Release Notes for Cisco IPICS Release 1.0(2)

June 1, 2006

These release notes describe the new features and caveats for the Cisco IP Interoperability and Collaboration System (hereafter referred to as Cisco IPICS) and the Push-to-Talk Management Center (hereafter referred to as PMC) release 1.0(2).

Note To view the release notes for Cisco IPICS, go to: http://www.cisco.com/univercd/cc/td/doc/product/cis/c_ipics/index.htm

Before you install Cisco IPICS, Cisco recommends that you review the "Important Notes" section on page 43 for information about issues that may affect your system.

For a list of the open and resolved caveats for Cisco IPICS release 1.0(2), see the "Resolved Caveats for Cisco IPICS - Release 1.0(2)" section on page 58 and the "Open Caveats for Cisco IPICS - Release 1.0(2)" section on page 62. Updates for these release notes occur with every maintenance release and major release.

To access the documentation suite for interoperability systems products, refer to the following URL:

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

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

You can access the latest software upgrades for all versions of Cisco IPICS on Cisco Connection Online (CCO) at the following URL:

http://www.cisco.com/cgi-bin/tablebuild.pl/ipics

Contents

These release notes discuss the following topics:

Introduction

This section provides an introduction to the Cisco IPICS product. It includes the following topics:

Overview

Cisco IPICS provides a high-quality IP standards-based solution that enables voice interoperability among disparate systems. The Cisco IPICS solution interconnects voice channels, talk groups, and virtual talk groups (VTGs) to bridge communications from radio networks to IP networks and devices, such as the Cisco IPICS Push-to-Talk Management Center (PMC) PC application, and supported models of the Cisco Unified IP Phone.

To provide this functionality, Cisco IPICS uses components, such as the Cisco IPICS server and the PMC. It also incorporates existing technologies, such as Land Mobile Radio (LMR), Cisco gateways, and Voice over IP (VoIP) technology, along with new applications of existing technologies, such as the use of the router media services (RMS) functionality for channel mixing.

As part of the Cisco IPICS solution, the server includes the Administration Console, which is an incident management framework graphical user interface (GUI). The Administration Console facilitates the tasks that are associated with operations and command and control. By extending the reach of push-to-talk (PTT) voice technology from the LMR environment to the IP network, Cisco IPICS enables rapid deployment and management of disparate audio communications systems.

The PMC application provides the interface for users to host push-to-talk audio communications. By using a simplified GUI, the PMC allows simultaneous monitoring and participation in one or more talk groups or VTGs at the same time.

The PMC includes buttons that allow you to interact with the Cisco IPICS server. Click with your mouse, or push, the PTT channel button and hold it to talk. When you are done talking, release the mouse button to return to listen-only mode. Other buttons on the GUI activate and deactivate the channel and control the volume level. The PMC also includes indicators that blink when you receive and transmit traffic and indicators to display the volume levels.

Because the Cisco IPICS server controls the configuration of the PMC application, PMC users have limited access to the configuration parameters; however, Cisco IPICS includes the ability for PMC users to customize the PMC GUI skins for mouse-based or touch screen-based display.

Where to Find More Information

- *Cisco IPICS Server Administration Guide, Release 1.0(1)*
- *Cisco IPICS PMC Installation and User Guide, Release 1.0(1)*

Cisco IPICS Components

The Cisco IPICS solution comprises the following major components, as described in Table 1:

Table 1 Cisco IPICS System Components

Component	Description
Cisco IPICS Server	This component provides the core functionality of the Cisco IPICS system. The Cisco IPICS server software runs on the Cisco Linux operating system (based on Red Hat Linux) on selected Cisco Media Convergence Server (MCS) platforms. (Refer to the Cisco 7800 Series Media Convergence Servers data sheets, or contact your Cisco representative, for information about the servers that Cisco IPICS supports.) The Cisco IPICS server software includes the Cisco IPICS Administration Console, which is an incident management framework administration GUI that enables dynamic resource management for users, channels, and VTGs. (In Cisco IPICS, VTGs combine one or more channels and/or users.) By using this GUI, authorized Cisco IPICS users can manage the system configuration and authentication and security services, policies and privileges, and database information. In addition, the server enables control of the configuration of the media resources that are installed in the router and which are used for audio mixing capabilities. Cisco IPICS supports several different user roles. For more information, see the "User Roles" section on page 5.
Push-to-Talk Management Center (PMC)	The PMC is a PC-based software application that comprises a stand-alone LMR PTT audio application that connects end-users, dispatch personnel, and administrators via an IP network. By using a simplified GUI, the PMC allows simultaneous monitoring and participation in one or more talk groups or VTGs at the same time. (VTGs are the voice channels that users attach to based on specific incidents.) PMC users may customize the appearance of the PMC user interface by choosing another Cisco-provided or custom skin. The PMC runs on the Microsoft Windows 2000 and Windows XP operating system. For more information about hardware and software requirements, see the "System Requirements" section on page 7.

Table 1 Cisco IPICS System Components (Continued)

Component	Description
Gateways	This 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.
Router Media Service	The Router Media Service (RMS) component enables the PMC to remotely attach to a VTG. It also provides support for remotely attaching (combining) two or more VTGs through its loopback functionality. The RMS provides support for mixing multicast channels in support of VTGs and for mixing remote PMC SIP-based (unicast) connections to a multicast channel or VTG. The RMS can be installed as a stand-alone component (RMS router) or as an additional feature that is installed in the LMR gateway.
Networking Components	The Cisco IPICS solution may include some of all of the following network components, depending on the functionality that you require: routers, switches, firewalls, mobile access routers, and wireless access points, and bridges.
Cisco Unified CallManager and VoIP Services	Cisco Unified CallManager functionality and VoIP services, such as the Cisco Unified IP Phone services, help to extend the reach of PTT technology to the IP network. The Cisco Unified IP Phone services allow participation in VTGs through the use of the Cisco Unified IP Phone 7960, Cisco Unified IP Phone 7970, and Cisco Unified Wireless IP Phone 7920 by enabling these phones to work with Cisco IPICS as IP phone multicast client devices.

Where to Find More Information

- *Cisco IPICS Server Administration Guide, Release 1.0(1)*
- *Cisco IPICS PMC Installation and User Guide, Release 1.0(1)*

User Roles

The Cisco IPICS solution authorizes access to different features based on the role that is assigned to each user. Cisco IPICS users may have one or more roles, including system administrator, operator, dispatcher, and user.

Table 2 describes the user roles that Cisco IPICS supports.

Table 2 Cisco IPICS User Roles

User Role	Description
System Administrator	The system administrator is responsible for installing, upgrading, and setting up Cisco IPICS resources, such as servers, routers, multicast addresses, locations, and PTT channels. The system administrator also creates ops views, manages the Cisco IPICS licenses and PMC versions, and monitors the status of the system and its users via the activity log files. For more information, refer to the *Cisco IPICS Server Administration Guide* and the *Cisco IPICS Server Installation Guide.*
Operator	The operator is responsible for setting up and managing users and policies, configuring access privileges, and assigning user roles and ops views. For more information, refer to the *Cisco IPICS Server Administration Guide*.
Dispatcher	The dispatcher is responsible for setting up the VTG templates, activating the VTGs to begin conferences, and adding and/or removing participants in VTG templates and active VTGs. The dispatcher also monitors the active VTGs and events, can mute and unmute PMC users, as necessary, and sets up system policies. For more information, refer to the *Cisco IPICS Server Administration Guide*.
User	The Cisco IPICS user may set up personal login information, download the PMC application, customize the PMC skin, and specify communication preferences that are used to configure audio devices. By using a predefined user ID and profile, the user can participate in PTT channels and VTGs by using the PMC or a supported Cisco Unified IP Phone model. For more information, refer to the *Cisco IPICS PMC Installation and User Guide.*

Where to Find More Information

- *Cisco IPICS PMC Installation and User Guide, Release 1.0(1)*
- *Cisco IPICS Server Administration Guide, Release 1.0(1)*
- *Cisco IPICS Server Installation Guide, Release 1.0(1)*

Cisco IPICS Support Team Communications

The Cisco IPICS Support Team provides an external mailing list that you can use to obtain additional support directly from the Cisco IPICS engineering team. To subscribe to this mailing list, create an email that includes "subscribe" in the subject line; then, send the email to the following address:

ask-ipics-support@external.cisco.com

Whenever you need additional support, or if you have questions about Cisco IPICS, send your request to ask-ipics-support@external.cisco.com.

A Cisco IPICS engineer will respond to your email to provide you with the assistance that you need.

System Requirements

This section contains information about systems requirements for the Cisco IPICS server and PMC components; it includes the following sections:

- Server Requirements, page 7
- PMC Requirements, page 9

Server Requirements

The Cisco IPICS server requires the following minimum versions of hardware and software:

Hardware

For a list of supported MCS servers and Cisco routers that you can use with Cisco IPICS, refer to the Cisco IPICS Compatibility Matrix at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/cis/c_ipics/index.htm

Note Make sure that you install and configure Cisco IPICS release 1.0(2) on a supported Cisco Media Convergence Server (MCS).

Software

- Cisco IPICS operating system, version 1.0(2), which includes Red Hat Enterprise Linux AS release 3 (Taroon Update 6); kernel version, 2.4.21-37.ELsmp

Note You must use only the Cisco-supported operating system for use with Cisco IPICS. No other operating system versions are supported.

- Cisco IPICS server software, version 1.0(2)

  The Cisco IPICS server software includes the following components:

  - Cisco IPICS Administration Console (Cisco IPICS, version 1.0(2))
  - Cisco IPICS Web Application Server (Tomcat Server, version 5.5)
  - Cisco IPICS Data Store (IBM Informix Dynamic Server, version 10.00.UC3W5)
  - Cisco Security Agent, version 4.5.1.639

- Cisco IOS release 12.4T (for use on the gateway router)

This release of Cisco IPICS requires the following minimum versions of Cisco Unified CallManager and Cisco Unified IP Phone firmware:

- Cisco Unified CallManager, version 4.1(2)
- Cisco Unified Wireless IP Phone 7920, Engineering Special (ES) cmterm_7920.4.0-03-00-ENG01.bin

Note The Cisco Unified Wireless IP Phone 7920 ES cmterm_7920.4.0-03-00-ENG01.bin is not available on CCO. For information about how to obtain a copy of this firmware, send an email to ask-ipics-support@external.cisco.com.

- Cisco Unified IP Phone 7960, Cisco Unified IP Phone 7960, SCCP version 8.0(2)

- Cisco Unified IP Phone 7970, SCCP version 8.0(2)SR1

Where to Find More Information

- *Cisco IPICS Server Installation Guide, Release 1.0(1)*

PMC Requirements

The following sections detail the minimum hardware and software requirements that Cisco IPICS supports for use with the PMC:

- PMC Hardware, page 9
- PMC Software, page 10

PMC Hardware

Table 3 shows the PMC minimum hardware requirements that Cisco IPICS supports. These requirements are dependent on the number of PMC channels that you use.

Table 3 PMC Minimum Hardware Requirements

Number of PMC Channels	PMC Hardware Requirements
4-Channel PMC	• 800 MHz Pentium III class, including Mobile Pentium • 256 MB RAM • 16 MB free space • Network interface card

Table 3 PMC Minimum Hardware Requirements (Continued)

Number of PMC Channels	PMC Hardware Requirements
8-Channel PMC	• 1.5 GHz Pentium IV class, including Mobile Pentium • 512 MB RAM • 16 MB free space • Network interface card
18-Channel PMC	• 3.2 GHz Pentium IV class, including Mobile Pentium • 1 GB RAM • 16 MB free space • Network interface card

Note The Cisco IPICS system allows you to turn on or turn off logging for individual PMC log files and set the debug log levels. To use the logging functionality, Cisco IPICS requires sufficient free disk space on the PMC client machine; that is, when the PMC detects that only 100 MB of disk space is available on the PMC client machine, it displays a warning message to alert you, and when the PMC detects only 50 MB of free disk space, it stops logging data to the log files.

Caution Because of the large amount of information that the system collects and generates when you set all of the debug options, Cisco recommends that you use debug logging only to isolate specific problems. When your debugging tasks have been completed, be sure to turn off debug logging by clearing the debug log. For more information, refer to the "Using the PMC Application Logs" chapter in the *Cisco IPICS PMC Installation and User Guide*.

PMC Software

Cisco IPICS supports the following operating system software for use with the PMC:

- Windows 2000 Professional SP4

- Windows XP Professional SP2

Note Make sure that you install the PMC application on a PC that has the required Windows operating system installed.

Where to Find More Information

- *Cisco IPICS PMC Installation and User Guide, Release 1.0(1)*

Determining the Software Version

The current version of the Cisco IPICS server software displays in the upper left corner of the Administration Console.

To find the version information for the PMC application, position your cursor so that it is located inside the PMC window; then right-click inside this window. Click **About.** The version information for your PMC application displays in a pop-up dialog box.

Compatibility Matrix

You can find the list of the hardware and software versions which are compatible with Cisco IPICS release 1.0(2) by referring to the *Cisco IPICS Compatibility Matrix* at the following URL:

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

Note Make sure that you check the Cisco IPICS Compatibility Matrix for the most current versions of compatible hardware components and software versions for use with Cisco IPICS.

Related Documentation

Refer to the *Cisco IPICS 1.0(2) Resources Card* for a list of documents that are related to Cisco IPICS release 1.0(2). You can access this document at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/cis/c_ipics/1_0/index.htm

New and Changed Information

The following sections describe the new features that are available and pertinent to this release of Cisco IPICS. These sections may include configuration tips for the administrator, information about users, and where to find more information.

Server Installation, Upgrade, and Backup Guidelines

This section contains information about the guidelines that apply to Cisco IPICS release 1.0(2) server installation, upgrade, and backup and restore procedures; it includes the following topics:

As a best practice, make sure that you adhere to the following guidelines when you perform Cisco IPICS server installation or backup and restore procedures:

- If your server includes more than one network interface card (NIC), make sure that you configure the eth0 port, as documented in the *Cisco IPICS Server Installation Guide.* Cisco IPICS requires that you configure the eth0 port, even if it is disabled, because the Cisco IPICS licensing mechanism performs its validation by using this NIC. Therefore, to ensure proper system operation, always configure the eth0 port.
- Make sure that you only perform system date changes before you install the Cisco IPICS software. Cisco IPICS does not support any modification of the system date in the operating system after the Cisco IPICS software has been installed. If the system date is not properly set to your local date and time, you must adjust it before you install the Cisco IPICS software. If you try to change the system date and time after you install the software, you will invalidate your license and cause the system to become inoperable.
- Always log in to the Cisco IPICS server with root user privileges before you begin the server installation or uninstallation process.
- Cisco recommends that you perform server installation tasks during a maintenance window or other off-peak hours to minimize service interruptions to users.
- The server installation process requires that you use the applicable Cisco IPICS operating system that relates to the version of software that you are installing.

Note You must use only the Cisco-supported operating system for use with Cisco IPICS. No other operating system versions are supported.

- The Cisco IPICS installation requires a minimum of 2 GB of memory on the Cisco IPICS server. You can check the amount of memory that is installed on your server by entering the following command from the root user account:

  [root] **#top**

  The amount of memory that is installed on the server displays as shown in the example below:

  ```
  Mem:  2055448k av, 1490160k used,  565288k free, 0k shrd,  142344k
  buff
  ```

To exit, press **Ctrl-C**.

- By default, the Cisco IPICS server boots up in run level 5 (GUI format); you may use run level 3 (console mode) to access the command-line interface. Cisco IPICS provides support for the following run levels (or operating modes):
  - Run Level 5— This is the default mode for the server; this run level displays the GUI format in Xwindows.

    To open a window in GUI mode, navigate to **Start > System Tools > Terminal**. If the terminal window does not open up (such as after an IP address change), restart the server.
  - Run Level 3—Use this run level to access the command-line interface (console format). To change the format from GUI mode to console mode, log in to the server by using the root user account and password; then, enter the following command:

    [root] **#init 3**
  - Run Level 0—Run level 0 specifies the system halt condition. Use this run level to shut down (power off) the system by entering the following command:

    [root] **#init 0**
  - Run Level 1—This run level boots up the server in safe mode to aid your troubleshooting efforts. (In run level 1, no daemons (services) are started.) Use this run level to boot up the server in safe mode by entering the following command:

    [root] **#init 1**
  - Run Level 6—Use run level 6 to restart the system by entering the following command:

    [root] **#init 6**
- You can execute the installation bin file when the system is in the default GUI mode (run level 5) with the Xwindows service running on it. (You must be physically connected to the system to perform the installation in GUI mode.) Alternatively, you can run the installation file by using console mode (run level 3) or by remotely accessing the system via SSH Secure Shell client software (or similar software).
- The Cisco IPICS server supports the following installation options:

  - Typical—This option installs the Cisco IPICS server software and the Cisco Security Agent (CSA) software.
  - Customize—This option allows you to customize your installation by providing you with the option to not install CSA as part of the Cisco IPICS server software installation. The default specifies "Install CSA."

    If you choose not to install CSA during the server installation process, you can install CSA at a later time. For more information about installing CSA manually, see the "Manually Installing CSA on the Server" section on page 16.

- After you install the server software, make sure that you generate the PMC installer so that the installation file is associated with the correct server IP address. To generate the PMC installer, log in to the Administration Console; then, navigate to **System Administrator > PMC Installer** to access the PMC Installer window. From this window, you can generate a new PMC installation file.

Note The Cisco IPICS server software includes the PMC application. You need to generate the PMC installer after the first time that you install the server software and after subsequent PMC application updates that include software fixes.

- The system enables access to a GUI-based database management link from the Administration Console. Access this window by navigating to **System Administrator > Database**; then, click the **Database** link to perform database backup and restore operations. For information about enhancements to the backup and restore processes, see the "Backup and Restore Updates" section on page 36.
  - Cisco IPICS backup and restore functionality supports full system backups and logical log file backups.
  - By default, the server runs a daily automatic backup at a preconfigured time; you may also run a manual backup at any time.
  - You can choose among the following choices to restore your data—default, local directory, or remote host destinations.

When you restore your data by using any of the available destinations, Cisco IPICS restores your data up to the specific point in time that the backup was taken.

Note To help ensure the security of your data, Cisco IPICS does not support the use of different user IDs for backup and restore operations that you perform on the same data set. Therefore, when you restore your data, make sure that you specify the same user ID as the one that you used to back up your data. If you specify a different user ID, the restore procedure does not succeed because of file accessibility issues; in this situation, Cisco IPICS displays "permission denied" error messages in the db-maintenance.log. As a best practice, Cisco recommends that you designate a specific user ID that you can use for all of your backup and restore activities.

Manually Installing CSA on the Server

If you did not install CSA at the time of the Cisco IPICS server software installation, you can perform the CSA installation manually at any time. To manually install CSA on the server, perform the following procedure:

Note You can execute the following commands from a terminal window when the system is in the default GUI mode (run level 5) with the Xwindows service running on it. Or, you can execute these commands by using console mode (run level 3).

Procedure

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

Step 2 Log in to the server by using the root user account and password.

Step 3 From GUI mode, open a command window by navigating to **Start > System Tools > Terminal**.

