

This chapter includes the following sections:

Troubleshooting PMC Application Problems

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, follow this procedure:

Procedure

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

Step 2 Click **Task Manager**.

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

Step 3 Click the **Processes** tab.

Step 4 Click **Image Name** to alphabetize the list of running processes.

Scroll down through this list to look for the PMC.exe process.

Step 5 Click **PMC.exe** to highlight or right-click **PMC.exe**; then, click **End Process**.

A warning message displays to ask if you are sure that you want to terminate this process.

Step 6 Click **Yes**.

Step 7 Close Windows Task Manager by clicking the "**X**" in the upper right corner.

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

Generating a PMC Installation Log File

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

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

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

To generate the PMC installation log file, follow this procedure:

Procedure

Step 1 Create a **C:\temp** directory in Windows, if this directory does not already exist.

Step 2 Use Windows Explorer to navigate to the location where you saved the pmcsetup.exe file, as described in the "Downloading and Installing the PMC Application" section of the "Installing and Upgrading the PMC Application" chapter in the *Cisco IPICS PMC Installation and User Guide, Release 2.0(1)*.

Step 3 Locate the **pmcsetup.exe** file in this stored location and click to highlight the file; then, right-click the **pmcsetup.exe** file and click **Copy**.

Step 4 Use Windows Explorer to navigate to the C:\temp directory and right-click in an open area in this directory; then, click **Paste** to copy the **pmcsetup.exe** file to the C:\temp directory.

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

Step 5 Open up a command line prompt (**Start > Run > cmd**) on the PMC client machine to access the C:\temp directory.

Step 6 To generate the PMC installation log file, enter the following command from the C:\temp directory:

pmcsetup.exe -log

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

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

Step 7 To close the command line prompt, enter the **exit** command.

Step 8 After you have created the PMC installation log file, contact your Cisco support personnel for further assistance.

Using the PMC Installer with an Encrypted File System

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

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

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

Procedure

Step 1 On the PMC client machine, open a command line prompt by choosing **Start > Run** and entering **cmd**.

A command line window displays.

Step 2 At the command line, enter the following command:

C:\ **echo %temp%**

The location of the TEMP folder displays.

If the folder that is specified by the %temp% environment variable is encrypted, you can assign the %temp% environment variable to a folder that is not encrypted.

Step 3 To reassign the %temp% environment variable to a nonencrypted folder, enter the following command:

C:\ **set TEMP=**<*new location*>

where:

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

The new location of the TEMP folder displays.

Step 4 To reassign the %tmp% environment variable to a nonencrypted folder, enter the following command:

C:\ **set TMP=**<*new location*>

where:

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

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

C:\ **run pmcsetup.exe**

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

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

Making PMC Configuration File Changes

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

Using the PMC Optional Settings

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

These submenu items become available by using the PMC optional settings. Refer to the "Using the Optional Settings Menu" section in the "Configuring the PMC Application" chapter in the *Cisco IPICS PMC Installation and User Guide, Release 2.0(1)* for additional information and caveats about using the PMC optional settings.

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

Resolving Footswitch/USB Device Issues

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

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

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

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

For more information about using a footswitch or other USB device, refer to the "Using Keyboard Mapping" section in the "Using the PMC Application" chapter in the *Cisco IPICS PMC Installation and User Guide, Release 2.0(1)*.

Configuring the Audio Settings

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

- Using a USB DSP Headset with the PMC, page 4-8
- Checking the Microphone with the PMC, page 4-9

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

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

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

For tips about how to ensure the best possible voice quality when you use the PMC, refer to the "Voice Quality Tips" section in the "Installing and Upgrading the PMC Application" chapter in the *Cisco IPICS PMC Installation and User Guide, Release 2.0(1)*.

Using a USB DSP Headset with the PMC

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

If you launch the PMC after you plug the headset into your PMC client machine, the PMC does not automatically remember the audio setting for the USB DSP headset; instead, the PMC reverts to the Windows operating system's default audio settings. Refer to the "Using a USB DSP Headset with the PMC" section in the "Installing and Upgrading the PMC Application" chapter in the *Cisco IPICS PMC Installation and User Guide, Release 2.0(1)* for more information about checking and reconfiguring the Windows audio settings for use with a USB DSP headset.

Note If you use the microphone on a USB headset for an extended period of time, your voice may become unintelligible. If this problem occurs, close the PMC and unplug the USB headset from the PMC client machine. Then, plug the USB headset back into the PMC client machine and restart the PMC.

Checking the Microphone with the PMC

You should also check the audio recording and playback capability of the microphone on your PMC client machine by accessing the Microsoft Sound Recorder to record your voice and then listen to the recording. (Make sure that you have an audio input device connected to your machine.)

- Make sure that you use a high-quality microphone with the PMC; otherwise, the Cisco IPICS system may not be able to accurately detect your voice and properly register transmit and/or receive traffic.
- If the Cisco IPICS system cannot detect your voice when you transmit, the system may squelch the transmission; in this situation, another Cisco IPICS user may start speaking over your transmission because your voice cannot be heard and the PMC receive indicator may not display any indication of the transmission.

Note Be aware that if the microphone on the PMC client machine is busy or if it cannot be opened by the PMC for other reasons, you will be able to listen to active conversations but you will not be able to talk.

Refer to the "Configuring the Audio Settings", the "Using a USB DSP Headset with the PMC" and "Using the Microphone with the PMC" sections in the "Installing and Upgrading the PMC Application" chapter in the *Cisco IPICS PMC Installation and User Guide, Release 2.0(1)* 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 Audio and Headset Issues, page 4-11
- Resolving IP Address Changes, page 4-13

Note Be aware that multicast issues may also contribute to problems with one-way audio. For more information, see the "Troubleshooting Multicast Communications Issues" section on page 4-20.

Tip Check the network connectivity for your PMC client machine to make sure that you have a valid IP address and that you can connect to the network before you start using the PMC. If you use SIP-based remote connections, make sure that the PMC can establish connectivity to the RMS. (The PMC connects to the RMS by using the IP address of the Loopback0 interface that is assigned to the RMS.) For more information, see the "Resolving IP Address Changes" section on page 4-13.

Using CLI Commands to Resolve Audio and Headset Issues

You can verify and isolate audio issues that you may experience by using CLI command options on the PMC. This section describes the CLI commands that you can use to help resolve audio issues.

Using CLI Commands to Resolve Headset Issues

If you encounter a situation where you cannot hear audio on the PMC, the problem may be due to the headset that you are using. You can verify and isolate one-way audio problems by using CLI command options on the PMC.

Be aware of the following caveats when you use CLI commands:

- Make sure that the PMC to which you are issuing the command is running; the command has no effect if the PMC is not running.
- Issue the command from the Windows command line on the PMC client machine; the command affects only that PMC.

To enter a CLI command on the PMC, follow this procedure:

Procedure

Step 1 On the PMC that has encountered the problem, open the Windows command line by following these steps:

a. Choose **Start > Run**.

The Windows dialog box displays.

b. Enter **cmd** in the Open field.

c. Press **Enter** or click **OK**.

The Windows command line window displays.

Step 2 In the Windows command line window, change the current directory to the folder in which the PMC is installed.

The following example shows the directory structure in which the PMC folder may appear:

C:\Program Files\Cisco Systems\Cisco IPICS\PMC

Step 3 Enter the desired CLI command and press **Enter**.

For a description of each CLI command, refer to Chapter 2, "Command Line Interface Commands" in the *Cisco IPICS Command Line Interface*.

Using the CLI Play Command to Resolve One-Way Audio Issues

To verify that the one-way audio problem is not a PMC application issue, you can enter the CLI **play** command from the Windows command line of the PMC.

