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)*.