Step 4 Install the Linux kernel source package by entering the following command:

[root] **#rpm -Uv kernel-source-2.4.21-32.0.1.EL.i386.rpm**

Step 5 Change the directory to the /tmp directory by entering the following command:

[root] **#cd /tmp**

Step 6 Enter the following command to untar the CSAStandAlone.tar file and place the extracted copy in the /tmp/CSCOcsa folder:

[root tmp] **#tar xvf /root/CSAStandAlone.tar**

Step 7 Change the directory to the /CSCOcsa directory by entering the following command:

[root tmp] **#cd CSCOcsa**

Step 8 To install the CSA software, enter the following command:

[root CSCOcsa] **#sh install_rpm.sh**

Step 9 Enter the following command to restart the server and complete the installation:

[root] **#init 6**

Installing Third Party Certificates On the Cisco IPICS Server

The Cisco IPICS server ships with a self-signed certificate. However, you may replace this certificate with a customer-specific, third party certificate that has been issued by a Certificate Authority (CA). A CA, as a trusted third party, issues and manages digital certificates that provide enhanced security by verifying the credentials of the user, organization, server, or other entity as specified in the certificate. VeriSign, Thawte, and Entrust are examples of CAs.

The following topics include information about requesting a third party certificate and installing the certificate on the Cisco IPICS server:

- Requesting a Third Party Certificate, page 17
- Installing a Third Party Certificate, page 20

Requesting a Third Party Certificate

To request a third party certificate, perform the following procedure:

Procedure

Step 1 Log in to the Cisco IPICS server by using the root user account and password.

The Cisco Linux desktop displays.

Step 2 Copy the tomcat.keystore file to the /root directory by entering the following command:

[root] **#cp /root/tomcat/current/conf/tomcat.keystore /root**

The tomcat.keystore file maintains all of the certificates for the server.

Step 3 Change to the /root/tomcat/current/conf/ directory by entering the following command:

[root] **#cd /root/tomcat/current/conf/**

Step 4 Execute the following command to delete the existing entry:

[root@ipics-server] **#keytool -delete -alias tomcat -keystore tomcat.keystore**

Step 5 When the system prompts you to enter the keystore password, enter the default password, **changeit**.

Step 6 Execute the following command to generate the new key that will be used for the Certificate Signing Request (CSR):

[root@ipics-server] **#keytool -genkey -alias tomcat -keyalg RSA -keystore tomcat.keystore -validity 360**

The validity may vary based on the number of days that the certificate needs to be valid.

Note Make sure that you enter the correct information so that the CA generates a valid certificate for your system.

Step 7 Enter your responses to the following system prompts:

```
Enter keystore password:
What is your first and last name?
What is the name of your organizational unit?
What is the name of your organization?
What is the name of your City or Locality?
What is the name of your State or Province?
What is the two-letter country code for this unit?
```

Note The information that you enter may vary depending on the CA that you use. For example, for the first and last name response, VeriSign requires that you enter the fully-qualified hostname of your Cisco IPICS server in the format of server.domain.com. For the name of your state or province, VeriSign requires that you spell out the complete name in lieu of using the abbreviated form.

Tip The default keystore password is **changeit**.

The following is an example of the information that the system displays:

```
Is CN=username, OU=user company name, O=user company name, L=user
city, ST=user state, C=user country correct? [no]:
```

Step 8 Enter **y** or **yes** if the information is correct.

Step 9 When the system displays the following message, press **Enter** to accept the default password:

```
Enter key password for <tomcat>
(RETURN if same as keystore password):
```

where <*tomcat*> is the default alias for the certificate

Note The system requires that you use the same value for the key password and the keystore password. If you enter different passwords, the Tomcat server will not be able to successfully restart. (When these passwords are the same, the system does not prompt you again for the key password.)

Step 10 Execute the following command to create the CSR file:

[root@ipics-server] **#keytool -certreq -alias tomcat -keyalg RSA -file certrequest.csr -keystore tomcat.keystore**

Step 11 When the system prompts you to enter the keystore password, enter the default value of **changeit**:

```
Enter keystore password:
```

Upon entry of the correct password, the system creates the CSR. (If you enter an incorrect password, the system displays an error.)

Note You need to use the text from this CSR file when you request the certificate. See Step 12.

Step 12 Copy the **certrequest.csr** file to your local workstation.

Depending on the CA that you use, you may need to copy and paste the contents of the certrequest.csr file into your browser or you may need to upload the CSR file to request the certificate.

Note If the CA does not accept your certificate request, repeat this procedure from Step 3 to regenerate your certificate request with the necessary modifications.

Step 13 After you receive the certificate from the CA, continue with the procedure in the "Installing a Third Party Certificate" section on page 20 to install the third party certificate.

Installing a Third Party Certificate

To install a third party certificate on the server, perform the following procedure:

Procedure

Step 1 Depending on the format in which you receive the certificate, take one of the following actions:

- If you receive the certificate file directly from the CA, rename the file to **thirdparty.cer**
- If you receive the certificate enclosed in an email, create a new file named **thirdparty.cer** (this file must contain only the certificate contents of the email)

CAs may use different procedures to send root CA certificates. Some CAs embed the root CA certificate into the certificate that they provide to you; other CAs provide the root CA certificate separately. (The root CA certificate allows you to establish a chain of trust from the CA to the third party certificate on your server.)

Step 2 Depending on the format in which the CA provides the root CA certificate, take one of the following optional actions:

- If you download the root CA certificate file directly from the CA website, rename the file to **thirdpartyca.cer**
- If the CA provides the root CA certificate enclosed in a web page, create a new file named **thirdpartyca.cer** (this file must contain only the root CA certificate contents of the web page)

Step 3 Copy the **thirdparty.cer** file (and the optional **thirdpartyca.cer** file) from the local workstation to the /root/tomcat/current/conf/ directory on the server by using Secure FTP.

Step 4 Enter the following command to verify that you are still in the /root/tomcat/current/conf/ directory:

[root] **#cd /root/tomcat/current/conf/**

Step 5 If you received a separate root CA certificate, install it first by executing the following command:

[root@ipics-server] **#keytool -import -alias thirdpartyca -keystore tomcat.keystore -trustcacerts -file thirdpartyca.cer**

Step 6 When the system prompts you to enter the keystore password, enter **changeit**.

Step 7 Enter **yes** to trust the certificate when the system displays the following prompt:

```
Trust this certificate? [no]:
```

The certificate installs and the following message displays:

```
Certificate was added to keystore
```

Step 8 To install the certificate, execute the following command:

[root@ipics-server] **#keytool -import -alias tomcat -keystore tomcat.keystore -trustcacerts -file thirdparty.cer**

Step 9 When the system prompts you to enter the keystore password, enter **changeit**.

The following error message displays if you did not install the root CA certificate (and it was required):

```
keytool error: java.lang.Exception: Failed to establish chain from
reply
```

If you encounter this error, contact the CA to locate the root CA certificate; then, repeat this procedure from Step 5.

Step 10 Enter **yes** to trust the certificate when the system displays the following prompt:

```
Trust this certificate? [no]:
```

The certificate installs and the following message displays:

```
Certificate reply was installed in keystore
```

Step 11 From root, enter the following command to restart the Tomcat web server:

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

Step 12 Verify that the certificate has been installed by executing the following command.

[root@ipics-server] **#keytool -list -keystore tomcat.keystore**

Step 13 When the system prompts you to enter the keystore password, enter the default value of **changeit**.

The system displays the certificate information, as shown in the following example:

```
Keystore type: jks
Keystore provider: SUN
Your keystore contains 1 entries
Tomcat, May 12, 2006, keyEntry,
Certificate fingerprint (MD5):
88:88:1A:34:38:0A:27:6F:B9:87:CA:8F:36:66:C4:73
```

If you installed the root CA certificate, the system display indicates that the keystore contains two entries, as shown in the following example:

```
Your keystore contains 2 entries
thirdpartyca, May 20, 2006, trustedCertEntry,
Certificate fingerprint (MD5):
B6:9D:A4:40:52:02:50:0D:D5:9C:E1:B8:4B:66:C4:AC
...
```

Note The finger print may vary based on your system.

Where to Find More Information

- *Cisco IPICS Server Installation Guide, Release 1.0(1)*
- *Cisco IPICS Backup and Restore Guide, Release 1.0(1)*

Server Enhancement to the Auto Update Feature for the PMC

Cisco IPICS simplifies the PMC auto update process by providing the ability for you to maintain automatic updates for the PMC without the need to first generate the PMC and then upload the PMC.dll file to the server.

With this enhancement, Cisco IPICS now adds the PMC.dll file as part of the server installation file and automatically uploads the PMC.dll file to the server whenever you install or upgrade the server software.

After the system uploads the PMC.dll file to the server, you can configure the recommended download version to apply to the PMC client machines that connect to the server. This configuration ensures that the PMC client machines first check for the recommended version of the PMC software; if the version does not match the server configuration, the system prompts the PMC user to update it, as shown in the following sequence:

1. Upon connection, the PMC client machine checks for the recommended version of the PMC software.
2. If the PMC does not have a PMC version that is greater than or equal to the recommended version, a pop-up dialog box displays to inform you that the version is not the recommended version and prompts you to download and run the recommended version.
3. When you click **Yes** to this prompt, the PMC.dll file for the recommended version downloads to the following directory on the PMC client machine:

   C:\Program Files\Cisco Systems\Cisco IPICS\PMC\Bin
4. After the PMC.dll file downloads, the system updates the location selection dialog box to provide you with the option of choosing this latest version.

Note Be aware that the PMC automatic update process installs the PMC.dll file only; with this update, the PMC skins and the online help are not updated. To get the latest, fully executable version, you need to uninstall and reinstall the PMC application.

For information about how to configure the recommended download version for the auto update feature of the PMC, see the "Server Enhancement to the Auto Update Feature for the PMC" section on page 76.

Upgrading to Cisco IPICS Release 1.0(2)

If your Cisco IPICS server is running release 1.0(1.1), you can upgrade your server system software to release 1.0(2) by using the Cisco-provided CD-ROM format that is available for this upgrade. (This upgrade software is only available on CD-ROM format; it is not available via web download.) If you are not sure about how to obtain this software, contact your Cisco representative for information.

Note Your server must be running Cisco IPICS release 1.0(1.1), which is release 1.0(1) plus SR1, to upgrade to Cisco IPICS release 1.0(2). If your server is running Cisco IPICS release 1.0(1), you must first upgrade to release 1.0(1.1) before you can upgrade your server software to release 1.0(2). (This Cisco IPICS Administration Console displays the current release information for your system.) For information about upgrading to release 1.0(1.1), refer to the Cisco IPICS Software Download website at the following URL: http://www.cisco.com/cgi-bin/tablebuild.pl/ipics

Tip To verify which versions of Cisco IPICS are compatible for upgrade, refer to the most recent version of the *Cisco IPICS Compatibility Matrix* at http://www.cisco.com/univercd/cc/td/doc/product/cis/c_ipics/index.htm

The Cisco IPICS operating system was modified as part of this release. Therefore, to accommodate database schema changes, you must follow this sequence of steps to fully upgrade your server software to Cisco IPICS release 1.0(2):

1. Upgrade the server software to Cisco IPICS release 1.0(2) by following the procedure, as described in the "Upgrading to Cisco IPICS Server Software, Release 1.0(2)" section on page 25.
2. Perform a remote backup of your data by accessing the **System Administrator > Database** window in the Cisco IPICS Administration Console. For information about the steps to follow, see the "Backing Up Your Database Files" section on page 27.
3. Install the Cisco IPICS operating system, release 1.0(2), which is an updated version of the operating system. For more information, see the "Installing Cisco IPICS Operating System Software, Release 1.0(2)" section on page 29.

4. Reinstall the Cisco IPICS release 1.0(2) server software. To reinstall this software, follow the procedure that is documented in the "Reinstalling Cisco IPICS Server Software, Release 1.0(2)" section on page 29. (You must perform this procedure in console mode.)
5. Restore your data by accessing the **System Administrator > Database** window in the Cisco IPICS Administration Console. For information about the steps to follow, see the "Restoring Your Database Files" section on page 32.

This section contains information about upgrading your software to Cisco IPICS release 1.0(2) and other actions that you must take to fully complete this upgrade process; it includes the following topics:

Upgrading to Cisco IPICS Server Software, Release 1.0(2)

To upgrade the Cisco IPICS system software to release 1.0(2), perform the following procedure:

Procedure

Step 1 Log in to the Cisco IPICS server by using the root user account and password.

The Cisco Linux desktop displays.

Step 2 Insert the Cisco IPICS installation CD into the server disk drive.

If CSA is not installed on the server, or if it is not running, continue with Step 4.

If CSA is installed on the server, you will be prompted with a CSA access permission dialog box.

Step 3 In the CSA access permission dialog box, click **Yes** to grant permission to the installation; then, click **Apply**.

Note Whenever CSA prompts you for permission, while you are performing installation-related activities on the server, be sure to always click **Yes** to grant permission and continue with that operation. Make sure that you take this action before CSA times out based on its default value of No.

The Cisco IPICS CD icon displays on the desktop.

Step 4 Double-click the CD icon to open the CD contents.

Cisco Linux displays a window that shows the Cisco IPICS installer file. The following name provides an example of the installation executable file name:

```
install_ipics_1_0_2.bin
```

Note The exact name of the installation executable file changes with each version as the new version number is incorporated into the name.

Step 5 To start the installation, double-click the installer file icon.

Cisco Linux displays a message that allows you to choose to display the file contents or run the installer file.

Step 6 When you are prompted to display the file contents or run the installer files, click **Run in Terminal**.

The Cisco IPICS installer introduction window displays.

Step 7 To continue, click **Next**.

The Cisco IPICS installer displays the End User License Agreement.

Step 8 Use the scroll bar in the License Agreement window to view the entire agreement. After you have read the text, click the **I accept the terms of the License Agreement** radio button. Then, click **Next**.

The Choose Install Set window displays.

Step 9 To upgrade Cisco IPICS, click **Upgrade**. Then, click **Next**.

The installer prompts you to change the password for the informix user.

Step 10 Enter a password for the informix user that is at least eight characters in length. Then, press **Tab** and reenter the password to confirm it. Click **Next**.

Caution Make sure that you only change the password for the informix user when you perform a Cisco IPICS installation or upgrade procedure by using the installer. If you manually change the informix password outside of the installation or upgrade process, the Cisco IPICS Administration Console becomes unusable.

The installer prompts you to change the password for the ipics user.

Step 11 Enter a password for the ipics user that is at least eight characters in length. Then, press **Tab** and reenter the password to confirm it. Click **Next**.

The Cisco IPICS installer Preinstallation Summary window displays. This summary includes information, such as the product name and version, the destination folder for the installation, the amount of disk space that is required for the installation, and the available disk space.

Step 12 To continue with the upgrade, click **Install**.

The Installation Progress window displays while the updated software is being installed.

Step 13 When you see the Cisco IPICS Install Complete window display, the upgrade is complete. To close the installer, click **Next**.

Step 14 Continue with the "Backing Up Your Database Files" section on page 27 to perform a backup your data files to a remote location.

For additional information about upgrading Cisco IPICS server system software, refer to the "Upgrading Cisco IPICS" chapter in the *Cisco IPICS Server Installation Guide*. For guidelines about Cisco IPICS installation and upgrade procedures, see the "Server Installation, Upgrade, and Backup Guidelines" section on page 12.

Backing Up Your Database Files

To back up your database files to a remote host location, perform the following procedure:

Procedure

Step 1 From the Cisco IPICS Administration Console, navigate to **System Administrator > Database** to access the Manage Database window.

Step 2 In the Database Backup pane of the Manage Database window, choose the following destination for your backup:

- **Remote Host**—This option allows you to back up your files to a remote location. When you choose this option, you must specify the following information:
  - Remote Host IP Address—Enter the IP address of the remote host
  - User Name—Enter a valid user ID for access to the remote host
  - User Password—Enter a valid password for this user.
  - Remote Directory—Enter the location of the full directory path on the remote host where you want the files to be stored.

Step 3 To begin the backup procedure, click **Backup Now**.

Cisco IPICS begins the backup process.

Step 4 To view the backup activity, click the **Refresh** button that appears under the Database Logs pane.

The Database Logs pane shows the log entries that pertain to the backup process.

Step 5 To view the details of your backup activity, wait for the window to refresh or click **Refresh** to check the successful completion of your backup.

Cisco IPICS provides the following visual identification of certain log entries:

- Log entries that display in blue text indicate the successful completion of a script.
- Entries that display in green text indicate the successful completion of a process.
- Entries that display in red text indicate that an error has occurred.

Step 6 After you have completed the backup process, access the remote host to validate that the backup files have been stored to the remote directory that you specified.

Step 7 Install the updated Cisco IPICS operating system, release 1.0(2), as described in the "Installing Cisco IPICS Operating System Software, Release 1.0(2)" section on page 29.

For more information about Cisco IPICS backup and restore procedures, refer to the *Cisco IPICS Backup and Restore Guide*.

Installing Cisco IPICS Operating System Software, Release 1.0(2)

To install the latest Cisco IPICS operating system software, follow the procedure that is documented in the *Cisco IPICS Server Installation Guide*.

If the Redundant Array of Disks (RAID) controller is enabled on your Cisco Media Convergence Server (MCS) server, make sure that you disable it, as described in the "Installing the Cisco Linux Operating System" section in the "Installing the Cisco IPICS Server Software" chapter in the *Cisco IPICS Server Installation Guide*.

After you have completed the installation of the Cisco IPICS operating system release 1.0(2), restore your data files, as described in the "Restoring Your Database Files" section on page 32.

Reinstalling Cisco IPICS Server Software, Release 1.0(2)

After you have completed the installation of the Cisco IPICS operating system software, you must reinstall the server software by using console mode.

Note Cisco IPICS does not support the use of GUI mode for the Cisco IPICS release 1.0(2) server software installation.

To reinstall the Cisco IPICS server software in console mode, perform the following procedure:

Procedure

Step 1 Place the Cisco IPICS installation CD in the disk drive of the Cisco IPICS server.

Step 2 Connect to the Cisco IPICS server by using one of the following options:

- If you have a monitor attached to the server, you can access the console directly and open a terminal window by following these steps:
  a. Navigate to the main menu on the Cisco Linux desktop.
  b. Click the **Red Hat** icon.
  c. Choose **System Tools > Terminal** to access the command line.

     A terminal window displays.
- To access the server remotely, follow these steps:
  a. Use SSH Secure Shell Client software (or similar software) to connect to the server from your local workstation by choosing **Start > Programs > SSH Secure Shell > Secure Shell Client**.
  b. Click **Quick Connect** to open up the Connection to Remote Host dialog box.
  c. In the Host field, enter the IP address for the server; then, press **Tab.**
  d. In the User Name field, enter **root**.
  e. Click **Connect** to connect to the server.
  f. Enter the root password; then, click **OK**.

     After the login completes, the SSH Secure Shell Client displays a root prompt for the Cisco IPICS server.

Step 3 At the command line, enter the following commands to view the contents of the CD:

[root] **#cd /mnt/cdrom**

[root] **#ls -l**

The name of the Cisco IPICS installer file displays with a .bin extension.

