Cisco IPICS PMC Installation and User Guide

Release 2.0(1)

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

Text Part Number: OL-7698-02

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0612R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Cisco IPICS PMC Installation and User Guide
Copyright © 2006 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface xi

- Introduction xi
- Audience xii
- Organization xii
- Related Documentation xiii
  - Cisco Unified CallManager Documentation xiv
  - Cisco Unified CallManager Express Documentation xv
  - Cisco 7800 Series Media Convergence Servers Documentation xv
  - Cisco Unified IP Phone Documentation xv
  - Cisco Land Mobile Radio over IP xv
  - Cisco Security Agent xv
  - Cisco IOS Documentation xvi
- Document Notes and Conventions xvi
- Obtaining Documentation xvii
  - Cisco.com xvii
  - Product Documentation DVD xviii
  - Ordering Documentation xviii
- Documentation Feedback xviii
- Cisco Product Security Overview xix
  - Reporting Security Problems in Cisco Products xix
- Product Alerts and Field Notices xx
- Obtaining Technical Assistance xxi

Cisco Support Website xxi
Submitting a Service Request xxii
Definitions of Service Request Severity xxiii
Obtaining Additional Publications and Information xxiii

CHAPTER 1 **Introducing Cisco IPICS and the PMC Application 1-1**
Overview of Cisco IPICS 1-1
Introduction 1-2
Cisco IPICS System Components 1-3
Cisco IPICS User Roles 1-5
About the PMC Application 1-7
Browser Support 1-12
Work Flow Activities 1-13
PMC Application Usage Caveats 1-13
Architecture/Deployment 1-15
System Requirements for the PMC Application 1-17
Hardware Requirements 1-17
Software Requirements 1-18
System Interactions 1-19
Server Interactions 1-19
User Interactions 1-20

CHAPTER 2 **Installing and Upgrading the PMC Application 2-1**
PMC-Server Interactions 2-1
Installing the PMC Application 2-2
InstallationCaveats 2-3
Downloading and Installing the PMC Application 2-4
Optimizing Your Audio on the PMC 2-7
Configuring the Audio Settings 2-7

Using a USB DSP Headset with the PMC 2-9
Using the Microphone with the PMC 2-10
Important Information about Using the Microphone 2-11
Checking the Microphone 2-11
Voice Quality Tips 2-12
Launching the PMC Application 2-14
Performing Additional PMC Tasks 2-16
Maintaining and Upgrading the PMC Application 2-16
Maintaining PMC Version Compatibility 2-17
Locating the PMC Version Information 2-18
Managing PMC Version Numbers 2-18
Support for Automatic Updates 2-21
Managing PMC Upgrades 2-22
Checking for PMC Updates 2-22
Performing an Optional Upgrade 2-23
Performing a Required Upgrade 2-25
Managing Alert Tone Upgrades 2-26
Reverting to a Previous Version of the PMC Application 2-27
Uninstalling the PMC Application 2-28

CHAPTER 3 **Understanding PMC Interactions and Supported Features 3-1**
Voice Interoperability 3-1
Scenarios for Using the PMC Application 3-2
Cisco IPICS Server-PMC Interaction Scenario 3-3
Incident Management Scenario 3-6
PMC User Interaction 3-7
The Role of the Cisco IPICS Server 3-8
Server-PMC Interaction 3-8
Cisco IPICS Server Commands 3-9

Implementing Policies 3-10
Supported Features 3-11
Channel Support 3-11
Channel Terminology 3-12
Channel Information 3-13
Configurable Server Attributes 3-15
Location Support 3-18
Codec Support 3-22

CHAPTER 4 **Using the PMC Application 4-1**
Logging In to the PMC Application 4-1
PMC Usage Guidelines 4-2
Tips for Using the PMC 4-2
Connectivity Tips for Using the PMC 4-3
Login Caveats 4-4
PMC Password Caveats 4-5
License Information 4-6
Server-PMC Login Sequence Interaction 4-6
PMC Offline Mode Caveats 4-7
PMC Login Procedure 4-8
Using the PMC Application 4-12
Accessing Online Help 4-13
Activating the PMC Buttons 4-13
Joining a VTG 4-14
Dynamic Configuration 4-14
Channel Interactions 4-15
Support for Maximum Number of Channels 4-15
End-user Channel Interaction 4-16
End-user Features and Interactions 4-20
Traffic Activity 4-35

Channel Traffic Activity Interaction 4-37
User Channel Activity Interaction 4-37
Logging Out of the PMC Application 4-39

CHAPTER 5 **Configuring the PMC Application 5-1**
Configuring the PMC End-User Interface 5-1
Configuring the PMC Skins 5-2
Skin Caveats 5-4
Using the Status Menu 5-6
Configuring the Channels and Advanced Settings 5-7
Configuring the Channels Menu Options 5-8
Configuring the Advanced Menu Options 5-14
Using the Optional Settings Menu 5-15

CHAPTER 6 **Recovering the PMC Application 6-1**
Support for Cisco IPICS Recovery 6-1
Recovering the PMC 6-3
Transparent Recovery Mechanism 6-3
System Recovery Caveats 6-4
PMC Recovery Scenarios 6-4
Cisco IPICS Server is Unavailable 6-5
Cisco IPICS Server is Down/RMS and PMC are Up 6-5
Cisco IPICS Server and RMS are Down/PMC is Up 6-6
Cisco IPICS Server Resumes Operation 6-7
Cisco IPICS Server and PMC are Up/Communications are Down 6-8
Cisco IPICS Server and PMC are Up/Network is Down 6-8
PMC Application Recovery 6-9

CHAPTER 7 **Using the PMC Application Logs** 7-1

Identifying the PMC Logs 7-1

Maintaining the PMC Log Files 7-1

Accessing the Logs Submenu Items 7-2

Accessing the PMC Logs 7-3

Using the PMC Logs 7-5

PMC Log File Caveats 7-6

PMC Log Descriptions 7-7

CHAPTER 8 **Troubleshooting Tips for the PMC Application** 8-1

Troubleshooting PMC Application Problems 8-1

Resolving PMC Execution Issues 8-2

Generating a PMC Installation Log File 8-3

Using the PMC Installer with an Encrypted File System 8-5

Making PMC Configuration File Changes 8-6

Using the PMC Optional Settings 8-6

Resolving Footswitch/USB Device Issues 8-7

Configuring the Audio Settings 8-7

Using a USB DSP Headset with the PMC 8-8

Checking the Microphone with the PMC 8-8

Using Cisco Security Agent with the PMC 8-9

PMC Coexistence with Other Voice Applications 8-10

Troubleshooting One-Way Audio 8-10

Using CLI Commands to Resolve Audio and Headset Issues 8-11

Resolving IP Address Changes 8-13

Troubleshooting Voice Quality Issues 8-14

Resolving Unknown Publisher Errors with Windows XP SP2 8-14

Troubleshooting PMC Connectivity Issues 8-15

Troubleshooting VPN Connectivity 8-15

Using the PMC with the Windows XP Firewall **8-18**
Troubleshooting Multicast Communications Issues **8-19**
Troubleshooting Winsock Corruption Issues **8-20**
Troubleshooting Offline Mode Issues **8-21**
Troubleshooting PMC Connectivity Issues with the RMS **8-21**
Troubleshooting PMC Connectivity Issues with a High Latency, Low Bandwidth Link **8-22**
Resolving Name Resolution Failures **8-23**
Identifying Channel Activation Issues **8-23**
Resolving Codec Mismatch Issues **8-24**
Support for Right-to-Left and Double-Byte Languages **8-25**
PMC Application Caveats **8-28**
Analyzing PMC Error Conditions **8-28**

GLOSSARY

INDEX

Preface

Introduction

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*) application enable integrated communications among disparate Land Mobile Radio (LMR) systems.

By using an IP standards-based solution, Cisco IPICS solves interoperability issues by extending LMR reachability to the IP network through the connection of radio networks to IP networks and devices. Cisco IPICS also provides the following benefits:

- Investment protection in legacy radio networks and applications
- Graceful migration to robust IP applications and devices
- Incident management framework for operations and command and control

This document provides you with the information that you need to install, configure, manage, and operate the PMC application.

This section describes the intended audience and organization of this *Cisco IPICS PMC Installation and User Guide* and includes the following topics:

- Audience, page xii
- Organization, page xii
- Related Documentation, page xiii
- Document Notes and Conventions, page xvi
- Obtaining Documentation, page xvii

- Documentation Feedback, page xviii
- Cisco Product Security Overview, page xix
- Product Alerts and Field Notices, page xx
- Obtaining Technical Assistance, page xxi
- Obtaining Additional Publications and Information, page xxiii

Audience

The *Cisco IPICS PMC Installation and User Guide* targets the end-user who needs to know how to install, operate, and maintain the PMC application.

Organization

This guide is organized in the following manner:

Chapter 1, "Introducing Cisco IPICS and the PMC Application"	This chapter introduces Cisco IPICS and the PMC application. It includes a product overview as well as guidelines for systems requirements and expected interaction behavior.
Chapter 2, "Installing and Upgrading the PMC Application"	This chapter describes the actions that you must take to download and install the PMC application. It also provides instructions about upgrading, patching, and reverting the PMC application to an earlier version.
Chapter 3, "Understanding PMC Interactions and Supported Features"	This chapter contains information about the scenarios where you might use the PMC, information about the server and PMC interactions, PMC supported features, and specific terminology that the Cisco IPICS solution uses.

Chapter 4, “Using the PMC Application”	This chapter provides information about using the PMC application.
Chapter 5, “Configuring the PMC Application”	This chapter provides information about configuring the PMC end-user interface.
Chapter 6, “Recovering the PMC Application”	This chapter provides information about the actions that you can take to recover the PMC application under specific circumstances.
Chapter 7, “Using the PMC Application Logs”	This chapter describes how to use the PMC application logs. It includes information about turning on/off the log facility and setting up individual logs.
Chapter 8, “Troubleshooting Tips for the PMC Application”	This chapter provides information about basic troubleshooting tips and error messages that you may encounter when you use the PMC application.

Related Documentation

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

- *Cisco IPICS PMC Quick Start Reference Card, Release 2.0(1)*—This document provides tips and quick references for the most frequently used procedures that a user can perform on the Cisco IPICS PMC.
- *Cisco IPICS PMC Debug Reference Quick Start Card, Release 2.0(1)*—This document provides a quick reference for troubleshooting and debugging the Cisco IPICS PMC.
- *Cisco IPICS Server Administration Guide, Release 2.0(1)*—This document contains information about the key configuration, operation, and management tasks for the Cisco IPICS server.
- *Cisco IPICS Server Quick Start Guide, Release 2.0(1)*—This document is a condensed version of the *Cisco IPICS Server Administration Guide* to help the administrator to quickly get started with Cisco IPICS.

- *Cisco IPICS Server Quick Start Reference Card, Release 2.0(1)*—This document provides tips, quick references, and usage guidelines for the Cisco IPICS server.
- *Cisco IPICS Server Installation and Upgrade Guide, Release 2.0(1)*—This document describes how to install, configure, and upgrade the Cisco IPICS server software and Cisco IPICS operating system.
- *Cisco IPICS Server Quick Start Installation Reference Card, Release 2.0(1)*—This document provides tips and quick references for installing and upgrading the Cisco IPICS server.
- *Cisco IPICS Troubleshooting Guide, Release 2.0(1)*—This document contains reference material about how to maintain and troubleshoot the Cisco IPICS system.
- *Cisco IPICS PMC Command Line Interface, Release 2.0(1)*—This document describes the commands that you can use from the command line interface (CLI) to obtain information or to change settings for the Cisco IPICS PMC.
- *Release Notes for Cisco IPICS Release 2.0(1)*—This document contains a description of the new and changed features, important notes, caveats, and documentation updates for this release of Cisco IPICS.
- *Cisco IPICS 2.0(1) Resources Card (Documentation Locator)*—This document provides a summary of the documentation that is available for this release of Cisco IPICS.
- *Solution Reference Network Design (SRND) for Cisco IPICS Release 2.0(1)*— This document provides information about design considerations and guidelines for deploying the Cisco IPICS solution.
- *Cisco IPICS Compatibility Matrix*—This document contains information about compatible hardware and software that is supported for use with Cisco IPICS.

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

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

Cisco Unified CallManager Documentation

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

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

Cisco Unified CallManager Express Documentation

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

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

Cisco 7800 Series Media Convergence Servers Documentation

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

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

Cisco Unified IP Phone Documentation

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

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

Cisco Land Mobile Radio over IP

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

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

Cisco Security Agent

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

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

Cisco IOS Documentation

The Cisco IOS software documentation set describes the tasks and commands necessary to configure certain system components and other Cisco products, such as access servers, routers, and switches. Each configuration guide can be used in conjunction with its corresponding command reference.