The play command outputs a wave audio file to the specified PTT channel. This command latches the PMC PTT button, plays the designated wave file, and then unlatches the PTT button. The syntax of the play command appears below:

PMC.EXE -Play *file* [**-line #**]

- The *file* argument specifies the path and file name of the wave file to play.
- The **-line #** option, where # is a number between 1 and 18, specifies the PTT channel line to which this command applies. (If you omit this option, the command applies to channel 1.)

The following command shows an example of the play command:

PMC.EXE -Play C:\aud1.wav -line 2

In this example, this command plays the aud1.wav file to PTT channel 2.

When you successfully execute this command, you can hear audio from one PMC to another PMC and eliminate the PMC as the source of the one-way audio problem. When this situation occurs, the problem can be isolated to a faulty headset. In that case, replace the headset and try again.

Note For detailed information about using PMC CLI command options, refer to the *Cisco IPICS Command Line Interface*.

Resolving IP Address Changes

The following section provides information about resolving IP address changes on the PMC client machine; it includes the following topics:

- Changing IP Addresses on the PMC Client Machine, page 4-13
- IP Address Change Notifications, page 4-14

Changing IP Addresses on the PMC Client Machine

If you change the IP address on your PMC client machine (for example, when switching from a wired to a wireless network), and the PMC is open, you may encounter one-way audio on the PMC. To resolve this issue, close and then restart the PMC.

If you change the IP address on your PMC client machine when the PMC is not open, the PMC should not be affected by the change. You should always establish network connectivity to make sure that you have a valid IP address before you open the PMC.

IP Address Change Notifications

Under normal conditions, the PMC chooses the first network connection that allows it to communicate with the server. If that network connection becomes unusable, the PMC chooses another network connection for its communications.

Cisco IPICS provides notification to the PMC user when the PMC changes the source IP address that it uses for communications with the server. However, on PMC client machines that include more than one network connection, the PMC may not provide this notification. In these instances, there is no impact to functionality; Cisco IPICS continues to operate normally when notification of the IP address change is not sent to the user.

Troubleshooting Voice Quality Issues

You may encounter voice quality issues, which can arise due to several factors, such as noise and voice distortion.

For detailed information about voice quality problems and symptoms, refer to the Recognizing and Categorizing Symptoms of Voice Quality Problems documentation, which can be found at the following URL: http://www.cisco.com/en/US/tech/tk652/tk698/technologies_white_paper09186a00801545e4.shtml.

This document categorizes and defines voice quality problem symptoms and may aid your troubleshooting efforts by helping you to identify specific problems through the use of sample sound recordings.

This document also includes a link to the TAC Case Collection Tool, which provides solutions by interactively identifying and troubleshooting common technology or product problems.

You can access the TAC Case Collection Tool at the following URL: http://www.cisco.com/en/US/customer/support/tsd_tac_case_collection.html

Resolving Unknown Publisher Errors with Windows XP SP2

As part of the browsing security enhancements that were implemented in Microsoft Windows XP Service Pack 2 (SP2), you may encounter an "Unknown Publisher" error when you use the Internet Explorer (IE) browser to download the PMC from the Cisco IPICS server.

This problem may occur when you try to run an executable file or an add-in program that contains an invalid signature and that you downloaded by using the IE version that is installed with Windows XP (SP2).

To resolve this issue, Microsoft recommends that you unblock the publisher and then try to save or run the file that you downloaded. Alternatively, you can modify the security settings on your PMC client machine, although this workaround is not recommended.

For detailed information about how to resolve this issue, refer to the Microsoft support site at http://support.microsoft.com/ and search for Article ID 843022.

Troubleshooting PMC Connectivity Issues

The following topics provide information about troubleshooting PMC connectivity issues:

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 4-17
- Enabling and Disabling the Stateful Firewall on the PMC Client Machine, page 4-17

Be aware of the following caveats that apply to specific versions of the Cisco Systems VPN Client.

Cisco Systems VPN Client Version Interoperability Caveats

When you use the Cisco Systems VPN Client version 3.6.3(x) with the PMC, the PMC may not be able to detect the IP address and route change after you establish or disconnect a VPN tunnel. This problem occurs when the Cisco Systems VPN Client does not communicate the IP address and route change information to the operating system. When this problem occurs, the channels on the PMC may not be able to receive audio.

To resolve this problem, access the **Settings > Advanced** menu in the PMC application after you have established or disconnected the VPN tunnel on your PMC client machine. When you access this menu, the PMC probes the Cisco Systems VPN Client to determine its activity and tunnel status and, from this menu, it can also detect an IP address change. For more information about the Express menu, refer to the "Configuring the Channels and Advanced Settings" section in the "Configuring the PMC Application" chapter in the *Cisco IPICS PMC Installation and User Guide, Release 2.0(1)*.

When you use the Cisco VPN Client version 4.0x, the SIP-based remote connection may not become activated. In this situation, you may need to deactivate and then reactivate the channel after you establish the VPN tunnel. To deactivate the channel, click the **Activate** button. Click the **Activate** button again to reactivate the channel.

About the VPN Client Stateful Firewall

The VPN Client integrated stateful firewall provides protection when split tunneling is in effect by safeguarding from Internet attacks while the VPN client is connected to a VPN concentrator through an IPSec tunnel.

When enabled, this "Stateful Firewall (Always On)" feature enforces more robust security by disallowing inbound sessions from all networks, regardless of whether a VPN connection is being used. This firewall is active for both encrypted and unencrypted traffic, except when you use the following protocols:

- Dynamic Host Configuration Protocol (DHCP)—The stateful firewall allows inbound traffic because requests to the DHCP server are sent out one port and responses are received through a different port.
- Encapsulating Security Payload (ESP)—The stateful firewall permits this traffic from the secure gateway because ESP rules are packet filters and not based on sessions.

For more information about exceptions, refer to the release notes for the VPN Client documentation at the following URL:
http://www.cisco.com/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 required protocols.

To modify your firewall settings, perform the following procedure:

Procedure

Step 1 On your Windows XP PMC client machine, navigate to **Start > Control Panel > Network and Internet Connections**.

The Network and Internet Connections window displays.

Step 2 Click the **Change Windows Firewall settings** link.

The Windows Firewall window displays.

Step 3 Click the **Exceptions** tab.

A list of programs and services displays.

Step 4 If you have already installed the PMC, check the **Cisco IPICS PMC** check box to add this program to the list of exceptions in the Windows Firewall; then, proceed to Step 6.

Step 5 If you have not yet installed the PMC, install and then launch the PMC.

For information about installing and launching the PMC, refer to the "Installing the PMC Application" and the "Launching the PMC Application" sections in the "Installing and Upgrading the PMC Application" chapter in the *Cisco IPICS PMC Installation and User Guide, Release 2.0(1)*.

a. After you launch the PMC, a Windows Security Alert displays to inform you that Windows XP has blocked the PMC.

b. Click **Unblock** to add this program to the list of exceptions in the Windows Firewall.

Step 6 Click **OK**.

Windows XP now allows the PMC to function properly.

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

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

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 experience one-way audio where they can hear, but they may not be heard by, other Cisco IPICS users.

Tip To ensure identification of this specific problem, please check to make sure that the microphone mute options on the headset and in the Windows operating system are not enabled. For more information about using the microphone with the PMC, refer to the "Using the Microphone with the PMC" section in the "Installing and Upgrading the PMC Application" chapter in the *Cisco IPICS PMC Installation and User Guide, Release 2.0(1)*.

This problem with multicast communications may be caused by the network component of the operating system being unable to transmit multicast traffic. Cisco IPICS PMC users who encounter this problem should connect to Cisco IPICS over a unicast connection by choosing the **remote** location from the location selection dialog box. (By choosing the remote location, Cisco IPICS uses SIP-based connectivity for all channels on the PMC.)