Step 4 To begin the installation, enter the following command:

[root] **#/mnt/cdrom/install_ipics_1_0_2.bin -i console**

The window displays a message that informs you that the installer is extracting.

After the files have been extracted, the installer displays introductory text.

Step 5 Press **Enter** to continue.

The End User License Agreement displays.

Step 6 Enter through all of the pages of the license agreement. After you have read the entire agreement, enter **Y** to accept the terms of the agreement.

The Choose Install Set menu displays.

Step 7 Enter the number that corresponds to either the Typical or Customize option to install the server software:

- 1–Typical—This option installs Cisco IPICS server software with CSA; this option specifies the default; press **Enter** to choose the Typical installation
- 2–Customize—This option allows you to choose whether to install Cisco IPICS server software with or without CSA
- 3–Upgrade—This option installs an upgrade to a previously installed version of Cisco IPICS server software

Note If you choose not to install CSA with this installation, you can manually install CSA at a later time. For more information, see the "Manually Installing CSA on the Server" section on page 16.

Step 8 When the system prompts you, enter a root password that is at least eight characters in length; then, press **Enter**.

Note Make sure that you only use passwords that begin with a-z, A-Z, or 0-9 when you enter the root password. Cisco IPICS does not support the use of special characters as the first character in the root password. If you enter a special character as the first character in the root password, your root login will become inoperable. To resolve the problem, you need to boot the system in single user mode to change the root password; then, reinstall the server software.

The installer prompts you to reenter the root password.

Step 9 Enter the root password again to confirm; then, press **Enter**.

The Cisco IPICS installer prompts you to enter a password for the ipicsadmin user, the informix user, and then for the ipics user.

Note Make sure that you only change the password for the informix user when you perform a Cisco IPICS installation or upgrade procedure by using the installer. If you manually change the informix password outside of the installation or upgrade process, the Cisco IPICS Administration Console becomes unusable.

The Cisco IPICS installer displays the Preinstallation Summary.

Step 10 To continue, press **Enter**.

The installation process begins. Upon completion, the system displays text to indicate that the installation has completed.

Step 11 To continue, press **Enter**.

The system prompts you to restart the server now or later.

Step 12 Choose from the following options to restart the server:

- 1—Restart now; this option specifies the default
- 2—Restart later

Step 13 To restart the server now, press **Enter**.

The system automatically reboots.

Step 14 If you were connected via SSH Secure Shell Client software, close this window by choosing **File > Disconnect**; then click **Ok**.

For more information about the server software installation procedures, refer to the *Cisco IPICS Server Installation Guide*.

Restoring Your Database Files

To restore your data files, perform the following procedure:

Procedure

Step 1 From the Cisco IPICS Administration Console, navigate to **System Administrator > Database** to access the Manage Database window.

Step 2 In the Restore from Backup pane of the Manage Database window, choose the following source location:

- **Remote Host**—This option allows you to restore your files from a remote location. When you choose this option, you must specify the following information:
  - Remote Host IP Address—Enter the IP address of the remote host.
  - User Name—Enter a valid user ID for the remote host.

Note To help ensure the security of your data, Cisco IPICS does not support the use of different user IDs for backup and restore operations that you perform on the same data set. Therefore, when you restore your data, make sure that you specify the same user ID as the one that you used to back up your data; otherwise, the procedure cannot succeed.

  - User Password—Enter the password for this user.
  - Remote Directory—Enter the directory on the remote host from which you want to retrieve your files. Use the full path.

Tip When you specify a remote host destination for your backup, Cisco IPICS creates a folder inside the remote directory that you specify and places your backup files in subdirectories that are labeled with a date and time; for example, 2005-11-02_14:04:52. When you restore data, make sure that you specify the entire path, including the subdirectory name.

Step 3 Click **Restore Now**.

Cisco IPICS begins the restore process and logs you out of the Administration Console.

As part of the restore process, the system restarts the Tomcat service. You must wait for the restore process to complete before you can log in again and view the log details.

Tip While the system is processing the restore operation, you can check the status in the db-maintenance.log. The db-maintenance.log file is located in the following folder on the server:
/opt/cisco/ipics/database/db-maintenance

Step 4 To view the status of the restore procedure, wait approximately 20 minutes; then log in to the Administration Console and navigate to the Manage Database window.

From the Database Logs pane, you can view status messages that pertain to the restore procedure.

Note If you attempt to log in before the restore process completes, Cisco IPICS displays a message that states that the database is unavailable. Please wait and then try your login again.

For more information about Cisco IPICS backup and restore procedures, refer to the *Cisco IPICS Backup and Restore Guide*.

New Prompt for ipics User Password

In Cisco IPICS release 1.0(1), users were not prompted to change the ipics user password as part of the installation process. Instead, Cisco IPICS defaulted the ipics user password to “cisco123.”

Cisco IPICS release 1.0(2) changes this behavior by now prompting you to change the password for the ipics user during the Cisco IPICS server software installation and upgrade procedures.

The ipics user can perform all administration functions that are related to the Cisco IPICS application. You use this user ID to log in with ipics application-level user capabilities in the Cisco IPICS Administration Console.

Enhanced Support for E1 Connectivity

With this release, Cisco IPICS extends your connectivity options by enabling RMS configuration support for E1 connectivity, in addition to T1 connectivity. To configure an RMS router for E1 connectivity, follow these guidelines:

- Configure at least two E1 controllers and assign ds0 groups to each controller.
- Allocate only as many ds0s on a controller as the RMS router can support simultaneously.
- Make sure that the ports that you allocate start with port 0 and are configured sequentially.
- Typically, an E1 controller will support 30 ds0s, but your controller may support fewer ds0s, depending on the number of available digital signal processors (DSPs).
- Be careful not to allocate more ds0s than a controller has resources to support; otherwise, you may encounter lost audio and other voice quality issues.
- Configure E1 controllers for individual voice ports by including the **ds0-group** *ds0-group-number* **timeslots** *timeslot-list* **type e&m-lmr** command in the router configuration.

For detailed steps about how to configure E1 support, see the procedure in the "Support for E1 Connectivity" section on page 78.

Support for Cisco Unified Wireless IP Phone 7920

In this release, Cisco IPICS expands your IP phone options by adding support for the Cisco Unified Wireless IP Phone 7920. With this addition, the Cisco Unified Wireless IP Phone 7920 joins the Cisco Unified IP Phone 7960 and the Cisco Unified IP Phone 7970 as part of the Cisco IPICS portfolio to provide enhanced productivity and call-handling capabilities.

For information about how to subscribe, access, and use the Cisco IPICS service on the Cisco Unified Wireless IP Phone 7920, see the "Support for Cisco Unified Wireless IP Phone 7920" section on page 84.

Backup and Restore Updates

In this release, Cisco IPICS includes enhancements and changes to the backup and restore functionality. This section includes the following topics:

Backup and Restore Enhancements

Cisco IPICS enables the following types of backup processes:

- Manual Level-0 (L0) backups—These backups contain data and they are run manually by the user. Cisco IPICS manages these backups.
- Scheduled Level-0 backups—These backups contain data and they are run on a predefined schedule. Cisco IPICS manages these backups.

Both of these backup processes write their data to the default location. Cisco IPICS then archives, or copies, the data from the default location to the local or remote host location, if specified.

Note To ensure data integrity in the event of system failure, Cisco recommends that you back up your files to a remote host location.

In this release, Cisco IPICS provides enhanced functionality for restore operations based on the following options:

- When you restore data from the default, local, or remote host destinations, Cisco IPICS restores your data up to the specific point in time that the backup was taken.
- From the Manage Database pane in the **System Administrator > Database** window, you can choose from the following options to restore your data:
  - **Default**—When you restore data that you have backed up to the default location, Cisco IPICS restores your data up to the specific point in time that the backup was taken.

Note Cisco recommends that you first try to restore your data from the default location because this location always contains the latest backup.

- **Local Directory or Remote Host**—When you restore data from backups that are stored on local or remote locations, Cisco IPICS restores your data up to the specific point in time that the backup was taken.

Note To ensure data integrity in the event of system failure, Cisco recommends that you back up your files by using the remote host destination.

Note Cisco IPICS has simplified the restore process. Therefore, the "Recovering from an Unsuccessful Restore Procedure" section that is documented in the *Cisco IPICS Backup and Restore Guide, Release 1.0(1)* is no longer applicable.

Guidelines for Data Recovery Procedures

The following guidelines pertain to general data recovery procedures. Cisco recommends that you perform the following recovery steps, in sequence, when you restore your data:

1. Because the default option contains the latest backup, first try to restore your data by using the default location option in the Administration Console GUI; choose this option even if you have chosen the local or remote option for your backup location. To perform this procedure, access the Manage Database pane in the Administration Console by navigating to **System Administrator > Database**.
2. If your attempt to restore data from the default location is not successful, try to restore your data from the remote location by using the Administration Console GUI.
3. If your attempt to restore data from the remote host is not successful, next try to restore your data by using the local backup.

Caution Proceed with caution when you choose this recovery option, which overwrites the contents of the default folder and may result in the loss of recent transactions.

Changes to the Database Status Logs

Cisco IPICS implements the following changes to the database status logs:

- The db-maintenance.log becomes the primary log that captures the higher-level logging information that is used by the backup and restore processes. The db-maintenance.log file does not appear on the server immediately after a new installation is done. Cisco IPICS generates the db-maintenance.log file after the first time that you complete the backup/restore process.
  - Cisco IPICS sends a copy of the db-maintenance.log, via email, to the root user after completion of each backup and restore operation.
  - The db-maintenance.log file contains the database maintenance logs that the system generates for the most recent execution of the scripts.
  - The system also generates the db-maintenance.log.<*date*>, which collects the database maintenance logs for the entire day (*date* specifies the date that the db-maintenance.log file was generated).

  The db-maintenance.log is located in the following folder on the server: **/opt/cisco/ipics/database/db-maintenance**.
- The bar_act.log now contains the lower-level logging information that pertains to the Cisco IPICS utilities that are used to perform the backup and restore procedures. You can use this log to aid your debugging efforts by tracking the progress of the backup and restore utilities.
- When you click **Download** from the **System Administrator > Database** window, the server now downloads a .zip archive file (instead of a text file) that contains the bar_act.log, db-maintenance.log, and any daily db-maintenance.log<*date*> logs that may exist.

Note Cisco recommends that you regularly check the database logs for status messages and/or error information that may be pertinent to recent backup and recovery activity.

PMC Installation and Upgrade Guidelines

This section includes information about the guidelines that apply to Cisco IPICS release 1.0(2) PMC installation and upgrade procedures:

- Cisco IPICS supports Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS) to ensure secure communications between the Microsoft Internet Explorer version 6.0.2 or later browser on the PMC client machine and the Cisco IPICS server.
- Install the PMC application on your local PC by downloading the software from the Cisco IPICS server. (The PMC installation involves downloading the self-extracting PMC installation program, which includes the PMC installation and configuration files, from the Cisco IPICS server.)
- The PMC installation program automatically runs the PMC installation file to install the PMC software on the client machine.
- Make sure that you close the PMC application before you install a new version of the PMC software.
- When the auto-update process updates the version of the PMC, it installs the PMC.dll file only; it does not include any changes to online help or the PMC skins.
  - To obtain the latest, fully executable PMC version that includes new PMC skins and online help, make sure that you download and install the latest, full PMC installation file from the server.
- Be aware that login user names are case-insensitive and passwords are case-sensitive.
- The PMC can maintain multiple versions, current and previous, of the PMC application to enable quick reversion to an earlier compatible version, if necessary.
- When you have Cisco Security Agent (CSA) installed on the PMC client machine, be aware that you may be prompted with CSA access permission dialog boxes for various operations that you are trying to perform. Whenever CSA prompts you for permission, while you are performing any operation on the PMC, be sure to always click **Yes** to grant permission and continue with that operation. For more information about using CSA, refer to the Cisco Security Agent documentation at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/vpn/ciscosec/csa/index.htm

Where to Find More Information

- *Cisco IPICS PMC Installation and User Guide, Release 1.0(1)*

Audio Playback Enhancement Added to the PMC Channels Menu

The PMC Channels menu includes a new field, Spatial Position, that allows you to control the speaker that the PMC uses for channel audio playback.

The Spatial Position field enables audio playback for selected channels on different speakers by allowing you choose the speaker that the selected channel uses. You can configure spatial playback for a specific channel by highlighting the channel and then choosing one of the following options for that channel:

- **Stereo**—This option, as the default value, plays out the channel audio by using both speakers.
- **Left**—This option plays out the channel audio by using only the left speaker.
- **Right**—This option plays out the channel audio by using only the right speaker.

For more information, refer to
http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc76783

Modification to the Behavior of the PMC Transmit Indicator

The PTT channel button on the PMC includes the following graphical indicators to enable clear identification of the PMC traffic streams:

- Receive indicator—This indicator blinks green when you are receiving traffic. It remains illuminated, in a solid color format, for several seconds after the receive transmission has ended to let you know that the voice traffic has stopped; this indicator also provides an indication of recent activity on a channel.
- Transmit indicator—This indicator blinks red when you are transmitting traffic.

Note Although the PMC skins may be customized to define the actual colors that are used, the Cisco standard defines the above conventions for the receive and transmit indicators.

In the prior release, the transmit indicator continued to blink as long as the PTT channel button was pressed or latched, even if the PMC did not detect voice activity from the microphone.

With this release, Cisco IPICS modifies and enhances the behavior of the transmit indicator by supporting silence detection. That is, when the PMC now detects silence on the channel/VTG, it stops sending voice packets to preserve CPU resources. That means, if you mute your microphone after you have pressed or latched the PTT button, the transmit indicator stops blinking. When you unmute your microphone, the transmit indicator starts blinking again.

This modification helps to improve the performance of the PMC by reducing CPU utilization on the PMC client machine and ensuring more efficient use of CPU resources.

For more information, refer to
http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd54266

Where to Find More Information

- *Cisco IPICS PMC Installation and User Guide, Release 1.0(1)*

Availability of 18-Channel PMC Skin

This release of Cisco IPICS extends the availability of the PMC skins by now supporting a higher-capacity, mouse-based 18-channel skin. This new skin displays in the following format: three columns by six rows, for a total of 18 channels.

Note The PMC automatic update process installs only the PMC.dll file; it does not include any changes to the PMC skins or online help. To obtain the latest, fully executable PMC version that includes new PMC skins and online help, make sure that you download and install the latest, full PMC installation file from the server.

You may configure your PMC to display this new skin by choosing the Cisco IPICS Mouse 18-Channel skin in the PMC Skin menu. You can access the Skin menu by navigating to **Settings > Skin** in the PMC application. For more information about configuring PMC skins, refer to the "Customizing the PMC Application" chapter in the *Cisco IPICS PMC Installation and User Guide*.

Tip Be aware that the PMC does not allow you to reconfigure the skin to one that contains a lesser number of channels if you already have more than that number of channels active. For example, if you use the 18-channel skin and you have any

number of channels between 9 and 18 active, and you want to reconfigure your PMC to use the 8-channel skin, you must first deactivate the active channels before the PMC would allow the skin change to occur. For more information about customizing PMC skins, refer to the "Customizing the PMC Application" chapter in the *Cisco IPICS PMC Installation and User Guide*.

To use the 18-channel skin, the PMC application requires the following minimum hardware (see the "PMC Requirements" section on page 9 for information about the PMC hardware and software requirements for all PMC skins):

Hardware

- 3.2 GHz Pentium IV class, including Mobile Pentium
- 1 GB RAM
- 16 MB free space
- Network interface card

This 18-channel skin contains the same features as the 4-channel and 8-channel skins; however, Cisco IPICS supports additional keyboard assignments only for channels 9 and 10. See Table 4 for the keystroke assignments that Cisco IPICS supports.

Table 4 PMC Button Accelerated Keystroke Assignments

Channel Number on the PMC	Keystroke to Activate or Deactivate the Channel	Keystroke to Latch (lock in) or Unlatch the PTT Button	Keystroke to Increase the Volume	Keystroke to Decrease the Volume
Channel 1	Shift-1	1	q	a
Channel 2	Shift-2	2	w	s
Channel 3	Shift-3	3	e	d
Channel 4	Shift-4	4	r	f
Channel 5	Shift-5	5	t	g
Channel 6	Shift-6	6	y	h
Channel 7	Shift-7	7	u	j
Channel 8	Shift-8	8	i	k

Table 4 PMC Button Accelerated Keystroke Assignments (Continued)

Channel Number on the PMC	Keystroke to Activate or Deactivate the Channel	Keystroke to Latch (lock in) or Unlatch the PTT Button	Keystroke to Increase the Volume	Keystroke to Decrease the Volume
Channel 9	Shift-9	9	o	l
Channel 10	Shift-0	0	p	;

Tip Be aware that the keystroke assignments are case-sensitive. Make sure that you do not have Caps Lock enabled when you use these keystroke assignments.

For more information about the keystroke assignments that Cisco IPICS supports, refer to the "Using the PMC Application" chapter in the *Cisco IPICS PMC Installation and User Guide.*

Important Notes

The following section contains important information that pertains to this release of Cisco IPICS.

Using Cisco Security Agent with the PMC

When you have Cisco Security Agent (CSA) installed on the PMC client machine, be aware that you may be prompted with CSA access permission dialog boxes for various operations that you are trying to perform.

Note Whenever CSA prompts you for permission, while you are performing any operation on the PMC, be sure to always click **Yes** to grant permission and continue with that operation.

CSA may prompt you for permission in the following instances:

- If you are prompted with a CSA access permission dialog box during the PMC installation process, be sure to click **Yes** to grant permission to the PMC installation.
- If you are prompted with a CSA access permission dialog box when you launch a new version of the PMC or after a system reboot, make sure that you click **Yes** to grant permission to allow the PMC to monitor the media device (microphone).

Note If you allow CSA to time-out based on its default value of No after you launch the PMC, the PMC will be able to receive traffic but it will not be able to send traffic; that is, you will still be able to listen to any active conversations but you will not be able to transmit.

- If you are prompted with an access permission dialog box when you activate a channel on the PMC, be sure to click **Yes** to grant permission.
- If you are prompted with an access permission dialog box when you uninstall the PMC, click **Yes** to grant permission.
- If the “Don’t ask me again” check box displays as an option, you may check it to instruct CSA not to prompt you again in the future.

For information about using CSA, refer to the Cisco Security Agent documentation at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/vpn/ciscosec/csa/index.htm

Support for Automatic Downgrades

Cisco IPICS does not support automatic downgrades of the PMC application when you have downloaded noncumulative versions from the server. (You can identify noncumulative versions by the release numbers, which appear out of sequence.)

If you need to downgrade to a PMC version that is earlier than the currently installed version, and if you have been running noncumulative versions, you must uninstall the current PMC before you can install a downgraded version.

To uninstall the PMC application from your client machine, perform the following procedure:

Procedure

Step 1 Navigate to **Start > Programs > Cisco IPICS > PMC > Uninstall PMC**.

Tip If you have CSA installed on your PMC client machine and you are prompted with an access permission dialog box, be sure to click **Yes** to grant permission to the PMC uninstallation process.