For information about Cisco IOS software configuration, refer to the documentation at this URL:

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

Document Notes and Conventions

This document uses the following conventions for instructions and information:

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

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

Table 1 Conventions

Convention	Description
boldface font	Commands and keywords appear in **boldface**.
italic font	Command input for which you supply the values appear in *italics*.
[ ]	Optional keywords and default responses to system prompts appear within square brackets.

Table 1 Conventions (continued)

Convention	Description
{**x** | **x** | **x**}	A choice of keywords (represented by **x**) appears in braces separated by vertical bars. You must select one.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
^ or Ctrl	Represent the key labeled *Control*. For example, when you read *^D* or *Ctrl-D*, you should hold down the Control key while you press the D key.
`screen` font	Examples of information displayed on the screen.
`boldface screen` font	Information that you must enter is in **`boldface screen`** font.
italic screen font	Arguments for which you supply values are in *italic screen* font.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

Cisco.com

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

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

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

Product Documentation DVD

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

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

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

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

Ordering Documentation

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

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

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

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

Documentation Feedback

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

Cisco Product Security Overview

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

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

From this site, you will find information about how to do the following:

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

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

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

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

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

Reporting Security Problems in Cisco Products

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

- For emergencies only—security-alert@cisco.com

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

- For nonemergencies—psirt@cisco.com

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

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

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

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

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

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

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

Product Alerts and Field Notices

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

To access the Product Alert Tool, you must be a registered Cisco.com user. Registered users can access the tool at this URL:

http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

To register as a Cisco.com user, go to this URL:

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

Obtaining Technical Assistance

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

Cisco Support Website

The Cisco 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 at this URL:

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

Access to all tools on the Cisco 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 Before you submit a request for service online or by phone, use the **Cisco Product Identification Tool** to locate your product serial number. You can access this tool from the Cisco Support website by clicking the **Get Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Tip **Displaying and Searching on Cisco.com**

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

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

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

Submitting a Service Request

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

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

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

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

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

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

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

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

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

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

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

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

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

  http://www.ciscopress.com

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

  http://www.cisco.com/ipj

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

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

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

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

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

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

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

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

Introducing Cisco IPICS and the PMC Application

This chapter provides an overview of the components that are used in the Cisco IPICS solution. It also documents system requirements for the PMC application and important information that you need to know about server and user interactions.

This chapter includes the following topics:

- Overview of Cisco IPICS, page 1-1
- System Requirements for the PMC Application, page 1-17
- System Interactions, page 1-19

Overview of Cisco IPICS

This section provides an overview of Cisco IPICS and the PMC application; it includes the following topics:

- Introduction, page 1-2
- Cisco IPICS System Components, page 1-3
- About the PMC Application, page 1-7
- Architecture/Deployment, page 1-15

Introduction

The Cisco IPICS solution provides a cost-effective and highly-efficient IP standards-based solution to enable voice interoperability among disparate systems. By interconnecting voice channels, talk groups, and virtual talk groups (VTGs), Cisco IPICS bridges communications from radio networks to the Cisco IPICS Push-to-Talk Management Center (PMC) PC application and supported models of Cisco Unified IP Phones.

To provide this functionality, Cisco IPICS uses new components, such as the Cisco IPICS server and the PMC, and 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.

Through the use of integrated web-based system management software, the Cisco IPICS solution facilitates the tasks that are associated with operations and command and control to extend the reach of push-to-talk (PTT) voice technology from the LMR environment to the IP network.

The following examples portray typical customers who use disparate networks:

- PTT radio networks (analog or digital at different frequencies)—These networks are used for voice communications within groups. Communications are usually restricted within a specified group or network.
- VoIP networks—These networks are used for voice on wired or wireless IP phones or other IP clients, such as personal data assistants and laptop PCs.

Benefits of Cisco IPICS

For these customers, the Cisco IPICS solution provides the following benefits:

- By incorporating an incident management framework graphical user interface (GUI), Cisco IPICS provides a cost-effective solution that allows you to streamline operations and command and control while protecting your investment in deployed radio networks and applications.
- Through easy-to-use installation, management, and operational features, the Cisco IPICS solution enables rapid deployment and management of disparate audio communications systems and it provides a migration path to more robust IP applications and devices to cost-effectively achieve greater operational efficiencies.

Related Topics

- Cisco IPICS System Components, page 1-3
- Cisco IPICS User Roles, page 1-5

Cisco IPICS System Components

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

Table 1-1 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 on selected Cisco Media Convergence Server (MCS) platforms. (Refer to the *Cisco IPICS Compatibility Matrix* 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. The server also enables control of the configuration of the media resources that are installed in the router and which are used for audio mixing capabilities. In addition, the server includes the Cisco IPICS policy engine (hereafter referred to as *policy engine*), which enables telephony dial functionality and is responsible for the management and execution of policies and user notifications. For more information about the role of the Cisco IPICS server, see the "The Role of the Cisco IPICS Server" section on page 3-8. For more information about the various user roles that Cisco IPICS supports, see the "Cisco IPICS User Roles" section on page 1-5.

Table 1-1 Cisco IPICS System Components (continued)

Component	Description
Push-to-Talk Management Center (PMC)	The PMC is a PC-based software application that comprises a stand-alone PTT audio application that connects end-users, dispatch personnel, and administrators via an IP network. This connection enables participation in one or more talk groups or VTGs at the same time. (VTGs are the voice channels that users connect to based on specific incidents.) PMC users may change 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. See the "System Requirements for the PMC Application" section on page 1-17 for information about PMC hardware and software requirements.
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. Cisco IPICS leverages the Cisco Hoot 'n' Holler feature, which is enabled in specific Cisco IOS versions, to provide radio integration into the Cisco IPICS solution. LMR is integrated by providing an ear and mouth (E&M) interface to a radio or other PTT devices, such as Nextel phones. Configured as a voice port, this interface provides the appropriate electrical interface to the radio. You configure this voice port with a connection trunk entry that corresponds to a voip dial peer, which in turn associates the connection to a multicast address. This configuration allows you to configure a corresponding channel in Cisco IPICS, using the same multicast address, which enables Cisco IPICS to provide communication paths between the desired endpoints.

Table 1-1 Cisco IPICS System Components (continued)

Component	Description
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 mixes multicast channels in support of VTGs as well as 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. For a list of Cisco IOS versions that Cisco IPICS supports for use as an RMS, refer to the *Cisco IPICS Compatibility Matrix*. (Each supported Cisco IOS version includes the Cisco Hoot 'n' Holler feature.)
Networking Components	The Cisco IPICS solution may include some or all of the following network components, depending on the functionality that you require: routers, switches, firewalls, mobile access routers, wireless access points, and bridges.
Cisco Unified CallManager and VoIP Services	Cisco IPICS provides support for SIP-based interoperability with supported versions of Cisco Unified CallManager and Cisco IOS, with optional Cisco Unified CallManager Express, and VoIP services, such as the Cisco Unified IP Phone services, to help extend the reach of PTT technology to the IP network. These services allow participation in channels and/or VTGs through the use of supported models of Cisco Unified IP Phones by enabling these phones to work with Cisco IPICS as IP phone multicast client devices.

Note For detailed information about supported hardware and software that is compatible for use with Cisco IPICS, refer to the *Cisco IPICS Compatibility Matrix.*

Cisco IPICS 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, such as system administrator, ops view administrator, operator, dispatcher, or user.

Table 1-2 describes the user roles that Cisco IPICS supports. For more information about how these roles interact, see the "Cisco IPICS Server-PMC Interaction Scenario" section on page 3-3.

Table 1-2 Cisco IPICS User Roles

User Role	Description
System Administrator	The system administrator is responsible for installing and setting up Cisco IPICS resources, such as servers, routers, multicast addresses, locations, and PTT channels. The system administrator also creates ops views, manages the Cisco IPICS licenses and PMC versions, and monitors the status of the system and its users via the activity log files. The system administrator has the ability to administer all resources in the Cisco IPICS system.
Ops View Administrator	The ops view administrator capabilities include managing and monitoring the activity logs that are filtered by ops views and accessible in the Administration Console (**Administration > Activity Log Management**) window.
Operator	The operator is responsible for setting up and managing users and policies, configuring access privileges, and assigning user roles, and ops views. Policy management activities include create/modify/delete policies, view policies, execute policies, and activate privileges.
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 manages policies, which activate/deactivate VTGs based on specific criteria and designated intervals. Policy management activities include create/modify/delete policies, view policies, execute policies, and activate privileges.

Table 1-2 Cisco IPICS User Roles (continued)

User Role	Description
User	The Cisco IPICS user may set up personal login information, download the PMC application, configure the PMC skin to select the PMC display mode and other options, and specify communication preferences that are used to configure audio devices. By using a predefined user ID and profile, the user can participate in PTT channels and VTGs by using the PMC, supported models of Cisco Unified IP Phones, and the Public Switched Telephone Network (PSTN) via the telephony dial functionality of the policy engine.

Related Topics

- About the PMC Application, page 1-7
- PMC Application Usage Caveats, page 1-13
- Architecture/Deployment, page 1-15
- System Requirements for the PMC Application, page 1-17
- System Interactions, page 1-19
- Cisco IPICS Server-PMC Interaction Scenario, page 3-3

About the PMC Application

This section contains information about the PMC application and it includes the following topics:

- Browser Support, page 1-12
- Work Flow Activities, page 1-13
- PMC Application Usage Caveats, page 1-13

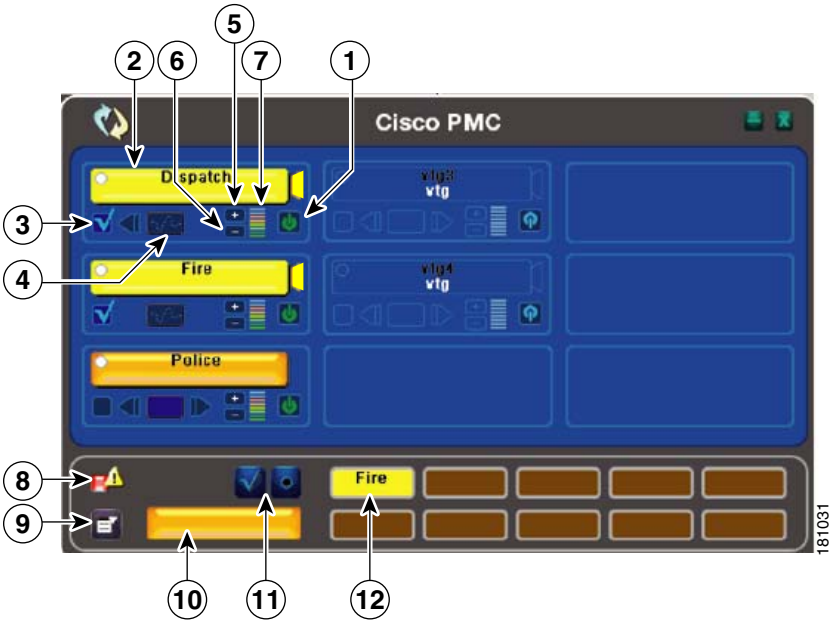
The PMC application provides the interface that enables push-to-talk audio communications. By using a simplified GUI, the PMC allows simultaneous monitoring and participation in one or more talk groups or VTGs at the same time.

The Cisco IPICS operator enables your user profile for access to the PMC application.

After you have been authorized to use the system, you can download the PMC software from the Cisco IPICS server and install it on your PMC client machine. For more information, see the "Downloading and Installing the PMC Application" section on page 2-4.

See Figure 1-1 for an illustration of the PMC application. This example shows a partial illustration of the PMC that has been configured for mouse-based use with the 18-channel advanced feature console.

Figure 1-1 PMC with Partially-Displayed 18-Channel Advanced Console Skin



1	Activation/ Deactivation Button	Click this button to activate a channel; click again to deactivate. The activation button highlights and changes orientation when you activate it. For more information about the PMC buttons, see the "Activating the PMC Buttons" section on page 4-13.

