Cisco IPICS Troubleshooting Guide

Release 4.10

December 14, 2016

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.
CONTENTS

INTRODUCTION v
AUDIENCE v
ORGANIZATION v
RELATED DOCUMENTATION vi
OBTAINING DOCUMENTATION, OBTAINING SUPPORT, AND SECURITY GUIDELINES vi

CHAPTER 1
FINDING TROUBLESHOOTING INFORMATION FOR CISCO IPICS 1-1

CHAPTER 2
TROUBLESHOOTING CISCO IPICS NETWORK PROCESSES 2-1
Performing Tomcat Service Procedures 2-1
Checking the Status of the Tomcat Service 2-2
Manually Stopping the Tomcat Service 2-2
Manually Starting the Tomcat Service 2-3
Manually Restarting the Tomcat Service 2-4
Performing Database Server Procedures 2-5
Checking the Status of the Database Server 2-5
Manually Restarting the Database Server 2-5
Manually Starting the Database Server 2-6
Performing License Manager Procedures 2-7
Checking the Status of the License Manager 2-7
Restarting the License Manager 2-8
Manually Starting the License Manager 2-8
Performing Dial Engine Procedures 2-9
Checking the Status of the Dial Engine 2-9
Manually Stopping the Dial Engine 2-10
Manually Restarting the Dial Engine 2-10
Manually Starting the Dial Engine 2-11

CHAPTER 3
TROUBLESHOOTING THE CISCO IPICS SERVER 3-1
Troubleshooting Cisco IPICS Installation Issues 3-1
Troubleshooting Cisco IPICS Administration Console Issues 3-1
Resolving Intermittent Browser Problems 3-2
Resolving Failures to Access the Server With an Administration Console Browser Session 3-3
Resolving LDAP Import Issues 3-6
Resolving “unexpected inconstancy” Message on Cisco IPIC Server Console Screen 3-6
Troubleshooting Browser Timeout Issues When You Configure an RMS with Twelve or More Loopback Interfaces 3-6
Cisco IPICS Displays “Server Initializing” for More than 1 Hour 3-8
Performing Database Procedures To Resolve Login Problems and Failure To Complete Tasks in the Administration Console 3-8
VTG Activates Without Dispatcher Action 3-9
Troubleshooting VTG Activation Problems 3-10
VTG Does Not Appear on User IDC 3-10
Troubleshooting an Ops View Save Failure 3-11
Resolving Administration Console Undefined Errors 3-12
Commands Fail Intermittently 3-12
Adding Fonts to Internet Explorer to Fix Language Character Display Problems 3-12
IDC Users Receive Error Messages During Login After a Database Restore Operation 3-13
Configuration Changes Do Not Get Saved When Multiple Users Configure Cisco IPICS 3-14
Recovering a Deleted System Administrator User 3-14
Troubleshooting Reporter Issues 3-15
Resolving Security Certificate Issues 3-15
Troubleshooting User ID and Password Issues 3-15
Resetting a Forgotten or Missing ipics User Password 3-15
Resetting the Password for the ipcsadmin or informix User ID 3-16
Changing the root User Password 3-16
Resetting a Locked or Disabled User Account 3-17
Troubleshooting License Issues 3-17
Resolving Invalid Base Server License Messages that Display After You Upload the License File 3-18
After Uploading Multiple License Files, All Features Do Not Display in the Administration Console 3-20
After Changing the Server IP Address, You Experience Host Name Mismatch or Problems Installing the License 3-21
Changing System Date Invalidates Time-Bound License 3-21
Suppressing Server Expiration Messages After Installing a More Recent Time-Bound License 3-22
Troubleshooting Policy Engine Issues 3-23
Uploading a Large Zipped File of Prompts Causes an Error 3-23
IppeAgentImpl ERROR Messages Display in the ipics.log File 3-24
Resolving Communication Problems Between the Policy Engine and the Prompt Manager 3-25
Resolving Reconnection Failures After a Dial-In Caller Uses the Hold or Call Waiting Feature 3-25
Troubleshooting Dial-In Call Connection Failures 3-25
Troubleshooting Dial-Out Invitation Failures 3-28
Troubleshooting Dial-Out Notification Failures 3-29
Troubleshooting Dial-Out Notification Failures Between Users in Different Ops Views 3-30
Understanding a PARTIAL_SERVICE Status For the Dial Engine and Subsystem Manager 3-30
Analyzing a SHUTDOWN Status For the SIP Subsystem 3-30

CHAPTER 4

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

Troubleshooting Communication Issues 4-1
Analyzing Communications Problems Between All Locations on a Channel 4-2
Troubleshooting Communication Failures Between VTG Participants 4-2
Resolving Communications Problems For Newly-Added IDC Users on a Channel 4-2
Removing a Logged-Out IDC User from the Active Users List 4-3
IDC Users Can Listen to Channels But Cannot Listen to VTGs 4-3
Configuring the RMS to Eliminate Automatic Channel Deactivation for SIP-Based Remote Connections 4-4
Eliminating Feedback Noise on VTG 4-4
Understanding Communication Problems Between Cisco IPICS End Point Devices and Radios that Require a Guard Tone 4-4

Troubleshooting Voice Quality Issues 4-5
Voice Quality Degrades for IDC 4-5
Troubleshooting Poor IDC Voice Quality 4-6
Dial Engine Calls Experience Degraded Voice Quality 4-6
Resolving Interruption of Voice Communications When You Use VTGs and SIP-Connected IDC Client Machines 4-6
Resolving LMR Voice Issues 4-7

Troubleshooting Equipment Issues 4-7
No Power to Cisco Unified IP Phones 4-7
Analyzing One-Way Audio Issues Between IDC Client Machines and Cisco Unified IP Phones 4-8
Resolving One-Way Audio Problems on the Cisco Unified IP Phone That Occurs After You Receive or Place a Call 4-8
Cisco Unified IP Phone Cannot Access the Cisco IPICS Service After Changing the Server IP Address 4-8
Resolving Interconnectivity Problems With Cisco Unified Wireless IP Phone 7920 4-9
Resolving Cisco Trunked Radio VTG Issues 4-9

Troubleshooting RMS Configuration Issues 4-9
Server Reboots Slowly Following RMS Configuration 4-10
You Attempt to Deactivate an RMS but its Status Does Not Change 4-10
VTG Activation Slow or RMS in Unreachable State After RMS Command Prompt Changed 4-11
RMS Fails or Remains in Unreachable State 4-11
Newly-Added RMS Does Not Display Loopbacks 4-12
Router Remains in Unreachable State 4-12
The Cisco IPICS Server Does Not Recognize All of the T1 Ports on the RMS 4-12
Router Indicator Lights for the Loopback Are Not Green 4-13
Voice Loops in VTGs and Router Configuration Shows Incorrect Information 4-14
Long Delays Between Pressing the IDC PTT Button and Media Establishment 4-15

Chapter 5: Troubleshooting the IDC and Cisco Instant Connect 5-1

Troubleshooting IDC Issues 5-1
  Resolving IDC Execution Issues 5-1
  Generating a IDC Installation Log File 5-2
  Using the idcsetup.exe Installer with an Encrypted File System 5-3
  Making idcsetup.exe Configuration File Changes 5-4
  Resolving IDC Dialer Issues 5-4
  Resolving Footswitch/USB Device Issues 5-4
  Configuring the Audio Settings 5-5
  IDC Coexistence with Other Voice Applications 5-6
  Troubleshooting IDC Voice Quality Issues 5-6
  Resolving Name Resolution Failures 5-8
  Identifying Channel Activation Issues 5-8

Troubleshooting Cisco Instant Connect Issues 5-9
  Resolving Cisco Instant Connect for Windows Issues 5-9
  Resolving Cisco Instant Connect for Android Issues 5-9

Chapter 6: Understanding the Cisco IPICS Logs 6-1

Understanding and Locating the Cisco IPICS Log Files 6-1
Generating and Modifying the IDC Log Levels 6-5
Understanding IDC Debug Log Information 6-6
Using the Debugging Log Level 6-7

Glossary
Index
Preface

Introduction

Cisco IPICS Troubleshooting Guide, Release 4.10 provides information that can assist you with troubleshooting issues that you may encounter when you install, configure, or use the Cisco IP Interoperability and Collaboration System (Cisco IPICS).

Audience

This document is intended for system administrators who install, configure, operate, or manage Cisco IPICS system and for end users who communicate with other users by using the IPICS Dispatch Console (IDC) or other end points.

Organization

This document is organized as follows:

| Chapter 1, “Finding Troubleshooting Information for Cisco IPICS” | Provides information about how to find troubleshooting information for Cisco IPICS |
| Chapter 2, “Troubleshooting Cisco IPICS Network Processes” | Provides information to help you to troubleshoot network processes that relate to Cisco IPICS |
| Chapter 3, “Troubleshooting the Cisco IPICS Server” | Describes how to resolve issues that you may encounter when you use the Cisco IPICS server |
| Chapter 4, “Troubleshooting Communication, Voice Quality and Other Equipment Issues” | Describes how to resolve communication and voice quality issues and hardware, firmware, and software issues that you might encounter with other equipment in a Cisco IPICS deployment |
| Chapter 5, “Troubleshooting the IDC and Cisco Instant Connect” | Provides information to help you troubleshoot issues that you may encounter when you use the IDC |
| Chapter 6, “Understanding the Cisco IPICS Logs” | Describes the logs that are available in Cisco IPICS, and how to retrieve and understand the information that is contained in the logs |
Related Documentation

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

Cisco also provides a wide variety of documentation that provides related information about Cisco IPICS components and the configuration of an infrastructure that supports Cisco IPICS. References to related documentation is provided throughout this manual as appropriate.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information about obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and recommended aliases and general Cisco documents, see the monthly What’s New in Cisco Product Documentation. This document also lists all new and revised Cisco technical documentation.

Finding Troubleshooting Information for Cisco IPICS

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

Table 1-1  Locating Troubleshooting Information

<table>
<thead>
<tr>
<th>Source of Problem</th>
<th>Where to Find Help</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IPICS installation</td>
<td>To troubleshoot problems that are related to the installation of Cisco IPICS, see the “Troubleshooting Cisco IPICS Installation Issues” chapter in the Cisco IPICS installation document for your Cisco IPICS release.</td>
</tr>
<tr>
<td>One of the following areas:</td>
<td>For problems that are related to the Cisco IPICS server, the policy engine, or the devices that communicate with the server, see Chapter 3, “Troubleshooting the Cisco IPICS Server.”</td>
</tr>
<tr>
<td>• The Cisco IPICS server</td>
<td>For help with gathering log information to aid your problem determination and resolution process, see Chapter 6, “Understanding the Cisco IPICS Logs.”</td>
</tr>
<tr>
<td>• Policy engine</td>
<td></td>
</tr>
<tr>
<td>• Communications between Cisco IPICS end-user devices</td>
<td></td>
</tr>
<tr>
<td>• Equipment, such as Cisco Unified IP Phones or radios</td>
<td></td>
</tr>
<tr>
<td>• RMS configuration</td>
<td></td>
</tr>
<tr>
<td>• General operation</td>
<td></td>
</tr>
<tr>
<td>One of the following areas:</td>
<td>For communications-related problems, problems with endpoint devices, and voice quality issues, see Chapter 4, “Troubleshooting Communication, Voice Quality and Other Equipment Issues.”</td>
</tr>
<tr>
<td>• Communications between Cisco IPICS endpoints</td>
<td></td>
</tr>
<tr>
<td>• Hardware, such as Cisco Unified IP Phones</td>
<td></td>
</tr>
<tr>
<td>• Router and RMS configuration</td>
<td></td>
</tr>
<tr>
<td>• Voice quality</td>
<td></td>
</tr>
</tbody>
</table>
To troubleshoot problems that you may encounter when you install or use the IDC, see Chapter 5, “Troubleshooting the IDC and Cisco Instant Connect.”

For help with gathering IDC log information to aid your problem determination and resolution process, see “Understanding Cisco IPICS Serviceability the and Diagnostic Information” chapter in Cisco IPICS Server Administration Guide for your Cisco IPICS release.

To obtain information about backing up or restoring the Cisco IPICS database, or to troubleshoot problems that you encounter during the backup or restore process, see the “Performing Cisco IPICS Database Backup and Restore Operations” chapter in Cisco IPICS Server Administration Guide for your Cisco IPICS release.

For information about problems that are related to the installation and use of licenses, see the “Troubleshooting License Issues” section on page 3-17.
Troubleshooting Cisco IPICS Network Processes

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

- Tomcat service
- Database server
- License manager
- Dial engine (if the policy engine is licensed for your Cisco IPICS deployment)

This chapter includes the following topics to help you to troubleshoot these processes:

- Performing Tomcat Service Procedures, page 2-1
- Performing Database Server Procedures, page 2-5
- Performing License Manager Procedures, page 2-7
- Performing Dial Engine Procedures, page 2-9

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

Performing Tomcat Service Procedures

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

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

The following sections provide information about the tomcat service:

- Checking the Status of the Tomcat Service, page 2-2
- Manually Stopping the Tomcat Service, page 2-2
- Manually Starting the Tomcat Service, page 2-3
- Manually Restarting the Tomcat Service, page 2-4
Checking the Status of the Tomcat Service

You can check the status of the tomcat service by navigating to the Serviceability > Diagnostics window of the Administration Console and viewing the Cisco IPICS Tomcat Web Server Status field. If the tomcat service or the database server is not running, you cannot check its status in the Administration Console. In this case, you must enter CLI commands to check its status. To check the status of the tomcat service by using CLI commands, perform the following procedure:

Procedure

Step 1 Connect to the Cisco IPICS server by using SSH Secure Shell client software (or similar software) and log in with root user privileges.

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

[root]# service ipics_tomcat status

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

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

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

Tomcat is not running on the system.

If the tomcat service is not running, you can start it manually by entering the service ipics_tomcat start CLI command from the root user ID. For more information, see the “Manually Starting the Tomcat Service” section on page 2-3.

Manually Stopping the Tomcat Service

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

To stop the tomcat service, perform the following procedure:

Procedure

Step 1 Connect to the Cisco IPICS server by using SSH Secure Shell client software (or similar software) and log in with root user privileges.

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

[root]# service ipics_tomcat stop

If the tomcat service stops, Cisco IPICS displays the message (OK).

If the tomcat service does not stop, an error message displays that indicates that Cisco IPICS cannot stop the service; if you receive this message, continue to Step 3.
Step 3 If the tomcat service fails to stop, you can terminate the processes that are running by performing the following procedure:

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

```
[root]# ps -ef | grep tomcat
```
This command shows you a list of the running tomcat processes.

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

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

```
[root]# kill -9 process-id
```
where:

`process-id` specifies the Process IDs that you noted in Step b.

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

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

```
[root]# service ipics_tomcat status
```
If the tomcat service stops successfully, the following message displays:

`Tomcat is not running on the system.`

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

```
[root]# tail -75 /root/tomcat/current/logs/ipics.log
```
The last 75 lines of the ipics.log file displays.

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

Step 6 Attempt to fix the problem based on the information that you view in the log file.
The information might include information about a running process that could not stop.

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

---

**Manually Starting the Tomcat Service**

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

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

**Procedure**

Step 1 Connect to the Cisco IPICS server by using SSH Secure Shell client software (or similar software) and log in with root user privileges.
Performing Tomcat Service Procedures

Step 2 Enter the following command to start the tomcat service:

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

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

---

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

---

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

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

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

---

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

---

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

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

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

---

Manually Restarting the Tomcat Service

To restart the tomcat service, perform the following procedure.

---

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

---

Procedure

Step 1 Connect to the Cisco IPICS server by using SSH Secure Shell client software (or similar software) and log in with root user privileges.

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

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

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

---

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

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

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

- Checking the Status of the Database Server, page 2-5
- Manually Restarting the Database Server, page 2-5
- Manually Starting the Database Server, page 2-6

Checking the Status of the Database Server

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

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

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Connect to the Cisco IPICS server by using SSH Secure Shell client software (or similar software) and log in with root user privileges.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>To check the status of the database server, enter the following command: [root]# service ipics_db status</td>
</tr>
</tbody>
</table>

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

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

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

```
Ipics Database is stopped.
```

If the database server is not running, you can manually start the database server by performing the procedure in the “Manually Starting the Database Server” section on page 2-6.

Manually Restarting the Database Server

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

- From the Administration Console, navigate to the Serviceability > Dashboard window and check the memory information that is displayed in the System Dashboard area.
Performing Database Server Procedures

• Log in to a terminal console session by using the root user ID; then, enter the `top` command.

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

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

To restart the database server, perform the following procedure:

**Procedure**

**Step 1** Connect to the Cisco IPICS server by using SSH Secure Shell client software (or similar software) and log in with root user privileges.

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

```
[root]# service ipics_db restart
```

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

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

---

**Manually Starting the Database Server**

Cisco IPICS starts the database server when the server boots up. You can also start the database server manually if you determine that the database has stopped. To check whether the database is running, see the “Checking the Status of the Database Server” section on page 2-5.

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

**Procedure**

**Step 1** Connect to the Cisco IPICS server by using SSH Secure Shell client software (or similar software) and log in with root user privileges.

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

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

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

**Step 3** If the database does not successfully start, contact your Cisco technical support representative for further assistance.
Performing License Manager Procedures

The license manager is the network process that manages the Cisco IPICS licenses. The license manager checks for new licenses every 24 hours. For a new license file to take effect immediately, you must restart the license manager.

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

- Checking the Status of the License Manager, page 2-7
- Restarting the License Manager, page 2-8
- Manually Starting the License Manager, page 2-8

Checking the Status of the License Manager

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

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

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

Procedure

Step 1 Connect to the Cisco IPICS server by using SSH Secure Shell client software (or similar software) and log in with root user privileges.

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

[root]# service ipics_lm status

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

ipics_lm is running (PID 20859).

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

ipics_lm is not running.
Performing License Manager Procedures

Step 3 If the license manager is not running, you can manually start the license manager by following the procedure in the “Manually Starting the License Manager” section on page 2-8.

Restarting the License Manager

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

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

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

Procedure

Step 1 Connect to the Cisco IPICS server by using SSH Secure Shell client software (or similar software) and log in with root user privileges.

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

[root]# service ipics_lm restart

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

Step 3 If you receive an error message that indicates that the license manager or lmgrd process could not start, contact your Cisco technical support representative for further assistance.

Manually Starting the License Manager

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

Procedure

Step 1 Connect to the Cisco IPICS server by using SSH Secure Shell client software (or similar software) and log in with root user privileges.

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

[root]# service ipics_lm start

If the license manager starts successfully, Cisco IPICS displays the message [OK].

Step 3 If the license manager does not start, check the status by performing the actions that are documented in the “Checking the Status of the License Manager” section on page 2-7.
Performing Dial Engine Procedures

The dial engine controls the dial-in and dial-out functionality for the policy engine. For more information about the policy engine and dial engine, see the “Using the Cisco IPICS Policy Engine” chapter in Cisco IPICS Server Administration Guide for your Cisco IPICS release.