A dialog box displays to ask if you are sure that you want to uninstall this product.

Step 2 Click **Yes**.

The PMC application is uninstalled from your client machine.

For more information about Cisco IPICS version numbers, see the "Understanding the To-be-fixed and the Integrated-releases Fields in the Online Defect Record" section on page 62.

Establishing PMC Connectivity with the RMS for SIP-Based Remote Connections

To connect the PMC via a SIP-based remote connection, make sure that the PMC can establish connectivity to the RMS router. (The PMC connects to the RMS by using the IP address of the Loopback0 interface that is assigned to the RMS.) If the PMC cannot establish connectivity to the RMS, PMC users may experience channel activation issues (such as fast busy) when they attempt to use a SIP-based remote connection.

To determine the IP address of the RMS, access the **Settings > Channels** menu in the PMC application. (If you cannot determine the IP address of the RMS, contact your System Administrator for assistance.) Click a remote connection channel to highlight it; then, scroll down the Channel Properties to the SIP Proxy field to find the IP address of the RMS for the associated channel. For more information about the Channels menu, refer to the "Customizing the PMC Application" chapter in the *Cisco IPICS PMC Installation and User Guide.*

From the PMC client machine command line interface, enter the ping command to ping this IP address and verify connectivity.

C:\ping <*SIP Proxy IP address*>

where *SIP Proxy IP address* represents the RMS component.

Note The PMC must be able to establish connectivity to the RMS to enable SIP-based remote connections. Make sure that you can successfully ping this IP address to ensure PMC connectivity to the RMS. If the PMC cannot connect to the RMS, you may experience channel activation issues (such as fast busy) when you attempt to use a SIP-based remote connection.

For more information, refer to
http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd33374

Cisco IPICS Usage and Licensing Guidelines

This section includes information about Cisco IPICS usage and licensing guidelines; it includes the following topics:

- PMC Usage Guidelines, page 49
- License Guidelines, page 52

Server Usage Guidelines

- Make sure that you only perform system date changes before you install the Cisco IPICS software. Cisco IPICS does not support any modification of the system date in the operating system after the Cisco IPICS software has been installed. If the system date is not properly set to your local date and time, you must adjust it before you install the Cisco IPICS software. If you try to change the system date and time after you install the software, you will invalidate your license and cause the system to become inoperable.
- Be aware of the following browser-related guidelines:
  - 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.
  - To avoid browser-related memory issues, exit your browser and then restart it after prolonged use of the Cisco IPICS Administration Console.
- Establish a policy channel, which is a dispatcher-only PTT channel, and add this channel to every PMC and VTG to allow the dispatcher to communicate with participants.

- If you change the IP address of your server, the server will restart. You will then need to regenerate the PMC installer and download it to all of your user PMC client machines so that they can communicate with the server.
- The Cisco IPICS server contains the associated connection configuration, which correlates to locations, to determine how the PMC users should connect. Cisco IPICS provides connection support for both multicast and unicast communications. Make sure that users are aware of the appropriate location information to use when they log in to Cisco IPICS.
- Users who are in the same multicast domain are also in the same Cisco IPICS location.
- Cisco IPICS server logs roll over and create multiple log files. When you download these logs, Cisco IPICS zips them into one file that contains all of the log files.
- Cisco IPICS does not support the use of multiple Cisco IPICS servers for the same RMS component because each server must have the use of resources on a corresponding RMS for proper functionality.
- Cisco IPICS provides support for more than one RMS component in the same location.
- To manually update the status of the RMS component, click the **Show Configuration** button that displays in the Administration Console **System Administrator > RMS** window. This action allows you to initiate an update to the RMS state at any time in lieu of waiting for the system to automatically process an update based on a predefined interval.
- Be aware of the number of participants in a conference and their type of connection to avoid resource contention.
- Inform new PMC users about how best to communicate when using Cisco IPICS. The following guidelines can help to assist new and experienced users with Cisco IPICS:
  - To talk on a channel, click and hold the PTT button before you speak.
  - Talk in short bursts and monitor the receive and transmit indicators to make sure that you are not talking over other Cisco IPICS users.
  - You can simultaneously participate in multiple voice channels that are activated.

  - Latching the PTT button blocks transmissions from half-duplex radios when these devices are attached to the channel or VTG via an LMR gateway.

PMC Usage Guidelines

This section includes guidelines for using the PMC; it includes the following sections:

- Using the PMC in Offline Mode, page 50
- PMC Coexistence with Other Voice Applications, page 51

The following guidelines pertain to the PMC:

- Only one instance of the PMC application can be open on a given PC at a time.
- A running PMC supports only one active user ID login on a given PC at a time.
- Any number of valid Cisco IPICS users can use the same PMC application, but not concurrently, based on PMC licensing requirements.
- Each PMC application connects to only one Cisco IPICS server.
- The PMC retrieves the personalized list of channels from the server.
- You can only view and use those voice channels that the dispatcher has assigned to you.
- You can choose to turn on any of the assigned PTT channels by clicking the **Activate** button on the PMC. Click and hold the **PTT** button to talk. Monitor the receive and transmit indicators to make sure that you are not talking over other Cisco IPICS users.
- You have the ability to simultaneously listen in on multiple voice channels that are activated on the PMC application. You can also talk on multiple lines at the same time by using the PTT latch functionality, however, this functionality blocks transmissions from half-duplex radios when these devices are attached to the channel or VTG via an LMR gateway.
- For optimum connectivity, use the most appropriate location for your connection type when you log in to the PMC. You can change locations by restarting the PMC and then choosing another available location from the drop-down list box in the location selection dialog box. If you are not sure which location to use, contact your system administrator for assistance.

- The PMC must be able to establish connectivity to the RMS to enable SIP-based remote connections. To determine the IP address of the RMS, access the **Settings > Channels** menu in the PMC application. Click a remote connection channel to highlight it; then, scroll through the Channel Properties pane to the SIP Proxy field to find the IP address of the RMS for the associated channel. For more information, see the "Establishing PMC Connectivity with the RMS for SIP-Based Remote Connections" section on page 46.
- If there is no traffic activity after a preconfigured period of time, channels that are activated via a SIP-based remote connection may be deactivated by the system. To reactivate a channel after it has been deactivated, click the **Activate** button on the PMC.
- Use a high-quality microphone and check the placement and settings of your audio devices before you begin to use the PMC. For more voice quality guidance and information, see the "Cisco IPICS Voice Quality Tips" section on page 56.
- If you use a docking station with your PMC client machine, make sure that you close the PMC application before you undock your PC; otherwise, your PC may become unresponsive and require you to reboot.
- When the dispatcher deactivates one or more VTG(s), you will no longer have access to the channel(s) that were created to support the VTG(s).
- If your ability to transmit on a channel has been disabled by the server, the PTT button will not highlight.
- When a channel is disabled, all of the PMC buttons are grayed-out or muted so that you cannot activate the channel. However, you can still view the channel or VTG label, if one was configured in the server.
- A channel that is unassigned appears on the PMC with all of the buttons grayed-out and no channel name. You cannot activate or use an unassigned channel.
- The PMC application does not provide support for the creation of ad hoc VTGs; that is, there is no support for direct PMC-to-PMC connectivity.

Using the PMC in Offline Mode

When the connection to the server goes offline, the PMC enters offline mode. Offline mode allows you to continue to communicate during periods of server downtime. The following caveats apply to the PMC offline mode:

- You must have at least one successful login to the server before you can use the PMC in offline mode.
- If the server goes offline while you are running the PMC, the system displays a message to alert you that the server is not available. The PMC enters offline mode with the current list of channels.
- If the server is offline when you start the PMC, the system displays a message to alert you. The PMC enters offline mode with the last online session's list of channels. (Be aware that some lines may no longer work, depending on the connection type.)
- After the server returns to an online state, you may encounter an invalid user or password error when you try to log in to the PMC. This situation may occur if the PMC attempts to connect to the server while the server database is being restored. In this case, the login dialog box may display several times until the server database has been fully restored.
- If your user ID was deleted while the PMC was operating in offline mode, the system displays a message to inform you that your user name is not valid. The PMC then logs out and displays the normal startup login dialog box.
- If the RMS entries become changed while you are running the PMC, your SIP channels may become disconnected. The PMC retrieves the updated channel list, with the newly-allocated SIP channels, after successful login to the server.

PMC Coexistence with Other Voice Applications

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

For example, Windows XP allows multiple applications to run concurrently and open and use the microphone at the same time. Windows 2000, however, does not provide support for this same capability; that is, only one voice application, such as the PMC or another voice application, may be active at the same time on a Windows 2000 client machine.

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

License Guidelines

To use the Cisco IPICS solution, you must obtain licenses that specify and enable the concurrent usage for Cisco IPICS ports, PMC users, and Cisco Unified IP Phone users. The Cisco IPICS server checks the license count for concurrent license usage to ensure that the limits are not exceeded.

Cisco IPICS displays the number of available licenses and concurrent usage information in the License browser window. You can access this window by navigating to the **System Administrator > License** link in the Administration Console.

When the ops view feature has been enabled on the server, the system displays a Cisco Ops View entry under the Configured License area in the License window, along with the word "Licensed" to indicate that the ops view functionality has been enabled. When ops views is not enabled, this entry displays "Not Licensed." For more information about ops views, see the "Using Ops Views" section on page 54.

Note The data that displays in the License browser window shows the usage at the time that the license window was last accessed. To view the most current license information, make sure that you update your browser window often and before you perform any server administration functions to ensure that you are working with the most current information. If you attempt to perform an administration update in a window that does not display the most current data, the update will not succeed and Cisco IPICS will display an error. If this situation occurs, update your browser window and retry the operation.

Cisco IPICS uses the following criteria to determine license consumption for Cisco IPICS ports and PMC usage:

- Cisco IPICS Ports Usage—Cisco IPICS ports determine the number of enabled channels and active VTGs that the system can use. An enabled channel or activated VTG consumes a port license. After the channel is deleted or disabled or the VTG is deactivated, the server releases the license and makes it available for use.

  - Cisco IPICS bases license usage for ports on the unique combination of a multicast address and a location; that is, if a channel has two multicast addresses that are assigned to the channel, two licenses are used. If one of the multicast addresses is removed, the system releases one of the licenses so that the port now consumes one license.

Note Make sure that the server has a sufficient number of licenses available for the configuration of policies. VTGs can be automatically activated by an enabled policy and, therefore, consume a license; if the number of licenses has been exceeded, the policy will not be able to activate the VTG.

- Cisco IPICS PMC Usage—A PMC user consumes a license each time that the user logs in to a PMC session.
  - If the same PMC user logs in to multiple PMC sessions from different PMC client machines, that user will consume multiple licenses (one for each PMC session).

Note If all Cisco IPICS licenses have been used, PMC user access to the system will be interrupted. Make sure that you are aware of the current status of PMC licenses and that additional user licenses are purchased and installed immediately if this situation occurs.

Additional licenses may be purchased at any time for some or all of the licensable features (Cisco IPICS ports, PMC users, Cisco Unified IP Phone users).

Cisco IPICS does not support removal or reduction of the number of licenses.

Caution Cisco IPICS does not support the edit or modification of the license file name or file contents in any capacity. If you change or overwrite the license file name, you may invalidate your license and cause the system to become inoperable.

Note If your server includes more than one network interface card (NIC), make sure that you configure the eth0 port, as documented in the *Cisco IPICS Server Installation Guide*. Cisco IPICS requires that you configure the eth0 port, even if

it is disabled, because the Cisco IPICS licensing mechanism performs its validation by using this NIC. Therefore, to ensure proper system operation, always configure the eth0 port.

Where to Find More Information

- *Cisco IPICS Server Installation Guide, Release 1.0(1)*
- *Cisco IPICS Server Administration Guide, Release 1.0(1)*
- *Cisco IPICS PMC Installation and User Guide, Release 1.0(1)*

Using Ops Views

Cisco IPICS provides the ability for you to organize or segment different entities, such as agencies, companies, departments, jurisdictions, municipalities, or sites, into separate views that are isolated from each other. In Cisco IPICS, these separate views are known as operational views, or ops views. While these views are maintained separately by the Cisco IPICS system administrator, this functionality also allows multiple entities to use one Cisco IPICS server to enable resource sharing across multiple ops views, according to business need.

Note The use of ops views allows segmentation of resources that authorized Cisco IPICS users may see on the Administration Console. It does not affect the channels and/or VTGs that may be assigned and viewable on the PMC or Cisco Unified IP Phone.

By default, Cisco IPICS disables the ops views functionality on the server. To enable this feature, you must purchase and install a Cisco IPICS license that includes a license for the ops views functionality; then, restart the server.

Tip You must restart the server to enable the ops views functionality.

You install this ops views license by uploading it to the server. Navigate to the **System Administrator > License** window in the Administration Console to view the license information.

Note Although the Ops Views check box is checked in the **System Administrator > Options** window by default, the feature is not actually enabled until you upload the license and restart the server. Make sure that you restart the server after you upload the license. For more information about enabling ops views, refer to the "Operational Views" chapter in the *Cisco IPICS Server Administration Guide*.

Tip Be aware that any changes to Cisco IPICS licensing (for example, license expiration or transition from a license that includes the ops views feature to a license that does not include ops views, or vice versa) requires you to restart the server.

When the ops view feature has been enabled on the server, the system displays a Cisco Ops View entry under the Configured License area in the License window, along with the word "Licensed" to indicate that the ops view functionality has been enabled. (When ops views is not enabled, this entry displays "Not Licensed.") Cisco IPICS also displays the number of available licenses and concurrent usage in this window. For more detailed information about license limits and current usage, navigate to the **System Administrator > Ops Views** window.

After you have installed the necessary license and restarted the server, the Ops Views window displays in the Administration Console and the ops views functionality becomes available for your use. To access the ops views window from the Administration Console, navigate to **System Administrator > Ops Views**. When you click **Ops Views**, the server displays the SYSTEM ops view by default. The SYSTEM ops view is the home base or system-wide view that Cisco IPICS administrators belong to; this view provides visibility across all of the ops views.

Cisco IPICS users who belong to the SYSTEM ops view have visibility to all ops views resources that are configured on the system.

Note Cisco IPICS displays the number of available licenses and concurrent usage information in the License browser window. As a best practice, make sure that you update your browser window often and before you perform any server administration functions to ensure that you are working with the most current information. If you attempt to perform an administration update in a window that

does not display the most current data, the update will not succeed and Cisco IPICS will display an error. If this situation occurs, update your browser window and retry the operation.

Only the system administrator can create new ops views on the server. Cisco IPICS allows the system administrator to create an unlimited number of ops views by navigating to the **System Administrator > Ops Views** link in the Administration Console.

After a new ops view has been created, the system administrator can associate resources, such as channels, to the ops view, while the operator creates an operator/dispatcher user to add to each individual ops view to enable ops view resource management.

Note When the ops views functionality is enabled, some Cisco IPICS user roles expand to assume additional responsibilities. For example, operators and dispatchers may assign resources, and define the resources that are accessible to, different ops views if they have the necessary permissions. Cisco recommends that each ops view contain at least one dispatcher and one operator to manage the resources that are visible to these roles.

When activated, the Cisco IPICS ops views feature adds attributes to various resources so that these resources can be owned and shared by different ops views. Ops views attributes apply to users, user groups, channels, channel groups, VTGs, and policies. You can view these attributes in the Ops View Attributes area of the Administration Console Edit (User/Channel) Details pane.

For detailed information about ops views, refer to the "Operational Views" chapter in the *Cisco IPICS Server Administration Guide.*

Where to Find More Information

- *Cisco IPICS Server Administration Guide, Release 1.0(1)*

Cisco IPICS Voice Quality Tips

Be aware of the following tips, which can help to ensure enhanced voice quality, when you use the PMC:

- Make sure that you use a high-quality headset and microphone, and check the placement and settings of both components, when you use the PMC. A high-quality and properly-configured headset can greatly enhance voice quality for both receive and transmit activity.
- For enhanced voice quality, make sure that you plug your USB headset or audio device into a dedicated USB port instead of a USB hub. The use of USB hubs, which multiplex data from USB devices into one data stream, can result in timing issues and impact voice quality.
- Check your audio settings to make sure that the volume is not set too low. If the volume is set low, increase the input gain on your microphone by sliding the bar up on the volume controls to increase the volume.
- For optimum connectivity, use the most appropriate location for your connection type when you log in to the PMC. For example, if you are using a wireless connection, choose the location that correlates to wireless connectivity for your organization. You can ensure higher quality audio by choosing the appropriate connection type.
- Make sure that you always use the most recent version of the PMC. Newer versions of software often contain voice quality updates that enhance functionality.
- Be aware that a slow-speed connection, such as a digital subscriber line (DSL) connection or any slow wired link, may affect voice quality. If possible, try to use a high-speed connection when you use the PMC.
- Try to limit the use of high-bandwidth applications on the PMC client machine at the same time that you use the PMC. If your CPU is overburdened by other programs that are running at the same time, there may insufficient CPU cycles for the PMC to run properly. Check the CPU activity on your PMC client machine and close any programs that do not need to be open.
- To ensure quality of service (QoS), the PMC installer attempts to install the Microsoft QoS Packet Scheduler service on each PMC client machine. The QoS Packet Scheduler ensures voice traffic priority across the network by marking each IP packet in the Differentiated Service Code Point (DSCP) with the highest value (expedited forwarding) during transmission between end points. However, this installation may not succeed if the PMC user does not have local administrative rights; in this situation, the network and the PMC client machine may drop or lose packets that are not marked by the QoS Packet Scheduler, which results in degraded voice quality. Therefore, you should check to make sure that the QoS Packet Scheduler has been installed

on each PMC client machine. For additional details and information about how to check for and install the Microsoft QoS Packet Scheduler, go to http://www.microsoft.com and search for "QoS Packet Scheduler."

Where to Find More Information

- *Cisco IPICS PMC Installation and User Guide, Release 1.0(1)*

Resolved Caveats for Cisco IPICS - Release 1.0(2)

You can find the latest resolved caveat information for this release of Cisco IPICS by using Bug Toolkit, which is an online tool that is available for customers to query defects according to their own needs.

Tip You need an account with Cisco.com (Cisco Connection Online) to use the Bug Toolkit to find open and resolved caveats of any severity for any release.

To access the Bug Toolkit, log on to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

This section includes the following topics:

Using Bug Toolkit

To access Bug Toolkit, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

To use Bug Toolkit, follow this procedure.

Procedure

Step 1 To access the Bug Toolkit, go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

Log on with your Cisco.com user ID and password.

Step 2 Click the **Launch Bug Toolkit** hyperlink.

Step 3 If you are looking for information about a specific caveat, enter the ID number in the "Enter known bug ID:" field.

To view all caveats for the Cisco IPICS server, go to the "Search for bugs in other Cisco software and hardware products" section, and enter **Cisco IPICS Server Software** in the Product Name field. Alternatively, you can scroll through the product name list and click **Cisco IPICS Server Software**.

To view all caveats for the PMC, enter **Cisco IPICS PMC Client Software** in the Product Name field or scroll through the product name list.

Step 4 Click **Next**. The Cisco IPICS search window displays.