2	PTT Channel Button with Receive Indicator and Latch Indicator PTT Channel with Warning Indicator	Click the **PTT** channel button with your mouse, or push, and hold it to talk. When you are done talking, release the left mouse button to return to listen-only mode. The PTT channel button highlights in a different color when the PMC is in transmission mode. (The touch screen skins include a transmit indicator that blinks red when the PMC is transmitting traffic; for more information about caveats that pertain to the touch screen skins, see the "Touch Screen Skin Caveats" section on page 4-18.) The PTT channel button includes a receive indicator, which blinks green when the PMC is receiving traffic. For more information about traffic activity indicators, see the "Traffic Activity" section on page 4-35. This button may include a latch indicator. If you have permission to use the latch functionality, you can latch this channel to talk on one or more channels at the same time. To latch, or lock in, the PTT channel, click the latch indicator that displays to the right of the PTT channel button. To clear the latch, click the latch indicator or click the **PTT** button to release and return to listen-only mode. For more information about using the latch functionality, see the "Using the Latch Functionality" section on page 4-17. **Note** If you encounter a SIP-based remote connection failure, the PMC displays a warning indicator in the form of a yellow triangle next to the specific channel, as shown in the column to the left. For more information, see the "Support for Cisco IPICS Recovery" section on page 6-1 and the "Identifying Channel Activation Issues" section on page 8-23.
3	Channel Select Check Box	Check or uncheck this check box to select or deselect the channel for PTT communications. For more information about using the channel select check box, see the "Selecting One or More Channels and Using the All Talk Channel" section on page 4-25.

4	Voice Replay Controls	Use the voice replay functionality to play back buffered voice transmissions and to view graphical representation of this functionality. **Note** You must click the jump back, or rewind, button to enter voice replay mode and play out the available, recorded audio. For more information about the voice replay feature, see the "Using the Voice Replay Feature" section on page 4-32.
5	Volume Up Button	Click this button to increase the volume on the channel.
6	Volume Down Button	Click this button to decrease the volume on the channel.
7	Volume Level Indicator Bar	This bar shows the current volume level on the channel in a graphical format. This indicator represents the changes that you make by clicking the volume up and volume down buttons.
8	Server Status Connectivity Indicator	This connectivity indicator specifies your connectivity status with the server. • When your PMC is connected to the server, a green connectivity indicator displays. • When your PMC is not connected to the server, a red connectivity indicator and an alert icon display, as shown in the graphic. **Note** The PMC updates this connectivity status dynamically based on the status of its connectivity with the server. For more information, see the "Using the Status Menu" section on page 5-6.
9	Menu Button	Click the menu button to access the PMC settings menus and online help.

10	All Talk Channel Button	Click the All Talk channel to simultaneously talk on all of the channels that you selected. For more information, see the "End-user Features and Interactions" section on page 4-20.
11	Select All and Deselect All Buttons	Click the Select All (multiselect) button to select all channels that are assigned to you; click the Deselect All button deselect all channels. For more information about selecting multiple channels, see the "Selecting One or More Channels and Using the All Talk Channel" section on page 4-25.
12	Alert Tone Buttons	Use these buttons to play out alert tones on one or more channels on the PMC. The PMC plays out alert tones only on the channel(s) that you select. For more information, see the "Playing out Alert Tones" section on page 4-26.

Tip You can change the appearance of the PMC user interface by choosing another Cisco-provided or custom skin. For more information, see the "Configuring the PMC End-User Interface" section on page 5-1.

Note Your ability to use some of the PMC advanced features depend on specific user permissions that are configured in the server. For more information about user privileges, see the "User Privileges" section on page 3-16.

The PMC GUI includes buttons that allow you to interact with the Cisco IPICS server. It also includes various indicators to enable visibility of the connection status of the server and inform you about activities such as transmission status, channel states and activity, and volume level indicators.

The PMC GUI includes the PTT channel button, and other buttons, such as the activation button and buttons to control the volume level. The advanced skin may also include additional functionality, such as voice replay, alert tone buttons, the All Talk button, and multiselect channel check boxes; be aware that you must have permission to use some of these features.

The GUI also includes an indicator that blinks when you receive traffic; when you transmit traffic, the PTT channel button highlights and changes color to indicate transmission. (The touch screen skins also include an indicator that blinks when you transmit.) See the "Traffic Activity" section on page 4-35 for more information about these indicators.

Note The PMC modifies the channel behavior when you use the touch screen skins; for more information, see the "Touch Screen Skin Caveats" section on page 4-18.

When a channel has been activated, the PTT button displays on the PMC in a highlighted color that is based on the configuration in the Cisco IPICS server.

Note If your ability to transmit on a channel has been disabled by the server, the PTT button will not highlight on the PMC.

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 modify some of the configuration elements, such as the PMC GUI skins for mouse-based or touch screen-based display and key mapping. For additional information about configuring the end-user interface, see Chapter 5, "Configuring the PMC Application."

Browser Support

You install the PMC application on your local PC by downloading the software from the Cisco IPICS server upon successful user authentication. Cisco IPICS supports secure Internet access to the server by providing support for the following browser:

- Internet Explorer 6.0.2

After successful software download and installation, you log in to the PMC application on your PC. See Chapter 2, "Installing and Upgrading the PMC Application," for additional information about installing and launching the PMC application.

Work Flow Activities

The following activities occur when you use the Cisco IPICS system:

1. The Cisco IPICS operator sets up the necessary channel and VTG definitions on the server.
2. The PMC then retrieves the personalized list of channels and/or VTGs from the server.
3. You can join VTG(s) by selecting the channel(s) that the dispatcher associates with the VTG(s) and assigns to your user ID. (Only active channels and VTGs display on your PMC.)
4. When the dispatcher deactivates one or more VTG(s), you will no longer have access to the channel(s) that were created to support these VTG(s).

Note Cisco IPICS enables the dispatcher to dynamically add or remove PTT channels.

PMC Application Usage Caveats

Be aware of the following caveats when you use the PMC application with this release of Cisco IPICS:

- 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. See the "License Information" section on page 4-6 for more information about these licensing requirements.
- Each PMC application connects to only one Cisco IPICS server. If the primary server becomes unavailable, you can connect to an alternate server by entering the alternate server IP address or host name or by choosing the IP address for an alternate server from the Cisco IPICS login dialog box. For more information about logging in to alternate servers, see the "PMC Login Procedure" section on page 4-8 and the "Support for Cisco IPICS Recovery" section on page 6-1.

- The dispatcher assigns the voice channels that you can use on your PMC application, as they are needed. The dispatcher also activates and deactivates the channels that support the VTGs.
- The PMC retrieves, from the server, the channel name that displays on an assigned channel on your PMC application. This name may change based on the configuration in the server.
- When the dispatcher deactivates one or more VTG(s), you will no longer have access to the VTG(s) and the VTG(s) are removed from your PMC.

Tip 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 channels at the same time by using the PTT latch functionality, if you have user permissions configured in the server. To latch, or lock in, the PTT button, click the latch indicator or position your cursor over the PTT button and then press the **Shift** key while you click the left mouse button. Follow this procedure for each channel that you want to talk on. To clear the latch, click the **PTT** button without holding the Shift key. Alternatively, and if you have user permissions, you can select the channels that you want to talk on and click and hold the **All Talk** channel. For more information about using the All Talk channel, see the "Selecting One or More Channels and Using the All Talk Channel" section on page 4-25.

Caution Be aware that when you latch the PTT button, this action blocks transmissions from half-duplex radios when these devices are attached to the channel or VTG via an LMR gateway.

For detailed information about using and configuring the PMC application, See Chapter 4, "Using the PMC Application" and Chapter 5, "Configuring the PMC Application."

Related Topics

- Installing the PMC Application, page 2-2
- Launching the PMC Application, page 2-14
- Maintaining and Upgrading the PMC Application, page 2-16
- Logging In to the PMC Application, page 4-1
- License Information, page 4-6

- Using the PMC Application, page 4-12
- Configuring the PMC End-User Interface, page 5-1

Architecture/Deployment

A Cisco IPICS server-client deployment consists of a Cisco IPICS server and multiple PMC client systems. The PMC client systems connect to the Cisco IPICS server through a wired or wireless network. Additional components, such as routers and gateways, enable interoperability and additional capabilities. (See Figure 3-1 on page 3-2 for an illustration of this interoperability.)

The PMC is a network-installable application that is remotely managed by the Cisco IPICS server. An authenticated and authorized user can perform the PMC installation via a secure Web login to the Cisco IPICS server. After the PMC is installed, any valid and authorized Cisco IPICS user can log in to the PMC application. The server validates the user login credentials.

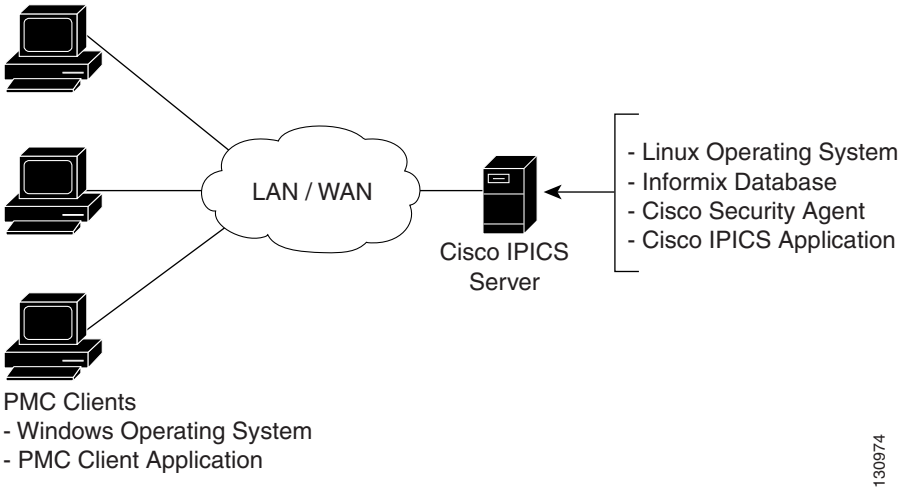
As a part of the login process, all user configuration information is downloaded and stored in conjunction with the login credentials. If the PMC becomes disconnected from the Cisco IPICS server, a user with a valid login may continue to use the application in offline mode.

The Cisco IPICS architecture includes centralized management of the PMC application, and specifically, the centralized (role-based) definition of the VTGs in the server. (This model compares to other PTT end-device models where the end-user defines the VTGs or uses a point-to-point session establishment mechanism.)

The fundamental design of the PMC is to present the end-user with channels, as managed by the Cisco IPICS dispatcher, and to provide users with the tools that they need to use these channels in an efficient manner.

Figure 1-2 shows a simplified version of a Cisco IPICS deployment by illustrating the interaction between the Cisco IPICS server and the PMC components.

Figure 1-2 Cisco IPICS Deployment



The following example represents a simplified flow that occurs between the Cisco IPICS server, the PMC, and other associated components:

1. The Cisco IPICS dispatcher creates a voice channel, or VTG, that correlates to a specific incident and assigns the necessary channels to the users.
2. By using the Cisco IPICS server GUI, the dispatcher includes the relevant users, channels, and other resources in the VTG.
3. Based upon this configuration, and after the dispatcher has activated the VTG, the server automatically refreshes the PMC so that it displays the VTG on the PMC client machine. (This voice channel contains the associated configuration to interwork as defined by the server; see 5. below.)
4. To directly join the channel, the PMC user clicks the **Activate** button on the PMC application. The Activate button highlights and the system attempts to connect to the channel or VTG. After the connection has been established, the remaining PMC buttons, including the PTT channel button, highlight to indicate that they are in an active state. (If your ability to transmit on a channel has been disabled by the server, the PTT button will not highlight.) See Figure 1-1 on page 1-8 for an illustration of the PMC application.
5. Depending on the configuration that the PMC retrieves from the Cisco IPICS server, the PMC directly joins the channel by using one of the following connection types, which are based on the defined location:

a. Remote connection—This type of connection uses SIP-based trunking into the RMS component, which is directly tuned into the multicast channel.

b. Multicast address/port—This type of connection enables the PMC to directly tune in to the multicast channel.

For more information about locations and types of connections, see the "Location Support" section on page 3-18.

6. The PMC user communicates with other members of the VTG by using push-to-talk capabilities.
7. When the incident has ended, the dispatcher deactivates the VTG; the server automatically refreshes the PMC and removes the VTG from the PMC application.

Related Topics

- Scenarios for Using the PMC Application, page 3-2
- Location Support, page 3-18

System Requirements for the PMC Application

This section includes information about hardware and software requirements for the PMC application, as well as pertinent caveats.

- Hardware Requirements, page 1-17
- Software Requirements, page 1-18

Hardware Requirements

The PMC application requires the following minimum hardware, as shown in Table 1-3. These requirements are dependent on the number of active PMC channels that you use.

Note Make sure that you install the PMC application on a PC that has the required Windows operating system installed. Cisco IPICS supports Windows 2000 Professional SP4 and Windows XP Professional SP2 for use with the PMC.