To positively identify this problem, use a network packet sniffer as described below:

1. Run the sniffer on the affected PMC client machine and filter for outgoing multicast UDP packets.
2. Then, launch the PMC application and click the **PTT** channel button on one of the channels and speak into the microphone or headset. (The channel highlights and changes color to indicate that you are transmitting traffic.)
3. Observe the sniffer; you will see that no multicast UDP packets are sent from the PMC client machine.

To fully resolve this problem, you must perform a fresh installation of the Windows 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.

Troubleshooting Offline Mode Issues

Cisco IPICS allows the PMC to operate in offline mode when the connection to the server has been interrupted so that you can continue to communicate during periods of server downtime.

There are several situations that may cause the PMC to enter offline mode, such as, the inability of the PMC to communicate with the server, networking issues that prevent routing from the PMC client machine to the server, and IE browser settings that cause your PC to work in offline mode.

For detailed information about the situations that apply to offline mode based on interactions between the PMC and the server, refer to the "PMC Offline Mode Caveats" section in the "Using the PMC Application" chapter in the *Cisco IPICS PMC Installation and User Guide, Release 2.0(1)*.

If you encounter a situation where Cisco IPICS returns a message that states that the PMC is in offline mode while the connection to the server is online, check to make sure that your IE browser is not operating in offline mode. To check this setting, choose **File** from the IE browser window. Scroll down to the Work Offline option and make sure that a check mark does not appear next to this option. (If a check mark does not appear next to this option, then it is disabled.)

If a check mark appears next to this option, click **Work Offline** to remove the check mark and disable offline mode.

Note Be sure that the "Work Offline" option in your IE browser settings is not enabled on your PMC client machine. If this option is enabled, you must disable it; otherwise, you may not be able to connect to the server.

Troubleshooting PMC Connectivity Issues with the RMS

To connect the PMC via a SIP-based remote connection, make sure that the PMC can establish connectivity to the RMS. (The PMC connects to the RMS by using the IP address of the Loopback0 interface that is assigned to the RMS and configured in the Cisco IPICS server.)

To determine the IP address of the RMS, access the **Settings > Channels** menu in the PMC application. Click a remote connection channel to highlight it; then, scroll through the Channel Properties pane to the SIP Proxy field to find the IP address of the RMS for the associated channel. (If you cannot determine the IP address of the RMS, contact your System Administrator for assistance.)

From the PMC client machine command line interface, enter the following command to ping this IP address to verify connectivity:

C:\>ping <*SIP Proxy IP address*>

where *SIP Proxy IP address* represents the RMS component.

Note The PMC must be able to establish connectivity to the RMS to enable SIP-based remote connections. Make sure that you can successfully ping this IP address to ensure PMC connectivity to the RMS. If the PMC cannot connect to the RMS, you may experience channel activation issues (such as fast busy) when you attempt to use a SIP-based remote connection.

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

When you first log in to a PMC that is connected via a high latency and/or low bandwidth link, such as when you use a satellite connection, an error message displays to inform you that the channels are being disabled. This error occurs because of the time delay to connect over this type of link. To recover from this error, click **OK**.

If the Cisco IPICS server times out while it is waiting for a response from one or more resources, the server does not have complete information to send to the PMC. In this case (after about one minute), the server sends an incomplete list of channels to the PMC while it waits for a response.

The server marks each channel that does not respond within the timeout interval as "unavailable" until the operation completes. When this situation occurs, the PMC displays a message that states that the "RMS resources may not be available."

You do not need to take any action to resolve this issue. After the server completes its tasks, the channels display on the PMC.

Note Be aware that the amount of time that it takes for the server to complete its tasks will vary depending on the amount of latency in the network.

For information about configuring the PMC for use with a high latency and/or low bandwidth link, refer to the "Configuring the Channels Menu Options" section in the "Configuring the PMC Application" chapter in the *Cisco IPICS PMC Installation and User Guide, Release 2.0(1)*.

Resolving Name Resolution Failures

Cisco IPICS requires IP name resolution. An incorrect Domain Name Service (DNS) IP configuration could result in a service outage.

To resolve name resolution failures, consult with your system administrator to confirm IP name resolution within the entire network, which includes local device IP configurations, network-based name resolution systems (such as DNS), and DHCP systems.

Identifying Channel Activation Issues

When you click the **Activate** button on the PMC, the system enters the activating state; that is, the Activate button highlights and the system attempts to connect to the Cisco IPICS server.

- When you click the Activate button immediately after a SIP-based (unicast) channel becomes available on the PMC, you may hear a busy tone if the RMS has not completely configured the line. If you encounter this situation, click the **Activate** button to deactivate the channel; then, wait a few seconds and click **Activate** again to reactivate the channel.

After the connection has been established, the remaining PMC buttons, including the PTT channel button, highlight to indicate that they are in an active state.

- If your ability to transmit on a channel has been disabled by the server, and/or if the channel has been configured by the server as a listen-only channel, the channel will appear dimmed. If the channel has been disabled by the server, you will not be able to activate the channel, as none of the buttons will appear.

If the remaining PMC buttons do not become active, and if you are using a SIP-based connection, one of the following conditions may be occurring:

- Network connectivity issues that prevent connection to the RMS.
- The RMS may be in an offline or invalid state.
- The RMS may be misconfigured in the server.
- The dial peers may not have been configured or the dial peers and/or the voice ports may be misconfigured in the RMS.

- The RMS may not have yet created the dial peers because of a delay between the server configuration and RMS dial peer creation. In this case, you should wait a couple of minutes and then restart the PMC to try again.

Note When SIP-based remote connections fail, the PMC displays a warning indicator in the form of a yellow triangle next to the channel. This indicator signifies that a problem exists with the remote end (PMC, RMS, or server) and that it may not be able to send or receive traffic. This situation may be caused by a network interruption or reset/restart activity at the remote end. During this period of interruption, the PMC continues to attempt to connect to the remote end. After operations return to normal, the PMC removes the warning indicator from view.

If there is no traffic activity after a 30 minute interval, channels that are activated via a SIP-based remote connection may be deactivated by the system.

- The PMC will automatically reactivate the connection after 30 seconds. Alternatively, you can reactivate the channel by clicking the **Activate** button on the PMC.

Resolving Codec Mismatch Issues

When the protocol type or codec type is misconfigured in the RMS LMR gateway, the PMC has the ability to detect this codec type mismatch (such as G.729 versus G.711) and thereby, preserve system resources and PMC functionality.

If the misconfiguration includes a specific codec type that Cisco IPICS supports (that is, G.729 or G.711), the PMC adapts the codec decoding to enable handling of the different version of that specific codec type. For example, the PMC can adapt to different versions of G.711, such as G.711 ulaw and G.711 alaw, and decode either version automatically to maintain functionality.

If the codec type mismatch is caused by the configuration of an incorrect or unsupported codec type, the PMC will drop the incorrect or unsupported encoded samples because it cannot decode them. In this case, the PMC user will not hear any audio.

For more information about the codecs that Cisco IPICS supports, refer to the "Codec Support" section in the "Understanding PMC Interactions and Supported Features" chapter in the *Cisco IPICS PMC Installation and User Guide, Release 2.0(1)*.

Support for Right-to-Left and Double-Byte Languages

Note Although this version of Cisco IPICS does not support localization, it does provide support for the PMC to display channel/VTG names that are configured in the server in certain right-to-left (RTL) and double-byte (character-based) languages. This support allows for the input of Arabic and Hebrew characters (RTL languages) and Chinese and Japanese characters (double-byte languages) for names and descriptions in the Cisco IPICS server.

To use a right-to-left language or a double-byte language in Windows 2000 and Windows XP, you need to configure the operating system to enable support for the specific language that you use.

Note If you try to use the Arabic or Hebrew language without enabling support for RTL, your text will display in reverse.

Procedure

To enable RTL support for the Arabic and Hebrew languages for use with Cisco IPICS, and to enable support for double-byte languages, perform the following procedure:

Procedure:

Step 1 If your client machine runs Windows 2000, follow this step. Otherwise, proceed with Step 2. On Windows 2000 client machines, navigate to **Start > Settings > Control Panel > Regional Options**.