Step 5 Choose the filters to query for caveats. You can choose any or all of the available options:

a. Choose the Cisco IPICS version:

- Choose the major version for the major releases (such as, 1.0).

  A major release contains significant new features, enhancements, architectural changes, and/or defect fixes.

- Choose the revision for more specific information; for example, choosing major version 1.0 and revision version 2 queries for release 1.0(2) caveats.

  A revision (maintenance) release primarily contains defect fixes to address specific problems, but it may also include new features and/or enhancements.

Note This option may not be available with the first release of a product.

b. Enter keywords to search for a caveat title and description, if desired.

c. Choose the Set Advanced Options, which includes the following items:

- Bug Severity level—Click the radio button that displays next to the specific severity level or the range of severity levels that you want to search for. The default specifies 1-3.
- Bug Status Group—Check the **Fixed** check box to search for resolved caveats. The default specifies Open and Fixed; to search for both open and fixed caveats, leave both of these check boxes checked.
- Release Note Enclosure—The default specifies Valid Release Note Enclosure.

d. Click **Next**.

Bug Toolkit returns the list of caveats on the basis of your query.

- You can modify your results by clicking the **Refine Search** button to submit another query and use different criteria.
- You can save your query for future use. See the "Saving Bug Toolkit Queries" section on page 60.

Note To see detailed online help about using Bug Toolkit, click **Help** on any Bug Toolkit window.

Saving Bug Toolkit Queries

Bug Toolkit allows you to create and then save your queries to monitor a specific defect or network situation. You can edit a saved search at any time to change the alert conditions, the defects being watched, or the network profile.

Follow this procedure to save your Bug Toolkit queries.

Procedure

Step 1 Perform your search for caveats, as described in the "Using Bug Toolkit" section on page 58.

Step 2 In the search result window, click the **This Search Criteria** button that displays on the results window.

A new window displays.

Step 3 In the Name of saved search field, enter a name for the saved search.

Step 4 Under My Bug Groups, use one of the following options to save your defects in a bug group:

- Click the **Existing group** radio button and choose an existing group name from the drop-down list box.
- Click the **Create new group named:** radio button and enter a group name to create a new group for this saved search.

Note This bug group will contain the bugs that are identified by using the search criteria that you have saved. Each time that a new bug meets the search criteria, the system adds it to the group that you chose.

Bug Toolkit saves your bugs and searches, and makes them available through the My Stuff window. (The My Stuff window allows you to view, create, and/or modify existing bug groups or saved searches. Choose the **My Stuff** link to see a list of all your bug groups.)

Step 5 Under Email Update Options, you can choose to set optional e-mail notification preferences if you want to receive automatic updates of a bug status change. Bug Toolkit provides the following options:

- **Do NOT send me any email updates**—If you choose this default setting, Bug Toolkit does not send e-mail notifications.
- **Send my updates to:**—Click the radio button to choose this option to send e-mail notifications to the user ID that you enter in this field. Additional notification options include
  - **Updates as they occur**—Bug Toolkit provides updates that are based on status change.
  - **Weekly summaries**—Bug Toolkit provides weekly summary updates.
- **Apply these email update options to all of my saved searches**—Check this check box to use these e-mail update options for all of your saved searches.

Step 6 To save your changes, click **Save**.

Step 7 A window displays the bug group(s) that you have saved. From this window, you can click a bug group name to see the bugs and the saved searches; you can also edit the search criteria.

Open Caveats for Cisco IPICS - Release 1.0(2)

Table 5 describes possible unexpected behaviors by Cisco IPICS release 1.0(2), sorted by component.

Tip For more information about an individual defect, click the associated Identifier in Table 5 to access the online record for that defect, including workarounds.

Understanding the To-be-fixed and the Integrated-releases Fields in the Online Defect Record

When you open the online record for a defect, you may see data in the "To-be-fixed" or "Integrated-releases" fields. The information that displays in these fields identifies the list of Cisco IPICS interim versions in which the defect was fixed. These interim versions then get integrated into Cisco IPICS releases.

Some versions include identification for Maintenance Releases (MR), Service Releases (SR) and/or Engineering Specials (ES). The following examples show the version number and its mapping to MR, SR, and ES releases:

- 1.0(1.1) = Cisco IPICS release 1.0 MR1 SR1
- 1.0(3.2.1) = Cisco IPICS release 1.0 MR3 SR2 ES1
- 1.2(2.0.201) = Cisco IPICS release 1.2 MR2 ES1 (in this example, no SR was released between MR2 and ES1)

The following examples show how you can decode the maintenance release interim version information. These examples show you the format of the interim version along with the corresponding Cisco IPICS release that includes that interim version. You can use these examples as guidance to better understand the presentation of information in these fields.

- 1.0(1.008) = Cisco IPICS release 1.0(2)
- 1.1(0.012) = Cisco IPICS release 1.1(1)

- 1.1(2.020) = Cisco IPICS release 1.1(3)
- 1.3(2.079) = Cisco IPICS release 1.3(3)

Note Because defect status continually changes, be aware that Table 5 reflects a snapshot of the defects that were open at the time this report was compiled. For an updated view of open defects, access Bug Toolkit and follow the instructions as described in the "Using Bug Toolkit" section on page 58.

Tip Bug Toolkit requires that you have an account with Cisco.com (Cisco Connection Online). By using the Bug Toolkit, you can find caveats of any severity for any release. Bug Toolkit may also provide a more current listing than this document provides. To access the Bug Toolkit, log on to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

Table 5 Open Caveats for Cisco IPICS Release 1.0(2)

Identifier	Headline
	Server Caveats
	Component: audio-ipphone
CSCsc35204	When you hold the PTT softkey on the Cisco Unified IP Phone and then stop talking, the LMR gateway unkeys the radio or causes the PMC receive indicator to blink intermittently. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc35204
	Component: db-server
CSCsd64476	When you export data by using one version of Cisco IPICS and then recover the data by using a different version, an incorrect version of the pmcinst.exe file displays in the Administration Console. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd64476
CSCse27719	A system problem causes the Administration Console page refresh mechanism to incorrectly display a database backup as continually in progress even if the backup has succeeded. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse27719

Table 5 Open Caveats for Cisco IPICS Release 1.0(2) (Continued)

Identifier	Headline
CSCse30292	If you perform a backup to a local directory that is not readable by the informix user, you will not be able to perform a restore from that directory. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse30292
CSCse31799	Backup attempts fail when you use a local or remote directory name that includes a space because the backup process does not support spaces in the directory names. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse31799
CSCse31821	Cisco IPICS may report incorrect backup or restore results when you perform a remote backup or restore operation by using secure copy (scp). http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse31821
CSCse32554	After you perform a database restore, the Administration Console may display incorrect version information for the pmcinst.exe file. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse32554
CSCse38355	If the security key for a trusted remote host changes (for example, as the result of reinstalling the operating system), the Cisco IPICS remote database backup and restore operations fail with the “Remote Host Identification has Changed” error. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse38355
	Component: installer-server
CSCsb71419	The server displays the console mode password entries in clear text. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb71419
CSCsc26642	When you run the server uninstaller in console mode, the uninstaller does not prompt you to continue or terminate the uninstallation. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc26642
CSCsd52866	The Cisco IPICS uninstallation process may unexpectedly terminate when you execute the uninstaller in GUI mode. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd52866
CSCsd64615	When you upgrade the server software and recover data from an exported dataset that was created before the upgrade, the pmc.dll that existed before the upgrade is no longer on the system. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd64615

Table 5 Open Caveats for Cisco IPICS Release 1.0(2) (Continued)

Identifier	Headline
CSCsd80306	If you create a system user name that is the same as the user names that are used by the Cisco IPICS system, the root password becomes corrupted. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd80306
CSCse30206	Under certain circumstances, some of the necessary components may not be installed on the server when you execute the installer in GUI mode. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse30206
	Component: ipphone-interface
CSCsb64542	The Cisco Unified IP Phone 7960 disconnects the incoming call when the user is logged into the Cisco IPICS service and not using the handset to participate in the call. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb64542
CSCsb64556	The Cisco Unified IP Phone 7960 does not preserve the state of the mute and speaker buttons when you use the phone in handset mode. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb64556
CSCsb81654	The Cisco Unified IP Phone 7970 does not preserve the state of the mute or speaker buttons when it is operating in handset mode. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb81654
CSCsc45962	Cisco IPICS does not enforce IP phone license count when you use the Cisco Unified IP Phone 7970. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc45962
	Component: log-server
CSCse30200	The system returns an error when you try to purge the activity log if it is 100% full. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse30200
	Component: media-server
CSCse21137	When you add an RMS in the Administration Console, the system appends an erroneous string to the hostname; in this situation, the running configuration includes “hostname” on multiple lines so that you cannot configure the RMS. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse21137
	Component: other-server

Table 5 Open Caveats for Cisco IPICS Release 1.0(2) (Continued)

Identifier	Headline
CSCsd44039	The PMC license usage count may display incorrectly in the Administration Console if Ops Views has been disabled and then reenabled. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd44039
CSCsd92965	The secure flag on a channel does not prevent it from being included in a VTG with nonsecure channels. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd92965
	Component: pmc-interface
CSCsc54069	PMC activity does not appear in the server activity logs for PMC users who have user names that contain international characters. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc54069
CSCsd94871	When RMS resources become available, the system does not automatically reenable PMC channels that have been disabled because of insufficient RMS resources. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd94871
	Component: rms-interface
CSCsb60367	When a parent VTG is added to a child VTG (and creates a second path), voice that is transmitted on either VTG can cause a packet storm and render the VTGs unusable for communication. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb60367
CSCsc42669	When users concurrently add loopbacks on the same RMS by using two different browser windows, Cisco IPICS overwrites the intermediate changes and saves the latest changes. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc42669
CSCsc47662	Cisco IPICS disables most of the assigned channels or VTGs when remote PMC users are assigned more than 16 channels or VTGs. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc47662
CSCsc66276	Resource contention issues may occur under heavy load conditions when many users log in simultaneously or when operators start and/or modify many VTGs. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc66276

Table 5 Open Caveats for Cisco IPICS Release 1.0(2) (Continued)

Identifier	Headline
CSCsc66305	Cisco IPICS may not successfully process all operations when some RMS operations, such as Update Configuration, consume a large number of resources. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc66305
CSCsc86446	SIP-based PMC calls may disconnect after 30 minutes if there is no voice traffic. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc86446
CSCsc54783	No RMS cleanup process exists when all resources are consumed on an RMS that becomes disconnected and subsequently unreachable. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd54783
	Component: ui-server
CSCsb98486	On Windows 2000 machines, the Administration Console login timeout functionality works intermittently. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb98486
CSCsc36900	When an RMS is added in two browser windows concurrently, the RMS gets added with an incorrect state. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc36900
CSCsc55624	Cisco IPICS displays an Action Exception error message when you press the Enter key while certain fields are displayed. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc55624
CSCsc56765	When you schedule a daily backup to a remote host, Cisco IPICS saves the password and destination directory in clear text. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc56765
CSCsc80025	Cisco IPICS displays a VTG loop error when you add two sub-VTGs to two different parent VTGs. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc80025
CSCse31673	If you perform a backup while a VTG is in the pending activation state, the VTG may be permanently held in this pending state upon restore. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse31673

Table 5 Open Caveats for Cisco IPICS Release 1.0(2) (Continued)

Identifier	Headline
CSCse32609	The system exhibits unexpected behavior when the hard disk drive on the server runs out of space because of a large number of database backup images or log files. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse32609
	PMC Caveats
	Component: audio-pmc
CSCsb47768	You may need to stop and restart the PMC if you attach an audio device to the system after the PMC has been started. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb47768
CSCsb91007	Active PMC SIP channels may be dropped and may not automatically reconnect after you restart the system. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb91007
CSCsc39798	Under heavy load, a SIP-based PMC connection may suddenly deactivate when the PMC user is connected over a VPN. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc39798
CSCsc74133	The audio output that is generated by the PMC is not equal across all audio types. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc74133
CSCse11184	On some systems, the PMC continues to transmit audio when the microphone is muted. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse11184
CSCse27646	The PMC cannot open the system microphone when the Cisco Unified VT Advantage client is performing a video check. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse27646
CSCse35759	When the PMC receives audio over a network with high jitter characteristics, such as a satellite link, the audio transmission sounds choppy when it is received and played out on the PMC. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse35759
	Component: debug-pmc

Table 5 Open Caveats for Cisco IPICS Release 1.0(2) (Continued)

Identifier	Headline
CSCse36568	Media-related PMC debug tracing needs to be enhanced to enable easier interpretation. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse36568
	Component: other-pmc
CSCsb69044	Voice quality may be impacted when the auto-update download process occurs. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb69044
CSCsb93731	The ipics.log file reports an exception in PMCActivityLogUpdate.parseChannelActivityLog() when the log file is malformed. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb93731
CSCsc50922	An activated VTG may not appear on the PMC. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc50922
CSCsd28540	Under specific circumstances, the PMC gets a busy indication when it attempts to activate a channel after logging in from a remote location. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd28540
CSCsd33374	When a PMC client machine has two active network interface connections, it must be able to connect to the RMS Loopback0 IP address to set up a SIP-based call. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd33374
CSCsd49103	The PMC may not connect to the server if the first of several possible network adapters fails during startup. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd49103
CSCsd66185	The PMC receives one-way audio after the Cisco Unified VT Advantage release 1.02 software drivers are installed. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd66185
CSCsd82546	The PMC client machine freezes when the PMC is running and the laptop is undocked. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd82546
CSCse00546	After an RMS restart and/or reload, channels that you log in to as remote appear to be active when they are non-operational. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse00546

Table 5 Open Caveats for Cisco IPICS Release 1.0(2) (Continued)

Identifier	Headline
CSCse12376	SIP-based channels become disabled after you exit the PMC in offline mode and then relaunch the PMC twice in succession. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse12376
CSCse27351	When you launch the PMC from a remote location, an automatically activated VTG causes intermittent, unexpected Real-time Transport Protocol (RTP) traffic. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse27351
	Component: ui-pmc
CSCsd59000	Because the PMC saves channel locations, the PMC displays a message to warn you that there are more channels than the PMC can display when the PMC is assigned more than 8 channels and the channels are subsequently removed; in this situation, the PMC does not display the additional channels. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd59000
CSCsd71907	The PMC becomes unresponsive if you do not click Apply after you change the spatial location for each channel. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd71907
CSCse06353	In certain situations, the PMC may appear to be connected to the server and the RMS even after it has lost connectivity to these components. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse06353

Documentation Updates

This section provides documentation changes that were unavailable when the Cisco IPICS release 1.0 documentation suite was released.

This section contains the following types of documentation updates:

Errors

This section includes information about errors in the Cisco IPICS Documentation suite.

Incorrect Reference to the Cisco IPICS Data Store Component

The "Installed Components" section in the "Overview" chapter in the *Cisco IPICS Server Installation Guide* incorrectly documents one of the installed components as Cisco IPICS Data Store (IBM Informix Database Server, version 10.0). This section should reflect Cisco IPICS Data Store (IBM Informix Dynamic Server, version 10.00.UC1).

Correction to Procedure to Upgrade Cisco IPICS Server Software

The "Upgrading Cisco IPICS" chapter in the *Cisco IPICS Server Installation Guide* specifies an incorrect sequence of steps to follow to upgrade the Cisco IPICS server software. The following information provides a correction to this procedure.

Note Before you begin the upgrade procedure, make sure that you back up your data and log files. For more information about backup and restore procedures, refer to the *Cisco IPICS Backup and Restore Guide*.

To upgrade Cisco IPICS from a CD, perform the following procedure:

Procedure

Step 1 Log in to the Cisco IPICS server by using the root user account and password.

The Cisco Linux desktop displays.

Step 2 Insert the Cisco IPICS installation CD into the server disk drive.

If CSA is not installed on the server, or if it is not running, continue with Step 4.

If CSA is installed on the server, you will be prompted with a CSA access permission dialog box.

Step 3 In the CSA access permission dialog box, click **Yes** to grant permission to the installation; then, click **Apply**.

Note Whenever CSA prompts you for permission, while you are performing installation-related activities on the server, be sure to always click **Yes** to grant permission and continue with that operation before CSA times out based on its default value of No.

The Cisco IPICS CD icon displays on the desktop.

Step 4 To open the CD contents, double-click the CD icon.

Cisco Linux displays a window that shows the Cisco IPICS installer file. The following name provides an example of the installation executable file name:

```
install_ipics_1_0_2.bin
```

Note The exact name of the installation executable file changes with each version as the new version number is incorporated into the name.

Step 5 To start the installation, double-click the installer file icon.

Cisco Linux displays a message that allows you to choose to display the file contents or run the installer file.

Step 6 When you are prompted to display the file contents or run the installer files, click **Run in Terminal**.

Note If you click **Run**, instead of **Run in Terminal**, you will experience a delay of a few minutes while the installer completes background security processes, such as extracting the necessary files for the installation. During this time, the screen may be appear unresponsive. Make sure that you do not click **Run** or **Run in Terminal** again so that you do not start an additional instance of the installer.

Step 7 To continue with the installation, click **Next**.

The Cisco IPICS installer displays the End User License Agreement.

Step 8 Scroll through the License Agreement to view the entire text. After you have read the text, click the **I accept the terms of the License Agreement** radio button. Then, click **Next**.

Note To continue, you must accept the terms of the End User License Agreement.

The Choose Install Set window displays with the following installation options:

- Typical—This option installs the Cisco IPICS server software and the Cisco Security Agent (CSA) software.
- Customize—This option allows you to customize your installation by providing you with the option to not install CSA as part of the Cisco IPICS server software installation. The default specifies "Install CSA."
- Upgrade—This option allows you to upgrade your version of the Cisco IPICS server software.

Step 9 To upgrade the Cisco IPICS server software, click **Upgrade**. Then, click **Next**.

The installer prompts you to change the password for the informix user.

Step 10 Enter a password for the informix user that is at least eight characters in length. Then, press **Tab** and reenter the password to confirm it. Click **Next**.

Caution Make sure that you only change the password for the informix user when you perform a Cisco IPICS installation or upgrade procedure by using the installer. If you manually change the informix password outside of the installation or upgrade process, the Cisco IPICS Administration Console becomes unusable.

The installer prompts you to change the password for the ipics user.

Step 11 Enter a password for the ipics user that is at least eight characters in length. Then, press **Tab** and reenter the password to confirm it. Click **Next**.

The Cisco IPICS installer displays the Preinstallation Summary

This summary includes information, such as the product name and version, the destination folder for the installation, the amount of disk space that is required for the installation, and the available disk space.

Step 12 To continue, click **Install.**

The Installation Progress window displays, showing the files and folders that are being written to the disk.

When the upgrade completes, the Cisco IPICS Install Complete window displays.

Step 13 To close the installer, click **Next**.

The Cisco Linux desktop displays.

Correction to User Minimum Password Length

The "Managing Your User Profile" section in the "Administration Console: User Tasks" chapter and the "Adding a User Section" in the "Administration Console: Operator Tasks" chapter in the *Cisco IPICS Server Administration Guide* incorrectly states that the user password must contain at least 8 characters.