Table 1-3 PMC Minimum Hardware Requirements

Number of PMC Channels	PMC Hardware Requirements
Up to 4 active channels	• 800 MHz Pentium III class, including Mobile Pentium • 512 MB RAM • 1 GB free space • Network interface card
Up to 6 active channels	• 1.5 GHz Pentium IV class, including Mobile Pentium • 512 MB RAM • 1 GB free space • Network interface card
Up to 18 active channels	• 3.2 GHz Pentium IV class, including Mobile Pentium • 2 GB RAM • 1 GB free space • Network interface card

Software Requirements

Table 1-4 includes reference information about the software and applications that you install on your PMC system.

Table 1-4 PMC Systems Software

Software	Description	Reference
Windows operating system	• Windows 2000 Professional SP4, or • Windows XP Professional SP2	Refer to your Microsoft Windows documentation for installation and configuration instructions.
PMC application	Provides access to the PMC features	See Chapter 2, "Installing and Upgrading the PMC Application."

System Interactions

This section includes information about some of the system interactions that occur when you use Cisco IPICS, and includes the following topics:

- Server Interactions, page 1-19
- User Interactions, page 1-20

Server Interactions

The following section provides information about server-level interactions with Cisco IPICS.

Configuration Management

The Cisco IPICS server manages the configuration of the PMC and provides regular updates to the PMC. The server controls activities such as user profile management, user authentication, enabling/disabling/muting/unmuting users, enabling/disabling channels, activating/deactivating VTGs, updating the PMC configuration, and managing the PMC logs.

Session Management

The Cisco IPICS server manages the sessions on each of the PMC client machines.

- For each PMC, the server generates a unique PMC ID to track requests between the PMC and the server.
- After a PMC session is authenticated and initiated, the server begins a periodic check with the PMC to execute commands or to update the configuration on the PMC.

  These updates can include activities such as refreshing the PMC application based on new channel assignments or VTG activations/deactivations and notifying the PMC about new updates to ensure version compatibility.

See the "Maintaining and Upgrading the PMC Application" section on page 2-16 and "Dynamic Configuration" section on page 4-14 for more information.

Login Authentication

The Cisco IPICS server manages the login requests from PMC users. Initial login to the PMC application includes logging through the PMC application in to the Cisco IPICS server. The server then creates a session and identifies the PMC by the unique PMC ID.

If the server goes offline, the PMC user may be able to continue to use the PMC in offline mode as long as the user has made one successful login to the server.

Channel Management

The Cisco IPICS server downloads all of the currently available channels that can be displayed for a particular user based on each PMC session. When the dispatcher adds a user to a particular VTG, the server notifies the PMC of that updated channel availability.

- If a name, or label, has been configured in the server for a PMC PTT channel button, that name displays in the channel area as part of the PTT button on the PMC.
- The name may change, based on the configuration in the Cisco IPICS server.
- The channel may also include a channel type, such as VTG or 2-way, for quick identification of the channel.
- The channel may also display other attributes, such as specific background text colors that uniquely identify the channels for added prominence.

  For more information, see the "Channel Information" section on page 3-13.
- The server may also download a designated channel (such as a dispatcher channel) to the PMC by setting up a policy. See the "Implementing Policies" section on page 3-10 for more information.

User Interactions

This section provides information about user-level interactions with Cisco IPICS.

End-User Application Interaction

The Cisco IPICS server provides the list of PMC skins that are available to the PMC application. The server also defines a default skin for the PMC. The PMC stores the skins locally on the PMC user client machine.

The PMC user may choose a different skin by accessing the **Settings > Skin** menu in the PMC application. The functionality that is available may vary based on the skin that you choose.

See Table 5-1 on page 5-2 for a list of the PMC skins that Cisco IPICS supports.

For more information about configuring the PMC skins, see the "Configuring the PMC Skins" section on page 5-2.

End-User Channel Interaction

Channels and VTGs display in various states on the PMC. See Table 4-1 on page 4-19 for a description of the states that Cisco IPICS supports for user interaction.

For more information about using the PMC application, see Chapter 4, "Using the PMC Application."

Related Topics

- PMC-Server Interactions, page 2-1
- Maintaining and Upgrading the PMC Application, page 2-16
- Implementing Policies, page 3-10
- Dynamic Configuration, page 4-14
- Using the PMC Application, page 4-12
- Channel Interactions, page 4-15
- Configuring the PMC Skins, page 5-2

Where to Find More Information

- *Cisco IPICS Server Administration Guide*

Installing and Upgrading the PMC Application

This chapter describes how to install, upgrade, and uninstall the PMC application. It also explains how to revert to an earlier compatible version of the PMC application after you perform an upgrade.

This chapter includes the following topics:

- PMC-Server Interactions, page 2-1
- Installing the PMC Application, page 2-2
- Optimizing Your Audio on the PMC, page 2-7
- Launching the PMC Application, page 2-14
- Performing Additional PMC Tasks, page 2-16
- Maintaining and Upgrading the PMC Application, page 2-16
- Reverting to a Previous Version of the PMC Application, page 2-27
- Uninstalling the PMC Application, page 2-28

PMC-Server Interactions

The Cisco IPICS server manages the PMC application. When you install, update, or upgrade the PMC application, the PMC interacts with the server in the following ways:

- The server manages the PMC software, user data and privileges, and configuration information.
- The server manages the PMC installation-related tasks, such as installation, upgrade, and PMC update activities.
- The PMC downloads the installation file and other necessary user files from the server. These files include the Cisco IPICS server information along with skin and user configuration data; it may also include alert tones. (The skin information specifies the "look and feel" of the PMC end-user interface.) For more information about the PMC skin, see the "Configuring the PMC End-User Interface" section on page 5-1.
- Upon login, the Cisco IPICS server provides information to the PMC about available versions; the PMC then performs a check for version compatibility and determines whether the PMC must be upgraded. See the "Managing PMC Version Numbers" section on page 2-18 for more information about version management.

  PMC upgrades can be optional or required. For more information, see the "Managing PMC Upgrades" section on page 2-22.

Related Topics

- System Interactions, page 1-19
- Configuring the PMC Skins, page 5-2

Installing the PMC Application

You install the PMC application on a client machine on which the required Windows operating system is already installed. See the "System Requirements for the PMC Application" section on page 1-17 for information about hardware and software requirements.

This section includes the following topics:

- InstallationCaveats, page 2-3
- Downloading and Installing the PMC Application, page 2-4

InstallationCaveats

The following information pertains to the PMC application installation on your client machine:

- The PMC installation involves downloading the self-extracting PMC installation program, which includes the PMC installation and configuration files along with the PMC skins, from the Cisco IPICS server. If you are authorized to use alert tones, the PMC installation program may also include alert tones (or they may be downloaded separately).
- The PMC installation program automatically installs the PMC software on your client machine.
- The PMC installation does not require connectivity to the server.
- The installation automatically adds an entry to the Windows Start menu for "Cisco IPICS PMC" along with a desktop shortcut.
- The PMC performs preinstallation version checks to ensure compatibility. For more information, see the "Managing PMC Upgrades" section on page 2-22.
- The PMC retrieves your configuration data from the Cisco IPICS server, which maintains the most current information.
- The system may retain copies of previous versions of the PMC software so that you can easily revert to an earlier compatible version, if necessary. See the "Managing PMC Version Numbers" section on page 2-18 for information about the number of versions that may be retained.
- In this release, you do not need the fully executable file to completely update the PMC. The PMC automatic upgrade feature can update the PMC.dll file, PMC skins (if necessary), alert tones (optional), and/or online help depending on the contents of the update package. For more information about the automatic update process, see the "Managing PMC Version Numbers" section on page 2-18 and the "Support for Automatic Updates" section on page 2-21.

Downloading and Installing the PMC Application

The PMC application uses Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS) to ensure secure communications between the PMC client machine and the Cisco IPICS server. HTTPS ensures that the user login password transports securely via the web.

Cisco IPICS uses HTTPS with supported versions of Internet Explorer. See the "About the PMC Application" section on page 1-7 for more information about supported browser versions.

To install the PMC application on your client machine, perform the following procedure.

Note Before you perform this procedure, check with your system administrator to make sure that the Cisco IPICS server application has been installed and configured on the server.

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:

https://<*IP address***>**

Note Contact your system administrator if you do not know the IP address of the Cisco IPICS server to which you must connect.

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

Tip 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.

The Cisco IPICS Administration Console displays.

Step 4 From the Server tab, click the **Home** drawer; then click the **Download PMC** link that displays on the **Home > Download PMC** window.

The Download PMC pane displays.

Step 5 Click the **Download PMC** button to download the latest version of the PMC installation program (pmcsetup.exe).

The file download dialog box displays.

Step 6 Click **Save** to save the PMC installation program to a temporary directory on your hard drive.

Note Be sure to save the PMC installation file to a clean, temporary directory and make a note of the directory where you saved the file.

Step 7 After you see the Download Complete dialog box, which indicates that the download has completed, click **Close**.

Step 8 Navigate to the directory where you saved the PMC installation program and double-click **pmcsetup.exe** to extract the PMC installation file and the PMC configuration file, and to automatically run the installation executable to install the PMC on your client machine.

Tip If you encounter a problem running the pmcsetup.exe file, you can generate an installation log file to help you identify and resolve the problem. For more information, see the "Generating a PMC Installation Log File" section on page 8-3.

The Cisco IPICS PMC InstallShield Wizard displays.

Step 9 Click **Next** to continue.

The End User License Agreement displays.

Step 10 Read and accept the terms of the license agreement by clicking the "I accept the terms in the license agreement" radio button; then, click **Next**.

The destination folder window displays.

Step 11 Click **Next** to install the PMC application to the default folder.

Alternatively, you can click **Change** to install the PMC application to a different folder.

If you already have the same version of the PMC software installed on your client machine as that which you downloaded from the Cisco IPICS server, a Program Maintenance window displays. You can choose among the options that display in this window to modify, repair, or remove the PMC software from your client machine. This window displays only if you have the same version of the PMC already installed on your client machine.

The ready to install window displays.

Step 12 Click **Install** to begin the installation.

Note If you have Cisco Security Agent (CSA) installed on your PMC client machine and you are prompted with an access permission dialog box, make sure that you click **Yes** to grant permission to the PMC installation. 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

Step 13 Click **Finish** to exit the Cisco IPICS PMC InstallShield Wizard.

To immediately launch the PMC application, check the **Launch Cisco IPICS PMC** check box.

Note By default, Cisco IPICS installs the PMC software in the following directory on your PMC client machine hard drive: **C:\Program Files\Cisco Systems\Cisco IPICS\PMC**.

Tip The installation process places a shortcut to Cisco IPICS on the Start menu and a shortcut on your desktop. You can access the Start menu shortcut by navigating to **Start > Programs > Cisco IPICS > PMC**.

Optimizing Your Audio on the PMC

After you have installed the PMC application, check the current settings for the playback and recording audio devices on your client machine to ensure that you are using the preferred or default sound devices with the PMC. This section guides you through the audio configuration and it includes information about properly using a USB DSP headset and microphone for record and playback capability in the following topics:

- Configuring the Audio Settings, page 2-7
- Using a USB DSP Headset with the PMC, page 2-9
- Using the Microphone with the PMC, page 2-10
- Voice Quality Tips, page 2-12

Configuring the Audio Settings

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

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 **OK**.

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**.

Note The capability for the PMC application to coexist with other Cisco 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. See the "PMC Coexistence with Other Voice Applications" section on page 8-10 for more information.

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

Using a USB DSP Headset with the PMC

When you use a USB DSP headset (that is, a headset that includes its own sound card) with the Windows operating system, Windows may configure the USB DSP headset as the default speaker and microphone. Therefore, make sure that you connect the USB DSP headset to the PMC client machine before you launch the PMC. If you launch the PMC after you plug the headset into your PMC client machine, the PMC may not automatically remember the audio setting for the USB DSP headset; instead, the PMC reverts to the default Windows operating system audio settings.

Tip If you change your audio settings while you are running the PMC, you may need to restart the PMC for the changes to become effective.

To resolve this situation and use the USB DSP headset with the PMC, follow this procedure:

Procedure

Step 1 Close the PMC by clicking **Exit** from the PMC menu or by clicking the "**X**" that is located at the top right corner of the PMC application window.

Step 2 Navigate to **Start > Settings > Control Panel > Sounds and Multimedia**; then click the **Audio** tab to check the Windows audio settings.