Your Cisco IPICS deployment must include a license for the policy engine before you can perform dial engine procedures. To check whether your deployment includes a license for the policy engine, navigate to the Administration > License Management > Summary tab in the Administration Console and check the Policy Engine Base License field. If your system includes a license for the policy engine, the field displays a status of Licensed. For more information about licenses, see the “Performing Cisco IPICS System Administrator Tasks” chapter in Cisco IPICS Server Administration Guide for your Cisco IPICS release.

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

- Checking the Status of the Dial Engine, page 2-9
- Manually Stopping the Dial Engine, page 2-10
- Manually Restarting the Dial Engine, page 2-10
- Manually Starting the Dial Engine, page 2-11

Checking the Status of the Dial Engine

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

Procedure

Step 1 Connect to the Cisco IPICS server by using SSH Secure Shell client software (or similar software) and log in with root user privileges.

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

```
[root]# service ippe.DialEngine status
```

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

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

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

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

Step 3 If the dial engine is not running, you can manually start the dial engine by performing the procedure in the “Manually Starting the Dial Engine” section on page 2-11.

Manually Stopping the Dial Engine

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

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

Procedure

Step 1 Connect to the Cisco IPICS server by using SSH Secure Shell client software (or similar software) and log in with root user privileges.

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

[root]# service ippe_dial_engine stop

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

Manually Restarting the Dial Engine

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

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

Procedure

Step 1 Connect to the Cisco IPICS server by using SSH Secure Shell client software (or similar software) and log in with root user privileges.

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

[root]# service ippe_dial_engine restart

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

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

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

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

The status displays as Licensed or Not Licensed.

c. Perform one of the following actions based on the output that displays:
Performing Dial Engine Procedures

- If the Policy Engine Base License field shows a status of Not Licensed, you are not licensed for the policy engine. To purchase a license that includes policy engine functionality, contact your Cisco representative.
- If the Policy Engine Base License field shows a status of Licensed, contact your Cisco technical support representative for further assistance.

Manually Starting the Dial Engine

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

**Procedure**

**Step 1** Connect to the Cisco IPICS server by using SSH Secure Shell client software (or similar software) and log in with root user privileges.

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

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

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

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

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

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

   The status displays as Licensed or Not Licensed.

c. Perform one of the following actions based on the output that displays:

   - If the Policy Engine Base License field shows a status of Not Licensed, you are not licensed for the policy engine. To purchase a license and obtain dial engine and policy engine functionality, contact your Cisco representative.
   - If the Policy Engine Base License field shows a status of Licensed, contact your Cisco technical support representative for further assistance.
CHAPTER 3

Troubleshooting the Cisco IPICS Server

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

- Troubleshooting Cisco IPICS Installation Issues, page 3-1
- Troubleshooting Cisco IPICS Administration Console Issues, page 3-1
- Troubleshooting User ID and Password Issues, page 3-15
- Troubleshooting License Issues, page 3-17
- Troubleshooting Policy Engine Issues, page 3-23

Troubleshooting Cisco IPICS Installation Issues

For information about troubleshooting problems that you may experience when you install Cisco IPICS, see the “Troubleshooting Cisco IPICS Installation Issues” chapter in the Cisco IPICS Installation document for your Cisco IPICS release.

Troubleshooting Cisco IPICS Administration Console Issues

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

This section includes the following topics:

- Resolving Intermittent Browser Problems, page 3-2
- Resolving Failures to Access the Server With an Administration Console Browser Session, page 3-3
- Resolving LDAP Import Issues, page 3-6
- Resolving “unexpected inconstancy” Message on Cisco IPIC Server Console Screen, page 3-6
- Troubleshooting Browser Timeout Issues When You Configure an RMS with Twelve or More Loopback Interfaces, page 3-6
- Cisco IPICS Displays “Server Initializing” for More than 1 Hour, page 3-8
- Performing Database Procedures To Resolve Login Problems and Failure To Complete Tasks in the Administration Console, page 3-8
- VTG Activates Without Dispatcher Action, page 3-9
Resolving Intermittent Browser Problems

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

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

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

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

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

- To ensure that a current browser window displays the most current information, refresh it by clicking the button or tab that you used to display it. Cisco IPICS does not support the use of the browser Refresh button to refresh a window in the Administration Console.

- The Cisco IPICS Administration Console uses browser pop-up windows for certain functionality. If you have any browser pop-up blocker software installed on your machine, you may be prevented from performing certain actions. To ensure that you are not blocked from performing administration tasks, disable any pop-up blocker software that is installed on your machine before you use the Administration Console.
Cisco IPICS does not support accessing the Administration Console in more than one browser session at the same time on the same machine. If you use multiple browser sessions to access the Administration Console, you may experience unexpected results. To ensure proper server operational behavior, do not open more than one browser session at a time on the same machine for Administration Console functions.

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

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

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

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

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

To resolve this problem, perform the following procedure:

**Procedure**

**Step 1**  Check for the following items to make sure that the URL that you entered is correct:

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

**Step 2**  If you still cannot access the Administration Console, connect to the Cisco IPICS server by using SSH Secure Shell client software (or similar software) and log in with root user privileges.

**Step 3**  Ensure that the tomcat service is running by entering the following command:

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

**Step 4**  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:

  ```bash
  [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:

  ```bash
  [root]# service ipics_tomcat status
  PID_SEARCH_RESULT=
  Tomcat is not running on the system.
  ```
If you receive output that indicates that the tomcat service is not running, continue with **Step 5**.

**Step 5**
Restart the tomcat service and the policy engine by entering the following command:

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

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

**Step 6**
If the tomcat service does not restart, perform the following actions:

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

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

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

b. If you receive a message that is similar to the following message, the tomcat cron file already exists. Skip to **Step 10**.

```
[root]# crontab -l -u ipicsadmin
#--------------------------------------------------------------
#  Module: ipicsadmin.cron - Cisco IPICS cron file for user 'ipicsadmin'
#---------------------------------------------------------------
SHELL=/bin/sh
MAILTO=root
HOME=/opt/cisco/ipics/tomcat
*/ * * * * /opt/cisco/ipics/bin/check_tomcat >>
/opt/cisco/ipics/tomcat/current/logs/ipicsadmin_cron.log 2>&1
```

c. If you receive a message such as **no crontab for ipicsadmin**, continue to **Step 7**.

**Step 7**
Install the crontab file by entering the following command:

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

Cisco IPICS installs the crontab file.

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

For information about checking the status of the tomcat service, see the “Performing Tomcat Service Procedures” section on page 2-1.

**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 network connectivity, enter the following command:

```
ping default gateway IP address
```

where:

- `default gateway IP address` represents the default gateway address for your network.

**Step 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 your server product documentation 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**

Check the security settings on the PC that you use to access the Administration Console.

**Step 15**

Take these actions to change your browser security settings to remove unsecure ciphers from the server.xml file:

1. Connect to the Cisco IPICS server by using SSH Secure Shell client software (or similar software) and log in with root user privileges.
3. Edit the `/opt/cisco/ipics/tomcat/versions/6.0.44/conf/server.xml` and replace the line the begins with `ciphers=` with the following line:
   ```plaintext
   ciphers="TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_3DES_EDE_CBC_SHA"
   ```
4. Save the server.xml file.
5. Enter the following command to restart the Cisco IPICS server
   ```
   [root]# service ipics restart
   ```
   **Note**
   Cisco IPICS cancels any active dial-in or dial-out calls when you enter the `service ipics restart` command.
6. Restart your browser.

**Step 16**

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

```
https://address
```
where:

\textit{address} is the IP address or host name of the server.

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

**Resolving LDAP Import Issues**

\textbf{Problem} When using Active Directory (LDAP), Active Directory users are not imported to Cisco IPICS.


**Resolving “unexpected inconstancy” Message on Cisco IPIC Server Console Screen**

\textbf{Problem} The Cisco IPICS server Console screen displays the following message:

\texttt{unexpected inconsistency; run fsck manually}

\textbf{Solution} Perform the following procedure to remove files that have errors and reindex files:

\textbf{Procedure}

\begin{itemize}
  \item \textbf{Step 1} Connect to the Cisco IPICS server by using SSH Secure Shell client software (or similar software) and log in with root user privileges.
  \item \textbf{Step 2} Enter the following command to enter single user mode:
    
    \texttt{[root]\# \texttt{init 1}}
  \item \textbf{Step 3} Enter the following command:
    
    \texttt{[root]\# \texttt{fsck}}
  \item \textbf{Step 4} Answer \texttt{yes} to each file cleanup question.
  \item \textbf{Step 5} Enter the following command:
    
    \texttt{[root]\# \texttt{shutdown -r now}}
\end{itemize}

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

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

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

For more information about how to back up, restore, and modify the registry, access the Microsoft Support site 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**

1. On the PC that you use to access the Administration Console, choose **Start > Run**.
2. In the Open dialog box, enter `regedit`.
   The Registry Editor displays.
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.
4. Click the `+` signs that display next to each of the folder names to navigate to the `Software\Microsoft\Windows\CurrentVersion\` folder.
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`.
6. In the Internet Settings folder, look for the `ReceiveTimeout` name.
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.
8. Click the **Decimal** radio button to display this value in decimal format.
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.
10. Click **OK** to save your change.
11. To exit the Registry Editor, choose **Registry > Exit**.
12. Restart your PC for the change to become effective.
Cisco IPICS Displays “Server Initializing” for More than 1 Hour

**Problem** After installing, restarting, or rebooting Cisco IPICS, you cannot log in to the Administration Console and you see the following message, which persists for more than 1 hour:

Cisco IPICS is now initializing. You will not be able to access the server until this operation has been completed

**Solution** Restart the Node Manager.

**Caution**

If you are configuring high availability (HA), be aware it usually takes 20 to 30 minutes for the primary Cisco IPICS server to replicate its data to the secondary Cisco IPICS server. If the primary server has been deployed for a long time before configuring HA, this initial data synchronization can take longer. The Cisco IPICS server allows you to log in only after this initial synchronization completes.

**Procedure**

**Step 1** Connect to the Cisco IPICS server by using SSH Secure Shell client software (or similar software) and log in with root user privileges.

**Step 2** Enter the following command:

```
[root]# service ipics_nm restart
```

**Step 3** Wait for about 2 minutes, then try to log in to the IPICS Administration Console.

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

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

**Solution** You may encounter this problem under the following conditions:

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

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

To troubleshoot this issue, perform the following procedure:

**Procedure**

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

- a. Connect to the Cisco IPICS server by using SSH Secure Shell client software (or similar software) and log in with root user privileges.
- b. Check to see if the database is running by entering the following command:
Troubleshooting Cisco IPICS Administration Console Issues

[3-9]

Chapter 3  Troubleshooting the Cisco IPICS Server

Troubleshooting Cisco IPICS Administration Console Issues

VTG Activates Without Dispatcher Action

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

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

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

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

Troubleshooting VTG Activation Problems

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

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

**Procedure**

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

**Step 2** Locate the policy that you activated.

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

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

**Step 5** If the status displays as Failed, click **Details** in the Message field.

The Message popup window displays with detailed information about the activation failure.

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

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

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

VTG Does Not Appear on User IDC

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

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

Check the *User Management > Users* window for users that have multiple user IDs and delete the extra IDs.
Troubleshooting an Ops View Save Failure

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

Cisco IPICS could not save ops view opsview name

where:

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

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

**Procedure**

**Step 1**  Log in to the Cisco IPICS Administration Console by using the ipics user ID.

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

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

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

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

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

---

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

**Step 7**  Search for the word “ERROR” in the ipics.log file.

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

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

**Step 8**  Take these actions to check whether the database is running:

a. Connect to the Cisco IPICS server by using SSH Secure Shell client software (or similar software) and log in with root user privileges.

b. Enter the following command:

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

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

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

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

If you determine that the database is not running, proceed to **Step 10**.

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

```
IBM Informix Dynamic Server Version 10.00.UC1 -- On-Line -- Up 00:16:14 -- 124036 Kbytes
```
If you determine that the database is running, contact your Cisco technical support representative for assistance.

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

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

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

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

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

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

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

---

### Resolving Administration Console Undefined Errors

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

**Solution** This problem occurs when the browser JavaScript engine cannot process advanced dynamic features because of installation of third party software or other setup issues. You can resolve this problem by reinstalling the JavaScript engine. To download the installation script to your PC, go to [http://www.microsoft.com](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 IDC.

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

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

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

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

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

To choose a new font for Internet Explorer, perform the following procedure:
Troubleshooting Cisco IPICS Administration Console Issues

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.

IDC Users Receive Error Messages During Login After a Database Restore Operation

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

**Solution**  This problem may occur if the tomcat service does not restart after the restore procedure has completed or if the IDC 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**  Connect to the Cisco IPICS server by using SSH Secure Shell client software (or similar software) and log in with root user privileges.

**Step 2**  Check to determine if the tomcat service is running by entering the following command:

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

**Step 3**  Perform one of the following actions, depending on the output that you receive:

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

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

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

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

  ```
  [root]# service ipics_tomcat status
  PID_SEARCH_RESULT=
  Tomcat is not running on the system.
  ```
If you receive output that indicates that the tomcat service is not running, restart the tomcat service and the policy engine by entering the following command:

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

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

### Step 4
If you continue to experience problems, contact your Cisco technical support representative for assistance.

---

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

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

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

---

**Recovering a Deleted System Administrator User**

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

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

### Note
You must be assigned the operator role and have an operator user ID and password to recover a deleted system administrator user. For more information about operators, see the “Performing Cisco IPICS Operator Tasks” chapter in *Cisco IPICS Server Administration Guide* for your Cisco IPICS release.

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

**Procedure**

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

**Troubleshooting Reporter Issues**

If you experience issues with the Cisco IPICS reporter, make sure that the reporting feature is properly set up and configured. For more information, see the “Managing Reporting” section in the “Performing Cisco IPICS System Administrator Tasks” chapter in *Cisco IPICS Server Administration Guide* for your release.

The reporter includes an Update feature, which fixes various communication issues and updates the report collector with the latest configuration from the Cisco IPICS server. For more information, see the “Repairing the Report Collector or Viewing Status Information” in the “Performing Cisco IPICS System Administrator Tasks” chapter in *Cisco IPICS Server Administration Guide* for your release.

**Resolving Security Certificate Issues**

**Problem** Certificate expired.

**Solution** See the “Generating SSL Certificates” appendix in *Cisco IPICS Server Administration Guide* for your Cisco IPICS release.

**Problem** Security or trust issue prevents a user from logging in to Cisco IPICS.

**Solution** Make sure that the Cisco IPICS server time and date are correct. If you are using an NTP server in your deployment, make sure that the Cisco IPICS server is properly synced with the NTP server.

**Troubleshooting User ID and Password Issues**

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

This section includes the following topics:

- Resetting a Forgotten or Missing ipics User Password, page 3-15
- Resetting the Password for the ipicsadmin or informix User ID, page 3-16
- Changing the root User Password, page 3-16
- Resetting a Locked or Disabled User Account, page 3-17

**Resetting a Forgotten or Missing ipics User Password**

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

**Solution** You entered an incorrect password for the ipics user. If you have root user access, you can reset the ipics user password and regain access to the Administration Console by entering the `reset_pw` command.
To reset the ipics user ID and resolve this problem, perform the procedure that is documented in the “Resetting, Changing, or Creating a Password With the reset_pw Tool” section on page 6-4.

### Resetting the Password for the ipicsadmin or informix User ID

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

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

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

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

**Procedure**

**Step 1** Connect to the Cisco IPICS server by using SSH Secure Shell client software (or similar software) and log in with root user privileges.

**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:
  ```bash
  [root]# su - ipicsadmin
  ```
- To log in as the informix user, enter the following command:
  ```bash
  [root]# su - informix
  ```

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

To reset the password for the ipicsadmin or informix user, perform the procedure that is documented in the “Resetting, Changing, or Creating a Password With the reset_pw Tool” section on page 6-4.

### Changing the root User Password

**Problem** You need to change the root user password.

**Solution** You can change the password for the root user ID, as needed, by performing the procedure that is documented in the “Resetting, Changing, or Creating a Password With the reset_pw Tool” section on page 6-4.
Resetting a Locked or Disabled User Account

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

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

- The number of invalid login attempts exceeded the number of maximum attempts and Cisco IPICS automatically locked the user. For more information, see the “Performing Cisco IPICS System Administrator Tasks” chapter in *Cisco IPICS Server Administration Guide* for your Cisco IPICS release.

- A user with Operator or All privileges manually locked or disabled the user. For more information about locking out or disabling a user, see the “Performing Cisco IPICS Operator Tasks” chapter in *Cisco IPICS Server Administration Guide* for your Cisco IPICS release.

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

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

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

- If you have access to the root user ID, perform the procedure that is documented in “Unlocking or Enabling a Locked or Disabled User With the enableuser Tool” section on page 6-2 to unlock or enable the user with CLI commands.

- If you are able to access the Administration Console with a user ID that has Operator or All privileges, perform one of the following actions to unlock or enable a user account; then, proceed to verify your configuration changes:
  - To unlock a user account in the Administration Console, follow the procedure in the “Locking or Unlocking a User Account” section in the “Performing Cisco IPICS Operator Tasks” chapter in *Cisco IPICS Server Administration Guide* for your Cisco IPICS release.

- To enable a user account in the Administration Console, follow the procedure in the “Changing User Status” section in the “Performing Cisco IPICS Operator Tasks” chapter in *Cisco IPICS Server Administration Guide* for your Cisco IPICS release.

Troubleshooting License Issues

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

- Resolving Invalid Base Server License Messages that Display After You Upload the License File, page 3-18
- After Uploading Multiple License Files, All Features Do Not Display in the Administration Console, page 3-20
- After Changing the Server IP Address, You Experience Host Name Mismatch or Problems Installing the License, page 3-21
- Changing System Date Invalidates Time-Bound License, page 3-21
- Suppressing Server Expiration Messages After Installing a More Recent Time-Bound License, page 3-22
Resolving Invalid Base Server License Messages that Display After You Upload the License File

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

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

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

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

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

Note  You can encounter license issues if you change the IP address of the server using an unsupported method. To change the server IP address, use the modify_ip command by following the procedure that is documented in the “Modifying Network Settings with the network_config Tool” section on page 6-3. Using other methods to change the server IP address can cause host mismatch problems and invalidate the license.

To resolve these conditions, perform the following procedure:

Procedure

Step 1  To determine that you have a valid license, check the following items:

- Make sure that the MAC address for the license file matches the MAC address of the eth0 interface of the Cisco IPICS server. To locate the hardware MAC address for the eth0 interface, connect to the Cisco IPICS server by using SSH Secure Shell client software (or similar software) and log in with root user privileges, then enter the following command and note the information that displays in the HWaddr field in the command output:

  [root]# ifconfig eth0

- Make sure that the license file has a file extension of .lic.
- Make sure that there are no spaces or special characters in the name of the license file.

Step 2  If you determine that your license file is invalid or misnamed, purchase a valid license file or obtain a new copy of your existing file. For more information, contact your Cisco representative.

Step 3  From the Administration Console, navigate to the Administration > License Management window; then, click the Apply button to restart the license manager.

Step 4  If the server continues to display the invalid license message, connect to the Cisco IPICS server by using SSH Secure Shell client software (or similar software) and log in with root user privileges.

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

  [root]# service ipics_lm status
Step 6 Perform the following action, depending on the message that Cisco IPICS displays:

- If the following message displays, the license manager is not running. Continue with Step 7.
  
ipics_lm is not running.

- If the following message displays, the license manager is running. Proceed to Step 10.
  
ipics_lm is running (PID 24856).

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

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

[root]# service ipics_lm restart

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

[root]# service ipics_lm status

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

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

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

a. Connect to the Cisco IPICS server by using SSH Secure Shell client software (or similar software) and log in with root user privileges.

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

[root]# cd /root/tomcat/current/webapps/license

c. Remove all of the license files that are in the /root/tomcat/current/webapps/license directory by entering the following command:

[root]# rm *.lic

d. Enter yes when the system prompts you to confirm the deletion of each license file.

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

e. Upload the license file(s) by following the procedure in the “Uploading the Cisco IPICS License Files” section in the “Installing Cisco IPICS” chapter in the Cisco IPICS installation document for your Cisco IPICS release.

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

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

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

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

where:
**output-file-name.log** is the name that you designate for the log file, and **tar-file-name.tar** is the name that you designate for the .tar file.

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

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

---

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

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

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

**Procedure**

**Step 1** Connect to the Cisco IPICS server by using SSH Secure Shell client software (or similar software) and log in with root user privileges.

**Step 2** To navigate to the directory that includes the license files, enter the following command:

```
[root]# cd tomcat/current/webapps/license
```

**Step 3** Remove all of the license files that are in the `tomcat/current/webapps/license` directory by entering the following command:

```
[root]# rm *.lic
```

**Step 4** Enter yes when the system prompts you to confirm the deletion of each license file.

**Note** Do not remove any other files in this directory.

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

**Step 6** Upload the license file(s) by following the procedure that is documented in the “Uploading the Cisco IPICS License Files” section in the “Installing Cisco IPICS” chapter in the Cisco IPICS installation document for your Cisco IPICS release.

**Note** Make sure that each license file has the correct MAC address.
After Changing the Server IP Address, You Experience Host Name Mismatch or Problems Installing the License

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

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

**Solution** Some methods of changing the IP address do not update the /etc/hosts file, which can cause host mismatch or other IP connectivity problems. To ensure that Cisco IPICS properly processes any IP address changes, use only the `network_config` tool to change the IP address by following the procedure that is documented in the “Modifying Network Settings with the network_config Tool” section on page 6-3.

Changing System Date Invalidates Time-Bound License

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

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

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

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

**Procedure**

**Step 1** Connect to the Cisco IPICS server by using SSH Secure Shell client software (or similar software) and log in with root user privileges.

**Step 2** Change the system date to a date that is after the system start date by entering the following command:

```
[root]# date mmddyyyy
```

where:

`mmddyyyy` is the current date.

**Step 3** Restart the license manager by entering the following command:

```
[root]# service ipics_lm restart
```
Suppressing Server Expiration Messages After Installing a More Recent Time-Bound License

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

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

**Procedure**

1. **Step 1**  Connect to the Cisco IPICS server by using SSH Secure Shell client software (or similar software) and log in with root user privileges.
2. **Step 2**  Navigate to the directory where Cisco IPICS stores the license files by entering the following command:
   
   ```
   [root]# cd tomcat/current/webapps/license
   ```
3. **Step 3**  View the license files by entering the following command:
   
   ```
   [root]# ls -l *.lic
   ```
   The license files display with the time and date that the license was last modified.
4. **Step 4**  Make a note of the licenses that you no longer need.
   The time and date that displays with the file information might assist you with determining which files you need to delete.
5. **Step 5**  Delete the unnecessary license files by entering the following command:
   
   ```
   [root]# rm licensefilename.lic
   ```
   where:
   
   - `licensefilename.lic` is the name of the license file that you want to delete.

   **Caution**  Make sure that you do not delete the cisco.opt file. This file is required for the correct operation of Cisco IPICS.
6. **Step 6**  Repeat Step 5 for each license file that you need to delete.
7. **Step 7**  Restart the server by entering the following command:
   
   ```
   [root]# service ipics restart
   ```
8. **Step 8**  Log in to the Administration Console by using the ipics user ID and navigate to the **Administration > License Management** window.
9. **Step 9**  To apply the license deletions to the system configuration, click **Apply**.
10. **Step 10**  If a message displays that indicates that a license is about to expire, click **Dismiss Warnings**.

---

**Chapter 3  Troubleshooting the Cisco IPICS Server**

**Troubleshooting License Issues**

3-22
Troubleshooting Policy Engine Issues

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

- Uploading a Large Zipped File of Prompts Causes an Error, page 3-23
- IppeAgentImpl ERROR Messages Display in the ipics.log File, page 3-24
- Resolving Communication Problems Between the Policy Engine and the Prompt Manager, page 3-25
- Resolving Reconnection Failures After a Dial-In Caller Uses the Hold or Call Waiting Feature, page 3-25
- Troubleshooting Dial-In Call Connection Failures, page 3-25
- Troubleshooting Dial-Out Invitation Failures, page 3-28
- Troubleshooting Dial-Out Notification Failures, page 3-29
- Troubleshooting Dial-Out Notification Failures Between Users in Different Ops Views, page 3-30
- Understanding a PARTIAL_SERVICE Status For the Dial Engine and Subsystem Manager, page 3-30
- Analyzing a SHUTDOWN Status For the SIP Subsystem, page 3-30

Uploading a Large Zipped File of Prompts Causes an Error

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

The form could not be properly constructed.

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

```java
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.PromptHandler.getPromptList(L215)
    at com.cisco.ipics.ippe.dialengine.promptmanagement.actions.PromptAction.doInit(L444)
    at com.cisco.ipics.ippe.dialengine.promptmanagement.actions.PromptAction.unspecified(L152)
```

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

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

```
```

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

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

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

**Procedure**

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

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

- If the field shows a status of Not Licensed, IppeAgentImpl messages typically display in the logs and require no action.
- If the field shows a status of Licensed, continue with **Step 3**.

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

- **a.**  Connect to the Cisco IPICS server by using SSH Secure Shell client software (or similar software) and log in with root user privileges.

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

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

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

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

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

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

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

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

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

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

Resolving Communication Problems Between the Policy Engine and the Prompt Manager

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

2006-08-18 14:20:56,747 [http-8443-Processor21] ERROR PromptUtil:200 -

Solution This situation indicates that the policy engine processes are not running. To start the policy engine processes, perform the procedure that is documented in the “Manually Starting the Dial Engine” section on page 2:11.

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

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

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

To successfully reconnect with a dial-in call, either add MTP resources to your SIP provider, or configure your SIP provider so that it can allocate MTP resources from another source. For more information about configuring the SIP provider, see the “Configuring the SIP Provider” section in the “Configuring and Managing the Cisco IPICS Policy Engine” chapter in Cisco IPICS Server Administration Guide for your Cisco IPICS release.

Troubleshooting Dial-In Call Connection Failures

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

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

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

To resolve this issue, perform the following procedure:

**Procedure**

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

The Ops Views window displays.

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

a. Click the name of the ops view.

   The **Ops Views > opsviename** window displays.

b. Determine if a dial-in number exists in the ops view configuration by checking the Dial Number field in the General tab.

c. If the Dial Number field is empty, enter the dial-in information in this field.

   For information about adding a dial-in number for an ops view, see the “Performing Ops Views Tasks” section in the “Configuring and Managing Cisco IPICS Operational Views” chapter in *Cisco IPICS Server Administration Guide* for your Cisco IPICS release.

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

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

For information about allocating dial ports for an ops view, see the “Allocating Dial Ports for the Dial-In/Invite and Notification Features” section in the “Configuring and Managing Cisco IPICS Operational Views” chapter in *Cisco IPICS Server Administration Guide* for your Cisco IPICS release.

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

- Dial ports reserved for dial-in/invite feature

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

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

- Add the ports that you removed to the **Dial ports reserved for dial-in/invite feature** field.

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

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

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

For more information about configuring SIP, see the “Configuring SIP” and “Configuring the SIP Provider” sections in the “Configuring and Managing the Cisco IPICS Policy Engine” chapter in *Cisco IPICS Server Administration Guide* for your Cisco IPICS release.
Step 9 Perform the following steps to make sure that the proper SIP configuration has been applied to the RMS:

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

a. Log in to the RMS.
b. Enter the following command in privileged mode to make sure that the `bind control source-interface Loopback0` command is applied to the running configuration of the RMS:
   ```bash
   Router# show running-config | include bind control source-interface
   ```
c. If the `bind control source-interface` command is present in the running configuration, continue to Step 10. If the `bind control source-interface` command is not present in the running configuration, continue to the next step to add the command.
d. Enter the following command, and view the output that displays in the Total call-legs field, to determine if there any active calls on the RMS:
   ```bash
   Router# show call active voice brief
   ```
e. If the Total call-legs field displays zero, continue to Step g. If the field displays a value that is greater than zero, enter voice port configuration mode for the call that is active; then, enter the following command to take the voice port offline and cancel any active voice calls:
   ```bash
   Note The following command takes the voice port out of service. Make sure that you enter this command during a maintenance window or other off-peak hours.
   Router(config-voiceport)# shutdown
   ```
f. Repeat Step e until you have taken all active calls offline.
g. Enter the following command in SIP configuration mode to bind the source address of SIP signaling packets to the IP address of the Loopback0 interface:
   ```bash
   Router(conf-serv-sip)# bind control source-interface Loopback0
   ```
h. To bring the voice ports back online, enter the following command in voice port configuration mode:
   ```bash
   Router(config-voiceport)# no shutdown
   ```
i. To verify that the output reflects the SIP configuration change that you performed in this procedure, enter the following command:
   ```bash
   Router# show running-config | include bind control source-interface
   ```
j. To update your configuration on the RMS, enter the following command:
   ```bash
   Router# copy running-config startup-config
   ```

Note For more information about configuring the RMS, see the “Configuring the Cisco IPICS RMS Component” appendix in *Cisco IPICS Server Administration Guide* for your Cisco IPICS release.
Step 10  If you made any changes to the SIP configuration, you must restart the policy engine and the tomcat service by performing the following procedure:

a. Connect to the Cisco IPICS server by using SSH Secure Shell client software (or similar software) and log in with root user privileges.

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

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

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

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

---

**Troubleshooting Dial-Out Invitation Failures**

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

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

**Procedure**

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


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 in the “Configuring and Managing the Cisco IPICS Policy Engine” chapter in Cisco IPICS Server Administration Guide for your Cisco IPICS release.

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.
Troubleshooting Policy Engine Issues

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

Troubleshooting Dial-Out Notification Failures

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

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

---

**Note**

If you are performing dial-out notifications from one ops view to another, see the “Troubleshooting Dial-Out Notification Failures Between Users in Different Ops Views” section on page 3-30.

**Procedure**

**Step 1** If the notification is a dial-out notification, make sure that you have configured an outbound dial number by completing Step 1 in the “Troubleshooting Dial-Out Invitation Failures” section on page 3-28.

**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 *Cisco IPICS Server Administration Guide* for your Cisco IPICS release.

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

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

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

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

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

b. Perform one of the following actions:

– Add the ports that you removed to the **Dial ports reserved for dial-in/invite feature** field.

– Take no action. Cisco IPICS adds the ports that you removed to the total number of ports that are reserved for dial-in calls, invitations, or notifications.
Troubleshooting Dial-Out Notification Failures Between Users in Different Ops Views

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

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

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

---

**Note**  This policy-to-ops-view association information does not apply to the SYSTEM ops view, to which all users belong. For more information about ops views, see the “Configuring and Managing Cisco IPICS Operational Views” chapter in *Cisco IPICS Server Administration Guide* for your Cisco IPICS release.

Understanding a PARTIAL_SERVICE Status For the Dial Engine and Subsystem Manager

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

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

---

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

Analyzing a SHUTDOWN Status For the SIP Subsystem

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

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

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

**Procedure**

**Step 1**  Check the status of your SIP configuration by navigating to the **Dial Engine > Control Center > Status** window.

If the status of the SIP Subsystem displays SHUTDOWN, continue to **Step 2**.
Step 2  Make sure that you have configured all of the required fields in the **Dial Engine > SIP Configuration** window. For information about how to configure the SIP Subsystem, see the “Configuring the SIP Provider” section in the “Configuring and Managing the Cisco IPICS Policy Engine” chapter in *Cisco IPICS Server Administration Guide* for your Cisco IPICS release.

Step 3  If the status of the SIP Subsystem continues to show a status of SHUTDOWN, restart the policy engine and the tomcat service by performing the following steps:

   a. Connect to the Cisco IPICS server by using SSH Secure Shell client software (or similar software) and log in with root user privileges.

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

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

   ___Note___

   You must restart the ipics service after you make any changes to the SIP subsystem configuration.

Step 4  If the SIP Subsystem continues to show a status of SHUTDOWN, contact your Cisco technical support representative for assistance.
CHAPTER 4

Troubleshooting Communication, Voice Quality and Other Equipment Issues

This chapter describes how to resolve communication and voice quality issues and hardware, firmware, and software issues that you might encounter with equipment in a Cisco IPICS deployment.

This chapter includes the following sections:

- Troubleshooting Communication Issues, page 4-1
- Troubleshooting Voice Quality Issues, page 4-5
- Troubleshooting Equipment Issues, page 4-7
- Troubleshooting RMS Configuration Issues, page 4-9

Troubleshooting Communication Issues

This following sections provide information about communications issues that you may encounter and how to troubleshoot them:

- Analyzing Communications Problems Between All Locations on a Channel, page 4-2
- Troubleshooting Communication Failures Between VTG Participants, page 4-2
- Resolving Communications Problems For Newly-Added IDC Users on a Channel, page 4-2
- Removing a Logged-Out IDC User from the Active Users List, page 4-3
- IDC Users Can Listen to Channels But Cannot Listen to VTGs, page 4-3
- Configuring the RMS to Eliminate Automatic Channel Deactivation for SIP-Based Remote Connections, page 4-4
- Eliminating Feedback Noise on VTG, page 4-4
- Understanding Communication Problems Between Cisco IPICS End Point Devices and Radios that Require a Guard Tone, page 4-4
Analyzing Communications Problems Between All Locations on a Channel

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

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

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


Troubleshooting Communication Failures Between VTG Participants

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

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

For more information about configuring the router, see the “Configuring the Cisco IPICS RMS Component” appendix in *Cisco IPICS Server Administration Guide* for your Cisco IPICS release. For more information about multicast troubleshooting, see *IP Multicast Troubleshooting Guide* at the following URL:


Resolving Communications Problems For Newly-Added IDC Users on a Channel

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

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

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

Removing a Logged-Out IDC User from the Active Users List

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

**Solution** The server did not receive a logout command from the IDC. This situation may occur if the IDC experienced a network connectivity disruption while the IDC 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 > IDC window. The IDC Users pane displays the list of active IDC users.

**Step 2** Locate the user ID of the logged-out IDC user.

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

**Step 4** Click *Logout*. The IDC 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.

---

**IDC Users Can Listen to Channels But Cannot Listen to VTGs**

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

**Solution** In Cisco IPICS, an RMS provides support for only one Cisco IPICS location (a Cisco IPICS location is defined as a multicast domain). All of the locations and routers that are configured in the Cisco IPICS system must be able to communicate by using the multicast addresses that have been defined in the global multicast address pool. All addresses in the multicast pool must be able to reach any RMS, IDC, 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, IDC clients, and Cisco Unified IP Phones.
- Deactivate any RMS components that cannot participate in the global multicast address pool. To deactivate an RMS component, navigate to the Configuration > RMS window in the Administration Console. Click the RMS that you need to deactivate; then, from the General tab, click *Deactivate*.
Configuring the RMS to Eliminate Automatic Channel Deactivation for SIP-Based Remote Connections

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

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

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

```
Router(config)# ip rtcp report interval 5001
Router(config)# gateway
Router(config-gateway)# media-inactivity-criteria all
Router(config-gateway)# timer receive-rtcp 5
```

For more information about the correct router configuration for Cisco IPICS, see the “Configuring the Cisco IPICS RMS Component” appendix in *Cisco IPICS Server Administration Guide* for your Cisco IPICS release.

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

Eliminating Feedback Noise on VTG

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

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

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

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

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

If the radio requires an LLGT but the LLGT is not statically configured on the LMR gateway, the audio that an IP phone or dial-in/dial-out user sends does not transmit to radio users. In this case, only the IDC, dial-in/dial-out, and other IP phone users can hear the transmission.
If the radio does not require an LLGT, transmissions flow as they would over a channel that does not have an associated radio connection. In this case, all end-users hear the IP phone or dial-in/dial-out user transmissions.

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

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

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

For additional information about LMRs, see the following documentation:

- “Cisco IPICS LMR Gateway Configurations” chapter in *Solution Reference Network Design (SRND) for Cisco IPICS, Release 4.10(2)*
- “Introducing Cisco IPICS” chapter in *Cisco IPICS Server Administration Guide* for your Cisco IPICS release

### Troubleshooting Voice Quality Issues

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

- **Voice Quality Degrades for IDC**, page 4-5
- **Troubleshooting Poor IDC Voice Quality**, page 4-6
- **Dial Engine Calls Experience Degraded Voice Quality**, page 4-6
- **Resolving Interruption of Voice Communications When You Use VTGs and SIP-Connected IDC Client Machines**, page 4-6
- **Resolving LMR Voice Issues**, page 4-7

### Voice Quality Degrades for IDC

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

**Solution** The IDC 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 IDC client machine. For additional details and information about how to install the Microsoft QoS Packet Scheduler, visit the Microsoft website and search for QoS Packet Scheduler.
Troubleshooting Poor IDC Voice Quality

**Problem** Voice quality for IDC users is very poor and some IDC 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 Communications Manager, or it can be performed in the Cisco IOS SIP gateway with sufficient DSP resources.

For detailed information about configuring a transcoder in Cisco Unified Communications Manager, release 5.1(2b), see your Cisco Unified Communications Manager documentation.

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

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

**Problem** Voice communications are interrupted when you use VTGs and SIP-connected IDC client machines. Symptoms may include one-way audio transmission, no voice transmission, dropped connections, and poor audio quality. The `debug vpm signaling` command returns unexpected results (regarding M-lead to E-lead mapping) for voice ports that connect VTGs via T1 loopback ports.

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