The Regional Options dialog box displays. In this dialog box, you can specify system settings such as locale, languages, currency, time, and date.

a. From the **General** tab, you can add support for the languages that you need to use:

- To add support for the Arabic language, check the **Arabic** check box in the Language Settings for the System area.
- To add support for the Hebrew language, check the **Hebrew** check box in the Language Settings for the System area.

- To add support for the Chinese language, check the **Traditional Chinese** or the **Simplified Chinese** check box in the Language Settings for the System area.
- To add support for the Japanese language, check the **Japanese** check box in the Language Settings for the System area.

b. Click **OK**.

c. Restart your PMC client machine for your changes to become effective.

Note After your PMC client machine restarts, your operating system will be enabled for the languages that you chose.

d. After the language files have been installed, navigate to Regional Options, as described above, and click the **Input Locales** tab to add the language input options that you want to use; then, click the **Change** button from the Input Languages and Methods pane.

e. From the Installed Services pane, click **Add**.

The Add Input Language dialog box displays.

f. From the Input Language drop-down list box, click to select and highlight the input language for one of the supported languages.

g. Check the **Keyboard Layout / IME** check box; from the drop-down list box, choose the keyboard layout to use.

h. Click **OK**.

The Text Services dialog box displays your selection in the Installed Services pane.

i. Click **Apply**; then, click **OK**.

j. Repeat Step d. to Step i. for each supported language that you want to add.

Step 2 On Windows XP client machines, navigate to **Start > Control Panel > Regional and Language Options**.

The Regional and Language Options dialog box displays. In this dialog box, you can specify options for regional and language settings on your system.

a. Click the **Languages** tab.

- To add support for supplemental languages, check the **Install files for complex script and right-to-left languages (including Thai)** check box in the Supplemental Language Support area.
- To add support for Chinese and Japanese languages, check the **Install Files for East Asian languages** check box.

  A pop-up message displays to inform you that the installation of supplemental language support requires a defined amount of available disk space.

b. Click **OK** to accept.

c. From the Regional and Language Options dialog box, click **Apply**; then, click **OK**.

d. If you are prompted, restart your PMC client machine for your changes to become effective.

Note After your PMC client machine restarts, your operating system will be enabled for the languages that you chose.

e. After the language files have been installed, navigate to Regional and Language Options, as described above, and click the **Details** button in the Text Services and Input Languages pane.

f. From the Installed Services pane, click **Add**.

   The Add Input Language dialog box displays.

g. From the Input Language drop-down list box, click to select and highlight the input language for one of the supported languages; then, click **OK**.

h. Check the **Keyboard Layout / IME** check box; from the drop-down list box, choose the keyboard layout to use.

i. Click **OK**.

   The Text Services and Input Languages dialog box displays your selection in the Installed Services pane.

j. Click **Apply**; then, click **OK**.

k. Repeat Step e. to Step i. for each supported language that you want to add.

PMC Application Caveats

The following caveats pertain to the PMC application:

- Only one instance of the PMC application can be open and each PMC supports only one user ID login on a given PC at one time.
- A PMC end-user can log in to an unlimited number of different PMC applications at the same time.
- Any number of valid Cisco IPICS users can use the same PMC application, but not concurrently, based on PMC licensing requirements.
- The PMC application can log in to the server that has been configured as the default server and from which the PMC installation file has been downloaded. If the primary server is not accessible, and if there are alternate servers to choose from, you can log in to a different server. For more information about connecting to alternate servers, refer to the "Support for Cisco IPICS Recovery" section in the "Recovering the PMC Application" chapter in the *Cisco IPICS PMC Installation and User Guide, Release 2.0(1)*.
- Refer to the "PMC Usage Guidelines" section in the "Using the PMC Application" chapter in the *Cisco IPICS PMC Installation and User Guide, Release 2.0(1)* for information about using the PMC.
- Refer to the "PMC Offline Mode Caveats" section in the "Using the PMC Application" chapter in the *Cisco IPICS PMC Installation and User Guide, Release 2.0(1)* for information about using the PMC in offline mode.
- Refer to the "Skin Caveats" section in the "Configuring the PMC Application" chapter in the *Cisco IPICS PMC Installation and User Guide, Release 2.0(1)* for information about PMC skin caveats.
- If you use a docking station with your PMC client machine, make sure that you close the PMC application before you undock your PC; otherwise, your PC may become unresponsive and require you to reboot.

Analyzing PMC Error Conditions

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

In some situations, the PMC may display an error message. In other situations, you may experience certain issues, such as audio quality issues, where a message does not display.

Table 4-1 describes some of these error conditions and audio quality issues and how to resolve them.

Table 4-1 PMC Error Conditions

Problem	Solution
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.	Invalid entries in the pmc.ini file may be the cause of this problem. To check this file, perform the following steps: 1. Navigate to **C:\Program Files\Cisco Systems\Cisco IPICS\PMC**. 2. Search for the **pmc.ini** file. 3. Right-click **pmc.ini** and click **Open With**. 4. Click **Notepad**; then, click **OK**. 5. Delete all entries in this file except the following fields: server_host, server_port, and server_port_ssl. 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.
You can hear other users but they cannot hear you.	Check your audio settings to make sure that your microphone is not set to mute. Refer to the "Configuring the Audio Settings" section in the "Installing and Upgrading the PMC Application" chapter in the *Cisco IPICS PMC Installation and User Guide, Release 2.0(1)*. **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.

Table 4-1 PMC Error Conditions (continued)

Problem	Solution
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.	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.
When you talk, other users tell you that your voice sounds choppy and breaks up at times during a conversation.	If VAD is enabled, disable the setting in the Channels menu. Refer to the "Configuring the Channels and Advanced Settings" section in the "Configuring the PMC Application chapter" in the *Cisco IPICS PMC Installation and User Guide, Release 2.0(1)* 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.
When you talk, other users tell you that your voice sounds low.	Check the placement of your microphone so that it is positioned between 2 and 6 inches from your mouth. If necessary, reposition the microphone for optimum use. 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.

Table 4-1 PMC Error Conditions (continued)

Problem	Solution
When you talk, other users tell you that they hear a persistent or intermittent noise, such as a hum.	The existence of a persistent or intermittent noise, such as a hum, when you talk may be due to defective headset hardware. In this situation, Cisco recommends that you isolate the source of the audio quality issue by replacing the defective headset with a new, high-quality headset. For more information about voice quality, refer to the "Voice Quality Tips" section in the "Installing and Upgrading the PMC Application" in the *Cisco IPICS PMC Installation and User Guide, Release 2.0(1)*.
When you attempt to log in to the PMC, you see an error message that states "invalid user or password."	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.
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.	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.

Table 4-1 PMC Error Conditions (continued)

Problem	Solution
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. 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.
When you try to launch the PMC, an error message displays because the PMC cannot access the media device.	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, Release 2.0(1)*
- *Cisco IPICS PMC Quick Start Reference Card, Release 2.0(1)*
- *Cisco IPICS PMC Debug Reference Quick Start Card, Release 2.0(1)*
- *Cisco IPICS PMC Command Line Interface, Release 2.0(1)*
- *Cisco IPICS Server Administration Guide, Release 2.0(1)*

Using the Cisco IPICS CLI Tools and Service Commands

This chapter describes the command-line interface (CLI) tools and service commands that are available in Cisco IPICS. You use the tools to fix system problems. You use the service commands to start, stop and restart the Cisco IPICS network processes.

This chapter includes the following sections:

Understanding the CLI-Based Tools

The CLI-based tools that are bundled with Cisco IPICS allow you to change the IP address for the server, perform password resets for a subset of users, and enable a user that has been locked out.

Table 5-1 lists the Cisco IPICS CLI-based tools.