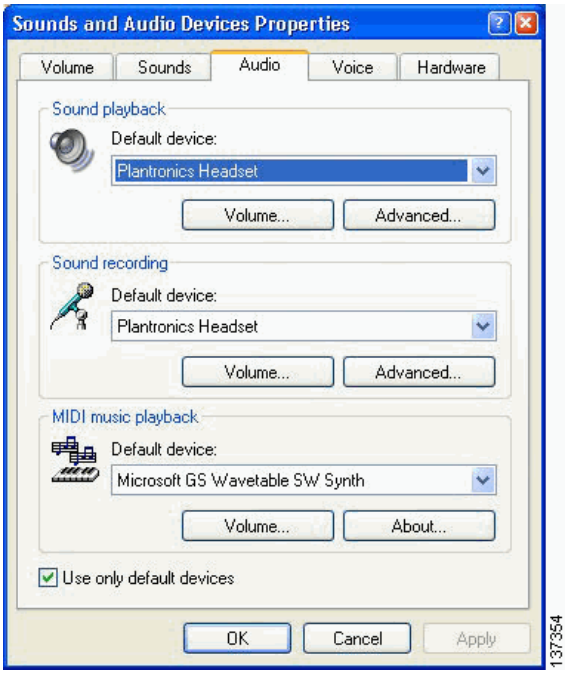
a. Configure the Windows audio settings to set the USB DSP headset as the default device by choosing the device from the drop-down list box.

b. Click **OK** to save your changes.

Step 3 Double-click the PMC icon on your desktop to start the PMC.

Figure 2-1 shows an illustration of the Sounds and Audio Devices Properties window with the default device specified and the "Use only default devices" option chosen.

Figure 2-1 Sounds and Audio Devices Properties Window



Note If you use the microphone on a USB headset for an extended period of time, your voice may become unintelligible. If this problem occurs, close the PMC and unplug the USB headset from the PMC client machine. Then, plug the USB headset back into the PMC client machine and restart the PMC.

Using the Microphone with the PMC

This section includes the following topics about operating the microphone and checking the settings to ensure proper use with the PMC:

- Important Information about Using the Microphone, page 2-11
- Checking the Microphone, page 2-11

Tip If you encounter a situation where you can hear other users but they cannot hear you, check to make sure that your microphone is not set to mute.

Important Information about Using the Microphone

Cisco IPICS might be configured to use voice activity detection to squelch (silence) transmissions that contain undetectable speech. To avoid issues that may arise from these incomplete transmissions, be sure to use a high-quality microphone and check the placement and settings of your microphone before you begin using the PMC.

Be aware of the following tips when you use the microphone:

- Make sure that you use a high-quality microphone with the PMC; otherwise, the Cisco IPICS system may not be able to accurately detect your voice and properly register transmit traffic.
- If the Cisco IPICS system cannot detect your voice when you transmit, the system may squelch the transmission; in this situation, another Cisco IPICS user may start speaking over your transmission because your voice cannot be heard and the PMC receive indicator of the listener may not display any indication of the transmission.

Checking the Microphone

To check the audio recording and playback capability of the microphone on your PMC client machine, access the Windows Sound Recorder to record your voice and then listen to the recording. (Make sure that you have an audio input device connected to your machine.)

To access the Sound Recorder on the PMC client machine, follow this procedure:

Procedure

Step 1 Navigate to **Start > Programs > Accessories > Entertainment > Sound Recorder**.

The Sound Recorder dialog box displays.

Step 2 Click **File > New**.

Step 3 To begin recording, click the **Record** button; this button displays in the lower right corner on the Sound Recorder dialog box.

Step 4 Speak into the microphone to record your voice.

Step 5 To stop recording, click the **Stop** button; this button displays to the left of the Record button.

Step 6 To listen to your recording, click the **Play** button; this button displays to the left of the Stop button.

You should hear your voice as it was recorded.

Alternatively, you can choose **File > Save as** and then enter a file name to save your recording file. Recorded sounds are saved as waveform (.wav) files. To play the file, choose **File > Open**, locate the sound file that you want to play; then, double-click the file.

Step 7 To stop playing the recording, click the **Stop** button.

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.

Note The use of a PC analog sound card and/or the use of the analog ports on most laptop computers typically results in lower quality voice transmissions. Therefore, Cisco recommends that you do not use your PC sound card and/or analog ports, as an alternative to a high-quality headset and microphone, for PMC communications.

- 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.

- If other Cisco IPICS users tell you that they hear a persistent or intermittent noise, such as an audible hum when you talk, the problem may be due to defective headset hardware. In this situation, Cisco recommends that you isolate the source of the audio quality issue by replacing the defective headset with a new, high-quality headset.
- 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 applications that consume high-CPU and high-network bandwidth 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.”

For more information about voice quality issues and tips, see Chapter 8, "Troubleshooting Tips for the PMC Application."

Launching the PMC Application

To launch the PMC application, perform the following procedure:

Procedure

Step 1 To launch the PMC application, choose 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.

Tip If you have network security software, such as 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 allow the PMC to monitor the media device (microphone). 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.

Note Be aware that if you allow CSA to time-out based on its default value of No, the PMC may not be able to receive or send traffic. For example you may be able to receive traffic but you may 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.

The Cisco IPICS login dialog box displays.

Step 2 To log in to the PMC, enter the following information:

a. Your **server IP address** or **server host name** (or choose your server IP address from the drop-down list box)

b. Your **user name**

c. Your **password**

d. Click **OK**

Tip Be aware that login user names and server host names are case-insensitive; that is, you can enter either upper case or lower case characters for these names. However, passwords are case-sensitive.

The location selection dialog box displays.

Step 3 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 location information that displays in the drop-down list box is configured in the Cisco IPICS server. Contact your system administrator if your location information does not display as an option or if you are not sure which location you should choose.

The PMC application opens on your desktop.

For detailed information about logging in to the PMC application, see the "PMC Login Procedure" section on page 4-8.

For more information about using the PMC application, see Chapter 4, "Using the PMC Application."

Note 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.

Related Topics

- About the PMC Application, page 1-7
- System Requirements for the PMC Application, page 1-17
- Location Support, page 3-18

- Using the PMC Application, page 4-12

Performing Additional PMC Tasks

After you install the PMC application, you can perform the tasks that are described in Table 2-1.

Table 2-1 Additional PMC Tasks

Task	Description	Reference
Download the PMC application	This task lets you download the PMC update files when you choose to download an operational or recommended update at a later time.	Downloading the PMC Update, page 2-23
Upgrade the PMC application	This task upgrades the PMC application when you choose to perform an upgrade to a recommended version of software at a later time.	Upgrading the PMC Application, page 2-24
Revert to a previous compatible version of the PMC application	This task allows you to revert to a previous compatible version of the PMC application.	Reverting to a Previous Version of the PMC Application, page 2-27

Related Topics

- Downloading the PMC Update, page 2-23
- Upgrading the PMC Application, page 2-24
- Reverting to a Previous Version of the PMC Application, page 2-27

Maintaining and Upgrading the PMC Application

This section describes how the PMC maintains compatibility with the server and the process that is used to upgrade the PMC application in the following topics:

- Maintaining PMC Version Compatibility, page 2-17
- Managing PMC Upgrades, page 2-22

- Managing Alert Tone Upgrades, page 2-26

Note Cisco IPICS does not support the use of previous PMC releases with a Cisco IPICS release 2.0(1) server. That is, you must use PMC release 2.0(1) with a Cisco IPICS server that also has release 2.0(1) installed. If you try to use a pre-2.0(1) version of the PMC with a server that has release 2.0(1) installed, the PMC pops up a message to alert you of the version mismatch. In this situation, you must access the Cisco IPICS server via your browser to download and then install the 2.0(1) version of the PMC.

Be aware that you will not be able to connect to your server by using the PMC until you upgrade your PMC. For information about accessing the server via your browser, see Step 2 in the "Downloading and Installing the PMC Application" section on page 2-4.

Tip Make sure that you close the PMC application before you install a new version of the PMC software. If you run the PMC at the same time that you install a new version, the system will prompt you to restart your machine after the installation has completed.

Maintaining PMC Version Compatibility

The Cisco IPICS server maintains information about version compatibility to ensure version control. This functionality also supports the ability to perform version upgrades to the next release of software, so that PMC users have the latest features and functionality, and the ability to revert to an earlier compatible version, if necessary. This version control extends to alert tone upgrades and skin downloads.

This section includes information about version compatibility and includes the following topics:

- Locating the PMC Version Information, page 2-18
- Managing PMC Version Numbers, page 2-18
- Support for Automatic Updates, page 2-21
- Managing PMC Upgrades, page 2-22

- Managing Alert Tone Upgrades, page 2-26

Locating the PMC Version Information

To locate the PMC application version information on your system, perform the following procedure:

Procedure

Step 1 If the PMC application is not already open, double-click the **PMC** icon on your desktop or navigate to **Start > Programs > Cisco IPICS > PMC** to launch the PMC application.

Step 2 To see the version information, click the **Menu** button or right-click in the PMC interface to see a list of options; then, click **About**.

The version information for your PMC application displays.

Note Alternatively, you can access the **Settings > Status** menu to see version information for the PMC. For more information, see the "Using the Status Menu" section on page 5-6.

Step 3 Click **OK** to exit.

Managing PMC Version Numbers

This section describes the various PMC versions that may be applicable to your installation.

Note Be aware that a Cisco IPICS server that runs version 2.0(1) provides support only for a PMC that also runs version 2.0(1). When a PMC that is running version 1.0(2) or earlier logs in to a 2.0(1) server, Cisco IPICS forces the PMC to upgrade to the 2.0(1) supported version. For more information, see the "Maintaining and Upgrading the PMC Application" section on page 2-16.

The PMC client system can maintain multiple versions, current and previous, of the PMC application. (The system may retain the previous versions, depending on the configuration, in the event that you need to revert to an earlier installed version.)

When the PMC initially starts up, the server communicates the PMC versions that are configured in the server and available to be run. See Table 2-2 for descriptive information about the range of PMC versions that Cisco IPICS supports.

Table 2-2 Cisco IPICS Server–PMC Version Information

Version Information	Description
Recommended	This version represents the recommended software version that should be run on the PMC. The server notifies the PMC of this recommended version and displays a message to inform you. The server then sends this version to the PMC and the PMC installs it after you respond positively to the message prompt or if other installed versions are not supported.
Staged	This version represents the software version that the PMC downloads according to the discretion of the administrator. The server sends this version to the PMC for download but the PMC does not install it until the administrator changes the state of this version to recommended or operational. At that time, the PMC may install the new version after you respond positively to the message prompt or if other installed versions are not supported.
Operational	This version represents a version of PMC software that is operational. This version is supported for use with the server but there may be a later version that is also supported. **Note** The server always extends priority to the PMC versions that it marks as recommended.

Table 2-2 Cisco IPICS Server–PMC Version Information (continued)

Version Information	Description
Not supported	This version represents an unsupported PMC software version. The server does not send this version to the PMC so that you cannot choose an unsupported version from the drop-down list box in the location dialog box. **Note** The server forces an upgrade on any PMC that is currently running an unsupported version of software.

By using the version information that is provided by the server, the PMC can take the following actions:

- Force a download and installation of a new PMC version if the version that is currently running is not supported.
- Allow you to continue to use a PMC version that is marked as operational.
- Prompt you to download the recommended version (the current version may be marked as operational).
  - You have the option to continue to use the earlier version or download and install the later version.
  - If you choose to download the recommended version, the PMC downloads and installs this version. Then, the PMC prompts you to log in again and choose the latest version from the location selection dialog box. For more information, see the "Support for Automatic Updates" section on page 2-21.
  - If the current version is not supported, the PMC forces an upgrade to the recommended version.
  - If the PMC is running the recommended version, no action is taken.
- Download the staged version without installing it. The PMC may download this version but does not install it until the server configuration has been updated to reflect this version as recommended or operational.
- Delete the versions that are not supported.

Support for Automatic Updates

This section contains information about the automatic PMC update process. It also includes information about managing skin downloads, as part of the PMC update process, in the "Managing Skin Downloads" section on page 2-21.

If your PMC client machine does not have the recommended version of the PMC software, a pop-up message displays to inform you that your version is not the recommended version and prompts you to download the recommended version.

- When you click **Yes** to this prompt, the PMC package for the recommended version downloads to the PMC client machine.

  The PMC package may include the PMC.dll file, PMC skins, alert tones, and online help, or a combination of components, depending on the specific configuration of the package.

After the PMC package downloads, the PMC version installs and the PMC prompts you to run the recommended version.

- When you click **Yes** to this prompt, the PMC login dialog box displays so that you can log in to the system again and choose the latest version from the location selection dialog box.

Note The PMC automatic update process may install only the PMC.dll file or it may install other components as well, depending on the contents of the package. The contents of the update package determine whether the PMC skins, alert tones, and online help are also updated as part of the automatic update process.