Cisco IPICS specifies 8 characters as the default minimum password length, however, the System Administrator can configure this setting in the **System Administrator > Options** window to range from 1 to 20 characters.

These sections should state that the default Cisco IPICS minimum password length contains 8 characters, but the user password may contain more or less characters, depending on the configuration in the server.

Note Cisco recommends that you use a minimum of 8 characters for user passwords.

Changes

This section contains changes that have occurred since the original release of the Cisco IPICS release 1.0 documentation. These changes may not appear in the current documentation or the online help for the Cisco IPICS application.

- Support for E1 Connectivity, page 78
- Support for Cisco Unified Wireless IP Phone 7920, page 84

Clarification to PMC User Name Case Sensitivity

The *Cisco IPICS PMC Quick Start Guide, Release 1.0(1)* states that user names and passwords are case-sensitive. PMC user names are actually case-insensitive; that is, you can enter user names by using either lower case or upper case characters.

The text in the *Cisco IPICS PMC Quick Start Guide* should state the following text to reflect this functionality:

Be aware that user names are case-insensitive; that is, you can enter either upper case or lower case characters for your PMC user name. However, passwords are case-sensitive.

Enhancement to the PMC Channels Menu for Audio Playback

The PMC Channels menu has been enhanced to include the following new option:

Spatial Position—This field enables audio playback for selected channels on different speakers by allowing you choose the speaker that the selected channel uses. You can configure spatial playback for a specific channel by highlighting the channel and then choosing one of the following options for that channel:

- **Stereo**—This option, as the default value, plays out the channel audio by using both speakers.
- **Left**—This option plays out the channel audio by using only the left speaker.
- **Right**—This option plays out the channel audio by using only the right speaker.

18-Channel PMC Skin Enhancement

The PMC Skin menu has been enhanced to include an 18-channel mouse skin. This higher-capacity, mouse-based 18-channel skin displays in the following format: three columns by six rows, for a total of 18 channels.

You may configure your PMC to display this new skin by choosing the Cisco IPICS Mouse 18-Channel skin in the PMC Skin menu. You can access the Skin menu by navigating to **Settings > Skin** in the PMC application.

The 18-channel skin contains the same features as the 4-channel and 8-channel skins; however, Cisco IPICS supports additional keyboard assignments only for channels 9 and 10. See Table 4 for the keystroke assignments that Cisco IPICS supports.

Be aware that the 18-channel skin has specific minimum hardware requirements, as described in the "PMC Requirements" section on page 9.

For more information about configuring PMC skins, refer to the "Customizing the PMC Application" chapter in the *Cisco IPICS PMC Installation and User Guide*.

New Prompt for ipics User Password

In Cisco IPICS release 1.0(1), users were not prompted to change the ipics user password as part of the installation process. Instead, Cisco IPICS defaulted the ipics user password to "cisco123."

Cisco IPICS release 1.0(2) changes this behavior by now prompting you to change the password for the ipics application-level user during the Cisco IPICS server software installation and upgrade procedures.

The ipics user is the Cisco IPICS application-level user. This user can perform all administration functions that are related to the Cisco IPICS application. You use the ipics user ID to log in to the Cisco IPICS Administration Console.

Note When you are prompted by the installer to change the ipics user password, make sure that you use a password that is at least eight characters in length.

Server Enhancement to the Auto Update Feature for the PMC

In release 1.0(2), Cisco IPICS simplifies the PMC auto update process by providing the ability for you to maintain automatic updates for the PMC without the need to first generate the PMC and then upload the PMC.dll file to the server.

With this enhancement, Cisco IPICS now adds the PMC.dll file as part of the server installation file and automatically uploads the PMC.dll file to the server whenever you install or upgrade the server software.

The following procedure provides an update to the "Managing PMC Automatic Updates" section in the "Administration Console: System Administrator Tasks" chapter in the *Cisco IPICS Server Administration Guide*.

Note Be aware that the PMC automatic update process installs the PMC.dll file only; with this update, the PMC skins and the online help are not updated. To get the latest, fully executable version, you need to uninstall and reinstall the PMC application.

To configure the recommended download version for the auto update feature of the PMC, perform the following procedure:

Procedure

Step 1 On your client machine, open a supported version of the Internet Explorer browser.

Step 2 In the Location or Address field, enter the following URL, replacing *IP address* with the IP address of the Cisco IPICS server:

http://<*IP address***>**

The Cisco IPICS Login window displays.

Step 3 Log in to the Cisco IPICS server by using the system administrator user name and password.

The Cisco IPICS server Administration Console displays.

Step 4 From the **System Administrator** tab, click the **PMC Auto Update** link.

The PMC version information displays.

In the PMC Versions pane, you can configure the following PMC versions:

- Maximum Available Version—This version represents the maximum software version that is available to run on the PMC.
- Minimum Supported Version—This version represents the minimum software version that is required to run on the PMC.
- Recommended Download Version—This version represents the recommended software version that should be run on the PMC.

Step 5 To set the auto update version for the PMC, choose the applicable version from the Recommended Download Version drop-down list box; then click **Save**.

Step 6 From your PMC client machine, launch the PMC application by choosing one of the following options:

- Double-click the **PMC** icon that appears on your desktop.
- Navigate to **Start > Programs > Cisco IPICS > PMC**; then, click the **PMC** icon.

The Cisco IPICS login dialog box displays.

Step 7 Enter your **user name** and **password**; then, click **OK**.

The PMC checks for the recommended version of software. If the PMC is not running a version that is greater than or equal to the recommended version, a pop-up dialog box displays to inform you and prompts you to download and run the recommended version.

Step 8 To download PMC.dll file for the recommended version and run it on your PMC client machine, click **Yes**.

After the PMC.dll file downloads to the PMC client machine, the location selection dialog box displays. By default, the new PMC version displays in the PMC Version field.

Step 9 Choose your default location and your PMC version from the drop-down list boxes; then, click **OK**.

Note The PMC Version drop-down list box includes the PMC versions that are installed on your client machine and compatible with the server.

The PMC application opens on your desktop.

Support for E1 Connectivity

With this release, Cisco IPICS expands your connectivity options by adding RMS configuration support for E1 connectivity. (For guidelines to follow when you configure an RMS router for E1 connectivity, see the "Enhanced Support for E1 Connectivity" section on page 35.)

To enable E1 connectivity, configure E1 controllers for individual voice ports (as you would configure for T1 controllers). The following command specifies the ds0 time slots that define logical voice ports on an E1 controller and configure the signaling type by which the router communicates with the PSTN:

ds0-group *ds0-group-number* **timeslots** *timeslot-list* **type e&m-lmr**

where:

- **ds0-group** *ds0-group number* identifies the ds0 group; for E1 connectivity, the allowable values range from 0 to 29.

Note Be aware that ds0 groups must start with 0 and they must be sequential.

- **timeslots** *timeslot-list* specifies a single time-slot number; for E1 connectivity, the allowable values range from 1 to 31.

For detailed configuration information, see the following procedure, which adds configuration information for E1 controllers and provides an update to the "RMS Configuration" appendix in the *Cisco IPICS Server Administration Guide.*

To configure E1 controllers on an RMS and enable it to interact with the Cisco IPICS server, perform the following procedure.

Procedure

Step 1 If you are using a T1/E1 combination interface card, such as the Cisco 1- and 2-port T1/E1 Multiflex Trunk (MFT) Voice/WAN Interface Card (VWIC2) and want to replace the T1 with an E1, enter the following command to change the card type configuration:

Router(config)# **no card type t1** *slot* [*bay*]

where:

slot specifies the port number of the interface, and *bay* is an optional parameter that specifies the card interface bay number in a slot on certain route/switch processor [RSP] platforms.

An example of this command appears below:

```
Router(config)# no card type t1 0 3
```

Note When you use the card type command to change your configuration, be aware that changes become effective only after you reload or reboot the router.

Step 2 Exit the router configuration mode by entering the following command:

Router(config)# **exit**

Step 3 Execute the following commands to save your changes and to reload the router:

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

Step 4 Configure the card type for E1 connectivity by entering the following command:

Router(config)# **card type e1** *slot* [*bay*]

where:

slot specifies the port number of the interface and *bay* is an optional parameter that specifies the card interface bay number in a slot on certain route/switch processor [RSP] platforms.

An example of this command appears below:

```
Router(config)# card type e1 0 3
```

Step 5 Configure ds0 groups on the E1 controllers by entering the following commands in the router configuration.

Note
- The clock command should be used for only one of the two E1 controllers in the loopback.
- In E1 framing and signaling, 30 of the 32 available channels, or time slots, are used for voice or data transmission. Time slot 0 and time slot 16, which you do not configure, do not carry voice or data. Time slot 0 provides frame synchronization, alarm transport, and international carrier use while time slot 16 provides supervisory signaling for the 30 voice and data channels.

a. To configure the first controller in the loopback pair, enter the following commands:

Router(config)# **controller e1** *slot port*
Router(config-controller)# **clock source internal**
Router(config-controller)# d**s0-group 0 timeslots 31 type e&m-lmr**
Router(config-controller)# **ds0-group 1 timeslots 1 type e&m-lmr**
Router(config-controller)# **ds0-group 2 timeslots 2 type e&m-lmr**
Router(config-controller)# **ds0-group 3 timeslots 3 type e&m-lmr**
Router(config-controller)# **ds0-group 4 timeslots 4 type e&m-lmr**
Router(config-controller)# **ds0-group 5 timeslots 5 type e&m-lmr**
Router(config-controller)# **ds0-group 6 timeslots 6 type e&m-lmr**
Router(config-controller)# **ds0-group 7 timeslots 7 type e&m-lmr**
Router(config-controller)# **ds0-group 8 timeslots 8 type e&m-lmr**
Router(config-controller)# **ds0-group 9 timeslots 9 type e&m-lmr**
Router(config-controller)# **ds0-group 10 timeslots 10 type e&m-lmr**
Router(config-controller)# **ds0-group 11 timeslots 11 type e&m-lmr**
Router(config-controller)# **ds0-group 12 timeslots 12 type e&m-lmr**
Router(config-controller)# **ds0-group 13 timeslots 13 type e&m-lmr**
Router(config-controller)# **ds0-group 14 timeslots 14 type e&m-lmr**
Router(config-controller)# **ds0-group 15 timeslots 15 type e&m-lmr**
Router(config-controller)# **ds0-group 16 timeslots 30 type e&m-lmr**
Router(config-controller)# **ds0-group 17 timeslots 17 type e&m-lmr**
Router(config-controller)# **ds0-group 18 timeslots 18 type e&m-lmr**
Router(config-controller)# **ds0-group 19 timeslots 19 type e&m-lmr**
Router(config-controller)# **ds0-group 20 timeslots 20 type e&m-lmr**
Router(config-controller)# **ds0-group 21 timeslots 21 type e&m-lmr**
Router(config-controller)# **ds0-group 22 timeslots 22 type e&m-lmr**
Router(config-controller)# **ds0-group 23 timeslots 23 type e&m-lmr**
Router(config-controller)# **ds0-group 24 timeslots 24 type e&m-lmr**
Router(config-controller)# **ds0-group 25 timeslots 25 type e&m-lmr**
Router(config-controller)# **ds0-group 26 timeslots 26 type e&m-lmr**
Router(config-controller)# **ds0-group 27 timeslots 27 type e&m-lmr**
Router(config-controller)# **ds0-group 28 timeslots 28 type e&m-lmr**
Router(config-controller)# **ds0-group 29 timeslots 29 type e&m-lmr**
Router(config-controller)# **no shutdown**

where:

slot port specifies the backplane slot number and port number on the interface. An example of this command appears below:

```
Router(config)# controller e1 0/3/0
```

b. To configure the second controller in the loopback pair, enter the following commands:

Router(config)# **controller e1** *slot port*
Router(config-controller)# d**s0-group 0 timeslots 31 type e&m-lmr**
Router(config-controller)# **ds0-group 1 timeslots 1 type e&m-lmr**
Router(config-controller)# **ds0-group 2 timeslots 2 type e&m-lmr**
Router(config-controller)# **ds0-group 3 timeslots 3 type e&m-lmr**
Router(config-controller)# **ds0-group 4 timeslots 4 type e&m-lmr**
Router(config-controller)# **ds0-group 5 timeslots 5 type e&m-lmr**
Router(config-controller)# **ds0-group 6 timeslots 6 type e&m-lmr**
Router(config-controller)# **ds0-group 7 timeslots 7 type e&m-lmr**
Router(config-controller)# **ds0-group 8 timeslots 8 type e&m-lmr**
Router(config-controller)# **ds0-group 9 timeslots 9 type e&m-lmr**
Router(config-controller)# **ds0-group 10 timeslots 10 type e&m-lmr**
Router(config-controller)# **ds0-group 11 timeslots 11 type e&m-lmr**
Router(config-controller)# **ds0-group 12 timeslots 12 type e&m-lmr**
Router(config-controller)# **ds0-group 13 timeslots 13 type e&m-lmr**
Router(config-controller)# **ds0-group 14 timeslots 14 type e&m-lmr**
Router(config-controller)# **ds0-group 15 timeslots 15 type e&m-lmr**
Router(config-controller)# **ds0-group 16 timeslots 30 type e&m-lmr**
Router(config-controller)# **ds0-group 17 timeslots 17 type e&m-lmr**
Router(config-controller)# **ds0-group 18 timeslots 18 type e&m-lmr**
Router(config-controller)# **ds0-group 19 timeslots 19 type e&m-lmr**
Router(config-controller)# **ds0-group 20 timeslots 20 type e&m-lmr**
Router(config-controller)# **ds0-group 21 timeslots 21 type e&m-lmr**
Router(config-controller)# **ds0-group 22 timeslots 22 type e&m-lmr**
Router(config-controller)# **ds0-group 23 timeslots 23 type e&m-lmr**
Router(config-controller)# **ds0-group 24 timeslots 24 type e&m-lmr**
Router(config-controller)# **ds0-group 25 timeslots 25 type e&m-lmr**
Router(config-controller)# **ds0-group 26 timeslots 26 type e&m-lmr**
Router(config-controller)# **ds0-group 27 timeslots 27 type e&m-lmr**
Router(config-controller)# **ds0-group 28 timeslots 28 type e&m-lmr**
Router(config-controller)# **ds0-group 29 timeslots 29 type e&m-lmr**
Router(config-controller)# **no shutdown**

where:

slot port specifies the backplane slot number and port number on the interface. An example of this command appears below:

```
Router(config)# controller e1 0/3/1
```

Step 6 Continue with Step 2 of the RMS configuration procedure that is documented in the "RMS Appendix" in the *Cisco IPICS Server Administration Guide* and follow this procedure to Step 7.

Step 7 Create a voice class that will be applied to all voice configurations by entering the following commands in the router configuration:

Router(config)# **voice class permanent 1**
Router(config-class)# **signal timing oos timeout disabled**
Router(config-class)# **signal keepalive disabled**
Router(config-class)# **signal sequence oos no-action**
Router(config-class)# **signal pattern idle transmit 0000**

Step 8 Continue with the remaining steps in the RMS configuration procedure that is documented in the "RMS Appendix" in the *Cisco IPICS Server Administration Guide*.

Step 9 If you reconfigured a T1/E1 combination interface card from T1 to E1 mode, you may need to reset the loopback cable. To determine if you need to reset the loopback cable, take one of the following actions:

- Check the LEDs on the interface card to see if the LP LED is amber.

  This LED should be off during normal operation.

- Enter the following CLI command to determine if there are alarms or errors displayed by the controller:

  Router# **show controllers e1**

  The command output should display the e1 in an "up" state with no alarms, as shown in the following sample output:

  ```
  e1 3/0 is up
  No alarms detected
  ```

  If the output displays the e1 in a "down" state, as shown in the following example, continue with Step 10:

  ```
  e1 3/1 is down
  alarm-trigger is not set
  ```

Step 10 To resolve this problem, disconnect the loopback cable from the router; then, reconnect it.

The LP LED should now be off.

Step 11 Verify that the e1 is up by entering the **show controllers e1** command, as shown in Step 9. The command output should display the e1 controllers in an "up" state, with no alarms detected, as shown in the following sample output:

```
e1 3/0 is up
No alarms detected

e1 3/1 is up
No alarms detected
```

For a complete update of the RMS configuration information, see the "Update to the RMS Configuration Information" section on page 94.

Support for Cisco Unified Wireless IP Phone 7920

With this release, Cisco IPICS adds support for the Cisco Unified Wireless IP Phone 7920.

The following information provides an update to the procedure in the "Setting Up and Using the Cisco Unified IP Phone with Cisco IPICS" appendix in the *Cisco IPICS Server Administration Guide*.

Using Cisco IPICS as a Service on the Cisco Unified IP Phone

Cisco Unified CallManager users can access the Cisco IPICS service directly from the Cisco Unified IP Phone after they have subscribed to the service.

To subscribe, access, and use the Cisco IPICS service on the Cisco Unified IP Phone, perform the following procedure:

Procedure

Step 1 To subscribe to the Cisco IPICS service, log in to the Cisco Unified CallManager User Options web site.

For more information about accessing the Cisco Unified CallManager User Options web site, and for additional information about the phone features for your specific model IP phone, refer to the Cisco Unified IP Phone documentation at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/index.htm

Step 2 From the Cisco Unified CallManager User Options Menu, choose your device type or profile from the drop-down list box.

Step 3 From the Cisco Unified CallManager User Options Menu, choose **Configure your Cisco IP Phone Services**.

Cisco Unified CallManager displays a list of subscribed services and also allows you to choose from a list of available services.

Step 4 In the Available Services drop-down list box, choose the **Cisco IPICS** service; then, click **Continue**.

Step 5 To subscribe to the Cisco IPICS service, click **Subscribe**.

The information that had been configured in Cisco Unified CallManager Administration, such as the service description, the IP address of the Cisco IPICS server, and the path to the service, displays in this window.

Step 6 Click **Log Off** to log off the Cisco Unified CallManager User Options web site.

Step 7 To access the Cisco IPICS service, take one of the following actions, depending on your specific model IP phone:

- To access the Cisco IPICS service on the Cisco Unified IP Phone model 7960 or 7970, press the **Services** button on the Cisco Unified IP Phone.
- To access the Cisco IPICS service on the Cisco Unified Wireless IP Phone 7920, follow these steps:
  a. Press the **Menu** softkey.
  b. Press the right or left arrow key to scroll to the **Services** menu.
  c. Press the **Select** softkey.

Note To enhance usability, you can customize the softkeys on the Cisco Unified Wireless IP Phone 7920 to enable direct access to the Services menu. For more information, refer to the Cisco Unified CallManager documentation at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/

Step 8 Use the Navigation button to scroll through the list and highlight the **Cisco IPICS** service; then press the **Select** softkey.

Step 9 Log in to the IP phone by entering a numeric **Digit ID** and **PIN**; then, press the **Submit** softkey.

The server includes the configuration that defines your corresponding digit ID and digital password in your user profile.

After you log in to the phone, Cisco IPICS displays the list of channels and/or VTGs that have been assigned to you and activated for your use.