```plaintext
2005-11-10 19:25:42,981 [pool-4-thread-1] ERROR IOSRMSCommunicator:433 - 10.32.65.127 getControllers() T1 is missing a required command: 'cablelength short 133ft'
2005-11-10 19:25:42,981 [pool-4-thread-1] ERROR IOSRMSCommunicator:437 - 10.32.65.127 getControllers() T1 controller 1/0/1 UNUSABLE. (Found 24 voice ports)
```
Solution  Cisco IPICS requires that the `cablelength short` command be configured on all T1 controllers. This command allows you to set a cable length of 133 feet or less for a T1 link on the router. For detailed RMS configuration information, see the “Configuring the Cisco IPICS RMS Component” appendix in Cisco IPICS Server Administration Guide for your Cisco IPICS release.

Resolving LMR Voice Issues

For information about LMR voice issues, see Cisco Land Mobile Radio over IP Solution Reference Network Design, which is available at the following URL:


Troubleshooting Equipment Issues

The following sections provide troubleshooting information for problems that you may encounter with the Cisco IPICS hardware. For issues that relate to communication difficulties, see the “Troubleshooting Communication Issues” section on page 4-1.

- No Power to Cisco Unified IP Phones, page 4-7
- Analyzing One-Way Audio Issues Between IDC Client Machines and Cisco Unified IP Phones, page 4-8
- Resolving One-Way Audio Problems on the Cisco Unified IP Phone That Occurs After You Receive or Place a Call, page 4-8
- Cisco Unified IP Phone Cannot Access the Cisco IPICS Service After Changing the Server IP Address, page 4-8
- Resolving Interconnectivity Problems With Cisco Unified Wireless IP Phone 7920, page 4-9
- Resolving Cisco Trunked Radio VTG Issues, page 4-9

No Power to Cisco Unified IP Phones

Problem  Cisco Unified IP Phones are not receiving power.

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

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

Note  For information about the firmware that Cisco IPICS supports for use with Cisco Unified IP Phones, see Cisco IPICS Compatibility Matrix.

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

```
[router] # show power
```

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

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

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

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

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

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

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

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

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

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

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

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

• If the “HTTP error 404” message or a blank prompt displays, the server IP address may not have been updated in Cisco Unified Communications Manager or Cisco Unified Communications Manager Express, and the Cisco IPICS service might be configured with an incorrect server IP address.
Resolving Interconnectivity Problems With Cisco Unified Wireless IP Phone 7920

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

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

Resolving Cisco Trunked Radio VTG Issues

Problem  When a trunked radio is in a VTG with other radios (trunked or non-trunked), a trunked radio plays a beep or bonk tone when you press the PTT button, which is heard on other radios and causes unexpected actions.

Solution  See the “Trunked Radio Optional Workaround” section in Solution Network Design (SRND) for Cisco IPICS, Release 4.0(2).

Troubleshooting RMS Configuration Issues

The following sections describe problems you may encounter with the RMS configuration:

- Server Reboots Slowly Following RMS Configuration, page 4-10
- You Attempt to Deactivate an RMS but its Status Does Not Change, page 4-10
- VTG Activation Slow or RMS in Unreachable State After RMS Command Prompt Changed, page 4-11
- RMS Fails or Remains in Unreachable State, page 4-11
- Newly-Added RMS Does Not Display Loopbacks, page 4-12
Server Reboots Slowly Following RMS Configuration

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

**Solution**  During a server reboot, the server sends commands to the RMS to verify that the RMS components and DS0s are operational. The server also checks for any changed configuration in the RMS. If a user adds many DS0s to the RMS, the server has to send numerous commands to the RMS after a reboot; for example, if a user adds 96 DS0s, the server sends between 800 and 1400 commands to the RMS. With higher performance routers, such as the Cisco 3900 series routers, the process of sending and receiving commands may take 10 to 20 seconds. With lower performance routers, such as the Cisco 2900 series routers, this process may take one to two minutes (60 to 120 seconds).

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

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

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

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

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

**Procedure**

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

**Step 2**  In the Virtual Talk Groups window, read the Status column to check the status of your VTGs. The status of this column displays as inactive or active.

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

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 supports only the default prompts.

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

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

RMS Fails or Remains in Unreachable State

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

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

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

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

```
Router# show users
```

To clear a VTY line, enter the following command:

```
Router# clear line line-number
```

where:
Newly-Added RMS Does Not Display Loopbacks

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

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

Router Remains in Unreachable State

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

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

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

To resolve the problem, perform the following procedure:

**Procedure**

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

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

**Step 3**  Delete the router configuration from the server by clicking **Delete**. Cisco IPICS removes the router from the system.

**Step 4**  Re-add the router to the configuration by following the procedure in the “Adding an RMS” section in the “Performing Cisco IPICS System Administrator Tasks” chapter in *Cisco IPICS Server Administration Guide* for your Cisco IPICS release.

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

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

**Solution**  Because the Cisco IPICS server does not recognize gaps in the RMS DS0 group configuration, make sure that you always configure sequential DS0 groups on the T1 controller. When DS0 groups are configured out of sequence, the server does not read the configuration that is defined beyond the last DS0 group number in the list.
See Example 4-1 for an example of misconfigured DS0s. If you configure DS0 groups 0 through 2 and then continue with DS0 group 4, the server will only recognize 3 ports on the RMS because DS0 group 3 is not defined. In this situation, the server does not recognize the T1 ports beyond the last sequential configuration (DS0 group 2):

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

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

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

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

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

**Procedure**

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

For additional details about configuring the RMS, see the “Configuring the Cisco IPICS RMS Component” appendix in *Cisco IPICS Server Administration Guide* for your Cisco IPICS release.

### Router Indicator Lights for the Loopback Are Not Green

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

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

- CD—When this light is green, there are no problems with the loopback
- Alarm Indication (AL)—When this light is red, one of the following problems exist:
Troubleshooting RMS Configuration Issues

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

Voice Loops in VTGs and Router Configuration Shows Incorrect Information

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

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

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

**Tip**

You can change the polling period by entering a new value in the **RMS Polling Frequency** field in the **Options** window in the Administration drawer. For more information, see the “Managing Cisco IPICS Options” section in the “Performing Cisco IPICS System Administrator Tasks” chapter in *Cisco IPICS Server Administration Guide* for your Cisco IPICS release.

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

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

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

Step 3  Choose Update from the Configuration drop down list box to update the configuration.

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

Long Delays Between Pressing the IDC PTT Button and Media Establishment

Problem  Intermittent delays of varying duration may occur from the time that you press the IDC PTT button to the time that the media is established between the remote IDC 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 Cisco IPICS Server Administration Guide for your Cisco IPICS release.
Troubleshooting the IDC and Cisco Instant Connect

This chapter describes how to resolve problems that you may encounter when you use the Cisco IPICS Dispatch Console (IDC), Cisco Instant Connect for Windows, and Cisco Instant Connect for Android devices, and includes the following sections:

- Troubleshooting IDC Issues, page 5-1
- Troubleshooting Cisco Instant Connect Issues, page 5-9

Troubleshooting IDC Issues

The following sections describe how to resolve problems that you may encounter when you use the IDC:

- Resolving IDC Execution Issues, page 5-1
- Generating a IDC Installation Log File, page 5-2
- Using the idcsetup.exe Installer with an Encrypted File System, page 5-3
- Making idcsetup.exe Configuration File Changes, page 5-4
- Resolving IDC Dialer Issues, page 5-4
- Resolving Footswitch/USB Device Issues, page 5-4
- Configuring the Audio Settings, page 5-5
- IDC Coexistence with Other Voice Applications, page 5-6
- Troubleshooting IDC Voice Quality Issues, page 5-6
- Resolving Name Resolution Failures, page 5-8
- Identifying Channel Activation Issues, page 5-8

Resolving IDC Execution Issues

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

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

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

**Procedure**

1. On the client machine, press **Ctrl-Alt-Delete** to launch the Windows Task Manager application.
2. Click **Task Manager**. Three tabs display on Windows Task Manager: Applications, Processes, and Performance. An additional tab, Networking, displays in the Windows XP Task Manager.
3. Click the **Processes** tab.
4. Click **Image Name** to alphabetize the list of running processes. Scroll down through this list to look for the IDC.exe process.
5. Click **IDC.exe** to highlight or right-click **IDC.exe**; then, click **End Process**. A warning message displays to ask if you are sure that you want to terminate this process.
6. Click **Yes**.
7. Close Windows Task Manager by clicking the “X” in the upper right corner.

**Note**

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

Generating a IDC Installation Log File

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

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

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

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

**Procedure**

1. Create a **C:\temp** directory in Windows, if this directory does not already exist.
**Step 2** Use Windows Explorer to navigate to the location where you saved the idcsetup.exe file, as described in the “Downloading the Cisco IPICS Dispatch Console Installation Program from the Cisco IPICS Server” section in the “Installing the Cisco IPICS Dispatch Console” section in the “Cisco IPICS Dispatch Console Installation, Configuration, and Maintenance” chapter in *Cisco IPICS Dispatch Console User Guide* for your release.

**Step 3** Locate the `idcsetup.exe` file in this stored location and click to highlight the file; then, right-click the `idcsetup.exe` file and click **Copy**.

**Step 4** Use Windows Explorer to navigate to the C:\temp directory and right-click in an open area in this directory; then, click **Paste** to copy the `idcsetup.exe` file to the C:\temp directory.

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

**Step 5** Open up a command line prompt (Start > Run > cmd) on the idcsetup.exe client machine to access the C:\temp directory.

**Step 6** To generate the IDC installation log file, enter the following command from the C:\temp directory:

```
idcsetup.exe -log
```

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

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

**Step 7** To close the command line prompt, enter the **exit** command.

**Step 8** After you have created the idcsetup.exe installation log file, contact your Cisco support personnel for further assistance.

---

**Using the idcsetup.exe Installer with an Encrypted File System**

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

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

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

**Procedure**

**Step 1** On the idcsetup.exe client machine, open a command line prompt by choosing **Start > Run** and entering **cmd**.

A command line window displays.

**Step 2** At the command line, enter the following command:

```
C:\> echo %temp%
```
Troubleshooting IDC Issues

The location of the TEMP folder displays.
If the folder that is specified by the %temp% environment variable is encrypted, you can assign the %temp% environment variable to a folder that is not encrypted.

**Step 3**
To reassign the %temp% environment variable to a nonencrypted folder, enter the following command:

```
C:\set TEMP=new location
```

where:

*new location* specifies the new, nonencrypted folder for the %temp% environment variable.
The new location of the TEMP folder displays.

**Step 4**
To reassign the %tmp% environment variable to a nonencrypted folder, enter the following command:

```
C:\set TMP=new location
```

where:

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

**Step 5**
Rerun the idcsetup.exe installation by entering the following command:

```
C:\run idcsetup.exe
```

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

For more information about the Encrypted File System, visit the Microsoft support website.

Making idcsetup.exe Configuration File Changes

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

Resolving IDC Dialer Issues

**Problem**  All IDC Dialers show “Unregistered.”

**Solution**  Make sure that the host name of the IP address of Cisco Unified Communications Manager or Cisco Unified Communications Manager Express is properly configured in Cisco IPICS. To do so, in the Administration Console, choose **Server** drawer > **Administration** > **Options** and enter the IP address in the CUCM Host Name or IP Address field.

Resolving Footswitch/USB Device Issues

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

If you use a footswitch or similar USB device, and you encounter a situation where the All Talk channel button flickers between orange and yellow, you may not have properly configured the device.
Make sure that the device can generate key down events when you hold down the footswitch pedal followed by a key up event when you release the pedal (to simulate pressing and holding a key on a keyboard and then releasing it).

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

### Configuring the Audio Settings

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

- Using a USB DSP Headset with the IDC, page 5-5
- Checking the Microphone with the IDC, page 5-6

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

<table>
<thead>
<tr>
<th>Tip</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you change your audio settings while you are running the IDC, you may need to restart the IDC for the changes to become effective.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>It is very important that you choose the preferred or default sound device option in the Windows audio settings in order to limit echo that can be caused by multiple microphones picking up traffic on the same machine.</td>
</tr>
</tbody>
</table>

### Using a USB DSP Headset with the IDC

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

If you launch the IDC after you plug the headset into your IDC client machine, the IDC does not automatically remember the audio setting for the USB DSP headset; instead, the IDC reverts to the Windows operating system’s default audio settings. For more information about checking and reconfiguring the Windows audio settings for use with a USB DSP headset, see the “Using a USB DSP Headset with the Cisco IPICS Dispatch Console” section in the “Cisco IPICS Dispatch Console Installation, Configuration, and Maintenance” chapter in *Cisco IPICS Dispatch Console User Guide* for your Cisco IPICS release.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you use the microphone on a USB headset for an extended period of time, your voice may become unintelligible. If this problem occurs, close the IDC and unplug the USB headset from the IDC client machine. Then, plug the USB headset back into the IDC client machine and restart the IDC.</td>
</tr>
</tbody>
</table>
Checking the Microphone with the IDC

You should also check the audio recording and playback capability of the microphone on your IDC client machine by accessing the Microsoft Sound Recorder to record your voice and then listen to the recording. (Make sure that you have an audio input device connected to your machine.)

- Make sure that you use a high-quality microphone with the IDC; otherwise, the Cisco IPICS system may not be able to accurately detect your voice and properly register transmit and/or receive traffic.

- If the Cisco IPICS system cannot detect your voice when you transmit, the system may squelch the transmission; in this situation, another Cisco IPICS user may start speaking over your transmission because your voice cannot be heard and the IDC receive indicator may not display any indication of the transmission.

Note

Be aware that if the microphone on the IDC client machine is busy or if it cannot be opened by the IDC for other reasons, you will be able to listen to active conversations but you will not be able to talk.

For related information about the audio setting configuration and sound recording capability, see the “Optimizing Audio for the Cisco IPICS Dispatch Console” section, the “Using a USB DSP Headset with the Cisco IPICS Dispatch Console” section, and the “Installing the Cisco IPICS Dispatch Console” section in the “Cisco IPICS Dispatch Console Installation, Configuration, and Maintenance” chapter in Cisco IPICS Dispatch Console User Guide for your Cisco IPICS release.

IDC Coexistence with Other Voice Applications

The capability for the IDC application to coexist with other voice applications depends on the operating system that you use.

For example, Microsoft Windows 7 allows multiple applications to run concurrently and open and use the microphone at the same time. Some operating systems, however, do not provide support for this same capability; that is, only one voice application, such as the IDC or another voice application, may be active at the same time on a IDC client machine.

For instance, if you try to open the IDC application while you are running Microsoft NetMeeting conferencing software, the IDC displays an error because it cannot access the media device. In this case, you must first close the NetMeeting application and then launch the IDC. You can then restart NetMeeting.

Troubleshooting IDC Voice Quality Issues

You may encounter voice quality issues, which can arise due to several factors, such as noise and voice distortion.

For detailed information about voice quality problems and symptoms, see Recognizing and Categorizing Symptoms of Voice Quality Problems, which can be found at the following URL:


This document categorizes and defines voice quality problem symptoms and may aid your troubleshooting efforts by helping you to identify specific problems through the use of sample sound recordings.
Troubleshooting Multicast Communications Issues

Certain IDC client machines that are running the Windows XP operating system may not be able to send multicast communications because of an issue with the operating system; in these situations, IDC multicast users may experience one-way audio where they can hear, but they may not be heard by, other Cisco IPICS users.

Tip

To ensure identification of this specific problem, please check to make sure that the microphone mute options on the headset and in the Windows operating system are not enabled. For more information about using the microphone with the IDC, see the “Using a Microphone with the Cisco IPICS Dispatch Console” section in the “Cisco IPICS Dispatch Console Installation, Configuration, and Maintenance” chapter in Cisco IPICS Dispatch Console User Guide for your Cisco IPICS release.

This problem with multicast communications may be caused by the network component of the operating system being unable to transmit multicast traffic. Cisco IPICS IDC users who encounter this problem should connect to Cisco IPICS over a unicast connection by choosing the remote location from the location selection dialog box. (By choosing the remote location, Cisco IPICS uses SIP-based connectivity for all channels on the IDC.)

To positively identify this problem, use a network packet sniffer as described below:

1. Run the sniffer on the affected IDC client machine and filter for outgoing multicast UDP packets.
2. Then, launch the IDC application and click the PTT channel button on one of the channels and speak into the microphone or headset. (The channel highlights and changes color to indicate that you are transmitting traffic.)
3. Observe the sniffer; you will see that no multicast UDP packets are sent from the IDC client machine.

To fully resolve this problem, you must perform a fresh installation of the Windows XP operating system on the IDC client machine.

Troubleshooting Offline Mode Issues

Cisco IPICS allows the IDC to operate in offline mode when the connection to the server has been interrupted so that you can continue to communicate during periods of server downtime.

There are several situations that may cause the IDC to enter offline mode, such as, the inability of the IDC to communicate with the server, networking issues that prevent routing from the IDC client machine to the server, and IE browser settings that cause your PC to work in offline mode.

If you encounter a situation where Cisco IPICS returns a message that states that the IDC is in offline mode while the connection to the server is online, check to make sure that your IE browser is not operating in offline mode. To check this setting, choose File from the IE browser window. Scroll down to the Work Offline option and make sure that a check mark does not appear next to this option. (If a check mark does not appear next to this option, then it is disabled.)

If a check mark appears next to this option, click Work Offline to remove the check mark and disable offline mode.

Note

Be sure that the “Work Offline” option in your IE browser settings is not enabled on your IDC client machine. If this option is enabled, you must disable it; otherwise, you may not be able to connect to the server.
Resolving Name Resolution Failures

Cisco IPICS requires IP name resolution. An incorrect Domain Name Service (DNS) IP configuration could result in a service outage.

To resolve name resolution failures, consult with your system administrator to confirm IP name resolution within the entire network, which includes local device IP configurations, network-based name resolution systems (such as DNS), and DHCP systems.

Identifying Channel Activation Issues

When you click the *Activate* button on the IDC, the system enters the activating state; that is, the Activate button highlights and the system attempts to connect to the Cisco IPICS server.

- When you click the Activate button immediately after a SIP-based (unicast) channel becomes available on the IDC, you may hear a busy tone if the RMS has not completely configured the line.
  - If you encounter this situation, click the *Activate* button to deactivate the channel; then, wait a few seconds and click *Activate* again to reactivate the channel.

After the connection has been established, the remaining IDC buttons, including the PTT channel button, highlight to indicate that they are in an active state.

- If your ability to transmit on a channel has been disabled by the server, and/or if the channel has been configured by the server as a listen-only channel, the channel will appear dimmed. If the channel has been disabled by the server, you will not be able to activate the channel, as none of the buttons will appear.

If the remaining IDC buttons do not become active, and if you are using a SIP-based connection, one of the following conditions may be occurring:

- Network connectivity issues that prevent connection to the RMS.
- The RMS may be in an offline or invalid state.
- The RMS may be misconfigured in the server.
- The dial peers may not have been configured or the dial peers and/or the voice ports may be misconfigured in the RMS.
- The RMS may not have yet created the dial peers because of a delay between the server configuration and RMS dial peer creation. In this case, you should wait a couple of minutes and then restart the IDC to try again.

*Note*

When SIP-based remote connections fail, the IDC displays a warning indicator in the form of a yellow triangle next to the channel. This indicator signifies that a problem exists with the remote end (IDC, RMS, or server) and that it may not be able to send or receive traffic. This situation may be caused by a network interruption or reset/restart activity at the remote end. During this period of interruption, the IDC continues to attempt to connect to the remote end. After operations return to normal, the IDC removes the warning indicator from view.

If there is no traffic activity after a 30 minute interval, channels that are activated via a SIP-based remote connection may be deactivated by the system.

The IDC automatically reactivates the connection after 30 seconds. Alternatively, you can reactivate the channel by clicking the *Activate* button on the IDC.
Troubleshooting Cisco Instant Connect Issues

The following sections describe how to resolve problems that you may encounter when you use Cisco Instant Connect for Windows or Cisco Instant Connect for Android Devices:

- Resolving Cisco Instant Connect for Windows Issues, page 5-9
- Resolving Cisco Instant Connect for Android Issues, page 5-9

Resolving Cisco Instant Connect for Windows Issues

**Problem** Cannot install Cisco Instant Connect for Windows on a PC.

**Solution** You must have Windows admin privileges on the local PC to install Cisco Instant Connect. When installing, right-click the installation file and choose Run as administrator.

**Problem** Cisco Instant Connect for Windows does not receive audio.

**Solution** Check sound card settings and headphone configuration in the Windows Control Panel.

**Problem** Cisco Instant Connect for Windows shuts down unexpectedly when running on Microsoft Windows 7.

**Solution** Update networking and display device drivers on the local machine.

**Problem** When sending a PTT transmission the remote party cannot hear you.

**Solution** Check the microphone settings on your system and check the speaker settings on the system of the receiver.

Resolving Cisco Instant Connect for Android Issues

**Problem** You cannot log in to Cisco IPICS server from Cisco Instant Connect for Android.

**Solution** Make sure that you are not logged in to Cisco IPICS from another endpoint such as the IDC or an IP Phone. Cisco IPICS allows a user to be logged in from only one endpoint at a time.

**Problem** You cannot find a channel, radio, or VTG in the list of talklines.

**Solution** Make sure that you are associated with the channel, radio, or VTG. For more information, see Cisco IPICS Server Administration Guide for your release.

**Problem** You can join a talkline but cannot transmit audio on it.

**Solution** Make make sure that multicast is configured properly in your network.

**Problem** You can join a talkline but cannot receive audio on it.

**Solution** Check network and multicast configuration and connectivity.

**Problem** Cannot make a point-to-point call.

**Solution** Try to determine whether the issue relates to the device that you are using or to multiple devices by make a point-to-point call from another Android device. If the issue affects to multiple devices, make sure that voice resources on the UMS components are available. If the issues affects only your device, reinstall the Cisco Instant Connect app on the device.
Understanding the Cisco IPICS Logs

This chapter describes the logs that are available in Cisco IPICS, and how to retrieve and understand the information that is contained in the logs. The logs can help you to troubleshoot problems that may occur with Cisco IPICS and the IDC.

This chapter includes the following sections:

- Understanding and Locating the Cisco IPICS Log Files, page 6-1
- Generating and Modifying the IDC Log Levels, page 6-5

Understanding and Locating the Cisco IPICS Log Files

The Cisco IPICS log files contain information that can be used for auditing or tracking the usage of Cisco IPICS. The log files can also help you to determine the root cause of an error.

Table 6-1 lists the Cisco IPICS logs.

<table>
<thead>
<tr>
<th>Log Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>catalina.out</td>
<td>Contains information about the Cisco IPICS web-based processes, including the tomcat service. The catalina.out file is located in the /root/tomcat/current/logs directory.</td>
</tr>
<tr>
<td>Cisco IPICS Activity Log</td>
<td>The Cisco IPICS activity logs store information about activities relating to channels, users, and VTGs. To download and view the information in the activity log in a Microsoft Excel spreadsheet format, log in to the Administration Console as the ipics user, navigate to the Administration &gt; Activity Log Management &gt; Logs window, and click Download Activity Logs. You can change the information that Cisco IPICS saves in the activity log by navigating to Administration &gt; Activity Log Options. For more information about the activity log, see the “Performing Cisco IPICS System Administrator Tasks” chapter in Cisco IPICS Server Administration Guide for your Cisco IPICS release.</td>
</tr>
<tr>
<td>csalog</td>
<td>Provides CSA startup and shutdown history. The csalog file and the securitylog.txt file contain the logging information for CSA. The csalog file is located in the /var/log directory.</td>
</tr>
</tbody>
</table>
Understanding and Locating the Cisco IPICS Log Files

Cisco IPICS names the initial file Cisco001MIVR0001.log. Subsequent files are named Cisco001MIVR0002.log, Cisco001MIVR0003.log, and so on.

You configure the size of each CiscoMIVRnnnn.log file, the total number of files that Cisco IPICS retains, and the information that Cisco IPICS logs in these files, by navigating to Policy Engine > Dial Engine > Control Center > Tracing in the Administration Console and changing the information in the Trace File Configuration and Trace Settings areas.

To download and view the Cisco001MIVR0001.log file, log in to the Administration Console as the ipics user, navigate to the Policy Engine > Dial Engine > Status window and click SIP Subsystem or Policy Engine Subsystem; then, click Cisco001MIVR0001.log. To download and view subsequent log files, navigate to the SIP subsystem or Policy Engine Subsystem window and click on the CiscoMIVRnnnn.log file that you want to view.

The CiscoMIVRnnnn.log files are located in the /opt/cisco/ippe/log/MIVR directory.

Cisco IPICS names the initial file Cisco001MVCD0001.log. Subsequent files are named Cisco001MVCD0002.log, Cisco001MVCD0003.log, and so on.

To download and view the Cisco001MVCD0001.log file, log in to the Administration Console as the ipics user, navigate to the Policy Engine > Dial Engine > Status window and click SIP Subsystem or Policy Engine Subsystem; then, click Cisco001MVCD0001.log. To download and view subsequent log files, navigate to the SIP subsystem or Policy Engine Subsystem window and click on the CiscoMVCDnnnn.log file that you want to view.

The CiscoMVCDnnnn.log files are located in the /opt/cisco/ippe/log/MVCD directory.

db-maintenance.log

Contains records of the database backup and restore operations.

To download and view the db-maintenance.log file, log in to the Administration Console as the ipics user, navigate to the Administration > Database Management > Log window and click Download.

The db-maintenance.log file is located in the /opt/cisco/ipics/database/logs directory.

For more information about the db-maintenance.log file, see the “Performing Cisco IPICS Database Backup and Restore Operations” chapter in Cisco IPICS Server Administration Guide for your Cisco IPICS release.

### Table 6-1 Cisco IPICS Log Files (continued)

<table>
<thead>
<tr>
<th>Log Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CiscoMIVRnnnn.log</td>
<td>These files provide you with information about call signaling and Session Initiation Protocol (SIP) information for the policy engine. Cisco IPICS names the initial file Cisco001MIVR0001.log. Subsequent files are named Cisco001MIVR0002.log, Cisco001MIVR0003.log, and so on. You configure the size of each CiscoMIVRnnnn.log file, the total number of files that Cisco IPICS retains, and the information that Cisco IPICS logs in these files, by navigating to Policy Engine &gt; Dial Engine &gt; Control Center &gt; Tracing in the Administration Console and changing the information in the Trace File Configuration and Trace Settings areas. To download and view the Cisco001MIVR0001.log file, log in to the Administration Console as the ipics user, navigate to the Policy Engine &gt; Dial Engine &gt; Status window and click SIP Subsystem or Policy Engine Subsystem; then, click Cisco001MIVR0001.log. To download and view subsequent log files, navigate to the SIP subsystem or Policy Engine Subsystem window and click on the CiscoMIVRnnnn.log file that you want to view. The CiscoMIVRnnnn.log files are located in the /opt/cisco/ippe/log/MIVR directory.</td>
</tr>
<tr>
<td>CiscoMVCDnnnn.log</td>
<td>These files provide you with error and status information for the cluster view daemon (CVD) component of the policy engine. The CVD is the node manager for the policy engine and is responsible for managing the startup process for the Cisco IPICS dial engine service. Cisco IPICS names the initial file Cisco001MVCD0001.log. Subsequent files are named Cisco001MVCD0002.log, Cisco001MVCD0003.log, and so on. To download and view the Cisco001MVCD0001.log file, log in to the Administration Console as the ipics user, navigate to the Policy Engine &gt; Control Center &gt; Status &gt; Cluster View Daemon window, and click Cisco001MVCD0001.log. To download and view subsequent log files, navigate to the SIP subsystem or Policy Engine Subsystem window and click on the CiscoMVCDnnnn.log file that you want to view. The CiscoMVCDnnnn.log files are located in the /opt/cisco/ippe/log/MVCD directory.</td>
</tr>
<tr>
<td>db-maintenance.log</td>
<td>Contains records of the database backup and restore operations. To download and view the db-maintenance.log file, log in to the Administration Console as the ipics user, navigate to the Administration &gt; Database Management &gt; Log window and click Download. The db-maintenance.log file is located in the /opt/cisco/ipics/database/logs directory. For more information about the db-maintenance.log file, see the “Performing Cisco IPICS Database Backup and Restore Operations” chapter in Cisco IPICS Server Administration Guide for your Cisco IPICS release.</td>
</tr>
</tbody>
</table>
### Table 6-1  Cisco IPICS Log Files (continued)

<table>
<thead>
<tr>
<th>Log Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dbm_log_archive.log.gz</td>
<td>A compressed file that contains archived data from previous db-maintenance.log daily log files. You can download the dbm_log_archive.log.gz file and save it to your PC by clicking the Download button in the Administration &gt; Database Management &gt; Log window. Once you download the files to your PC, you can view them as a text file. The dbm_log_archive.log.gz file is located in the /opt/cisco/ipics/database/logs directory. For more information about this archive file, see the “Performing Cisco IPICS Database Backup and Restore Operations” chapter in Cisco IPICS Server Administration Guide for your Cisco IPICS release.</td>
</tr>
<tr>
<td>diagnostics.log</td>
<td>Contains messages that are related to the database subsystem, and is located in the /opt/cisco/ipics/database/logs directory.</td>
</tr>
<tr>
<td>driverManager(n).log</td>
<td>The driverManager log files contain policy engine-specific information for the media that are associated with each call. To configure the level of detail that the driverManager logs capture, navigate to the Policy Engine &gt; Control Center &gt; Tracing window in the Administration Console and check or uncheck the LIB_MEDIA check boxes. Cisco IPICS sets the size and total number of driverManager files; you cannot change these settings. When a log file reaches the configured maximum size, Cisco IPICS closes that log file and creates a new empty log file, and increments the number of the new log file by one. The driverManager(n).log files are located in the /opt/cisco/ippe/log/MIVR directory.</td>
</tr>
<tr>
<td>install.log</td>
<td>Shows details about the Cisco IPICS operating system installation, including the packages that were installed and any errors that occurred during the installation. The install.log file is located in the /root directory.</td>
</tr>
</tbody>
</table>
### Table 6-1  Cisco IPICS Log Files (continued)

<table>
<thead>
<tr>
<th>Log Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipics.log</td>