Managing Skin Downloads

Cisco IPICS manages downloads of PMC skins, including customized skins, that are included in the PMC package as part of the automatic update process. To minimize any impact to performance, Cisco IPICS downloads the skin files when the PMC starts up. Upon download, the skin files become available to all PMC users who connect to any Cisco IPICS server.

The server downloads the skins in a compressed .zip file format and then automatically uncompresses the file on the PMC client machine. If the server downloads a new version of the skin that you currently use, you must reselect the skin from the **Settings > Skin** menu to use the most updated version.

Note

- When you upgrade the PMC from one version to the next, the PMC provides support for only the most current version of the skins, as displayed in the **Settings > Skin** menu. However, the PMC does not remove the obsolete skins from the Skins directory that resides on the PMC client machine hard drive.
- Be aware that when you download skin names that match existing skin names, the PMC overwrites these names in the Skins directory on the PMC client machine hard drive.

Managing PMC Upgrades

This section includes information about the types of PMC upgrades that are available. It includes the following topics:

- Checking for PMC Updates, page 2-22
- Performing an Optional Upgrade, page 2-23
- Performing a Required Upgrade, page 2-25

Checking for PMC Updates

To ensure version compatibility, the PMC regularly polls the Cisco IPICS server to determine if PMC upgrades are available. When updates become available, the server automatically notifies the PMC and a pop-up message displays to alert you.

When the PMC receives a message from the server that indicates that new upgrades are available, the PMC may be forced to download and upgrade a new version immediately if the system detects version incompatibility (this situation occurs when the PMC is currently running a version that is not supported).

Alternatively, an option may be provided to download and upgrade a recommended version of software at a later time (this situation occurs when the PMC is currently running an operational version). The current version of the PMC application continues to operate when a new version becomes available as long as the current version is marked as operational or recommended.

Table 2-3 describes the types of upgrades that Cisco IPICS supports.

Table 2-3 Types of Cisco IPICS Upgrades

Type of Upgrade	Description	Reference
Optional Upgrade	This upgrade is optional if the current PMC version is operational or recommended. In this case, you may choose not to download the update. After a preconfigured period of time, the PMC will prompt you to download the update and perform the upgrade; you can choose to download now or at a later time.	For more information, see the "Performing an Optional Upgrade" section on page 2-23.
Forced Upgrades	This upgrade is required when the system detects a version incompatibility because the current PMC version is not supported. In this case, the PMC application must be upgraded immediately; a warning message displays to alert you of the necessity to upgrade your software. The download and upgrade procedures then run automatically.	For more information, see the "Performing a Required Upgrade" section on page 2-25.

Tip The PMC logs all update and upgrade activities to a log file. Be aware that the system may reset your debug log settings after you perform installation activities (such as install, upgrade, or repair) on the PMC. Check your debug log settings to make sure that the options that you need are enabled. For more information about how to identify, access, and use these logs, see Chapter 7, "Using the PMC Application Logs."

Performing an Optional Upgrade

This section describes the process that you need to follow to perform an optional upgrade of the PMC.

Downloading the PMC Update

When an optional update becomes available for the PMC, you may choose to perform the upgrade now or at a later time. In this situation, a message displays the next time that the PMC connects to the Cisco IPICS server to alert you that an update is available for download.

When you see this message, choose one of the following options to continue:

- **Yes**—Choose this option to instruct the PMC application to download the new version of the PMC application from the Cisco IPICS server.

Note The PMC manages the download and upgrade tasks in the background, so that you do not need to take any action.

- **No**—Choose this option to instruct the PMC application to not download the new version now and to prompt you later.

Note The PMC prompts you to download the update each time that you log in to the system.

Upgrading the PMC Application

When a PMC upgrade is outstanding, a message displays to inform you and asks if you want to upgrade the PMC now; this message displays the next time that you log in to the PMC application.

When you see this message, choose one of the following options to continue:

- **Yes**—Choose this option to instruct the PMC application to upgrade.
- **No**—Choose this option to instruct the PMC application to not upgrade now and to prompt you at a later time.

If you choose **Yes**, the PMC is upgraded to the recommended version.

Note The PMC prompts you to perform the upgrade every time that you log in. Be aware that network performance may be impacted during the upgrade process.

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

After the upgrade has been completed, choose your default location and the upgraded PMC version from the location selection dialog box drop-down list box; then, click **OK**.

Note The PMC version drop-down list box includes the PMC versions that are installed on the PMC client machine and compatible with the server. The location information that displays in the drop-down list box is configured in the Cisco IPICS server. Contact your system administrator if your location information does not display as an option.

Performing a Required Upgrade

The system typically requires an immediate upgrade of the PMC application when the Cisco IPICS server has been upgraded to a version that is not compatible with the PMC application (this situation occurs when the PMC is running a version that is not supported).

If an immediate upgrade of the PMC is required, a message alerts you. The required update downloads and the system performs the upgrade in the background, so you do not need to take any action. After the entire process completes, the previous PMC version exits. You can then log in to the system by choosing your default location and the upgraded PMC version from the location selection dialog box.

Note When a PMC upgrade must be installed because the current version is not supported, the system automatically downloads the updated version and upgrades the software in the background; you do not need to take any action. Be aware that audio quality might be impacted during this time.

Related Topics

- Identifying the PMC Logs, page 7-1
- Using the PMC Logs, page 7-5

Managing Alert Tone Upgrades

Cisco IPICS stores alert tones in a set on the server. An alert tone set is associated with an ops view; therefore, each PMC user can see only one tone set based on the ops view association. For more information about ops views, refer to the *Cisco IPICS Server Administration Guide*.)

If you are authorized to use alert tones, the PMC downloads the defined tone set from the server. To ensure that you have the appropriate tones, and to minimize impact to voice quality, Cisco IPICS downloads the alert tone set when the PMC starts up.

If the association between a tone set is modified in the ops view to which you belong and after the PMC has started up, a pop-up message displays to inform you that a tone set is available for download. You may choose to proceed with the download or cancel the operation.

- If you click **Yes** to the download prompt, the tone set downloads and the PMC refreshes to display the new alert tones.
- If you click **No**, the PMC cancels the operation and prompts you the next time that you log in to Cisco IPICS.

The server manages the alert tone download process in a similar manner to the automatic update process such that the server can force the download or prompt you to download the new alert tone set. Cisco IPICS supports the following alert tone version control categorizations:

- Required—When the server determines that the alert tone download is required, the file is automatically downloaded to the PMC.
- Recommended—If the download is recommended, Cisco IPICS prompts you to download the alert tone file now or at a later time. (If you choose to download at a later time, the system prompts you the next time that you log in to the server.)

Note Be aware that voice quality may be affected when you download alert tone sets.

Related Topics

- Playing out Alert Tones, page 4-26

Reverting to a Previous Version of the PMC Application

When you upgrade the PMC application, the PMC may maintain copies of the previous versions of the application. If necessary, and if an earlier version is compatible with the current version of the Cisco IPICS application, you can revert to any previous compatible version of the PMC application.

Note The system does not allow you to revert to a PMC version that is not compatible with the Cisco IPICS server.

To revert to any previous, compatible version of the PMC application, perform the following procedure:

Procedure

Step 1 Launch the PMC application, as described in the "Launching the PMC Application" section on page 2-14.

Step 2 From the drop-down list box in the location selection dialog box, choose the PMC version that you want to revert to.

The drop-down list box contains a list of the PMC versions that are compatible with the server.

Step 3 Click **OK**.

The PMC version that you choose becomes available for your use.

Related Topics

- Launching the PMC Application, page 2-14

Uninstalling the PMC Application

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.

Where to Find More Information

- *Cisco IPICS Server Administration Guide*

CHAPTER 3

Understanding PMC Interactions and Supported Features

This chapter provides information about the scenarios where you might use the PMC, information about the server and PMC interactions, PMC supported features, and specific terminology that the Cisco IPICS solution uses.

This chapter includes the following sections:

- Voice Interoperability, page 3-1
- Scenarios for Using the PMC Application, page 3-2
- The Role of the Cisco IPICS Server, page 3-8
- Supported Features, page 3-11

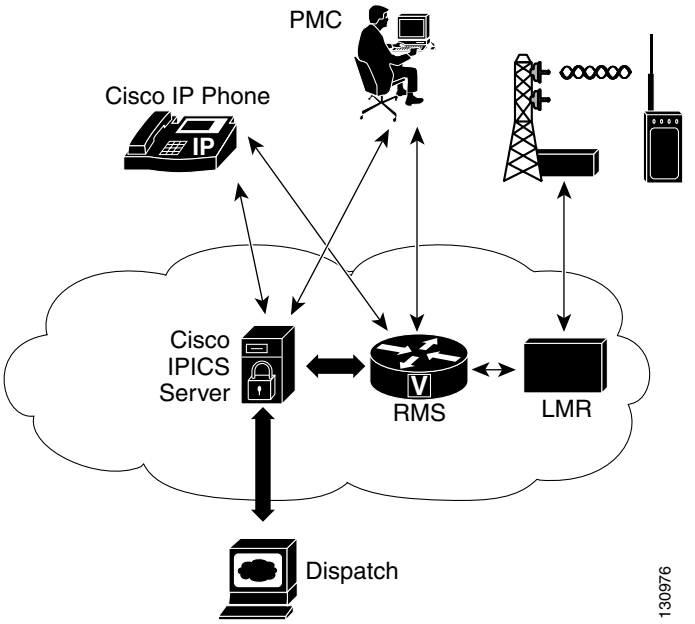
Voice Interoperability

Cisco IPICS solves the problem of voice interoperability between disparate systems by bridging PTT communications between multiple LMR systems, IP phones and PSTN phones, and the Cisco IPICS PMC.

As a PC-based software application, the PMC comprises a stand-alone PTT audio application that enables users, and dispatch and administrative personnel to participate in one or more VTGs at the same time.

Figure 3-1 shows an illustration of the various components that interoperate with the Cisco IPICS solution.

Figure 3-1 Cisco IPICS Interoperability Solution



For more information about the Cisco IPICS components, see the "Cisco IPICS System Components" section on page 1-3.

For information about Cisco IPICS deployment, see the "Architecture/Deployment" section on page 1-15.

Scenarios for Using the PMC Application

The following scenarios show how the Cisco IPICS solution combines the server and the PMC to enable voice interoperability. This section describes the following topics:

- Cisco IPICS Server-PMC Interaction Scenario, page 3-3
- Incident Management Scenario, page 3-6

- PMC User Interaction, page 3-7

Cisco IPICS Server-PMC Interaction Scenario

The following sequence of events shows how the Cisco IPICS server interacts with the PMC user, and includes information about the tasks that are performed by the various Cisco IPICS user roles:

1. The Cisco IPICS system administrator sets up the Cisco IPICS server from which the PMC user can download and install the PMC application. The system administrator also sets up and imports the user preference themes, which include graphics, XML, and tones for the PMC.

   The PMC retrieves the PMC installation file from the Cisco IPICS server along with the PMC user configuration data.

2. The Cisco IPICS operator sets up the users and the channels for the PMC user.

3. The Cisco IPICS dispatcher assigns the channels to the PMC user and sets up the talk groups by activating and deactivating the VTGs.

4. The PMC user downloads and installs the PMC application. For more information, see the "Downloading and Installing the PMC Application" section on page 2-4.

   The Cisco IPICS server checks the license count for concurrent license usage. See the "License Information" section on page 4-6 for information about licenses for concurrent PMC usage.

5. The PMC user initiates a session with the server by using the PMC application. See the "Launching the PMC Application" section on page 2-14.

   During the login sequence, the server provides information to the PMC about available versions to ensure compatibility. For more information, see the "Managing PMC Version Numbers" section on page 2-18.

6. The PMC sends a request to the server to authenticate the user. See the "Server-PMC Login Sequence Interaction" section on page 4-6.

7. After successful authentication, the server uses the unique PMC ID to track requests and to manage the session with the PMC. The following activities can occur during these sessions:

a. The server can execute a command or update the configuration on the PMC.

b. At regular intervals, as configured in the server, the PMC can check with the server for updates.

8. The PMC retrieves a personalized list of channels from the server, along with the configuration settings that provide user-specific channel restrictions and customization information.

   For more information about the user-specific settings, see the "Configurable Server Attributes" section on page 3-15. For more information about reordering PMC channels, see the "Reordering Your Channels" section on page 4-28.

9. The PMC user may modify some of the PMC configuration elements, such as defining the PMC skin, mapping keys to specific channels, and reordering the appearance of the channels on the PMC.

   For more information about configuring the PMC, see the "Configuring the PMC End-User Interface" section on page 5-1.

10. The PMC only displays, and the PMC user can only use and activate, those channels that have been assigned by the dispatcher.