Note The channels and/or VTGs that display in the menu are those that are available when the Cisco IPICS service starts. To view an updated list of channels, you must press the **Update** softkey. The Cisco IPICS server does not automatically download channel or VTG information to the phone until you press this softkey.

Step 10 Press the **Update** softkey to receive any new channels and/or VTGs.

Note Be aware that you must press the **Update** softkey to receive channel and/or VTG updates from the server.

Step 11 To participate in a channel or VTG, use the Navigation button to scroll to the specific channel or VTG in which you want to participate; then press the **Select** softkey.

When you choose a channel or VTG from this menu, that conference becomes active on your IP phone.

Step 12 To talk on the channel or VTG, press and hold the **PTT** softkey.

Note If you want to latch, or lock in, the channel or VTG, press the **Latch** softkey on the Cisco Unified IP Phone model 7960 or 7970. You can disengage the latch by pressing the **Stop** softkey.

To latch the channel or VTG on the Cisco Unified Wireless IP Phone 7920, press the right or left arrow key to scroll to Latch; then, press the **Latch** softkey. You can disengage the latch by pressing the right or left arrow key to scroll to Stop; then press the **Stop** softkey.

Step 13 When you are done talking, release the **PTT** softkey to return to listen-only mode.

Step 14 To log out of the Cisco IPICS service, take one of the following actions, depending on your specific model IP phone:

- If you are using a Cisco Unified IP Phone model 7960 or 7970, press the **Logout** softkey when you are done using the Cisco IPICS service.
- If you are using a Cisco Unified Wireless IP Phone 7920, press the right or left arrow key to scroll to Logout; then, press the **Logout** softkey.

Note Upon completion of your session, make sure that you press the **Logout** softkey to log out of the Cisco IPICS service.

Omissions

This section lists new and additional information that the current version of the Cisco IPICS documentation may not include:

Updated Loopback0 Information for Adding an RMS

The “Adding an RMS” section in the “Administration Console: System Administrator Tasks” chapter in the *Cisco IPICS Server Administration Guide* does not identify the Loopback0 interface that you configure in the IP address field as the address that is assigned to the RMS router.

The following information provides an update to Step 2a of this procedure:

Procedure

Step 2a. In the IP Address field, enter the IP address of the Loopback0 interface that is assigned to the RMS router.

Note This loopback address must be configured to support SIP calls on the PMC. (The PMC uses this IP address to connect to the RMS.) If the PMC cannot establish connectivity to the RMS, PMC users may experience channel activation issues (such as fast busy) when they attempt a SIP-based remote connection.

This section also includes the following update to this information:

- IP Address—IP address of the Loopback0 Interface that is assigned to the RMS router.

Note The PMC uses this IP address to connect to the RMS. The PMC must be able to establish connectivity to the RMS; otherwise, PMC users may be unable to activate channels by using the SIP-based remote connection type.

Clarification to the Adding a User to a User Group Procedure

The "Adding a User to a User Group" section in the "Administration Console: Operator Tasks" chapter in the *Cisco IPICS Server Administration Guide* does not clarify the affect of displaying the details of a user group when you add a user to a user group.

The following information provides an update to Step 1 of this procedure.

Procedure

Step 1 In the Manage Users window User Group area, click to highlight the user group to which you want to add the user.

Note To add users to a user group, make sure that you do not click the **Details** button to view the user group details; otherwise, the Save and Revert buttons become disabled. If you click **Details** to view the user group details for any group, you must click the **Cancel** button that displays at the bottom of the window to reenable the Save and Revert buttons before you can add users to the user group.

Using DNS with Cisco Unified IP Phone Services

The "Configuring Cisco IPICS as a Phone Service" section in the "Setting Up and Using the Cisco Unified IP Phone with Cisco IPICS" chapter in the *Cisco IPICS Server Administration Guide* does not include the following information about ensuring proper configuration of valid Domain Name System (DNS) servers:

Note The Cisco Unified IP Phone service configuration fields refer to the Phone URL parameter values that you configure in Cisco Unified CallManager Administration by navigating to **System > Enterprise Parameters Configuration > Phone URL Parameters**. If you use host names in the URL fields, instead of IP addresses, make sure that you properly configure valid Domain Name System (DNS) server(s) to resolve the host names. If the DNS server(s) that the IP phones are configured to use are not configured correctly, they will not be able to resolve the host names and the Cisco Unified IP Phone services will not be operable.

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

The "Troubleshooting the Cisco IPICS Server" chapter in the *Cisco IPICS Troubleshooting Guide* omits information about the 500 error messages that you may receive when you try to access the Administration Console. The following text provides a correction to this information.

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

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


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

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

When this problem occurs, the system may display a message in the ipics.log file, as shown in Example 1:

Example 1 Exception Message

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

Without access to the Administration Console **System Administrator > System Status** window to view these log entries, you need to use an alternate method to determine if there is a caching problem.

Perform the following procedure to manually access the log entries to look for the applicable error messages, such as “Incompatible magic value” or “Class not found.” HTML files do not generate a log message, but they may be missing (404 error message) or not function properly.

Procedure

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

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

Step 3 Change the directory by entering the following command:

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

Step 4 View the tail end of the ipics.log file by entering the following command:

[root] **#tail -100 ipics.log**

Solution To correct this problem, delete one or more copies of the ipics_server folder by performing the following procedure:

Procedure

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

Step 2 To preserve the contents of the pmcdownloads folder before you delete the ipics_server folder, move the pmcdownloads folder to a temporary location by entering the following command:

[root] **#mv /ops/cisco/ipics/tomcat/current/webapps/ipics_server/pmcdownloads /opt/cisco/ipics/tomcat/current/webapps**

Step 3 Delete the ipics_server folder in the webapps location by entering the following command:

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

Step 4 Delete the ipics_server folder in the work location by entering the following command:

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

Step 5 Restart the Tomcat service by entering the following command:

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

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

Note When the Tomcat service restarts, the system creates a new ipics_server folder.

Step 6 To remove the pmcdownloads folder from its temporary location and move it back to the ipics_server folder, enter the following commands:

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

[root] **#mv /opt/cisco/ipics/tomcat/current/webapps/pmcdownloads /opt/cisco/ipics/tomcat/current/webapps/ipics_server**

Step 7 Open a supported version of the Internet Explorer browser.

Step 8 In the Location or Address field, enter the following URL, replacing *IP address* with the IP address of the Cisco IPICS server:

http://<*IP address***>**

You should be able to access the Administration Console.

Omission of Server Reboot Message After Uninstallation

The "Uninstalling Cisco IPICS from the Cisco IPICS Server" section in the "Uninstalling Cisco IPICS" chapter in the *Cisco IPICS Server Installation Guide* omits information about the server rebooting after the uninstallation process has been completed.

Step 6 of this procedure should state that, after you click **Done**, the server displays a system reboot message in the terminal from which the uninstaller was launched and then automatically reboots the system.

Updated Procedure for Configuring Your Audio Settings

The "Configuring the Audio Settings" section in the "Installing and Upgrading the PMC Application" chapter in the *Cisco IPICS PMC Installation and User Guide* omits information about checking the microphone subdevice when you configure your audio settings. The following procedure provides an update to this section:

To configure your audio settings for use with the PMC, perform the following procedure:

Procedure

Step 1 Take one of the following actions, depending on the operating system that you use. If you use Windows 2000, proceed to Step 2. If you use Windows XP, continue with Step 3.

Step 2 On Windows 2000 client machines, perform this procedure:

a. Navigate to **Start > Settings > Control Panel > Sounds and Multimedia**.

The Sounds and Multimedia Properties window displays.

b. Click the **Audio** tab.

c. Check the **Use only preferred devices** check box.

d. Click the **Volume** button for the selected recording device to view the volume control settings.

e. If it is not already checked, check the **Select** check box that displays for the Microphone Balance settings in the Recording Control window to make sure that the PMC uses the correct subdevice. Then, exit this window.

f. Click **OK**.

Step 3 On Windows XP client machines, perform this procedure:

a. Navigate to **Start > Settings >Control Panel > Sounds and Audio Devices**.

The Sounds and Audio Devices Properties window displays.

a. Click the **Audio** tab.

b. Check the **Use only default devices** check box.

c. Click the **Volume** button for the selected recording device to view the volume control settings.

d. If it is not already checked, check the **Select** check box that displays for the Microphone Balance settings in the Recording Control window to make sure that the PMC uses the correct subdevice. Then, exit this window.

e. Click **OK**.

Update to the RMS Configuration Information

The following section contains guidelines for using T1 and E1 connectivity with Cisco IPICS and configuration procedures that you must follow for these card types; it also includes additional configuration details for the RMS.

Note

- Before you can use an RMS with Cisco IPICS or perform RMS management tasks, you must first configure the RMS.
  - You manage the RMS from the Cisco IPICS server.
  - You must configure at least one RMS per Cisco IPICS server.
  - You cannot configure the same RMS in multiple Cisco IPICS servers.
- To ensure proper functionality, make sure that you map one RMS to one Cisco IPICS server; otherwise, you may encounter usability issues. For example, if the same RMS is mapped to more than one server, PMC users may hear a busy tone when they attempt to activate a channel or VTG because of configuration discrepancies.
- Be aware that Cisco IPICS provides support only for RMS components that are configured as described in this appendix.

This section provides a complete update to the "RMS Configuration" appendix in the *Cisco IPICS Server Administration Guide*; it includes the following topics.

Configuring Security Features

As with other routers that you use, Cisco recommends that you configure security features, such as access control, on the RMS. Access control allows you to designate the users who may access the router and specific services. The Cisco IOS software enables authentication, authorization, and accounting (AAA) network security services to provide access control on your router.

Cisco recommends that you configure AAA as your primary method for access control to provide an additional layer of security for your network. Specifically, Cisco recommends that you configure authentication on the RMS to enable the identification of users before they are permitted to access the network and network services. This identification includes login and password dialog, challenge and response, messaging support, and encryption (depending on the security protocol that you choose).

You configure AAA authentication by defining a named list of authentication methods, and then applying that list to various interfaces. The method list defines the types of authentication to be performed and the sequence in which they will be performed; it must be applied to a specific interface before any of the defined authentication methods will be performed.

Note Cisco IPICS supports the *default* method list, which is automatically applied to all interfaces if no other method list is defined.

To configure AAA and implement a basic level of security on the RMS, perform the following procedure:

Procedure

Step 1 To enable the AAA access control system, enter the following CLI command in global configuration mode:

Router(config)# **aaa new-model**

This command initializes AAA.

Step 2 To set AAA authentication at login to use the default method with the *local* method keyword, enter the following command:

Router(config)# **aaa authentication login default local**

The default method list is automatically applied to all interfaces.

The *local* method keyword configures the router to use the local user name database for authentication.

Step 3 To configure a password for privileged EXEC mode, enter the following command:

Router(config)# **enable password** <*password*>

where *password* specifies the enable password.

Step 4 Establish a username-based authentication system by entering the following command in global configuration mode.

Router(config)# **username** <*name*> **privilege 15 password 0** <*password*>

where:

name specifies the user name that you configure on the RMS and *password* specifies the user enable password that you configured in Step 3.

Note Make sure that you configure the RMS with a valid user name and password.

This command creates a user name and password on the router. You enter this user name and password in the Cisco IPICS Administration Console when you configure the RMS.

The privilege parameter defines the privilege level for the user; this value ranges from 0 to 15, with 15 designating the highest privilege level.

Note To ensure successful authentication, the Cisco IPICS server requires that the user name that you create to access the RMS be configured with a minimum privilege level of 7.

The single digit that follows the password parameter defines whether the text that follows the password is encrypted; a value of 0 signifies that the password is entered in clear text.

You may implement more stringent security measures and harden your system security by configuring additional security features that Cisco IOS provides. For more information about configuring authentication, password security, and additional layers of security, refer to the *Cisco IOS Security Guide* at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hsec_c/index.htm

RMS Connectivity Guidelines

To configure an RMS router for T1 or E1 connectivity, follow these guidelines:

- Configure at least two T1 or E1 controllers and assign ds0 groups to each controller.
- Allocate only as many ds0s on a controller as the RMS router can support simultaneously.
- Make sure that the ports that you allocate start with port 0 and are configured sequentially.
- Typically, a T1 controller will support 24 ds0s, but your controller may support fewer ds0s, depending on the number of available digital signal processors (DSPs).
- Typically, an E1 controller will support 30 ds0s, but your controller may support fewer ds0s, depending on the number of available DSPs.
- Be careful not to allocate more ds0s than a controller has resources to support; otherwise, you may encounter lost audio and other voice quality issues.
- Configure T1 or E1 controllers for individual voice ports by entering the following command in the router configuration:

  ds0-group *ds0-group-number* **timeslots** *timeslot-list* **type e&m-lmr**

  This command specifies the ds0 time slots that define logical voice ports on a T1 or E1 controller and configure the signaling type by which the router communicates with the PSTN.

  where:

  – **ds0-group** *ds0-group number* identifies the ds0 group; for T1 connectivity, the allowable values range from 0 to 23; for E1 connectivity, the allowable values range from 0 to 29.

Note Be aware that ds0 groups must start with 0 and they must be sequential.

  – **timeslots** *timeslot-list* specifies a single time-slot number; for T1 connectivity, the allowable values range from 1 to 24; for E1 connectivity, the allowable values range from 1 to 31.

Note For detailed configuration information, see the procedure in the "Configuring T1/E1 Controllers" section on page 99.

RMS IP Address Selection Guidelines

The following guidelines pertain to the IP addresses that you must use with Cisco IPICS, as described in the "Configuring T1/E1 Controllers" section on page 99.

For successful interoperability with Cisco IPICS components, you must configure the following interfaces for the RMS:

- Ethernet0 Interface
  - This interface is the physical port that provides network connectivity
  - The IP address that you configure must be routable; that is, reachable by the network
- Loopback0 Interface
  - This virtual interface is used for network connectivity
  - The IP address that you configure must be routable (that is, reachable by the network); otherwise, your SIP connectivity will be affected
  - This IP address is assigned as the RMS IP address
  - The server and the PMC components use this address to connect to the RMS
- Vif1 Interface
  - This virtual interface (VIF) is used to associate an IP address with the voice ports on the RMS
  - The VIF subnet that you configure must be routable (that is, reachable by the network); otherwise, your Cisco IPICS network connectivity will be affected
  - The actual IP address that is associated with the voice ports is the configured vif1 address + 1

Note Be aware that the IP addresses that you configure for both the Loopback0 and the Vif interfaces must be routable; this requirement is mandatory for both of these interfaces to ensure proper operation with Cisco IPICS. If the IP addresses for either of these interfaces are not routable, you may experience intermittent delays, of varying duration, from the time that you press the PMC PTT button to the time that the media is established between the remote PMC and multicast channels. This delay results from the inability of the RMS to perform Reverse Path Forwarding (RPF) checks on multicast Real-time Transport Protocol (RTP) packet source addresses. Therefore, to avoid this issue, make sure that the IP addresses for both the Loopback0 and the Vif interfaces are routable.

Configuring T1/E1 Controllers

The Cisco IPICS solution requires that you install at least one T1 or E1 loopback in the RMS to support mixing. (The RMS provides support for mixing multicast channels in support of VTGs and for mixing remote PMC SIP-based (unicast) connections to a multicast channel or VTG.)

The configuration steps that are required to implement the loopback pairs may vary depending on card type, Cisco IOS version, and the type of supported RMS that you use.

Note For a complete list of supported interface cards and RMS routers, refer to the *Cisco IPICS Compatibility Matrix* at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/cis/c_ipics/index.htm

To configure T1 or E1 controllers on an RMS, perform the following procedure.

Procedure

Step 1 If you use a T1/E1 combination interface card, such as the Cisco 1- and 2-port T1/E1 Multiflex Trunk (MFT) Voice/WAN Interface Card (VWIC2), you must configure the card type for T1 or E1 by entering the following command:

Router(config)# **card type {t1 | e1}** *slot* [*bay*]

where:

slot specifies the port number of the interface, and *bay* is an optional parameter that specifies the card interface bay number in a slot on certain route/switch processor [RSP] platforms.

Examples of this command for both T1 and E1 connections appears below:

```
Router(config)# card type t1 0 3
Router(config)# card type e1 0 3
```

If you are using a T1/E1 combination interface card and want to replace one card type for another, proceed to Step 2. Otherwise, continue with Step 3.

Note Be aware that you cannot use an E1-only interface card or a T1/E1 combination interface card in E1 mode with other interface cards, such as T1-only, in the same router because the global **signal pattern idle transmit 0000** command is not supported with all interface cards. (This command is supported for use only with the E1-only interface card and the T1/E1 combination card in E1 mode.) For more information about this command, see Step 13.

Step 2 To change the card type configuration and replace the T1 with an E1, as an example, enter the following commands:

a. Router(config)# **no card type t1** *slot* [*bay*]

Note When you use the card type command to change your configuration, be aware that changes become effective only after you reload or reboot the router.

b. Exit the router configuration mode by entering the following command:

Router(config)# **exit**

a. Execute the following commands to save your changes and to reload the router:

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

b. Configure the card type for E1 connectivity by entering the following command:

Router(config)# **card type e1** *slot* [*bay*]

where:

slot specifies the port number of the interface and *bay* is an optional parameter that specifies the card interface bay number in a slot on certain route/switch processor [RSP] platforms.

An example of this command appears below:

```
Router(config)# card type e1 0 3
```

Step 3 To enable the ports on the interface card to use the network clock for timing and ensure that the router backplane clock references are synchronized with the T1/E1 interface card, enter the following command:

Router(config)# **network-clock-participate** [**slot** *slot-number* | **wic** *wic-slot* | **aim** *aim-slot-number*]

where:

slot *slot-number* is an optional parameter that specifies the network module slot number on the router chassis
wic *wic-slot* specifies the WAN interface card (WIC) slot number on the router chassis
aim *aim-slot-number* specifies the Advanced Integration Module (AIM) in the specified slot (for applicable hardware)

An example of this command appears below; wic 3 designates the WAN interface card in physical slot 3:

```
Router(config)# network-clock-participate wic 3
```

To configure T1 controllers, proceed to Step 4. To configure E1 controllers, continue with Step 5.