<td>Contains messages regarding all transactions that occur in the Cisco IPICS server. For example, this file contains information about the tomcat service, policy engine entries, or external notifications. The information that is contained in this log file can help you to troubleshoot problems that you might encounter with Cisco IPICS. Each message is marked with a severity level. There are seven severities, from TRACE to FATAL. By default, the ipics.log file captures all logging from the INFO to the FATAL level. You can view recent system logs in the Serviceability &gt; System Logs window of the Administration Console. To download and view the information in the ipics.log, navigate to the Serviceability &gt; System Logs window and click Download. For more information about accessing and downloading the ipics.log file, see the “Understanding Cisco IPICS Serviceability and Diagnostic Information” chapter in Cisco IPICS Server Administration Guide for your Cisco IPICS release. The ipics.log file is located in the /root/tomcat/current/logs directory.</td>
</tr>
<tr>
<td>ipics_audit.log</td>
<td>Records user activity. This activity includes successful and unsuccessful attempts by users to log in to the server, and actions that Cisco IPICS users perform when they are logged in to the Administration Console. The ipics_audit.log file is located in the /root/tomcat/current/logs directory.</td>
</tr>
<tr>
<td>ipics-install-log.txt</td>
<td>Shows details of the Cisco IPICS server software installation, including the packages that were installed, the user names that were created, and any errors that occurred during the installation. The install.log file is located in the /var/opt/CSCOipics/run/yyyyymmddhhmmss/ipics-install-log.txt directory, where: yyyyymmddhhmmss represents the date and time that you performed the server software installation.</td>
</tr>
<tr>
<td>ipics_idc.log</td>
<td>Collects information for IDC users. Cisco IPICS updates the log file when IDC users log in and log out, or when users update their IDCs. The ipics_idc.log file is located in the /root/tomcat/current/logs directory. <strong>Note</strong> To retrieve additional IDC data for a user, you can upload logging information from a IDC to the server. For more information, see the “Generating and Modifying the IDC Log Levels” section on page 6-5.</td>
</tr>
<tr>
<td>ipics_rms.log</td>
<td>Collects log data for the RMS components that are part of the Cisco IPICS system. The ipics_rms.log file is located in the /root/tomcat/current/logs directory.</td>
</tr>
</tbody>
</table>
The IDC application generates logs that can help you analyze user activity and troubleshoot problems that you may encounter when you use the application. The IDC writes the logs to the hard disk of the IDC client machine, so that the application can continue logging if the communication to the server is disrupted.

From the Administration Console, you can modify the IDC log settings in the User Management > Users > Username > IDC tab. For more information about setting and modifying the log settings, see the “Performing Cisco IPICS Operator Tasks” chapter in Cisco IPICS Server Administration Guide for your Cisco IPICS release.

You can download activity logs for IDC users in the Administration > Activity Log Management > Logs tab of the Administration Console. The information that you download includes details about user associations to channels and VTGs, channel activation activities, and conference participation. You configure the activity logs to capture the IDC information in the Administration > Activity Log Options window. For information about the activity logs, see the “Performing Cisco IPICS System Administrator Tasks” chapter in Cisco IPICS Server Administration Guide for your Cisco IPICS release.

This section contains the following topics:

- Understanding IDC Debug Log Information, page 6-6
- Using the Debugging Log Level, page 6-7

### Generating and Modifying the IDC Log Levels

The IDC application generates logs that can help you analyze user activity and troubleshoot problems that you may encounter when you use the application. The IDC writes the logs to the hard disk of the IDC client machine, so that the application can continue logging if the communication to the server is disrupted.

From the Administration Console, you can modify the IDC log settings in the User Management > Users > Username > IDC tab. For more information about setting and modifying the log settings, see the “Performing Cisco IPICS Operator Tasks” chapter in Cisco IPICS Server Administration Guide for your Cisco IPICS release.

You can download activity logs for IDC users in the Administration > Activity Log Management > Logs tab of the Administration Console. The information that you download includes details about user associations to channels and VTGs, channel activation activities, and conference participation. You configure the activity logs to capture the IDC information in the Administration > Activity Log Options window. For information about the activity logs, see the “Performing Cisco IPICS System Administrator Tasks” chapter in Cisco IPICS Server Administration Guide for your Cisco IPICS release.

This section contains the following topics:

- Understanding IDC Debug Log Information, page 6-6
- Using the Debugging Log Level, page 6-7

### Understanding IDC Debug Log Information

The IDC application generates logs that can help you analyze user activity and troubleshoot problems that you may encounter when you use the application. The IDC writes the logs to the hard disk of the IDC client machine, so that the application can continue logging if the communication to the server is disrupted.

From the Administration Console, you can modify the IDC log settings in the User Management > Users > Username > IDC tab. For more information about setting and modifying the log settings, see the “Performing Cisco IPICS Operator Tasks” chapter in Cisco IPICS Server Administration Guide for your Cisco IPICS release.

You can download activity logs for IDC users in the Administration > Activity Log Management > Logs tab of the Administration Console. The information that you download includes details about user associations to channels and VTGs, channel activation activities, and conference participation. You configure the activity logs to capture the IDC information in the Administration > Activity Log Options window. For information about the activity logs, see the “Performing Cisco IPICS System Administrator Tasks” chapter in Cisco IPICS Server Administration Guide for your Cisco IPICS release.

This section contains the following topics:

- Understanding IDC Debug Log Information, page 6-6
- Using the Debugging Log Level, page 6-7
Generating and Modifying the IDC Log Levels

Chapter 6 Understanding the Cisco IPICS Logs

Understanding IDC Debug Log Information

Cisco IPICS organizes the DebugLog.txt data fields into three categories: User Interface, Signaling, and Media. These data fields are then divided into three logging levels, so that you can capture more precisely the debugging information that you need. The Debug Log categories contain the following information:

- **User Interface**—These fields provide information about aspects of the user interface for the IDC. The category includes everything that the user can see on the IDC application, such as the buttons and volume controls. The User Interface category also includes information for debugging communication problems with the Cisco IPICS server.

  Table 6-2 describes the information that Cisco IPICS gathers, by log level:

<table>
<thead>
<tr>
<th>Logging Level</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Cisco IPICS retrieves information for the following problems at this logging level:</td>
</tr>
<tr>
<td></td>
<td>• The user cannot log in</td>
</tr>
<tr>
<td></td>
<td>• The user has difficulty activating channels</td>
</tr>
<tr>
<td></td>
<td>• The user cannot close the IDC</td>
</tr>
<tr>
<td></td>
<td>• The IDC unexpectedly goes into offline mode</td>
</tr>
<tr>
<td></td>
<td>• The server is reporting errors</td>
</tr>
<tr>
<td>Medium</td>
<td>Cisco IPICS reports information that can help translate XML communication from the server.</td>
</tr>
<tr>
<td>High</td>
<td>Cisco IPICS gathers information regarding authentication, the GUI, and the IDC server update function.</td>
</tr>
</tbody>
</table>

- **Signaling**—The Signaling category includes fields that provide information about the starting and stopping of voice channels. You would turn Signaling on when a user is not able to activate or deactivate a IDC channel.

  Table 6-3 describes the information that Cisco IPICS reports by signaling levels:

<table>
<thead>
<tr>
<th>Logging Level</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low and Medium</td>
<td>Messages at these log levels describe issues with the high level state machines.</td>
</tr>
<tr>
<td>High</td>
<td>Messages at this level report issues with SIP messaging.</td>
</tr>
</tbody>
</table>

- **Media**—These fields involve items related to the voice stream, such as the packets and the codecs that handle the data between end points. You would use Media information to diagnose any voice quality problem.

  Table 6-4 describes the type of information you can gather with the Media log levels.
When you choose to begin logging debug information for a IDC user, you select one or more of the information categories, each of which includes a list of debugging fields. You choose the category and logging level as it corresponds to the fields that you want to capture in the log.

Table 6-5 shows the fields that are included in each logging level.

The log levels for each category are cumulative. If you choose the Medium level for a category, the IDC writes Low- and Medium-level logs into the DebugLog.txt file. When you set the logging to High, you capture all the fields for that category.

Always start debugging by collecting Low-level log data, which may provide all of the data that you require. Using this setting allows you to gather several days of log activity without filling the hard disk of the IDC client machine. If you cannot locate the cause of the problem, you can next set the logging to Medium or High.

Use the High level only for short durations. If you use the High level, you should closely monitor the hard drive of the user IDC client machine so that the High-level logs do not overwhelm the client hard drive or degrade the performance of the IDC.

Because of the large amount of information that the system collects and generates when you set all of the debug options, Cisco recommends that you use debug logging only to isolate specific problems. When you complete your debugging tasks, be sure to turn off debug logging by clearing the debug log.

Table 6-5 lists the debug categories, and the fields and log levels that are associated with each category.
### Table 6-5  Debug Log Fields and Log Levels

<table>
<thead>
<tr>
<th>Category</th>
<th>Field</th>
<th>Log Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Interface</td>
<td>channel-activation-debug</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>error</td>
<td></td>
</tr>
<tr>
<td></td>
<td>exit-debug</td>
<td></td>
</tr>
<tr>
<td></td>
<td>sending-source-debug</td>
<td></td>
</tr>
<tr>
<td></td>
<td>sock-init-cleanup</td>
<td></td>
</tr>
<tr>
<td></td>
<td>xml-events</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td>xml-post</td>
<td></td>
</tr>
<tr>
<td></td>
<td>xml-vars</td>
<td></td>
</tr>
<tr>
<td>Auth</td>
<td>critical-section-tune-debug</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>download-debug</td>
<td></td>
</tr>
<tr>
<td></td>
<td>gui-debug</td>
<td></td>
</tr>
<tr>
<td></td>
<td>server-task-debug</td>
<td></td>
</tr>
<tr>
<td></td>
<td>server-verbose</td>
<td></td>
</tr>
<tr>
<td></td>
<td>xml-deck</td>
<td></td>
</tr>
<tr>
<td>Signaling</td>
<td>cc</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>fim</td>
<td></td>
</tr>
<tr>
<td></td>
<td>fsm</td>
<td></td>
</tr>
<tr>
<td></td>
<td>gsm</td>
<td></td>
</tr>
<tr>
<td></td>
<td>lsm</td>
<td></td>
</tr>
<tr>
<td></td>
<td>multicast-signaling-debug</td>
<td></td>
</tr>
<tr>
<td></td>
<td>sip-reg-state</td>
<td></td>
</tr>
<tr>
<td></td>
<td>sip-state</td>
<td></td>
</tr>
<tr>
<td></td>
<td>vcm</td>
<td></td>
</tr>
<tr>
<td></td>
<td>sip-task</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td>sip-trx</td>
<td></td>
</tr>
<tr>
<td>Auth</td>
<td>cc-msg</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>sip-messages</td>
<td></td>
</tr>
<tr>
<td></td>
<td>xml-events</td>
<td>Medium</td>
</tr>
</tbody>
</table>
### Table 6-5  Debug Log Fields and Log Levels (continued)

<table>
<thead>
<tr>
<th>Category</th>
<th>Field</th>
<th>Log Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media</td>
<td>AMuteTrans</td>
<td>Low</td>
</tr>
<tr>
<td>Media</td>
<td>AudioSource</td>
<td>Low</td>
</tr>
<tr>
<td>Media</td>
<td>MediaStream</td>
<td>Low</td>
</tr>
<tr>
<td>Media</td>
<td>OpenALAudioSink</td>
<td>Low</td>
</tr>
<tr>
<td>Media</td>
<td>RTPAudioSink</td>
<td>Low</td>
</tr>
<tr>
<td>Media</td>
<td>RTPAudioSockets</td>
<td>Low</td>
</tr>
<tr>
<td>Media</td>
<td>RTPAudioSource</td>
<td>Low</td>
</tr>
<tr>
<td>Media</td>
<td>RTPAudioStream</td>
<td>Low</td>
</tr>
<tr>
<td>Media</td>
<td>RTPJitterBuf</td>
<td>Low</td>
</tr>
<tr>
<td>Media</td>
<td>sock-init-Cleanup</td>
<td>Low</td>
</tr>
<tr>
<td>Media</td>
<td>WaveAudioSource</td>
<td>Low</td>
</tr>
<tr>
<td>Media</td>
<td>WaveFileSource</td>
<td>Low</td>
</tr>
<tr>
<td>Media</td>
<td>RxStats</td>
<td>Low</td>
</tr>
<tr>
<td>Media</td>
<td>TxStats</td>
<td>Low</td>
</tr>
<tr>
<td>Media</td>
<td>WACMTrans</td>
<td>Medium</td>
</tr>
<tr>
<td>Media</td>
<td>ASL</td>
<td>Medium</td>
</tr>
<tr>
<td>Media</td>
<td>AudioBufferAndPlayback</td>
<td>Medium</td>
</tr>
<tr>
<td>Media</td>
<td>dsp</td>
<td>Medium</td>
</tr>
<tr>
<td>Media</td>
<td>FilePlay</td>
<td>Medium</td>
</tr>
<tr>
<td>Media</td>
<td>PCMMixer</td>
<td>Medium</td>
</tr>
<tr>
<td>Media</td>
<td>PCMVolTrans</td>
<td>Medium</td>
</tr>
<tr>
<td>Media</td>
<td>PCMVolMax</td>
<td>Medium</td>
</tr>
<tr>
<td>Media</td>
<td>RTPAudioStreamMgr</td>
<td>Medium</td>
</tr>
<tr>
<td>Media</td>
<td>RxDetailStats</td>
<td>Medium</td>
</tr>
<tr>
<td>Media</td>
<td>VAD</td>
<td>Medium</td>
</tr>
</tbody>
</table>
### Table 6-5  Debug Log Fields and Log Levels (continued)

<table>
<thead>
<tr>
<th>Category</th>
<th>Field</th>
<th>Log Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media</td>
<td>AudioDump</td>
<td>High</td>
</tr>
<tr>
<td>Media</td>
<td>AudioSamp</td>
<td></td>
</tr>
<tr>
<td>Media</td>
<td>AudioSampLost</td>
<td></td>
</tr>
<tr>
<td>Media</td>
<td>AudioSampMgr</td>
<td></td>
</tr>
<tr>
<td>Media</td>
<td>AudioTrans</td>
<td></td>
</tr>
<tr>
<td>Media</td>
<td>AutomaticGainControl</td>
<td></td>
</tr>
<tr>
<td>Media</td>
<td>dtmf</td>
<td></td>
</tr>
<tr>
<td>Media</td>
<td>FIRTrans</td>
<td></td>
</tr>
<tr>
<td>Media</td>
<td>FSAudioBuf</td>
<td></td>
</tr>
<tr>
<td>Media</td>
<td>G7112PCMTrans</td>
<td></td>
</tr>
<tr>
<td>Media</td>
<td>G7232PCMTrans</td>
<td></td>
</tr>
<tr>
<td>Media</td>
<td>G729A2PCMTrans</td>
<td></td>
</tr>
<tr>
<td>Media</td>
<td>Limiter</td>
<td></td>
</tr>
<tr>
<td>Media</td>
<td>PCM2G711Trans</td>
<td></td>
</tr>
<tr>
<td>Media</td>
<td>PCM2G723Trans</td>
<td></td>
</tr>
<tr>
<td>Media</td>
<td>PCM2G729ATrans</td>
<td></td>
</tr>
<tr>
<td>Media</td>
<td>RTCPPacket</td>
<td></td>
</tr>
<tr>
<td>Media</td>
<td>TimeSample</td>
<td></td>
</tr>
<tr>
<td>Media</td>
<td>TimeRxSample</td>
<td></td>
</tr>
<tr>
<td>Media</td>
<td>TimeTxSample</td>
<td></td>
</tr>
</tbody>
</table>
**GLOSSARY**

**A**

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

**activating**  
A VTG state that becomes effective when the Activate button is clicked. The Activate button appears highlighted while the other IDC buttons remain in an inactive state as the system attempts to activate and connect.

**activation button**  
This button toggles activate and deactivate functionality on the IDC. Click this button on the IDC to activate a channel (to call out); click it again to deactivate the channel.

**active virtual talk group**  
A virtual talk group (VTG) becomes active when Cisco IPICS commits global resources, such as a multicast address and any necessary dial-in peers, so that the participants in the VTG can communicate with each other.

**Administration Console**  
The graphical user interface (GUI) in the Cisco IPICS server software through which authorized Cisco IPICS users can manage and configure Cisco IPICS resources, events and VTGs.

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

**B**

**backward compatibility**  
The ability of newer radio equipment to operate within an older system infrastructure or to directly intercommunicate with an older radio unit. The term usually applies to digital radios that are also capable of analog signal transmission.

**bandwidth**  
The difference between the highest and lowest frequencies that are available for network signals. The term also describes the rated throughput capacity of a specific network medium or protocol. Bandwidth specifies the frequency range that is necessary to convey a signal measured in units of hertz (Hz). For example, voice signals typically require approximately 7 kHz of bandwidth and data traffic typically requires approximately 50 kHz of bandwidth.

**base station**  
A land station in the land mobile radio service. In the personal communication service, the common name for all the radio equipment that is located at one fixed location and used for serving one or several calls.
C

CAI common air interface. The standard for the digital wireless communications medium that is employed for P25-compliant radio systems and equipment. The standard for P25 Phase I incorporates Frequency Division Multiple Access (FDMA) technology.

call Radio terminology that defines a call as beginning at the moment that you press the transmit key and concluding when you release the transmit key. The term “per call” implies that some form of control causes the radio to select a specific frequency before it transmits audio. Some radios may be configured to automatically return to a predefined RF channel when the call ends.

call delay The delay that occurs when there is no idle channel or facility available to immediately process a call that arrives at an automatic switching device.

call setup time The time that is required to establish a circuit-switched call between users or terminals.
carrier A wave that is suitable for modulation by an information-bearing signal.
CAS channel associated signaling. The transmission of signaling information within the voice channel. CAS signaling often is referred to as robbed-bit signaling because user bandwidth is being robbed by the network for other purposes.
channel A communication path that is wide enough to permit a single RF transmission. Multiple channels can be multiplexed over a single cable in certain environments. There are many different types of channels in Cisco IPICS, including direct dial, 2-way, VTGs, and radio channels. Channels can be dynamically or statically allocated. Channels may have one or more channel connections that define the source for the channel. See PTT channel.
channel capacity The maximum possible information transfer rate through a channel, subject to specified constraints.
channel connection One or more methods by which a content stream can be obtained. For instance, a particular channel may be found on several different multicast addresses in different locations and also on several different radios at different locations.
channel folder A logical grouping of channels
channel select check box Provides the ability to select or deselect the specified channel on the IDC for audio transmission.
channel spacing The distance from the center of one channel to the center of the next-adjacent-channel. Typically measured in kilohertz.
Cisco Unified Communications Manager (CallManager) The software-based call-processing component of the Cisco IP telephony solution. Cisco Unified Communications Manager (CallManager) extends enterprise telephony features and functions to packet telephony network devices, such as Cisco Unified IP Phones, media processing devices, VoIP gateways, and multimedia applications.
Cisco IPICS Cisco IP Interoperability and Collaboration System. The Cisco IPICS system provides an IP standards-based solution for voice interoperability by interconnecting voice channels, talk groups, and VTGs to bridge communications amongst disparate systems.
Cisco IPICS policy engine Integrated with the Cisco IPICS server, this component enables telephony dial functionality and is responsible for the management and execution of policies and user notifications.
Cisco IPICS server | Provides the core functionality of the Cisco IPICS system. The Cisco IPICS server software runs on the Linux operating system on selected Cisco Media Convergence Server (MCS) platforms. The server software includes an incident management framework administration GUI that enables dynamic resource management for users, channels, and VTGs. The server also includes the Cisco IPICS policy engine, which enables telephony dial functionality and is responsible for the management and execution of policies and user notifications.

Cisco Unified IP Phone | A full-featured telephone that provides voice communication over an IP network. A user can participate in a PTT channel or VTG by using a Cisco Unified IP Phone as a PTT device.

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

codec | coder-decoder.

1. Integrated circuit device that typically uses pulse code modulation to transform analog signals into a digital bit stream and digital signals back into analog signals.

2. In Voice over IP, Voice over Frame Relay, and Voice over ATM, a DSP software algorithm that is used to compress/decompress speech or audio signals.

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

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

COR | carrier operated relay. An electrical signal that is used to signal when a radio is receiving traffic.

coverage | In radio communications, the geographical area that is within the range of, or that is covered by, a wireless radio system to enable service for radio communications. Also referred to as service delivery area.

D

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

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

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

dial engine scripts | Scripts that the Cisco IPICS dial engine executes to provide the telephony user interface (TUI) for interaction with incoming and outgoing phone calls.

dial-in | A phone call that is dialed in to the policy engine.

dial-in floor control | A feature that allows one dial-in user, at a time, to talk in a VTG or a channel. The telephony user interface provides this dial-in floor control feature to support dial-in users. It does not provide support for floor control for other PTT users.
**dial number**  The phone number that is used by the policy engine and the SIP provider and configured in the Dial Information pane in the Ops Views window. Dialing this number provides user access to the telephony user interface.

**dial out invite**  An action that invites selected user(s) to the selected VTG.

A phone call that is dialed out by the policy engine to a phone user to invite the user in to a talk group.

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

**digit ID**  A numeric identifier that is chosen by a Cisco IPICS user and stored in the user profile. Cisco IPICS uses this ID and a numeric password to authenticate a Cisco Unified IP Phone user.

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

**discrete tone**  Any tone that is sent without any summed or added tone. For example, adding a function tone with a low level guard tone may impact the recognition of the function tone. Contrast with mixed tones.

**dispatcher**  The Cisco IPICS dispatcher is responsible for setting up the VTGs, activating the VTGs to begin conferences, and adding and/or removing participants in inactive VTG and active VTGs. The dispatcher also monitors the active VTGs and events, can mute and unmute IDC users, as necessary, and manages policies, which activate/deactivate VTGs based on specific criteria and designated intervals. Policy management activities include create/modify/delete policies, view policies, execute policies, and activate privileges.

**DS0**  digital service zero (0). Single timeslot on a DS1 (also known as T1) digital interface—that is, a 64-kbps, synchronous, full-duplex data channel, typically used for a single voice connection on a PBX.

**DTMF**  dual tone multi-frequency. The signal to the phone company that you generate when you press keys on a telephone keypad. With DTMF, each key that you press on your phone (0 through 9, ‘*’ and ‘#’) generates two tones of specific frequencies; one tone is generated from a high frequency group of tones and the other from a low frequency group. Voice gateways often strip these inband tones and present them out-of-band in SIP, H.323, or other messages.

**dynamic radio channel (dynamic control)**  The controls that are used to preset radio characteristics so that channels are available to clients.

**dynamic regrouping**  A trunking system feature that allows multiple radios to be placed upon a specific talk group without manual manipulation of the programming of the radios. Dynamic regrouping is initiated through a system control console and transmitted to the radio via the trunking systems control channel.
E