    The PMC user may also be able to communicate and interact with the dispatcher through a policy channel, which may be configured as a designated channel that remains always open on the PMC. As a PMC user, you could use this policy channel, if it is configured, to initiate a request to the dispatcher to set up a new VTG when the situation arises. For more information about policies, see the "Implementing Policies" section on page 3-10.

11. The PMC user clicks the **Activate** button on the PMC application to directly join the channel. The Activate button highlights and the system attempts to connect to the channel or VTG. After the connection has been established, the remaining PMC buttons for that channel, including the PTT channel button, highlight to indicate that they are in an activated state.

Tip The PMC displays its connection status with the server. When the PMC is connected to the server, a green connectivity indicator displays; when the PMC is not connected to the server, a red connectivity indicator and an alert icon display to make you aware of the disconnection.

Note You may see different channel states on your PMC. For instance, if your ability to transmit on a channel has been disabled by the server, and/or if the channel has been configured by the server as a listen-only channel, the channel will appear dimmed. In this case, you may listen in to the channel but you may not transmit. If the channel has been disabled by the server, you will not be able to activate the channel, as none of the buttons will appear. For more information about the various channel states, see the "Configurable Server Attributes" section on page 3-15.

The type of connection that Cisco IPICS uses depends on the configuration that the PMC retrieved from the server. The PMC connection types include remote connection by using SIP-based trunking into the RMS component (which is directly tuned into the multicast channel) and multicast connection by directly tuning into the multicast channel. See the "Location Support" section on page 3-18 for more information about these types of connections.

12. The PMC user can listen in and talk on one or more channels at the same time. In this case, the PMC mixes the audio on the PMC client machine so that the PMC user can join multiple VTGs simultaneously.

Note Be aware that you may experience echo when you simultaneously listen to a VTG and a channel that is bound to that VTG.

Tip Your ability to latch a channel is configured in the server. If enabled, you can use the PTT latch functionality to talk on multiple channels at the same time. For more information, see the "Using the Latch Functionality" section on page 4-17. (You can also use the All Talk channel to talk on multiple channels that you select. For more information about the All Talk functionality, see the "Selecting One or More Channels and Using the All Talk Channel" section on page 4-25.)

13. The PMC checks the server for updates at regular intervals. When an update occurs (such as the activation or deactivation of a VTG), the PMC retrieves the updated information from the server.

    Based on the updates from the server, the PMC display refreshes automatically to reflect the changes that were made by the dispatcher.

14. The PMC logs the details of the channel assignments, including activation and deactivation. At predefined intervals, the Cisco IPICS server retrieves these logs from the PMC. See the "Using the PMC Logs" section on page 7-5 for more information about the logging facility.

Incident Management Scenario

In a Cisco IPICS scenario, the occurrence of an event or incident leads to the creation and activation of a VTG. The dispatcher can perform this VTG setup on an ad hoc (as needed) basis or by preconfiguring the VTG. Preconfigured VTGs could be scheduled to run at defined intervals or activated on demand.

The following example portrays an incident management scenario at an enterprise customer that shows how the various Cisco IPICS system components work together to deliver the Cisco IPICS solution.

1. The dispatcher receives a 911 emergency call and creates a voice channel that correlates to a specific incident.
2. From the Cisco IPICS server administration console, the dispatcher includes the police department in the talk group.
3. By using the PMC application, the dispatcher communicates directly with the police officer at the scene by using push-to-talk (PTT) functionality.
4. Upon discovering the magnitude of the emergency, the police officer informs the dispatcher of the need to communicate directly with the fire department.
5. Again, from the Cisco IPICS server administration console, the dispatcher adds the fire department into the talk group.
6. The police officer, dispatcher, and the fire department are all included in the expanded VTG and they are enabled to use PTT capabilities to communicate with each other.
7. Next, as a decision is made to dispatch fire engines to the scene, the dispatcher communicates with the public utility department and adds their radio channel into the talk group. During this time, the participants who are included in the talk group can make real-time decisions about items such as road conditions, routes to follow, and any necessary lane clearances.

8. Finally, the dispatcher seamlessly patches the enterprise security team and the facilities team, who use their own radio channels, into the talk group and they discuss evacuation procedures with all of the various agencies that are included in the call.

PMC User Interaction

The PMC user interacts with the PMC to join the VTG by clicking the PMC buttons after the dispatcher assigns channels to the user.

1. The PMC retrieves the personalized list of voice channels that the dispatcher assigns; the PMC display then refreshes automatically based on the updates that it receives from the server. The order of the channels, as they display on the PMC, is determined by the server. However, you can rearrange the order of your channels by navigating to the **Settings > Channels** menu. For detailed instructions, see the "Configuring the Channels Menu Options" section on page 5-8.
2. After the PMC has completed its startup processes, the PMC user clicks the **Activate** button on the PMC application to turn on and join in the VTG.
3. The Activate button highlights and the system attempts to connect to the channel or VTG. After the connection has been established, the remaining PMC buttons for that channel, including the PTT button, highlight to indicate that they are in an active state.

Note You may see different channel states on your PMC. For instance, the appearance of dimmed channels may indicate that your ability to transmit on a channel has been disabled by the server. For more information about the various channel states, see the "Configurable Server Attributes" section on page 3-15.

4. The PMC user clicks and holds the **PTT** button to talk. The PTT channel button highlights and changes color to indicate the occurrence of voice transmission. To return to listen-only mode, release the button.
5. When the incident has ended, the dispatcher deactivates the VTG; the server automatically refreshes the PMC, based on the new configuration, and removes the VTG from the PMC application.

Related Topics

- Cisco IPICS System Components, page 1-3
- Architecture/Deployment, page 1-15
- Launching the PMC Application, page 2-14
- Location Support, page 3-18
- Server-PMC Login Sequence Interaction, page 4-6
- Activating the PMC Buttons, page 4-13
- Joining a VTG, page 4-14

The Role of the Cisco IPICS Server

This section includes information about the role of the Cisco IPICS server and how it interacts with the PMC; it includes the following topics:

- Server-PMC Interaction, page 3-8
- Cisco IPICS Server Commands, page 3-9
- Implementing Policies, page 3-10

Server-PMC Interaction

The PMC depends on the Cisco IPICS server to provide its configuration, connection, management, authentication, and alert tone distribution information. Some of the specific features that the server provides are included in the following list:

- Detecting and preventing audio looping, which causes recurring echo, by determining when the addition of a channel into an active VTG may cause a loop
- Configuring and managing multicast and SIP resources and ensuring that the appropriate resource types are provided to the PMC
- Authenticating Cisco IPICS users
- Providing indication of user-specific restrictions and/or customization that may apply to channels

- Configuring and distributing alert tones and the associated button names, along with user permissions

While Cisco IPICS allows the PMC to operate in offline mode when the connection to the server is not available, the following operations require that the server be online and that an operable link with the PMC exists:

- Notification of assignment, removal or change of channel characteristics
- Updates to user access permissions (allowing or revoking user access)
- Download of new alert tones, skins, online help or PMC versions
- Upload of the PMC log files

For more information about PMC operations in offline mode, see the "PMC Offline Mode Caveats" section on page 4-7.

Cisco IPICS Server Commands

Table 3-1 describes the commands that can be sent from the Cisco IPICS server to the PMC in XML format.

Table 3-1 Cisco IPICS Server Commands

Command	Description
Channel List	Upon log in to the server, the PMC retrieves the channel list from the server. This list includes the names of the channels that the dispatcher assigns for each PMC user along with the connection type (location information). **Note** The PMC retrieves the entire channel list, even if the PMC has been configured to display fewer channels than that which is contained in the list. In this case, a message displays to alert you of the channel mismatch and that you may not be able to view all of the assigned channels/VTGs. See the "Skin Caveats" section on page 5-4 for more information. For information about reordering your channels, see the "Reordering Your Channels" section on page 4-28.

Table 3-1 Cisco IPICS Server Commands (continued)

Command	Description
Disable User	This command disables the PMC user from accessing the Cisco IPICS system. If the user is disabled while the PMC is communicating with the server, Cisco IPICS logs the PMC user off after processing this command.
Disable Channel	This command disables one or more channels on the PMC. Channels that are in a disabled state appear as non-activated channels but they cannot be activated.
Retrieve Logs	This command retrieves the logs from the PMC.
Set Logging Level	This command turns on and off the individual logs on the PMC. It also sets the debug levels within the debug log.
Mute User	This command mutes a PMC user from talking or transmitting voice on one or more channels. **Note** The PMC displays a pop-up message and the PTT channel appears dimmed to alert you that permission to transmit has been revoked.

Implementing Policies

The Cisco IPICS server includes the functionality to create/update/delete, enable/disable, and execute/run policies. Policies associate events or triggers to an action.

The following list includes the events or triggers that can initiate a policy:

- Selecting a button on the PMC
- Dialing in to the policy engine by using PSTN devices
- Explicitly triggering a policy (this action can be done by the dispatcher from the administration console)
- Using time-based triggering

Policies can include a set sequence of actions, such as activating and deactivating VTGs, inviting VTG participants to join the VTG, and sending messages to a list of recipients.

Cisco IPICS provides the functionality for the dispatcher to predefine these policies as recurring or non-recurring policies. By using policies, talk groups can be quickly set up or predefined to operate on a regular basis.

For more information about policies, refer to the *Cisco IPICS Server Administration Guide*.

Dispatcher Channel

The dispatcher may also set up a policy channel by which you can communicate through the PMC. This policy channel, if it is configured and designated by the dispatcher on the PMC, acts as a channel that is always open and enables your interaction with the dispatcher.

By using this channel on the PMC, you could initiate a request to the dispatcher to set up a new VTG when the situation arises.

Supported Features

This release of Cisco IPICS provides support for the following features:

- Channel Support, page 3-11
- Location Support, page 3-18
- Codec Support, page 3-22

Channel Support

This section includes information about channel terminology, the types of channels that Cisco IPICS supports, and the configurable server attributes that pertain to the channel, user, and connection information. It contains the following topics:

- Channel Terminology, page 3-12
- Channel Information, page 3-13
- Configurable Server Attributes, page 3-15

Channel Terminology

Channels form the fundamental building blocks of all the talk groups in the Cisco IPICS solution. Each channel contains a PTT button with various controls, such as send/receive feedback, volume control, and an activation control button that toggles on and off. The appearance of the channels on the various PMC skins may vary based on user permissions and the skin that is used. For an illustration of the 18-channel advanced console, see Figure 1-1 on page 1-8.

Table 3-2 describes the terminology that Cisco IPICS uses.

Table 3-2 Cisco IPICS Terminology

Term	Description
Channel	A channel consists of a single unidirectional or bidirectional path for sending and/or receiving signals. In the Cisco IPICS solution, a channel represents one LMR gateway port that maps to a conventional radio physical radio frequency (RF) channel. **Note** If a name, or label, has been configured in the server for the PTT button, that name displays in the channel area as part of the PTT button on the PMC. In this area, you may also see certain background text colors to uniquely identify a channel and a type indication for the channel, such as channel, VTG or 2-way.
Direct Two-way Channel	A PMC direct two-way channel directly connects two PMC users. Both of the PMC users must be online to engage in this direct, point-to-point connection. The channel type for this channel displays as 2-way. For more information, see the "Communicating with PMC Users via Direct Two-Way Channels" section on page 4-28.
Direct Dial Channel	A PMC direct dial channel supports the use of direct, point-to-point connections that enable a PMC user to directly dial a phone number that is connected via the PSTN or an IP phone that is reachable via the customer network. The channel type for this channel displays as direct dial. For more information, see the "Communicating with Phone Users via Direct Dial Channels" section on page 4-30.

Table 3-2 Cisco IPICS Terminology (continued)

Term	Description
Talk Group	A talk group comprises a subgroup of radio users who, under normal circumstances, only coordinate actions amongst users who are in the same talk group; radio interface with other subgroups is not required. With Cisco IPICS, a channel maps to a logical talk group; that is, all the participants who talk on the same radio frequency belong to a talk group
Virtual Talk Group	A virtual talk group, or VTG, represents interoperability of a group of channels and maps to a voice channel that users attach to based on a specific incident. The PMC directly joins the VTG based on the location configuration that is configured in the server. See the "Location Support" section on page 3-18 for more information. In this release of Cisco IPICS, a VTG represents an audio meeting.
Virtual Channel	A virtual channel is similar to a channel but a radio system may not be attached. By creating a virtual channel, participants who do not use physical handheld radios to call into a VTG become enabled by using the PMC application or a supported Cisco Unified IP Phone model.

Channel Information

This section includes information about the channels that display on the PMC; it also includes information about channel visual indicators in the "Channel Visual Indicators" section on page 3-14.