Note The following steps use Protocol Independent Multicast, or ip pim, sparse-dense-mode on the interface. Check to make sure that the design of your multicast network does not require you to use a different ip pim mode. For more information about multicast configurations, refer to the Cisco IOS Software Release 12.4 product documentation at the following URL and click the link for "Cisco IOS IP Multicast Configuration Guide, Release 12.4"
http://www.cisco.com/en/US/products/ps6350/tsd_products_support_configure.html

Step 4 Configure ds0 groups on the T1 controllers by entering the following commands in the router configuration:

Note The clock command should be used for only one of the two T1 controllers in the loopback.

a. To configure the first controller in the loopback pair, enter the following commands:

```
Router(config)# controller T1 1/0
Router(config-controller)# framing esf
Router(config-controller)# clock source internal
Router(config-controller)# linecode b8zs
Router(config-controller)# cablelength short 133
Router(config-controller)# ds0-group 0 timeslots 24 type e&m-lmr
Router(config-controller)# ds0-group 1 timeslots 1 type e&m-lmr
Router(config-controller)# ds0-group 2 timeslots 2 type e&m-lmr
Router(config-controller)# ds0-group 3 timeslots 3 type e&m-lmr
Router(config-controller)# ds0-group 4 timeslots 4 type e&m-lmr
Router(config-controller)# ds0-group 5 timeslots 5 type e&m-lmr
Router(config-controller)# ds0-group 6 timeslots 6 type e&m-lmr
Router(config-controller)# ds0-group 7 timeslots 7 type e&m-lmr
Router(config-controller)# ds0-group 8 timeslots 8 type e&m-lmr
Router(config-controller)# ds0-group 9 timeslots 9 type e&m-lmr
Router(config-controller)# ds0-group 10 timeslots 10 type e&m-lmr
Router(config-controller)# ds0-group 11 timeslots 11 type e&m-lmr
Router(config-controller)# ds0-group 12 timeslots 12 type e&m-lmr
Router(config-controller)# ds0-group 13 timeslots 13 type e&m-lmr
Router(config-controller)# ds0-group 14 timeslots 14 type e&m-lmr
Router(config-controller)# ds0-group 15 timeslots 15 type e&m-lmr
Router(config-controller)# ds0-group 16 timeslots 16 type e&m-lmr
Router(config-controller)# ds0-group 17 timeslots 17 type e&m-lmr
Router(config-controller)# ds0-group 18 timeslots 18 type e&m-lmr
Router(config-controller)# ds0-group 19 timeslots 19 type e&m-lmr
Router(config-controller)# ds0-group 20 timeslots 20 type e&m-lmr
Router(config-controller)# ds0-group 21 timeslots 21 type e&m-lmr
Router(config-controller)# ds0-group 22 timeslots 22 type e&m-lmr
Router(config-controller)# ds0-group 23 timeslots 23 type e&m-lmr
Router(config-controller)# no shutdown
```

where:

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

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

b. To configure the second controller in the loopback pair, enter the following commands:

```
Router(config)# controller T1 1/1
Router(config-controller)# framing esf
Router(config-controller)# linecode b8zs
Router(config-controller)# cablelength short 133
Router(config-controller)# ds0-group 0 timeslots 24 type e&m-lmr
Router(config-controller)# ds0-group 1 timeslots 1 type e&m-lmr
Router(config-controller)# ds0-group 2 timeslots 2 type e&m-lmr
Router(config-controller)# ds0-group 3 timeslots 3 type e&m-lmr
Router(config-controller)# ds0-group 4 timeslots 4 type e&m-lmr
Router(config-controller)# ds0-group 5 timeslots 5 type e&m-lmr
Router(config-controller)# ds0-group 6 timeslots 6 type e&m-lmr
Router(config-controller)# ds0-group 7 timeslots 7 type e&m-lmr
Router(config-controller)# ds0-group 8 timeslots 8 type e&m-lmr
Router(config-controller)# ds0-group 9 timeslots 9 type e&m-lmr
Router(config-controller)# ds0-group 10 timeslots 10 type e&m-lmr
Router(config-controller)# ds0-group 11 timeslots 11 type e&m-lmr
Router(config-controller)# ds0-group 12 timeslots 12 type e&m-lmr
Router(config-controller)# ds0-group 13 timeslots 13 type e&m-lmr
Router(config-controller)# ds0-group 14 timeslots 14 type e&m-lmr
Router(config-controller)# ds0-group 15 timeslots 15 type e&m-lmr
Router(config-controller)# ds0-group 16 timeslots 16 type e&m-lmr
Router(config-controller)# ds0-group 17 timeslots 17 type e&m-lmr
Router(config-controller)# ds0-group 18 timeslots 18 type e&m-lmr
Router(config-controller)# ds0-group 19 timeslots 19 type e&m-lmr
Router(config-controller)# ds0-group 20 timeslots 20 type e&m-lmr
Router(config-controller)# ds0-group 21 timeslots 21 type e&m-lmr
Router(config-controller)# ds0-group 22 timeslots 22 type e&m-lmr
Router(config-controller)# ds0-group 23 timeslots 23 type e&m-lmr
Router(config-controller)# no shutdown
```

where:

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

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

Step 5 Configure ds0 groups on the E1 controllers by entering the following commands in the router configuration.

Note

- The clock command should be used for only one of the two E1 controllers in the loopback.
- In E1 framing and signaling, 30 of the 32 available channels, or time slots, are used for voice or data transmission. Time slot 0 and time slot 16, which you do not configure, do not carry voice or data. Time slot 0 provides frame synchronization, alarm transport, and international carrier use while time slot 16 provides supervisory signaling for the 30 voice and data channels.

a. To configure the first controller in the loopback pair, enter the following commands:

Router(config)# **controller e1** *slot port*
Router(config-controller)# **clock source internal**
Router(config-controller)# d**s0-group 0 timeslots 31 type e&m-lmr**
Router(config-controller)# **ds0-group 1 timeslots 1 type e&m-lmr**
Router(config-controller)# **ds0-group 2 timeslots 2 type e&m-lmr**
Router(config-controller)# **ds0-group 3 timeslots 3 type e&m-lmr**
Router(config-controller)# **ds0-group 4 timeslots 4 type e&m-lmr**
Router(config-controller)# **ds0-group 5 timeslots 5 type e&m-lmr**
Router(config-controller)# **ds0-group 6 timeslots 6 type e&m-lmr**
Router(config-controller)# **ds0-group 7 timeslots 7 type e&m-lmr**
Router(config-controller)# **ds0-group 8 timeslots 8 type e&m-lmr**
Router(config-controller)# **ds0-group 9 timeslots 9 type e&m-lmr**
Router(config-controller)# **ds0-group 10 timeslots 10 type e&m-lmr**
Router(config-controller)# **ds0-group 11 timeslots 11 type e&m-lmr**
Router(config-controller)# **ds0-group 12 timeslots 12 type e&m-lmr**
Router(config-controller)# **ds0-group 13 timeslots 13 type e&m-lmr**
Router(config-controller)# **ds0-group 14 timeslots 14 type e&m-lmr**
Router(config-controller)# **ds0-group 15 timeslots 15 type e&m-lmr**
Router(config-controller)# **ds0-group 16 timeslots 30 type e&m-lmr**

Router(config-controller)# **ds0-group 17 timeslots 17 type e&m-lmr**
Router(config-controller)# **ds0-group 18 timeslots 18 type e&m-lmr**
Router(config-controller)# **ds0-group 19 timeslots 19 type e&m-lmr**
Router(config-controller)# **ds0-group 20 timeslots 20 type e&m-lmr**
Router(config-controller)# **ds0-group 21 timeslots 21 type e&m-lmr**
Router(config-controller)# **ds0-group 22 timeslots 22 type e&m-lmr**
Router(config-controller)# **ds0-group 23 timeslots 23 type e&m-lmr**
Router(config-controller)# **ds0-group 24 timeslots 24 type e&m-lmr**
Router(config-controller)# **ds0-group 25 timeslots 25 type e&m-lmr**
Router(config-controller)# **ds0-group 26 timeslots 26 type e&m-lmr**
Router(config-controller)# **ds0-group 27 timeslots 27 type e&m-lmr**
Router(config-controller)# **ds0-group 28 timeslots 28 type e&m-lmr**
Router(config-controller)# **ds0-group 29 timeslots 29 type e&m-lmr**
Router(config-controller)# **no shutdown**

where:

slot port specifies the backplane slot number and port number on the interface. An example of this command appears below:

```
Router(config)# controller e1 0/3/0
```

b. To configure the second controller in the loopback pair, enter the following commands:

Router(config)# **controller e1** *slot port*
Router(config-controller)# d**s0-group 0 timeslots 31 type e&m-lmr**
Router(config-controller)# **ds0-group 1 timeslots 1 type e&m-lmr**
Router(config-controller)# **ds0-group 2 timeslots 2 type e&m-lmr**
Router(config-controller)# **ds0-group 3 timeslots 3 type e&m-lmr**
Router(config-controller)# **ds0-group 4 timeslots 4 type e&m-lmr**
Router(config-controller)# **ds0-group 5 timeslots 5 type e&m-lmr**
Router(config-controller)# **ds0-group 6 timeslots 6 type e&m-lmr**
Router(config-controller)# **ds0-group 7 timeslots 7 type e&m-lmr**
Router(config-controller)# **ds0-group 8 timeslots 8 type e&m-lmr**
Router(config-controller)# **ds0-group 9 timeslots 9 type e&m-lmr**
Router(config-controller)# **ds0-group 10 timeslots 10 type e&m-lmr**
Router(config-controller)# **ds0-group 11 timeslots 11 type e&m-lmr**
Router(config-controller)# **ds0-group 12 timeslots 12 type e&m-lmr**
Router(config-controller)# **ds0-group 13 timeslots 13 type e&m-lmr**
Router(config-controller)# **ds0-group 14 timeslots 14 type e&m-lmr**
Router(config-controller)# **ds0-group 15 timeslots 15 type e&m-lmr**
Router(config-controller)# **ds0-group 16 timeslots 30 type e&m-lmr**

```
Router(config-controller)# ds0-group 17 timeslots 17 type e&m-lmr
Router(config-controller)# ds0-group 18 timeslots 18 type e&m-lmr
Router(config-controller)# ds0-group 19 timeslots 19 type e&m-lmr
Router(config-controller)# ds0-group 20 timeslots 20 type e&m-lmr
Router(config-controller)# ds0-group 21 timeslots 21 type e&m-lmr
Router(config-controller)# ds0-group 22 timeslots 22 type e&m-lmr
Router(config-controller)# ds0-group 23 timeslots 23 type e&m-lmr
Router(config-controller)# ds0-group 24 timeslots 24 type e&m-lmr
Router(config-controller)# ds0-group 25 timeslots 25 type e&m-lmr
Router(config-controller)# ds0-group 26 timeslots 26 type e&m-lmr
Router(config-controller)# ds0-group 27 timeslots 27 type e&m-lmr
Router(config-controller)# ds0-group 28 timeslots 28 type e&m-lmr
Router(config-controller)# ds0-group 29 timeslots 29 type e&m-lmr
Router(config-controller)# no shutdown
```

where:

slot port specifies the backplane slot number and port number on the interface. An example of this command appears below:

```
Router(config)# controller e1 0/3/1
```

Step 6 Determine if dspfarms are enabled by executing the following command:

Router# **show run**

If dspfarms are enabled, the output displays as shown in the following example; continue with Step 8:

```
voice-card 0
 dspfarm
!
voice-card 1
 dspfarm
```

If dspfarms are not enabled, the output displays as shown in this example; proceed to Step 7 to enable dspfarms:

```
voice-card 0
 no dspfarm
!
voice-card 1
 no dspfarm
```

Note When you enable dspfarms, you add specific voice cards to the DSP resource pool; this configuration allows multiple interface cards to share the installed DSP resources. At a minimum, you should enable one dspfarm.

Step 7 To enable dspfarms, enter the following commands:

Router(config)# **voice-card** <*slot number*>
Router(config-voicecard)# **dspfarm**

where:

slot number specifies the slot number for the voice interface card.

For example, the following command enables the dspfarm on the interface card that is installed in slot 0:

```
Router(config)# voice-card 0
Router(config-voicecard)# dspfarm
```

Step 8 To enable multicast routing, enter the following command:

Router(config)# **ip multicast-routing**

When IP multicast routing is enabled, the Cisco IOS software is enabled to forward multicast packets.

Step 9 Create a virtual interface for multicast communications by entering the following commands:

Router(config)# **interface vif1**
Router(config-if)# **ip address** *ip_address subnet_mask*
Router(config-if)# **ip pim sparse-dense-mode**

where:

ip_address specifies the IP address that you assign to this interface
subnet_mask specifies the 30-bit subnet mask that you assign to this interface; for example, 255.255.255.252

This command configures a virtual interface that is similar to a loopback interface; that is, a logical IP interface that is always up when the router is active. The RMS assigns a virtual address of vif1 + 1 as the source address when it mixes voice traffic and then sends out this traffic via multicast.

For more information about IP address guidelines, see the "RMS IP Address Selection Guidelines" section on page 98.

Step 10 To enable loopback mode and assign an IP address and subnet mask to the interface, create a loopback interface for voice signaling and media by entering the following commands:

Router(config)# **interface Loopback0**
Router(config-if)# **ip address** *ip_address subnet_mask*
Router(config-if)# **ip pim sparse-dense-mode**

where:

ip_address specifies the IP address that you assign to this interface; this IP address gets assigned to the RMS
subnet_mask specifies the 30-bit subnet mask that you assign to this interface; for example, 255.255.255.252
0 specifies the identification number that you assign to the loopback interface

This command creates a software-only loopback interface that emulates an interface that is always up. (This virtual interface is supported on all platforms.) For more information about IP address guidelines, see the "RMS IP Address Selection Guidelines" section on page 98.

Step 11 To configure voice signaling and media on the loopback interface, enter the following commands:

a. Router(config)# **voice service voip**

This command switches to voice-service configuration mode, from global configuration mode, and specifies the voice encapsulation type.

b. Router(conf-voi-serv)# **sip**

This command enables Session Initiation Protocol (SIP) configuration mode.

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

These commands bind the source address for signaling and media packets to the IP address of the loopback interface.

Step 12 To enable multicast routing for each interface that routes multicast traffic, enter the following command (for each interface):

Router(config-if)# **ip pim sparse-dense-mode**

This command enables Protocol Independent Multicast (PIM) on an interface. When you configure sparse-dense-mode, the interface can operate by using either sparse mode or dense mode, depending on the operating mode of the multicast group.

Step 13 To create a voice class that will be applied to all voice configurations, enter the following commands based on your connectivity:

a. When you use T1 connectivity, enter these commands:

Router(config)# **voice class permanent 1**
Router(config-class)# **signal timing oos timeout disabled**
Router(config-class)# **signal keepalive disabled**
Router(config-class)# **signal sequence oos no-action**

where:

1 specifies the unique number that you assign to the voice class.

b. When you use an E1-only interface card or a T1/E1 combination interface card specifically for E1 connectivity, enter all of the following commands:

Router(config)# **voice class permanent 1**
Router(config-class)# **signal timing oos timeout disabled**
Router(config-class)# **signal keepalive disabled**
Router(config-class)# **signal sequence oos no-action**
Router(config-class)# **signal pattern idle transmit 0000**

where:

1 specifies the unique number that you assign to the voice class.

Note Make sure that you enter only the first four commands when you use T1 connectivity; when you use an E1-only interface card or a T1/E1 combination interface card specifically for E1 connectivity, you must also enter the **signal pattern idle transmit 0000** command as documented in Step 13.

Be aware that the **signal pattern idle transmit 0000** command is a global command that is supported for use only with E1-only interface cards and T1/E1 combination interface cards that you configure for E1 mode. (This command is not supported for use with other interface cards, such as T1-only and E1-only cards.) When you configure this command, it affects all interface cards in the router; therefore, make sure that all interface cards are E1-only interface cards or T1/E1 combination cards in E1 mode and that you do not mix T1-only, E1-only, and T1/E1 combination card types in the same router when you use this command.

Step 14 Create a cryptographic key to enable SSL (HTTPS) secure access from the Cisco IPICS server by entering the following command:

Router(config)# **ip http secure-server**

Step 15 To enable log in by using Telnet and SSH, enter the following commands:

Router(config)# **line vty 0 15**
Router(config-line)# **transport input telnet ssh**
Router(config-line)# **exec-timeout 22 0**
Router(config-line)# **privilege level 15**

Note The exec-timeout parameter sets the interval that the EXEC command interpreter waits until user input is detected. Optimally, you should set the exec-timeout to 22 (22 minutes). Setting this value to a shorter time, such as 5 or 10 minutes, can cause undesirable delays every time that Cisco IPICS accesses the router (such as when you change a VTG). Setting a longer time, such as 60 minutes, can cause authorized logins to accumulate and result in the router running out of open lines. Make sure that you do not set the exec-timeout to 0, which specifies no timeout.

Step 16 Configure the SIP inactivity timeout by entering the following commands:

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

This command configures the average reporting interval between subsequent Real-Time Control Protocol (RTCP) report transmissions.

b. Router(config)# **gateway**

This command enables the H.323 VoIP gateway.

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

This command enables the RTCP timer and configures a multiplication factor for the RTCP timer interval for SIP or H.323.

Step 17 Configure the list of codecs that Cisco IPICS will support by entering the following commands:

Router(config)# **voice class codec 1**
Router(config-class)# **codec preference 1 g729r8**
Router(config-class)# **codec preference 2 g711ulaw**

These commands enable voice-class configuration mode, assign an identification tag number for a codec voice class, and specify the preferred codecs to use on a dial peer.

Step 18 Create the following inbound dial peer by entering the following commands:

Router(config)# **dial-peer voice 555 voip**
Router(config-dial-peer)# **voice-class codec 1**
Router(config-dial-peer)# **session protocol sipv2**
Router(config-dial-peer)# **incoming called-number .**
Router(config-dial-peer)# **no vad**

These commands configure the voice dial peer and turn off voice activity detection (VAD) on the default SIP PMC connection.

Step 19 Enter the following command to reset the router command prompt:

Router(config)# **no prompt**

Step 20 Execute the following command to display the contents of the current, running configuration file and verify that the output reflects the modifications that you performed in this procedure:

Router# **show running-config**

Step 21 Execute the following command to save your changes:

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

Step 22 If you reconfigured a T1/E1 combination interface card from T1 to E1 mode, you may need to reset the loopback cable. To determine if you need to reset the loopback cable, take one of the following actions:

- Check the LEDs on the interface card to see if the LP LED is amber.

  This LED should be off during normal operation.

- Enter the following CLI command to determine if there are alarms or errors displayed by the controller:

  Router# **show controllers e1**

  The command output should display the e1 in an “up” state with no alarms, as shown in the following sample output:

  ```
  e1 3/0 is up
  No alarms detected
  ```

  If the output displays the e1 in a “down” state, as shown in the following example, continue with Step 21:

```
e1 3/1 is down
alarm-trigger is not set
```

Step 23 To resolve this problem, disconnect the loopback cable from the router; then, reconnect it.

The LP LED should now be off.

Step 24 Verify that the e1 is up by entering the **show controllers e1** command, as shown above. The command output should display the e1 controllers in an "up" state, with no alarms detected, as shown in the following sample output:

```
e1 3/0 is up
No alarms detected

e1 3/1 is up
No alarms detected
```

Cisco IPICS supports the use of Land Mobile Radio (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. For detailed LMR gateway configuration information, refer to the Land Mobile Radio over IP documentation at the following URL:

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

Obtaining Documentation

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

Cisco.com

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

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

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

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

Documentation DVD

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

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

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

Cisco Marketplace:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

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

You can order Cisco documentation in these ways:

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

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

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

Documentation Feedback

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

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

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

We appreciate your comments.

Cisco Product Security Overview

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

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

From this site, you can perform these tasks:

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

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

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

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

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

Reporting Security Problems in Cisco Products

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

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com

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

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on

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

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

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

http://www.cisco.com/techsupport

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

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

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

Submitting a Service Request

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

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

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

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

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

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

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

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

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

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

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

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

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

  http://www.cisco.com/ipj

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

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

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.