Table 5-1 CLI-Based Tools That Are Used with Cisco IPICS

Log Name	Description
modify_ip	This tool changes the IP address for your server. If you do not use the **modify_ip** tool to change the server IP address, the /etc/hosts file might not get updated with your new IP address, which can cause license and connectivity problems. See the "Changing the Server IP Address With the modify_ip Tool" section on page 5-2 for information about the **modify_ip** tool.
enableuser	This tool enables a user that has been disabled, or unlocks a user that has been locked out. See the "Unlocking or Enabling a Locked or Disabled User With the enableuser Tool" section on page 5-4 for information about the **enableuser** tool.
reset_pw	This tool resets the ipics password, creates the ipicsadmin and informix passwords, and changes the root password. See the "Resetting, Changing, or Creating a Password With the reset_pw Tool" section on page 5-5 for information about the **reset_pw** tool.

Using the CLI-Based Tools

This section contains instructions on how to use the CLI-based tools and includes the following topics:

Changing the Server IP Address With the modify_ip Tool

Perform the following procedure to change the IP address of the server:

Procedure

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

Step 2 To change your IP address, enter the following command:

[root]# **modify_ip**

The system displays the following text:

```
Use this tool to faciliate changing the Cisco IPICS server network
settings, such as IP address or host name.

To change the current settings, enter the new values below.  To accept
the existing values without making any changes, press Enter.

ip address for interface eth0[x.x.x.x]:
```

Step 3 Enter the IP address for your server; then, press **Enter**.

Note If you have an existing value for this field, or for any of the fields in the following steps, the data in the square brackets displays the current value. Press **Enter** without entering any value to retain the existing value.

The system displays the following text:

```
Subnet mask for interface eth0[]:
```

Step 4 Enter the subnet mask for your IP address; then, press **Enter**.

Step 5 The system displays the following text:

```
default gateway[]:
```

Step 6 Enter the default gateway for your network; then, press **Enter**.

The system displays the other fields that you configure to ensure network connectivity.

Step 7 Enter the host name, domain name, primary DNS server and (optional) any secondary DNS servers at the command line when you are prompted. Press **Enter** after each entry.

Note Make sure that you also update your DNS servers if you want to access Cisco IPICS by using the host name.

The system displays the following text:

```
Enter Y to confirm the new settings[No]:
```

Step 8 Press **Y**; then, press **Enter** to confirm the entries.

Note If you press **No**, or press **Enter** with no text, the system returns you to the beginning of the configuration steps, starting with Step 3.

The system displays the following text:

```
The tool is now ready to modify your system configuration.
After changing the configuration files, the tool will initiate a
system shutdown and restart the server.
If you are using a network connection, your session will be
interrupted and you will need to
reconnect by using the new settings:
    IP Address: 10.1.1.1       Hostname: myhostname

Enter Y to proceed with these values or N to cancel[N]:
```

Step 9 Enter **Y**; then, press **Enter** to confirm your choices and reboot the server.

The server reboots and returns you to Login screen.

Unlocking or Enabling a Locked or Disabled User With the enableuser Tool

A user can be locked out or disabled in the following ways:

- The number of invalid login attempts exceeded the number of maximum attempts, and Cisco IPICS automatically locked out the user. For more information, refer to the "Performing Cisco IPICS System Administrator Tasks" chapter in the *Cisco IPICS Server Administration Guide, Release 2.0(1)*.
- A user with Operator or All privileges manually locked out or disabled the user. For more information about locking out or disabling a user, refer to the "Performing Cisco IPICS Operator Tasks" chapter in the *Cisco IPICS Server Administration Guide, Release 2.0(1)*.

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

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

Perform the following procedure to unlock or enable a user:

Procedure

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

Step 2 To log in as the informix user, enter the following command:

[root]# **su - informix**

Step 3 To unlock or enable the user, enter the following command:

[informix]# **enableuser** <*user-id*>

where:

<*user-id*> represents the user ID that you would like to unlock or enable.

Note Enter the user ID in all lower case letters.

Resetting, Changing, or Creating a Password With the reset_pw Tool

If you need to reset the ipics password, create the ipicsadmin or informix passwords, or change the root password, perform the following procedure:

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

Step 2 To reset, change or create a password, enter the following command:

[root]# **reset_pw**

The system displays the following text:

```
Select the user name for password reset:

1) ipics
2) ipicsadmin
3) informix
4) root
5) quit
```

Step 3 To reset, create or change a password, perform one of the following actions:

- Enter **1** to reset the password for the ipics user.
- Enter **2** to create the password for the ipicsadmin user.
- Enter **3** to create the password for the informix user.
- Enter **4** to change the password for the root user.

The system prompts you to enter a new password for the user.

Step 4 Enter a new password for the user; then, press **Enter**.

Note To ensure a strong password, you must create a password that is at least eight characters long, and includes the following elements:

- At least one lower case letter
- At least one upper case letter
- At least one number
- At least one of the following special characters:

  @ [ ] ^ _ ` ! " # $ % & ' ( ) * + , - . / : ; { < | = } > ~ ?

The system prompts you to reenter the new password.

Step 5 Reenter the new password for the ipicsadmin or informix user; then, press **Enter**.

Cisco IPICS changes the ipicsadmin or informix user password. To test the new password, log in to the server by using the ipicsadmin or informix user ID.

For more information about the ipicsadmin and informix users, see the "Glossary" chapter of this document.

Configuring and Checking Cisco IPICS Network Processes With Service Commands

Service commands start, stop or restart network processes that are used with Cisco IPICS, such as the tomcat service or the license manager. You can also check the status of the network processes with some service commands.

For more information about network processes and the commands that are described in this section, see the "Troubleshooting Cisco IPICS Network Processes" section on page 2-1.

Table 5-2 lists the service commands that you use with Cisco IPICS.

Table 5-2 CLI-Based Tools That Are Used with Cisco IPICS

Log Name	Description
service ciscosec {**start** | **stop**}	This command starts and stops the Cisco Security Agent (CSA). For more information about starting and stopping CSA, see the "Performing CSA Procedures" section on page 2-15.
service ipics {**start** | **stop** | **restart** | **status**}	This command allows you to start, stop, restart, and check the status of the Cisco IPICS policy engine (known hereafter as policy engine) and the tomcat service. For more information about the policy engine, refer to the "Using the Cisco IPICS Policy Engine" chapter in the *Cisco IPICS Server Administration Guide, Release 2.0(1)*.
service ipics_db {**start** | **stop** | **restart** | **status**}	This command allows you to start, stop, restart, and check the status of the database server. For more information about the database server, refer to the "Understanding the Cisco IPICS Databases" section in the "Performing Cisco IPICS Database Backup and Restore Operations" chapter in the *Cisco IPICS Server Administration Guide, Release 2.0(1)*.

Table 5-2 CLI-Based Tools That Are Used with Cisco IPICS (continued)

Log Name	Description
service ipics_lm {**start** | **stop** | **restart** | **status**}	This command allows you to start, stop, restart, and check the status of the license manager. For more information about licenses and the license manager, refer to the "Managing Licenses" section in the "Performing Cisco IPICS System Administrator Tasks" chapter in the *Cisco IPICS Server Administration Guide, Release 2.0(1)*.
service ipics_tomcat {**start** | **stop** | **restart** | **status**}	This command allows you to start, stop, restart, and check the status of the tomcat service. The tomcat service is the Web server for Cisco IPICS and enables access to the Administration Console. For more information about the tomcat service, see the "Performing Tomcat Service Procedures" section on page 2-2.
service ippe_dial_engine {**start** | **stop** | **status**}	This command allows you to start, stop, and check the status of the dial engine. For more information about the dial engine, refer to the "Configuring and Managing the Cisco IPICS Policy Engine" chapter in the *Cisco IPICS Server Administration Guide, Release 2.0(1)*.