E & M

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

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

2. A type of signaling that is traditionally used in the telecommunications industry. Indicates the use of a handset that corresponds to the ear (receiving) and mouth (transmitting) component of a telephone.

e-lead

The ear portion of the E & M interface. The e-lead is the receive path of the LMR gateway.

cipher

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

code

To modify information into the required transmission format.

encryption

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

event

An active VTG in the Cisco IPICS solution.

F

FDM

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

FDMA

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

floor control

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

frame

A logical grouping of information sent as a data link layer unit over a transmission medium. Often refers to the header and the trailer, used for synchronization and error control, that surround the user data contained in the unit. The terms cell, datagram, message, packet, and segment also describe logical information groupings at various layers of the OSI reference model.

frequency

For a periodic function, frequency represents the number of cycles or events per unit of time. Frequency is used in several different contexts. For example, transmission frequency (the band on which the radio sends signals) or the frequency of an audible signal measured in hertz (Hz). All tone control operations require audible tones that fall within a narrow band of a specific frequency and at a specific volume (amplitude).

frequency assignment

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

frequency hopping

The repeated switching of frequencies during radio transmission according to a specified algorithm, intended to minimize unauthorized interception or jamming of telecommunications.
frequency modulation
- Modulation technique in which signals of different frequencies represent different data values.

frequency sharing
- The assignment to or use of the same radio frequency by two or more stations that are separated geographically or that use the frequency at different times.

function tone
- A tone that follows the high level guard tone and causes the radio to perform a specific function, such as selecting a new transmit frequency. Function tones are often referred to as F1, F2, F3, and so on. See preamble and high level guard tone.

G

gateway
- Device that performs an application-layer conversion of information from one protocol stack to another. In Cisco IPICS, the gateway component includes LMR gateways, which functionality is usually installed as an additional feature in a supported Cisco router. LMR gateways provide voice interoperability between radio and non-radio networks by bridging radio frequencies to IP multicast streams.

GRE
- Generic routing encapsulation. Tunneling protocol that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP internetwork. By connecting multiprotocol subnetworks in a single-protocol backbone environment, IP tunneling that uses GRE allows network expansion across a single-protocol backbone environment. GRE is generally used to route multicast traffic between routers.

guard tone
- The most common guard tones are the high level guard tone (HLGT) and the low level guard tone (LLGT). The HLGT is used to alert the radio that a function tone follows. The LLGT is used as a hold tone or keying tone. See tone keyed.

H

H.323
- Defines a common set of codecs, call setup and negotiating procedures, and basic data transport methods to allow dissimilar communication devices to communicate with each other by using a standardized communication protocol.

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

HLGT
- high level guard done. Also known as awake tone. This tone is set at high volume and is usually the first tone in a preamble. It is used to alert the radio that another tone, usually a function tone, will follow. See guard tone.

Hoot ‘n’ Holler (Hootie)
- A communications system where the loudest and most recent talker or talkers are mixed into one multicast output stream. Also known as hootie, these networks provide “always on” multiuser conferences without requiring that users dial in to a conference.

Cisco enables the Cisco Hoot ‘n’ Holler feature in specific Cisco IOS versions.
IDC Cisco IPICS Dispatch Console. A component of the Cisco IPICS that installs and runs on a client (standalone) PC. It is a graphical-based application that allows you to communicate with other users via radio, telephone, mobile device, or PC. It also lets you participate in VTGs and incidents, manage and operate a variety of resources, and perform a variety of other activities.

idle tone The tone that a radio may deliver on the m-lead to signal the LMR gateway that there is no incoming traffic. When the idle tone is removed, the LMR gateway deems all signals to be valid voice traffic.

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

inband Traffic that is sent inband is included in the same stream as the real-time traffic protocol (RTP). Inband signals can be encoded signals and RFC 2833 signals.

incident management framework A software framework that includes an adaptable GUI to facilitate resources, such as users, radio channels, cameras, and sensor information, for delivery that is based upon policy or incident needs.

informix linux group Members of this group have full permission to Cisco IPICS server folders, files, and scripts that are related to the Informix database application. Members of this group include the informix and ipicsdba users.

informix user ID The Cisco IPICS Linux user that belongs to both the informix linux group, which includes full permission to the Cisco IPICS database server folders, files, and scripts, and the ipics linux group, which includes permission to Cisco IPICS application-related folders, files, and scripts. In addition, this user has full administrative permission to the Informix database instance. Cisco IPICS creates this Linux system user ID and generates the password during the software installation process. The password for this user ID never expires.

To access the informix user, log in to the Cisco IPICS server by using the root user ID; then, enter `su - informix` (superuser from root).

interference The effect of unwanted energy due to one or a combination of emissions, radiation, or inductions upon reception in a radio communication system, manifested by any performance degradation, misinterpretation, or loss of information, which could be extracted in the absence of such unwanted energy.

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

invitation policy A policy that can be invoked only through the telephony user interface and can include only the invite to VTG action. After joining a talk group, a user can access the breakout menu and invoke invitation policies. The talk group that this user has joined is the talk group that the invited users join.

invite to VTG A version of the dial out invite action where users to be invited are preconfigured but the VTG that they are invited to depends on which VTG the invoker of the policy is dialed into.
ipicsadmin user ID  The Cisco IPICS Linux user that, as part of the ipics linux group, has full permission to the Cisco IPICS server folders, files, and scripts that are related to the Cisco IPICS application and database backup and restore operations. In addition, the ipicsadmin user has permission to read and write data from and/or to the Informix database. Cisco IPICS creates this Linux system user ID during the software installation process. The password for this user ID never expires.

ipicsdba user ID  The Cisco IPICS Linux user that belongs to both the informix linux group, which includes full permission to the Cisco IPICS database server folders, files, and scripts, and the ipics linux group, which includes permission to Cisco IPICS application-related folders, files, and scripts. In addition, the ipicsdba user has permission to read data, write data, create tables, and create databases in the Informix database instance. Cisco IPICS creates this Linux system user ID and generates the password during the software installation process. The password for this user ID never expires.

To access the ipicsdba user, log in to the Cisco IPICS server by using the root user ID; then, enter su - ipicsdba (superuser from root).

ipics linux group  Members of this group have full permission to Cisco IPICS server folders, files, and scripts that are related to the Cisco IPICS application and database backup and restore operations. Members of this group include the ipicsadmin, ipicsdba, and informix users.

ipics user ID  The Cisco IPICS application-level user ID that can perform all administration-related tasks via the Cisco IPICS Administration Console. Cisco IPICS creates this web-based user ID during the software installation process.

IPSec  IP Security. A framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer. IPSec uses IKE to handle the negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPSec. IPSec can protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

K

keepalive  A message that is sent by one network device to inform another network device that the virtual circuit between the two devices is still active.

key  The parameter that defines an encryption code or method.

Key (a radio) causes the radio to transmit. See tone keyed.

kilohertz (kHz)  A unit of frequency that denotes one thousand Hz.

L

latch  The IDC functionality that allows a Cisco IPICS user to lock in a PTT channel.

linear modulation  A radio frequency transmission technique that provides the physical transport layer of a radio system. This technology is compatible in digital and analog system environments and supports channel bandwidths of 5 kHz to 50 kHz.

LLGT  low level guard tone. This tone is used as a hold tone or keying tone. See guard tone.
LMR  
Land Mobile Radio. A Land Mobile Radio (LMR) system is a collection of portable and stationary radio units that are designed to communicate with each other over predefined frequencies. They are deployed wherever organizations need to have instant communication between geographically dispersed and mobile personnel.

This term is often used interchangeably between a handheld or vehicle-mounted device and a stationary transmitter. Stationary devices are typically referred to as base stations.

Cisco IPICS leverages the Cisco Hoot 'n' Holler feature, which is enabled in specific Cisco IOS versions, to provide radio integration into the Cisco IPICS solution. LMR is integrated by providing an ear and mouth (E&M) interface to a radio or other PTT devices, such as Nextel phones. Configured as a voice port, this interface provides the appropriate electrical interface to the radio. You configure this voice port with a connection trunk entry that corresponds to a VoIP dial peer, which in turn associates the connection to a multicast address. This configuration allows you to configure a corresponding channel in Cisco IPICS, using the same multicast address, which enables Cisco IPICS to provide communication paths between the desired endpoints.

LMR gateway  
Land Mobile Radio gateway. Refers to the router E&M interface that converts IP traffic from digital to analog for use by radios.

location  
In Cisco IPICS, location signifies reachability; meaning, channels or users who are associated with the same location can communicate with each other without additional network configuration. Location may refer to a physical or virtual location, as defined in the server.

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

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

mixed tone  
Two tones that are mixed together. DTMF is an example of a mixed tone. To be transmitted properly, tone signals must be mixed with the LLGT. See DTMF.

m-lead  
The mouth portion of the E&M interface. The m-lead is the transmit path of the LMR gateway.

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

multicast  
Single packets that are copied by the network and sent to a specific subset of network addresses. Multicast refers to communications that are sent between a single sender and multiple recipients on a network.

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

multicast address/port  
Cisco IPICS uses this type of connection to enable the IDC to directly tune in to the multicast channel. Multicast address/port combinations are also used by gateways and RMS components.

multicast pool  
Multicast IP addresses that are defined as part of a multicast pool. Cisco IPICS allocates a multicast address from this pool of resources when a dispatcher activates a VTG.
**multiplexing**

The combination of two or more information channels on to a common transmission medium. In electrical communications, the two basic forms of multiplexing are time-division multiplexing (TDM) and frequency-division multiplexing (FDM).

**multipurpose policy**

A policy that can include any of the supported actions; may be invoked through the telephony user interface or the Cisco IPICS administration console.

**multiselect buttons**

Provides the ability to select or deselect all channels on the IDC for audio transmission.

**mute**

The functionality that enables a dispatcher to mute an IDC user from talking or transmitting voice on one or more channels. The dispatcher can mute the microphone of the user or both the microphone and the speaker.

**mutual aid channel**

A national or regional channel that has been set aside for use only in mutual aid interoperability situations. Restrictions and guidelines governing usage usually apply.

**narrowband channels**

Channels that occupy less than 20 kHz.

**National Public Safety Planning Advisory Committee**

The committee that was established to conduct nationwide planning and allocation for the 821–824 MHz and 866–869 MHz bands.

**National Telecommunication and Information Administration**

The United States executive branch agency that serves as the principal advisor to the president on telecommunications and information policies and that is responsible for managing the federal government’s use of the radio spectrum.

**near end**

The device or devices that are physically connected to the Ethernet or an RS-232 link. Compare with far end, which refers to devices on the other side of the broadcast. A base station that is connected to an LMR gateway is a near end device while a handheld radio that receives over-the-air signals from the base station is a far end device.

**network**

An interconnection of communications entities.

**NAT**

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

**not activated**

A VTG state that becomes effective when the Activate button is clicked a second time (to deactivate the channel) or if the connection terminates. No IDC buttons appear highlighted.

**notification**

An action that notifies selected user(s) via email, SMS, pager, or phone. The necessary IDs and phone numbers are configured in the communication preferences for each user. Notifications that are sent via the phone require user authentication before the notification prompt is heard.

An email, SMS, pager, or phone call that is placed to a user for the purpose of sending a notification message.
**offline mode**  
When the connection to the server goes offline, the IDC enters offline mode. Offline mode enables continuous communication during periods of server downtime. Using offline mode requires at least one successful login to the server.

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

**ops view**  
operational view. A Cisco IPICS feature that provides the ability to organize users, user groups, channels, channel groups, VTGs, and policies into different user-definable views across multiple organizations or agencies that normally would not share resources. While ops views are maintained separately by the Cisco IPICS system administrator and/or ops view administrator, this functionality also allows multiple entities to use one Cisco IPICS server to enable resource sharing across multiple ops views, according to business need.

**ops view administrator**  
The ops view administrator capabilities include managing and monitoring the activity logs that are filtered by ops views and accessible in the Administration Console (Administration > Activity Log Management) window.

**OTAR**  
over-the-air re-keying. Provides the ability to update or modify over radio frequency the encryption keys that are programmed in a mobile or portable radio.

**P**

**packet**  
A logical grouping of information that includes a header that contains control information. Usually also includes user data.

**packet switching**  
The process of routing and transferring data by using addressed packets so that a channel is occupied during the transmission of the packet only. Upon completion of the transmission, the channel is made available for the transfer of other traffic.

**PIM**  
Protocol Independent Multicast. Multicast routing architecture that allows the addition of IP multicast routing on existing IP networks. PIM is unicast routing protocol independent and can be operated in two modes: PIM dense mode and PIM sparse mode.

**PIM dense mode**  
One of the two PIM operational modes. PIM dense mode is data-driven and resembles typical multicast routing protocols. Packets are forwarded on all outgoing interfaces until pruning and truncation occurs. In dense mode, receivers are densely populated, and it is assumed that the downstream networks want to receive and will probably use the datagrams that are forwarded to them. The cost of using dense mode is its default flooding behavior. Sometimes called dense mode PIM or PIM DM.

**PIM sparse mode**  
One of the two PIM operational modes. PIM sparse mode tries to constrain data distribution so that a minimal number of routers in the network receive it. Packets are sent only if they are explicitly requested at the RP (rendezvous point). In sparse mode, receivers are widely distributed, and the assumption is that downstream networks will not necessarily use the datagrams that are sent to them. The cost of using sparse mode is its reliance on the periodic refreshing of explicit join messages and its need for RPs. Sometimes called sparse mode PIM or PIM SM.
### Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>policy</td>
<td>Policies include one or more actions that execute sequentially and can be manually activated via the Cisco IPICS administration console or the telephony user interface. Cisco IPICS provides support for multiple policy types.</td>
</tr>
<tr>
<td>policy channel</td>
<td>A channel that can be set up by the dispatcher and configured as a designated channel; that is, a channel that is always open to enable your interaction with the dispatcher.</td>
</tr>
<tr>
<td>policy execution status</td>
<td>An indicator of policy execution success or failure. The Cisco IPICS administration console provides a status for each action under a policy.</td>
</tr>
<tr>
<td>portalization</td>
<td>A web programming paradigm for customizing the interface and functionality of a client application.</td>
</tr>
<tr>
<td>preamble</td>
<td>The sequence of tones that precede a transmission. The preamble generally includes the HLGT and the function tone.</td>
</tr>
<tr>
<td>protocol</td>
<td>A set of unique rules that specify a sequence of actions that are necessary to perform a communications function.</td>
</tr>
<tr>
<td>PTT</td>
<td>Push-to-talk. A signal to a radio transmitter that causes the transmission of radio frequency energy.</td>
</tr>
<tr>
<td>PTT channel</td>
<td>A channel consists of a single unidirectional or bidirectional path for sending and/or receiving signals. In the Cisco IPICS solution, a channel represents one LMR gateway port that maps to a conventional radio physical radio frequency (RF) channel.</td>
</tr>
<tr>
<td>PTT channel button</td>
<td>The button on the IDC that you click with your mouse, or push, and hold to talk. You can use the latch functionality on this button to talk on one or more channels at the same time.</td>
</tr>
<tr>
<td>PTT channel group</td>
<td>A logical grouping of available PTT channels that can be used for categorization.</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of service. A measurement of performance for a transmission system, including transmission quality and service availability.</td>
</tr>
<tr>
<td>queue</td>
<td>Represents a set of items that are arranged in sequence. Queues are used to store events occurring at random times and to service them according to a prescribed discipline that may be fixed or adaptive.</td>
</tr>
<tr>
<td>queuing delay</td>
<td>In a radio communication system, the queuing delay specifies the time between the completion of signaling by the call originator and the arrival of a permission to transmit to the call originator.</td>
</tr>
</tbody>
</table>

### R

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>radio channel</td>
<td>Represents an assigned band of frequencies sufficient for radio communication. The bandwidth of a radio channel depends upon the type of transmission and its frequency tolerance.</td>
</tr>
</tbody>
</table>
**radio control service**  The logical element in the Cisco IPICS system that can tune a radio to the desired channel without manual intervention. Refers to a serial control entity.

**radio equipment**  Any equipment or interconnected system or subsystem of equipment (both transmission and reception) that is used to communicate over a distance by modulating and radiating electromagnetic waves in space without artificial guide. This equipment does not include microwave, satellite, or cellular telephone equipment.

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

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

**RF**  radio frequency. Any frequency within the electromagnetic spectrum that is normally associated with radio wave propagation. RF generally refers to wireless communications with frequencies below 300 GHz.

**RFC 2833**  The Internet Engineering Task Force (IETF) specification that describes how to carry DTMF signaling, other tone signals, and telephony events in RTP packets. Using RFC 2833 a packet can be compactly composed to play a series of tones, including DTMF, in a specific sequence that includes specified durations and volume levels.

**RF repeater**  An analog device that amplifies an input signal regardless of its nature (analog or digital). Also, a digital device that amplifies, reshapes, retimes, or performs a combination of any of these functions on a digital input signal for retransmission.

**RMS**  router media service. Component that enables the IDC to remotely attach to a VTG. It also provides support for remotely attaching (combining) two or more VTGs through its loopback functionality. The RMS mixes multicast channels in support of VTGs and it also mixes IDC SIP-based (unicast) connections to a multicast channel or VTG. The RMS can be installed as a stand-alone component (RMS router) or as an additional feature that is installed in the LMR gateway.

**root user ID**  The Cisco IPICS Linux user that has access to all files in the Cisco IPICS server. Strong passwords are enforced and Linux operating system password expiration rules apply to this user ID.

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