Understanding the Cisco IPICS Logs

This chapter describes the logs that are available in Cisco IPICS, and how to retrieve and understand the information that is contained in the logs. The logs can help you to troubleshoot problems that may occur with Cisco IPICS and the PMC.

This chapter includes the following sections:

Understanding and Locating the Cisco IPICS Log Files

The Cisco IPICS log files contain information that can be used for auditing or tracking the usage of Cisco IPICS. The log files also can also help you to determine the root cause of an error.

Table 6-1 lists the Cisco IPICS logs.

Table 6-1 Logs That Are Used with Cisco IPICS

Log Name	Description
Cisco IPICS Activity Log	The Cisco IPICS logs store information about activities relating to channels, users, and VTGs. To download and view the information in the activity log in a Microsoft Excel spreadsheet format, log in to the Administration Console as the ipics user, navigate to the **Administration > Activity Log Management > Logs** tab, and click **Download Activity Logs**. You can change the information that Cisco IPICS saves in the activity log by navigating to **Administration > Activity Log Options**. For more information about the activity log, refer to the "Performing Cisco IPICS System Administrator Tasks" chapter in the *Cisco IPICS Server Administration Guide, Release 2.0(1)*.
csalog	The csalog file contains messages that are related to CSA. The csalog file is located in the **/var/log** directory. For more information about the caslog file, see the "Opening a Security Events Log with CLI Commands" section on page 6-14.
db-maintenance.log	The db-maintenance.log file contains records of any database actions, such as a database backup or restore operation. To download and view the db-maintenance.log file, log in to the Administration Console as the ipics user, navigate to the **Administration > Database Management > Log** tab and click **Download**. The db-maintenance.log file is located in the **/opt/cisco/ipics/database/logs** directory. For more information on the db-maintenance.log file, refer to the "Performing Cisco IPICS Database Backup and Restore Operations" chapter in the *Cisco IPICS Server Administration Guide, Release 2.0(1)*.
diagnostics.log	The diagnostics.log file contains messages that are related to the database subsystem. The diagnostics.log file is located in the **/opt/cisco/ipics/database/logs** directory.

Table 6-1 Logs That Are Used with Cisco IPICS (continued)

Log Name	Description
install.log	The install.log file shows details of the Cisco IPICS installation, including the packages that were installed and any errors that occurred during the installation. The install.log file is located in the **/root** directory.
ipics.log	The ipics.log file contains information regarding all transactions that occur in the Cisco IPICS server. There are seven severities, from TRACE to FATAL. By default, the ipics.log captures all logging from the INFO to the FATAL level. You can view recent system logs in the **Serviceability > System Logs** window of the Administration Console. To download and view the information in the ipics.log, navigate to the **Serviceability > System Logs** window and click **Download**. For more information on the ipics.log file, refer to the "Understanding Cisco IPICS Serviceability and Diagnostic Information" chapter in the *Cisco IPICS Server Administration Guide, Release 2.0(1)*. The ipics.log file is located in the **/root/tomcat/current/logs** directory.
ipics_audit.log	The ipics_audit.log records user activity. This activity includes successful and unsuccessful attempts by users to log in to the server, and actions that Cisco IPICS users perform when they are logged into the Administration Console. The ipics_audit.log file is located in the **/root/tomcat/current/logs** directory.
ipics_rms.log	The ipics_rms.log collects log data for the RMS components that are part of the Cisco IPICS system. The ipics_rms.log file is located in the **/root/tomcat/current/logs** directory. When the log reaches approximately 1 MB in size, Cisco IPICS creates a new ipics_rms.log, and closes and archives the previous logs.

Table 6-1 Logs That Are Used with Cisco IPICS (continued)

Log Name	Description
lmgrd.log	The lmgrd.log file contains information regarding Cisco IPICS licenses and the component that manages the licenses (known as the license manager). Cisco IPICS logs any actions that the license manager performs in the lmgrd.log file. You can download and view the lmgrd.log file by accessing the Administration Console as the ipics user, then navigating to the **Serviceability > Diagnostics** window and clicking **Download Diagnostic Results**. You receive a zipped file that contains the lmgrd.log and ipics.log files, along with the information that displays in the Diagnostics window. The lmgrd.log file is located in the **/opt/cisco/ipics/license/versions/2.0/logs** directory.
messages	The messages file logs the following: • Messages that are related to CSA • Users that have logged into the Cisco IPICS server using SSH • Processes that have stopped or started The messages file is located in the **/var/log** directory. After seven days, CSA creates a new log and renames the previous log with a numbered extension so that the logs are named **messages.0**, **messages.1**, **messages.2**, and so on.

Table 6-1 Logs That Are Used with Cisco IPICS (continued)

Log Name	Description
Dial engine log files	The Cisco IPICS dial engine, which controls dial-in and dial-out functionality for the policy engine, produces two sets of log files: • Cisco001MIVR—These log files provide you with information about call signaling and the Session Initiation Protocol (SIP). You configure the size of each Cisco001MIVR file, the total number of files that Cisco IPICS retains, and the information that Cisco IPICS logs in these files, by navigating to **Policy Engine > Control Center > Tracing** in the Administration Console and changing the trace settings. When a log file reaches the configured maximum size, Cisco IPICS closes that log file and creates a new empty log file, and increments the number of the new log file by one. • driverManager—The driverManager logs contain information related to the media that are associated with each call. To configure the level of detail that the driverManager logs capture, navigate to **Policy Engine > Control Center > Tracing** in the Administration Console, and check or uncheck the LIB_MEDIA check boxes. Cisco IPICS sets the size and total number of driverManager files, and you cannot change these settings. The dial engine log files are located in the **/opt/cisco/ippe/log/MIVR** directory. You can also view these files by navigating to **Policy Engine > Control Center > Status > Dial Engine** in the Administration Console. You configure the size of each file, the number of log files that are retained, and the logging levels by navigating to **Policy Engine > Control Center > Tracing** in the Administration Console and changing the trace settings. For more information, refer to the "Configuring and Managing the Cisco IPICS Policy Engine" chapter in the *Cisco IPICS Server Administration Guide, Release 2.0(1)*.

Generating and Modifying the PMC Log Levels

The PMC application generates logs that can help you analyze user activity and troubleshoot problems that you may encounter when you use the application. The PMC writes the logs to the hard disk of the PMC client machine, so that the application can continue logging if the communication to the server is disrupted.

Cisco IPICS retrieves logs from the PMC if one of the following conditions are met:

- When you click **Get Logs from PMC** from the **User Management > Users >** *Username* **> PMC** tab.

Note You can prevent the server from uploading the logs from the PMC user by navigating to **Settings > Channels** in the PMC application and checking the **Optimize for low bandwidth** check box. You should check this box if you are using the PMC in a low bandwidth, high latency network environment. The PMC still generates logs on the hard drive of the PMC client machine.

- When you set the logs to be uploaded to the Cisco IPICS server automatically when the PMC user logs in, and then out of, a session (this event is called rollover).

  Rollover occurs for the Authentication, Channel Statistics and User Interface logs, but not for the Debug Log. In the case of the Debug Log, the file continues to accumulate data until the server requests that the file be uploaded. For more information about a rollover occurrence, refer to the "Using the PMC Application Logs" chapter in the *Cisco IPICS PMC Installation and User Guide, Release 2.0(1)*.

Users can modify the PMC logs in the following ways:

- The PMC user can adjust settings within the PMC application. For more information about adjusting settings in the PMC application, refer to the "Using the PMC Application Logs" chapter in the *Cisco IPICS PMC Installation and User Guide, Release 2.0(1)*.

- From the Administration Console, the Cisco IPICS operator can modify the log settings in the **User Management > Users >** *Username* **> PMC** tab. See the "Performing Cisco IPICS Operator Tasks" chapter in the *Cisco IPICS Server Administration Guide, Release 2.0(1)* for more information about setting and modifying the log settings.

For a list of the log files and their descriptions, refer to the "Using the PMC Application Logs" chapter in the *Cisco IPICS PMC Installation and User Guide, Release 2.0(1)*.

You can download activity logs for PMC users in the **Administration > Activity Log Management > Logs** tab of the Administration Console. The information that you download includes details about user associations to channels and VTGs, channel activation activities, and conference participation. You configure the activity logs to capture the PMC information in the **Administration > Activity Log Options** window. For information about the activity logs, refer to the "Performing Cisco IPICS System Administrator Tasks" chapter in the *Cisco IPICS Server Administration Guide, Release 2.0(1)*.

This section has the following topics:

Understanding PMC Debug Log Information

Cisco IPICS organizes the DebugLog.txt data fields into three categories: User Interface, Signaling, and Media. These data fields are then divided into three logging levels, so that you can capture more precisely the debugging information that you need. The Debug Log categories contain the following information:

- User Interface—These fields provide information about aspects of the user interface for the PMC. The category includes everything that the user can see on the PMC application, such as the buttons and volume controls. The User Interface category also includes information for debugging communication problems with the Cisco IPICS server.

  Table 6-2 describes the information that Cisco IPICS gathers, by log level:

Table 6-2 User Interface Log Levels

Logging Level	Purpose
Low	Cisco IPICS retrieves information for the following problems at the Low log level: • The user cannot log in • The user has difficulty activating channels • The user cannot close the PMC • The PMC unexpectedly goes into offline mode • The server is reporting errors
Medium	Cisco IPICS reports information that can help translate XML communication from the server.
High	Cisco IPICS gathers information regarding authentication, the GUI, and the PMC server update function.

- Signaling—The Signaling category includes fields that provide information about the starting and stopping of voice channels. You would turn Signaling on when a user is not able to activate or deactivate a PMC channel.

  Table 6-3 describes the information that Cisco IPICS reports by signaling levels.

Table 6-3 Signaling Log Levels

Logging Level	Purpose
Low and Medium	Messages at these log levels describe issues with the high level state machines.
High	Messages at this level report issues with SIP messaging.

- Media—These fields involve items related to the voice stream, such as the packets and the codecs that handle the data between end points. You would use Media information to diagnose any voice quality problem.

  Table 6-4 describes the type of information you can gather with the Media log levels.

Table 6-4 Media Log Levels

Logging Level	Purpose
Low	This information provides RX and TX networking statistics.
Medium	This information can help you diagnose audio mixing issues, such as the combining of audio signals in a channel or VTG.
High	This information provides you with information regarding the conversion of audio using audio codecs.

Using the Debugging Log Level

When you choose to begin logging debug information for a PMC user, you select one or more of the information categories, each of which includes a list of debugging fields. You choose the category and logging level as it corresponds to the fields that you want to capture in the log.

Table 6-5 shows the fields that are included in each logging level.

The log levels for each category are cumulative. If you choose the Medium level for a category, the PMC writes Low- and Medium-level logs into the DebugLog.txt file. When you set the logging to High, you capture all the fields for that category.

Tip Always start debugging by collecting Low-level log data, which may provide all of the data that you require. Using a log level of Low allows you to gather several days of log activity without filling the hard disk of the PMC user. If you cannot locate the cause of the problem, you can set the logging to Medium or High.

Use the High level only for short durations. If you use the High level, you should closely monitor the hard drive of the user so that the High-level logs do not overwhelm the client hard drive or degrade the performance of the PMC.

Caution Because of the large amount of information that the system collects and generates when you set all of the debug options, Cisco recommends that you use debug logging only to isolate specific problems. When you complete your debugging tasks, be sure to turn off debug logging by clearing the debug log.

Table 6-5 lists the debug categories, and the fields and log levels that are associated with each category.

Table 6-5 Debug Log Fields and Log Levels

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

Table 6-5 Debug Log Fields and Log Levels (continued)

Category	Field	Log Level
Signaling	cc	Low
	fim	
	fsm	
	gsm	
	lsm	
	multicast-signaling-debug	
	sip-reg-state	
	sip-state	
	vcm	
	sip-task	Medium
	sip-trx	
	Auth	High
	cc-msg	
	sip-messages	

Table 6-5 Debug Log Fields and Log Levels (continued)

Category	Field	Log Level
Media	AMuteTrans	Low
	AudioSink	
	AudioSource	
	MediaStream	
	OpenALAudioSink	
	RTPAudioSink	
	RTPAudioSockets	
	RTPAudioSource	
	RTPAudioStream	
	RTPJitterBuf	
	sock-init-Cleanup	
	WaveAudioSource	
	WaveFileSource	
	RxStats	
	TxStats	
Media	ACMTrans	Medium
	ASL	
	AudioBufferAndPlayback	
	dsp	
	FilePlay	
	PCMMixer	
	PCMVolTrans	
	PCMVolumeMax	
	RTPAudioStreamMgr	
	RxDetailStats	
	VAD	

Table 6-5 Debug Log Fields and Log Levels (continued)

Category	Field	Log Level
Media	AudioDump	High
	AudioSamp	
	AudioSampLost	
	AudioSampMgr	
	AudioTrans	
	AutomaticGainControl	
	dtmf	
	FIRTrans	
	FSAudioBuf	
	G7112PCMTrans	
	G7232PCMTrans	
	G729A2PCMTrans	
	Limiter	
	PCM2G711Trans	
	PCM2G723Trans	
	PCM2G729ATrans	
	RTCPPacket	
	TimeSample	
	TimeRxSample	
	TimeTxSample	

Checking CSA Logs

If CSA denies a system action, the process generates a message that you can access in one of the following ways:

- You can open the CSA Utility to view the messages in the Message pane
- You can view the Security Events Log, which includes all security events that have occurred on the system
- You can navigate to the **/var/log** directory, and view the current and archived CSA logs

This section includes the following topics:

Viewing the CSA Messages from the CSA Utility

To view status messages in the CSA utility, perform the following procedure:

Procedure

Step 1 Double-click the CSA tray icon (the red flag) to open the CSA Utility.

The CSA Utility displays.

Step 2 To access the Security Logs, click **Messages**.

Status messages display in the Messages pane.

Step 3 To view the CSA log, click **View Log**.

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

Opening a Security Events Log with CLI Commands

The **/var/log** directory in the Cisco IPICS server contains the current and archived CSA logs.

The file name of the 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.

To view a security event log by using CLI commands, perform the following procedure:

Procedure

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

Step 2 To navigate to the **/var/log** directory, enter the following command:

Step 3 [root] **#cd /var/log**

Step 4 To view a list of the files in the directory, enter the following command:

Step 5 [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 6 To view the contents of a log file, enter the following command:

Step 7 [root] **#cat csalog** [**.***x*]

Where:

x is the file extension of the csalog file you would like to view.

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

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

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 select check box Provides the ability to select or deselect the specified channel on the PMC for audio transmission.

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

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

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 policy engine Integrated with the Cisco IPICS server, this component enables telephony dial functionality and is responsible for the management and execution of policies and user notifications.

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. The server also includes the Cisco IPICS policy engine, which enables telephony dial functionality and is responsible for the management and execution of policies and user notifications.

Cisco Unified 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 Unified 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 engine scripts Scripts that the Cisco IPICS dial engine executes to provide the telephony user interface (TUI) for interaction with incoming and outgoing phone calls.

dial-in A phone call that is dialed in to the policy engine.

dial-in floor control A feature that allows one dial-in user, at a time, to talk in a VTG or a channel. The telephony user interface provides this dial-in floor control feature to support dial-in users. It does not provide support for floor control for other PTT users.

dial number The phone number that is used by the policy engine and the SIP provider and configured in the Dial Information pane in the Ops Views window. Dialing this number provides user access to the telephony user interface.

dial out invite An action that invites selected user(s) to the selected VTG.