**RTCP**  Real-time Transport Control Protocol. The standard for notifying senders and receivers of important events or transmission statistics. The most common forms of RTCP are the sender report and the receiver report.

**S**

**scanning**  A subscriber unit feature that automatically allows a radio to change channels or talk groups to enable a user to listen to conversations that are occurring on different channels or talk groups.

**script prompts**  The audio prompts that the dial engine scripts play out during execution and that callers hear when they are interacting with the telephony user interface.
secure channel
A channel that is connected to a radio that provides secure (encrypted or scrambled) communications on the Common Air Interface (CAI) side of the radio. (The level of security that is configured in the data network determines the security of the communications between the LMR gateway and a network attached device, such as an IDC or Cisco Unified IP Phone.)

An attribute that is set in the server to indicate that a channel is secure. A PTT channel that is configured as secure cannot be combined with unsecure channels in a VTG.

serial controlled radio
A type of control for a radio that uses out-of-band signaling (usually RS-232). See radio control service.

service delivery area
See coverage.

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

skin
Skins form the appearance of the IDC. In Cisco IPICS, skins are customizable and available in various options, including 4-channel and 8-channel mouse and touch screen formats.

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

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

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

spoken names
The recorded names that are used for entities, such as channels, channel groups, VTGs, users, user groups, ops views, and policies. The names can be recorded through the policy engine or externally-recorded .wav files that can be uploaded into the system.

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

statically configured tone control
Every stream of data that flows to the LMR gateway can be applied with a preamble and/or guard tone by using a static configuration in the LMR gateway. When traffic is sent on a multicast address, the radio automatically switches (because of the preamble) to the specific radio channel that is requested by the tone control sequence.

stored VTG
Also referred to as inactive VTG.

subchannel
A channel that shares the same multicast address as another channel or channels. These multiple source streams (channels) may be present on a single radio channel. On the IDC, you access these channels by pressing the channel selector buttons on the radio channel.

subscriber unit
A mobile or portable radio unit that is used in a radio system.
**system administrator**
The Cisco IPICS system administrator is responsible for installing and setting up Cisco IPICS resources, such as servers, routers, multicast addresses, locations, and PTT channels. The system administrator also creates ops views, manages the Cisco IPICS licenses and IDC versions, and monitors the status of the system and its users via the activity log files.

**system architecture**
The design principles, physical structure, and functional organization of a land mobile radio system. Architectures may include single site, multi-site, simulcast, multicast, or voting receiver systems.

---

**T**

**T1**
Digital WAN carrier facility. T1 transmits DS-1-formatted data at 1.544 Mbps through the telephone-switching network, using alternate mark inversion (AMI) or binary 8 zero suppression (B8ZS) coding.

**T1 loopback**
Allows mapping from multicast to unicast so that unicast phone calls can be patched into an LMR or into other multicast audio streams. A loopback is composed of two of the available T1 interfaces.

**talk group**
A VTG or a channel.

A subgroup of radio users who share a common functional responsibility and, under normal circumstances, only coordinate actions among themselves and do not require radio interface with other subgroups.

**TCP**
Transmission Control Protocol. A connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack.

**TDMA**
time division multiple access. Type of multiplexing where two or more channels of information are transmitted over the same link by allocating a different time interval ("slot" or "slice") for the transmission of each channel; that is, the channels take turns to use the link.

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

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

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

**tone control**
The process of using inband tone sequences to change the behavior of a radio end point. An inband tone can be used to control functions, such as modifying (retuning) the radio frequency (RF channel), changing the transmit power level, and monitoring a channel. The most basic form of tone control (tone keyed) is used to key the radio. With the Cisco IPICS solution, the radio that is being controlled is directly connected to the LMR gateway E&M leads.

**tone frequency**
A specific form of a function tone. The tone that is used to signal the radio to select a frequency. These audible tone frequencies are generated in the router and combined in a specific sequence to perform a tone control function.

**tone keyed**
A tone keyed radio requires the presence of a specific tone on the incoming analog (e-lead) port. Without this tone, the radio cannot transmit. The tone is generally used to prevent spurious transmission that may occur because of injected noise.
tone signaling  Any form of over-the-air audible signals that are intended to terminate at the far end. Examples include alerting tones, DTMF tones, and paging tones.

transmit indicator On the IDC, this indicator blinks red when traffic is being transmitted.

trigger A time-based event that invokes a policy on a scheduled basis, without manual intervention.

trunk A physical and logical connection between two switches across which network traffic travels. In telephony, a trunk is a phone line between two central offices (COs) or between a CO and a PBX.

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

trunked radio system Integrates multiple channel pairs into a single system. When a user wants to transmit a message, the trunked system automatically selects a currently unused channel pair and assigns it to the user, decreasing the probability of having to wait for a free channel.

TUI telephony user interface. The telephony interface that the dial engine provides to enable callers to perform tasks, such as joining talk groups and invoking policies.

tune (a radio) To change the current send and receive frequencies on a radio. This task is usually accomplished via a preset with some form of radio control.

U user The Cisco IPICS user may set up personal login information, download the IDC application, and specify communication preferences that are used to configure audio devices. By using a predefined user ID and profile, the user can participate in PTT channels and VTGs by using the IDC, supported models of Cisco Unified IP Phones, and the Public Switched Telephone Network (PSTN) via the telephony dial functionality of the Cisco IPICS IP policy engine. Users may have one or more Cisco IPICS roles, such as system administrator, ops view administrator, operator or dispatcher.

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

V VAD Voice Activity Detection. When VAD is enabled on a voice port or on a dial peer, only audible speech is transmitted over the network. When VAD is enabled on Cisco IPICS, the IDC only sends voice traffic when it detects your voice.

virtual channel A virtual channel is similar to a channel but a radio system may not be attached. By creating a virtual channel, participants who do not use physical handheld radios to call into a VTG become enabled by using the IDC application or a supported Cisco Unified IP Phone model.

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

voice replay A feature that allows the IDC user to replay buffered audio on a per channel basis.
| **VoIP** | Voice over Internet Protocol. By digitalizing and packetizing voice streams, VoIP provides the capability to carry voice calls over an IP network with POTS-like functionality, reliability, and voice quality. |
| **volume indicator** | The volume indicator on the IDC that shows the current volume level on the channel in a graphical format. |
| **volume up/down buttons** | The buttons on the IDC that let you control the volume level. |
| **VOX** | Voice-operated transmit. A keying relay that is actuated by sound or voice energy above a certain threshold and sensed by a connected acousto-electric transducer. VOX uses voice energy to key a transmitter, eliminating the need for push-to-talk operation. |
| **VTG** | virtual talk group. A VTG can contain any combination of channels, channel groups, users, and user groups. A VTG can also contain other VTGs. |
| **VTG add participant** | An action that adds selected participant(s) to the selected VTG. |
| **W** | 
| **wavelength** | The representation of a signal as a plot of amplitude versus time. |
| **wideband channel** | Channels that occupy more than 20 kHz. |
INDEX

A

Administration Console
  browser guidelines 3-2
  cannot log in 3-3
  cannot log in with ipics user ID 3-15
  cannot perform tasks 3-8
  changes not saved when multiple users are configuring 3-14
  not functioning 3-8

B

browser
  refreshing window 3-10
  troubleshooting access to the server 3-3
  browser guidelines 3-2

C

cablelength router command 4-7
CallManager
  See Cisco Unified CallManager
CallManager Express
  See Cisco Unified CallManager Express
call waiting, dial-in calls disconnect after using 3-25
cannot deactivate
  stopping state, in RMS 4-10
cannot log in to administration console 3-15
catalina.out log file 6-1
changing IP address, troubleshooting problems 3-21
changing system date and time, problems with time-bound licenses 3-21
channel
  choosing codec 4-6
  feedback noise 4-4
  IDC deactivates by itself 4-4
  troubleshooting access to multiple channels 4-2
  troubleshooting multicast address problems 4-2
channels
  connectivity failure indicator 5-8
  visual indicators
    connectivity failure 5-8
characters, language, incorrect display 3-12
checking status of the license manager 2-7
Cisco Instant Connect
  for Android Devices 5-9
  for Windows 5-9
Cisco IPICS
  Activity Log 6-1
  operating system
    See operating system, Cisco IPICS
Cisco IPICS IP
  Policy Engine
    See policy engine
Cisco IPICS service, cannot use after changing server IP address 4-8
Cisco IP Phone
  See Cisco Unified IP Phone
CisconnnMIVR$	ext{n}nnn$.log file 6-2
Cisco Unified IP Phone
  404 or host not found message 4-8
  cannot access Cisco IPICS service 4-8
  cannot communicate with IDCs in a channel 4-8
  no power 4-7
  one-way audio after receiving or placing a phone call 4-8
radio users cannot hear IP phone users 4-4
troubleshooting power problems 4-7
voice quality issues with policy engine dial-in or dial-out calls 4-6

clear counters router command 4-7
clear line router command 4-11
clock source router command 4-7

codec, voice quality and command, server
  enableuser 3-17
  reset_pw 3-15
  service ipics_lm 3-18, 3-19
Command failed error 3-12

communication issue
  IDCs and Cisco Unified IP Phones cannot communicate on a channel 4-8
  some IDCs cannot talk on channel 4-2
  VTG participants cannot hear each other 4-2
communication issue, VTGs and SIP IDCs connectivity, verifying with ping command 3-5
connectivity indicators
  SIP-based remote connections 5-8
controller, limiting number of DS0s 4-10
cslog log file 6-1
database server
  checking status 2-5
  manually starting 3-5
  performing procedures 2-5
  restarting 2-5
  starting 2-6
  stopping 2-5, 2-6
troubleshooting 3-8
db-maintenance.log file, about 6-2, 6-3
deactivating RMS, to edit router details 4-12
deactivation fails for RMS 4-10
debugging
  IDC 6-7
  using log files 6-1
diagnostics.log file 6-3
dial engine
  checking status 2-9
  error after uploading prompt file 3-23
  PARTIAL_SERVICE status 3-30
  performing service procedures 2-9
  restarting 2-10
  starting 2-11
  stopping 2-10
  voice quality problems 4-6
dial-in calls
  disconnect after using hold or call waiting feature 3-25
  do not connect 3-25
  radio users cannot hear dial-in users 4-4
dial-out calls, radio users cannot hear dial-out users 4-4
dial-out invites do not connect 3-28
dial-out notifications do not connect 3-29, 3-30
driverManager.log files 6-3
DS0, limiting number on router 4-10
DSCP 4-5
DSPs, insufficient 4-2
design:
echoes, in conferences 4-14
e-mail, outgoing notifications do not connect 3-29, 3-30
encrypted file system 5-3
error
  authorization after changing ipics user password 3-15
  command failed 3-12
  IDC gets unknown response 3-13
  undefined javascript 3-12

Cisco IPICS Troubleshooting Guide, Release 4.10
feedback
  in conferences  4-14
  on VTG or channel  4-4
finding troubleshooting information  1-1
footswitch, troubleshooting  5-4

G
G.711 codec, voice quality and  4-6
G.729 codec, voice quality and  4-6
G711 codec, voice quality and  4-6
G729 codec, voice quality and  4-6

H
hardware, locating MAC address for  3-18
hold, dial-in calls disconnect after using  3-25
host mismatch error, troubleshooting  3-18, 3-21

I
IDC
  cannot communicate with IP Phones in a channel  4-8
deaactivates channel by itself  4-4
Dialer issues  5-4
log entries  6-4
poor voice quality  4-6
SIP-connected voice communication interrupted  4-6
some cannot communicate on channel  4-2
troubleshooting
  audio settings  5-5
  channel activation issues  5-8
  coexistence  5-6
  configuration file changes  5-4
  DNS issues  5-8
  execution  5-1
footswitch device  5-4
generating an IDC installation log file  5-2
headset  5-5
microphone  5-6
multicast connections  5-7
offline mode  5-7
unknown response error  3-13
using an encrypted file system  5-3
voice quality  5-6
VTG not appearing on  3-10
users are not logged out after terminating session  4-3
using debugging log level  6-7
voice quality degrades for SIP user  4-5
IDC DebugLog.txt  6-6, 6-8
IDC log levels, modifying  6-5
ifconfig command, using to obtain MAC address  3-18
informix user, resetting password  3-8
install.log file  6-3
installation, troubleshooting  3-1
installation log file  5-2
Internet Explorer
  refreshing browser window  3-10
  troubleshooting browser access to the server  3-3
Internet Explorer browser guidelines  3-2
invitations, dial-out invites do not connect  3-28
IP address
  troubleshooting problems after changing  3-21
  verifying Cisco IPICS  3-5
ipics_audit.log file  6-4
ipics_idc.log file  6-4
ipics_rms.log file  6-4
ipics.log file  6-4
ipicsadmin user, resetting password  3-16
ipics-install-log.txt log file  6-4
IP Phone
  See Cisco Unified IP Phone
**J**

javascript error, troubleshooting undefined 3-12

**L**

language characters, incorrect display 3-12
LDAP import issues. 3-6
license
  all features do not display after loading multiple license files 3-20
  locating MAC address 3-18
  troubleshooting after changing IP address 3-21
  troubleshooting installation 3-18, 3-21
  troubleshooting time-bound 3-21
  troubleshooting time-bound license files 3-21
license manager
  checking status 2-7
  restarting 2-8
  starting 2-8
lmgrd.log file 6-5
LMR voice issues 4-7
log files
  catalina.out 6-1
  Cisco IPICS Activity Log 6-1
  CiscoMMIVRnmmn.log 6-2
csalog 6-1
db-maintenance 6-2, 6-3
diagnostics.log 6-3
driverManager.log 6-3
IDC, modifying levels 6-5
install.log 6-3
ipics_audit.log 6-4
ipics_idc.log 6-4
ipics_rms.log 6-4
ipics.log 6-4
ipics-install-log.txt 6-4
lmgrd.log 6-5
tacout 6-5
login, cannot log in after changing password 3-15
loopback, indicator lights for 4-13
low level guard tone (LLGT), E&M port does not transmit after a port deactivation and activation 4-4

**M**

MAC address, obtaining 3-18
Media category, IDC DebugLog.txt 6-6, 6-9
Microsoft QoS Packet Scheduler 4-5
multicast, troubleshooting problems 4-2

**N**

Network Time Protocol (NTP)
  logs 6-5
no prompt router command 4-11
notifications, dial-out notifications do not connect 3-29, 3-30

**O**

one-way audio
  between IDC and Cisco Unified IP Phone 4-8
  with Cisco Unified IP Phone after placing or receiving a phone call
    troubleshooting
      one-way audio problems with Cisco Unified IP phones 4-8
operating system, Cisco IPICS
  checking database status 2-5
  checking tomcat service status 2-2
database procedures 2-5
database server procedures 2-5
restarting database 2-5
starting database 2-6
starting tomcat service 2-3, 2-4
stopping
tomcat service 2-2
tomcat service procedures 2-1
ops views, dial-out notifications do not work between ops views 3-30

P
packets, IP marked incorrectly 4-5
Packet Scheduler, Microsoft QoS 4-5
PARTIAL_SERVICE status
  for dial engine 3-30
  for subsystem manager 3-30
password
  changing, for root user 3-16
  resetting
    for informix user 3-16
    for ipicsadmin user 3-16
    for ipics user 3-15
PIM, sparse and sparse-dense modes 4-2
ping command, using to verify Cisco IPICS IP address 3-5
pins, mapping for a T1 on router 4-14
PoE module 4-7
policy, VTG not activating in policy engine
  cannot communicate with the prompt manager 3-25
  checking dial engine status 2-9
  log files 6-2
  performing dial engine service procedures 2-9
  restarting dial engine 2-10
  starting the dial engine 2-11
  stopping dial engine 2-10
  voice quality problems from dial engine 4-6
prompt file, error after uploading 3-23
prompt manager error messages 3-25

Q
QoS, Microsoft Packet Scheduler 4-5
R
radio
  low level guard tone not sent after E&M port deactivation and activation 4-4
  trunked 4-9
  users in channel cannot hear Cisco Unified IP Phone or policy engine users 4-4
recovering a deleted user with system administrator privileges 3-14
refreshing browser window 3-10
reporter 3-15
restarting
  database 2-5
  dial engine 2-10
  license manager 2-8
restore, IDC gets error after 3-13
RMS 4-10
  configuration, long wait after restarting Cisco IPICS 4-10
  deactivating 4-12
  failing 4-11
  limiting DS0s on router 4-10
  log entries 6-4
  no loopbacks displayed on new 4-12
  SIP-based connectivity 5-8
  unrecognized T1 ports 4-12
  updating login information causes unreachable state 4-12
router
  clear line command 4-11
  configuration shows wrong information 4-14
  insufficient DSPs on 4-2
  IOS software version 4-7
  long delays between pressing IDC PTT button and media establishment 4-15
  long wait for restart after configuring 4-10
  mapping pins for T1 4-14
  no green indicator lights 4-13
  no loopbacks displayed on new RMS 4-12
  no prompt command 4-11
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIM modes</td>
<td>4-2</td>
</tr>
<tr>
<td>PoE module</td>
<td>4-7</td>
</tr>
<tr>
<td>show users command</td>
<td>4-11</td>
</tr>
<tr>
<td>slow VTG activation</td>
<td>4-11</td>
</tr>
<tr>
<td>T1 configuration</td>
<td>4-7</td>
</tr>
<tr>
<td>unreachable state</td>
<td>4-11, 4-12</td>
</tr>
<tr>
<td>updating configuration in Cisco IPICS</td>
<td>4-14</td>
</tr>
<tr>
<td>VTY lines</td>
<td>4-11</td>
</tr>
<tr>
<td>router media service</td>
<td></td>
</tr>
<tr>
<td>See RMS</td>
<td></td>
</tr>
</tbody>
</table>

**Index**

**T**

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1</td>
<td></td>
</tr>
<tr>
<td>configuration</td>
<td>4-7</td>
</tr>
<tr>
<td>loopbacks not displayed on new RMS</td>
<td>4-12</td>
</tr>
<tr>
<td>mapping pins on router</td>
<td>4-14</td>
</tr>
<tr>
<td>unrecognized ports</td>
<td>4-12</td>
</tr>
<tr>
<td>tacout log file</td>
<td>6-5</td>
</tr>
<tr>
<td>time-bound license, troubleshooting</td>
<td>3-21</td>
</tr>
<tr>
<td>tomcat service</td>
<td></td>
</tr>
<tr>
<td>checking status</td>
<td>2-2, 3-3</td>
</tr>
<tr>
<td>performing procedures</td>
<td>2-1</td>
</tr>
<tr>
<td>restarting</td>
<td>3-4, 3-14</td>
</tr>
<tr>
<td>starting</td>
<td>2-3, 2-4</td>
</tr>
<tr>
<td>stopping</td>
<td>2-2</td>
</tr>
<tr>
<td>tomcat service, stopping</td>
<td>2-2</td>
</tr>
</tbody>
</table>

**Troubleshooting**

- Administration Console not functioning: 3-8
- authorization error after changing password: 3-15
- cannot reach server from browser: 3-3
- Command failed error: 3-12
- communication disrupted: 4-6
- configuration changes not saved when multiple users configuring: 3-14
- connectivity between Cisco Unified Wireless IP Phone 7920 models: 4-9
- database stopped: 3-8
- dial engine: 3-30
- dial engine voice quality: 4-6
- dial-in call cannot reconnect after using call waiting feature: 3-25
- dial-in call disconnects after placing on hold: 3-25
- dial-in calls: 3-25
- dial-out invites: 3-28
- dial-out notifications: 3-29, 3-30
- displaying loopbacks in Add Router window: 4-12

**S**

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>security certificate issues</td>
<td>3-15</td>
</tr>
<tr>
<td>server, database</td>
<td></td>
</tr>
<tr>
<td>checking status</td>
<td>2-5</td>
</tr>
<tr>
<td>manually starting</td>
<td>3-5</td>
</tr>
<tr>
<td>restarting</td>
<td>2-5</td>
</tr>
<tr>
<td>starting</td>
<td>2-6</td>
</tr>
<tr>
<td>stopping</td>
<td>2-5, 2-6</td>
</tr>
<tr>
<td>service ipics_lm command</td>
<td>3-18, 3-19</td>
</tr>
<tr>
<td>Show Configuration feature</td>
<td>4-14</td>
</tr>
<tr>
<td>show users router command</td>
<td>4-11</td>
</tr>
<tr>
<td>SHUTDOWN status, for SIP subsystem</td>
<td>3-30</td>
</tr>
<tr>
<td>Signaling category, IDC DebugLog.txt</td>
<td>6-6, 6-8</td>
</tr>
<tr>
<td>SIP-based connection failure</td>
<td>5-8</td>
</tr>
<tr>
<td>SIP subsystem SHUTDOWN status</td>
<td>3-30</td>
</tr>
<tr>
<td>spoken name prompt file, error after uploading</td>
<td>3-23</td>
</tr>
<tr>
<td>starting</td>
<td></td>
</tr>
<tr>
<td>dial engine</td>
<td>2-11</td>
</tr>
<tr>
<td>starting database server</td>
<td>2-6</td>
</tr>
<tr>
<td>starting the license manager</td>
<td>2-8</td>
</tr>
<tr>
<td>starting tomcat service</td>
<td>2-3, 2-4</td>
</tr>
<tr>
<td>status</td>
<td></td>
</tr>
<tr>
<td>checking database server</td>
<td>2-5</td>
</tr>
<tr>
<td>checking tomcat service</td>
<td>2-2</td>
</tr>
<tr>
<td>stopping</td>
<td></td>
</tr>
<tr>
<td>database server</td>
<td>2-5, 2-6</td>
</tr>
<tr>
<td>dial engine</td>
<td>2-10</td>
</tr>
<tr>
<td>stopping tomcat service</td>
<td>2-2</td>
</tr>
<tr>
<td>subsystem manager, PARTIAL_SERVICE status</td>
<td>3-30</td>
</tr>
<tr>
<td>system administrator user, recovering a deleted user</td>
<td>3-14</td>
</tr>
</tbody>
</table>

---

See RMS
feedback noise on VTG, channel 4-4
host mismatch error 3-18, 3-21
IDC deactivates channel by itself 4-4
IDCs cannot communicate on channel 4-2
IDC users not logged out after terminating session 4-3
installation issues 3-1
language characters display incorrectly 3-12
license installation 3-18, 3-21
login problems from browser 3-3
multicast problems 4-2
new RMS has no loopbacks 4-12
no green lights on router 4-13
non-activating policy 3-10
no power to Cisco Unified IP Phones 4-7
no table data 3-12
password problems, ipicsadmin or informix user 3-16
password problems for ipics user 3-15
password problems for root user 3-16
policy engine voice quality 4-6
poor IDC voice quality 4-6
poor voice quality for SIP-based IDC 4-5
power for Cisco Unified IP Phones 4-7
RMS fails 4-11
router configuration long delays between pressing IDC PTT button and media establishment 4-15
router configuration shows wrong information 4-14
SIP subsystem 3-30
slow VTG activation 4-11
subsystem manager 3-30
time-bound licenses 3-21
tomcat service not running 3-3
undefined javascript error 3-12
unreachable RMS state after updating login 4-12
unreachable router state 4-11
unresponsive IDC channel 4-2
using log files 6-1
voice loops in conferences 4-14
VTG activating itself 3-9
VTG feedback 4-4
VTG not appearing on IDC 3-10
VTG participants cannot communicate 4-2
trunked radio 4-9
unreachable state on router 4-11, 4-12
Update Configuration feature 4-14
user ID, multiple IDs for same user 3-10
user interface, IDC debug log information 6-6, 6-8
voice LMR issues 4-7
loops 4-14
poor quality
from policy engine dial-in or dial-out calls 4-6
on IDC 4-6
quality issues 5-6
voice, poor quality with dial engine calls 4-6
VTG activates by itself 3-9
feedback noise 4-4
not activating in policy 3-10
not appearing on IDC 3-10
participants cannot hear each other 4-2
slow activation 4-11
voice interruptions 4-6
VTY lines 4-11