A phone call that is dialed out by the policy engine to a phone user to invite the user in to a talk group.

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

digit 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 Unified 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 PMC users, as necessary, and manages policies, which activate/deactivate VTGs based on specific criteria and designated intervals. Policy management activities include create/modify/delete policies, view policies, execute policies, and activate privileges.

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.

Cisco enables the Cisco Hoot 'n' Holler feature in specific Cisco IOS versions.

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.

informix linux group Members of this group have full permission to Cisco IPICS server folders, files, and scripts that are related to the Informix database application. Members of this group include the informix and ipicsdba users.

informix user ID The Cisco IPICS Linux user that belongs to both the informix linux group, which includes full permission to the Cisco IPICS database server folders, files, and scripts, and the ipics linux group, which includes permission to Cisco IPICS application-related folders, files, and scripts. In addition, this user has full administrative permission to the Informix database instance. Cisco IPICS creates this Linux system user ID and generates the password during the software installation process. The password for this user ID never expires.

To access the informix user, log in to the Cisco IPICS server by using the root user ID; then, enter **su - informix** (superuser from root).

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.

invitation policy A policy that can be invoked only through the telephony user interface and can include only the invite to VTG action. After joining a talk group, a user can access the breakout menu and invoke invitation policies. The talk group that this user has joined is the talk group that the invited users join.

invite to VTG A version of the dial out invite action where users to be invited are preconfigured but the VTG that they are invited to depends on which VTG the invoker of the policy is dialed into.

ipicsadmin user ID The Cisco IPICS Linux user that, as part of the ipics linux group, has full permission to the Cisco IPICS server folders, files, and scripts that are related to the Cisco IPICS application and database backup and restore operations. In addition, the ipicsadmin user has permission to read and write data from and/or to the Informix database. Cisco IPICS creates this Linux system user ID during the software installation process. The password for this user ID never expires.

ipicsdba user ID The Cisco IPICS Linux user that belongs to both the informix linux group, which includes full permission to the Cisco IPICS database server folders, files, and scripts, and the ipics linux group, which includes permission to Cisco IPICS application-related folders, files, and scripts. In addition, the ipicsdba user has permission to read data, write data, create tables, and create databases in the Informix database instance. Cisco IPICS creates this Linux system user ID and generates the password during the software installation process. The password for this user ID never expires.

To access the ipicsdba user, log in to the Cisco IPICS server by using the root user ID; then, enter **su - ipicsdba** (superuser from root).

ipics linux group Members of this group have full permission to Cisco IPICS server folders, files, and scripts that are related to the Cisco IPICS application and database backup and restore operations. Members of this group include the ipicsadmin, ipicsdba, and informix users.

ipics user ID The Cisco IPICS application-level user ID that can perform all administration-related tasks via the Cisco IPICS Administration Console. Cisco IPICS creates this web-based user ID during the software installation process.

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.

Cisco IPICS leverages the Cisco Hoot 'n' Holler feature, which is enabled in specific Cisco IOS versions, to provide radio integration into the Cisco IPICS solution. LMR is integrated by providing an ear and mouth (E&M) interface to a radio or other PTT devices, such as Nextel phones. Configured as a voice port, this interface provides the appropriate electrical interface to the radio. You configure this voice port with a connection trunk entry that corresponds to a voip dial peer, which in turn associates the connection to a multicast address. This configuration allows you to configure a corresponding channel in Cisco IPICS, using the same multicast address, which enables Cisco IPICS to provide communication paths between the desired endpoints.

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 address/port combinations are also used by gateways and RMS components.

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).

multipurpose policy A policy that can include any of the supported actions; may be invoked through the telephony user interface or the Cisco IPICS administration console.

multiselect buttons Provides the ability to select or deselect all channels on the PMC for audio transmission.

mute The functionality that enables a dispatcher to mute a PMC user from talking or transmitting voice on one or more channels. The dispatcher can mute the microphone of the user or both the microphone and the speaker.

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 Telecommunication 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.

notification — An action that notifies selected user(s) via email, SMS, pager, or phone. The necessary IDs and phone numbers are configured in the communication preferences for each user. Notifications that are sent via the phone require user authentication before the notification prompt is heard.

An email, SMS, pager, or phone call that is placed to a user for the purpose of sending a notification message.

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 across multiple organizations or agencies that normally would not share resources. While ops views are maintained separately by the Cisco IPICS system administrator and/or ops view administrator, this functionality also allows multiple entities to use one Cisco IPICS server to enable resource sharing across multiple ops views, according to business need.

ops view administrator The ops view administrator capabilities include managing and monitoring the activity logs that are filtered by ops views and accessible in the Administration Console (**Administration > Activity Log Management**) window.

OTAR over-the-air re-keying. Provides the ability to update or modify over radio frequency the encryption keys that are programmed in a mobile or portable radio.

P

packet A logical grouping of information that includes a header that contains control information. Usually also includes user data.

packet switching The process of routing and transferring data by using addressed packets so that a channel is occupied during the transmission of the packet only. Upon completion of the transmission, the channel is made available for the transfer of other traffic.

PIM Protocol Independent Multicast. Multicast routing architecture that allows the addition of IP multicast routing on existing IP networks. PIM is unicast routing protocol independent and can be operated in two modes: PIM dense mode and PIM sparse mode.

PIM dense mode One of the two PIM operational modes. PIM dense mode is data-driven and resembles typical multicast routing protocols. Packets are forwarded on all outgoing interfaces until pruning and truncation occurs. In dense mode, receivers are densely populated, and it is assumed that the downstream networks want to receive and will probably use the datagrams that are forwarded to them. The cost of using dense mode is its default flooding behavior. Sometimes called dense mode PIM or PIM DM.

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 Policies include one or more actions that execute sequentially and can be manually activated via the Cisco IPICS administration console or the telephony user interface. Cisco IPICS provides support for multiple policy types.

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.

policy execution status An indicator of policy execution success or failure. The Cisco IPICS administration console provides a status for each action under a policy,

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 also mixes PMC SIP-based (unicast) connections to a multicast channel or VTG. The RMS can be installed as a stand-alone component (RMS router) or as an additional feature that is installed in the LMR gateway.

root user ID The Cisco IPICS Linux user that has access to all files in the Cisco IPICS server. Strong passwords are enforced and Linux operating system password expiration rules apply to this user ID.

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.

script prompts The audio prompts that the dial engine scripts play out during execution and which callers hear when they are interacting with the telephony user interface.

secure channel A channel that is connected to a radio that provides secure (encrypted or scrambled) communications on the Common Air Interface (CAI) side of the radio. (The level of security that is configured in the data network determines the security of the communications between the LMR gateway and a network attached device, such as a PMC or Cisco Unified IP Phone.)

An attribute that is set in the server to indicate that a channel is secure. A PTT channel that is configured as secure cannot be combined with unsecure channels in a VTG.

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.

spoken names The recorded names that are used for entities, such as channels, channel groups, VTGs, users, user groups, ops views, and policies. The names can be recorded through the policy engine or externally-recorded.wav files that can be uploaded into the system.

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 VTG or a channel.

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 On some of the PMC skins, this indicator blinks red when traffic is being transmitted.

trigger A time-based event that invokes a policy on a scheduled basis, without manual intervention.

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.

TUI telephony user interface. The telephony interface that the dial engine provides to enable callers to perform tasks, such as joining talk groups and invoking policies.

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, supported models of Cisco Unified IP Phones, and the Public Switched Telephone Network (PSTN) via the telephony dial functionality of the Cisco IPICS IP policy engine. Users may have one or more Cisco IPICS roles, such as system administrator, ops view administrator, operator or dispatcher.

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 a supported Cisco Unified IP Phone model.

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

voice replay A feature that allows the PMC user to replay buffered audio on a per channel basis.

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 add participant An action that adds selected participant(s) to the selected VTG.

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.

Numerics

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V