By accessing the administration console, Cisco IPICS authorized personnel can register, assign, activate, and deactivate channels for PMC users; these activities affect the channel, configuration, and connection information for each PMC.

The PMC retrieves the channel information, along with other configuration data, when the server sends notification to the PMC about the availability of the channel. The order in which the channels display on the PMC may be initially determined by the server; however, you may reorder the appearance of the channels on the PMC.

For more information, see the "Reordering Your Channels" section on page 4-28 and the "Configuring the Channels Menu Options" section on page 5-8.

Channel Visual Indicators

The PMC may display the following visual indicators on the channel, depending on configuration and/or connectivity status:

- The channel name, or label, that displays in the channel area as part of the PTT button on your PMC represents a logical name that has been assigned to the channel and defined in the server. (Likewise, the associated button names for the alert tones that display on the PMC, if you are permitted to use them, also represent the names that have been configured in the server.)
- The channel also includes information about the type of channel, such as channel or VTG, and other visual indicators to uniquely identify specific channels, such as the addition of an icon on the channel.
- Another type of visual indicator for a channel includes the use of a specific background color for the label text on the channel button to uniquely identify the channel. The system administrator may configure channels in the server by using a predefined color to differentiate and add prominence to certain channels. When this configuration is performed, the PMC displays the channel with a specific color indicator so that it can be easily distinguished from other channels on the PMC. These visual indicators display on a per-channel basis on the PMC.

Note If the channel name that was configured in the server includes more characters than the PMC can display, the PMC may truncate the name on the channel.

- When SIP-based remote connections fail, the PMC displays a visual indicator in the form of a yellow triangle next to the channel. For more information, see the "Support for Cisco IPICS Recovery" section on page 6-1 and the "Identifying Channel Activation Issues" section on page 8-23.

Configurable Server Attributes

This section contains information about the configurable server attributes that pertain to the channel, user, and connection information. It includes the following topics:

- Server Channel Provisions, page 3-15
- User Privileges, page 3-16
- Connection Support, page 3-17

Server Channel Provisions

The server configuration includes provisions for the following per-channel features, as shown in Table 3-3, to ensure that the PMC properly authorizes and displays data about the channels that are assigned to each PMC user:

Table 3-3 Server Channel Provisions for the PMC

Feature	Description
Channel color	This setting, as configured in the server, uniquely identify specific channels by using predefined colors for the background text that appears on the channel. This feature enables specific channels to be easily distinguished from other channels on the PMC.
Secure channel indicator	Setting this attribute in the server enables the PMC to provide a visual indication of a secure channel by displaying a highlighted icon in the lower left corner of the PTT button.
Listen-only channel	This setting specifies whether the user has permission to talk on the channel or VTG. When enabled, you may listen in to the channel but you cannot transmit. When enabled, this attribute enables the PMC to display a channel in listen-only mode. In this case, the channel appears dimmed on the PMC to indicate that you may not transmit.
Allow latch	This channel latch permission setting specifies whether you have permission to use the latch functionality to latch a channel.

Table 3-3 Server Channel Provisions for the PMC (continued)

Feature	Description
Enable Voice Activity Detection (VAD)	This setting specifies if VAD should be enabled; if VAD is enabled, the PMC only sends voice traffic when it detects a voice transmission. **Note** If the VAD attribute is changed in the server, the PMC channel restarts to configure the new value. If you previously selected the PMC channel by checking the Channel Select check box, you will need to reselect it after the channel restarts.
Mute RX on PTT	This attribute specifies the transmission settings for all channels or only one channel; it controls the audio from the active channels while you are transmitting.
Disable audio	This setting specifies whether the user has permission to talk and listen on the channel or VTG. When enabled, the user cannot talk or listen in to the channel or VTG.

User Privileges

In addition, the server configuration contains the level of user privileges that are provided to the PMC. These user privileges enable or disable your ability to perform certain activities, such as latching a channel or using alert tones on the PMC.

The Cisco IPICS server maintains the user privileges for each PMC user.

- These privileges extend to the list of PMC channels that you can view and use.
- When the dispatcher activates a VTG for you, you are granted VTG privileges that may allow greater interaction than the privileges of the channel itself. For example, a channel may be configured as listen only, but the VTG may allow transmission.

The server configuration includes provisions for the following per-user features, as shown in Table 3-4, to ensure that the PMC properly authorizes and displays data about the channels based on user permissions:

Table 3-4 Server User Provisions for the PMC

Feature	Description
Disable audio	This setting specifies whether the user has permission to talk and listen on the channel or VTG. When enabled, the user cannot talk or listen in to the channel or VTG.
Listen only	This attribute specifies that you are restricted to listening only on the channel; no transmission is allowed.
Allow latch	This latch permission setting specifies whether you have permission to use the latch functionality.
Advanced PMC permissions	These attributes specify whether you are enabled for the following features on the PMC: • Channel multiselect for voice and tone transmissions • Alert tones transmissions • DTMF tones transmissions • All Talk channel transmissions

Connection Support

The Cisco IPICS server also contains the associated connection configuration, which correlates to locations, to determine how the PMC should connect. Cisco IPICS provides connection support for both multicast and unicast communications.

- Multicast refers to communications that are sent between a single sender and multiple recipients on a network.

Tip Be sure to prequalify your PMC client machine for multicast communications. Certain Windows 2000 and Windows XP PMC client machines may encounter issues with sending multicast communications; in these situations, the PMC client machine may be able to receive but not transmit traffic. For more information, see the "Troubleshooting Multicast Communications Issues" section on page 8-19.

- Unicast refers to communications that are sent between a single sender and a single recipient on a network.

Note For more information about choosing your location and your type of connection, see the "Location Support" section on page 3-18.

For more information about the multicast technology, refer to the following URL: http://www.cisco.com/en/US/products/ps6552/products_ios_technology_home.html

Location Support

In the Cisco IPICS solution, location signifies "reachability;" that is, channels or users who are associated with the same location can communicate with each other without additional network configuration. Location is functionally equivalent to a multicast domain such that users who are in the same multicast domain are also in the same Cisco IPICS location.

The label that the system administrator configures in the Cisco IPICS server may refer to the location; this label could correspond to a physical or a virtual location.

Tip The location determines the type of channel communication that is appropriate for the location. If you choose a location and you do not hear any voice traffic, choose a different location until you hear the audio on the channel. You can change your location by restarting the PMC and then choosing another available location from the drop-down list box in the location selection dialog box.

The system administrator configures the channel and the location information in the Cisco IPICS server for each PMC user.

- These location definitions correspond to the different locations from which a PMC user can access assigned channels or VTGs.

Note The PMC may truncate the location name that was configured in the server if the location name includes more characters than the PMC can display.

As a PMC user, you can directly join the channel by using one of the following connection types:

- Remote connection—This type of connection uses SIP-based trunking into the RMS component, which is directly tuned into the multicast channel. This communication flows over a unicast channel that establishes a point-to-point session with the RMS.
  - When SIP-based communications are used, the RMS tracks and enforces the maximum allowable number of voice streams that the PMC can transmit.
  - When SIP-based remote connections fail, the PMC displays a visual indicator in the form of a yellow triangle next to the channel. For more information, see the "Identifying Channel Activation Issues" section on page 8-23.

  Cisco IPICS may deactivate channels that are connected via remote connection if there is no traffic activity after a specified time interval, as configured in the server. To reactivate a channel after it has been deactivated, click the **Activate** button on the PMC.
- Multicast address/port—This type of connection enables the PMC to directly tune in to the multicast channel. See the "Troubleshooting Multicast Communications Issues" section on page 8-19 for information about troubleshooting multicast communications.
  - The PMC supports a maximum of 3 simultaneous multicast voice streams per channel or VTG.
  - The PMC does not transmit any voice streams that exceed the maximum allowable number. The PMC continually tracks the number of voice streams and transmits only when the limit is not exceeded.
  - The PMC does not provide any visual or audible indication when the channel or VTG is not transmitting.

Note Be sure to always monitor the receive indicator for PMC traffic so that you do not talk over other Cisco IPICS users. When the receive indicator shows activity, you are receiving traffic. If you talk while the receive indicator shows activity, you are likely not being heard.

Table 3-5 describes the PMC behavior when it stops transmitting because the maximum number of voice streams has been exceeded.

Table 3-5 PMC Behavior When Exceeding Maximum Number of Voice Streams

Feature	Behavior
Latching a channel	If you try to latch a channel when the maximum number of streams has been exceeded, the PTT channel button and the latch indicator highlight, as if you were transmitting. The PMC attempts to transmit at random intervals.
Latched channel	If the channel had been latched and then the PMC stops transmission because the maximum number of streams has been exceeded, the PTT channel button and the latch indicator remain highlighted, as if you were transmitting. The PMC attempts to transmit at random intervals.
DTMF tone transmissions	When you transmit a DTMF tone on one or more channels, the PMC does not provide any indication when it stops transmission on any one of the channels. The DTMF tone continues to play out on all channels except the channel(s) that stopped transmitting. When the PMC is able to resume transmission, it continues to play out the DTMF tone from its current point. All of the PTT channel buttons return to non-transmit mode at the end of the transmission.
Alert tone transmissions	When you transmit an alert tone on one or more channels, the PMC does not provide any indication when it stops transmission on any one of the channels. The alert tone continues to play out on all channels except the channel(s) that stopped transmitting. When the PMC is able to resume transmission, it continues to play out the alert tone from its current point. All of the PTT channel buttons return to non-transmit mode at the end of the transmission.
All Talk channel transmissions	When you transmit by using the All Talk channel, the PMC does not provide any indication when it stops transmission on any one of the channels. The voice transmission continues on all other channels except the channel(s) that stopped transmitting. When the PMC is able to resume transmission, the voice transmission continues from its current point.

Upon initial PMC login, the PMC retrieves the personalized channel list and list of defined locations from the server. A dialog box displays to prompt you to choose a location from the list. (This prompt occurs only one time per PMC instance and immediately after your initial login.) For more information about choosing your location, see the "Launching the PMC Application" section on page 2-14.

You choose a location that corresponds to the type of network access connectivity that you will use for the PMC session.

- The server uses this location to specify the type of channel communication (SIP-based unicast or multicast) that is appropriate for the location.
- In the event that you move to another location, the system allows you to explicitly change the location by choosing another available location.

Tip Your system administrator can provide instructions about how to choose the proper location. If you choose an incorrect location and you do not hear any voice traffic, choose a different location until you hear the audio on the channel. You can change your location by choosing another available location from the drop-down list box in the location selection dialog box. If no location seems appropriate, you can choose the remote location, although this location increases network resource utilization and transmission delay on the channel.

Default Location

A default location may be defined for each PMC user.

- As part of its configuration, the Cisco IPICS server communicates the default location to the PMC.
- The PMC notifies the server about whether the default location, or another system-defined location, is being used.
- The system preselects the default location, or the location that you most recently chose, in the list that displays in the location selection window.

Codec Support

Voice-compression algorithms are commonly referred to as codecs (coder/decoder). Coding involves the process of encoding a digitized signal into a more efficient form for transmission; decoding encompasses the process of restoring the coded signal to its original form.

Codecs differ in terms of voice quality, compression rate and bandwidth, ability to carry dual-tone multifrequency (DTMF) and modem traffic, and the number of channels (calls) that can be supported.

The Cisco IPICS server defines the codecs that the PMC uses on a per-channel basis and sends this information to the PMC. (The PMC may override the codec setting, if necessary.)

With this release, the PMC supports the following codecs:

- G.711—G.711 performs pulse code modulation (PCM); it is the standard digital channel that is used in the public telephone network. PCM provides no compression and it does not require any digital signal processor (DSP) resources for transcoding.
- G.729—G.729 is a medium complexity codec that compresses speech or audio signal components into 8-kbps streams. G.729 requires DSP resources for transcoding.

Note Be aware that misconfigured codecs can cause an audio problem on the PMC. For more information, see the "Resolving Codec Mismatch Issues" section on page 8-24.

For more information about VoIP per-call bandwidth requirements and guidelines, refer to Voice Over IP - Per Call Bandwidth Consumption at http://www.cisco.com/en/US/tech/tk652/tk698/technologies_tech_note09186a00080094ae2.shtml.

An interactive tool that provides guidance about how to calculate bandwidth requirements for packet voice calls is available by accessing the Voice Codec Bandwidth Calculator at http://tools.cisco.com/Support/VBC/do/CodecCalc1.do. This tool provides information about the bandwidth that is used by different codecs for various voice protocols over different types of media.

Related Topics

- Cisco IPICS System Components, page 1-3
- Architecture/Deployment, page 1-15
- Launching the PMC Application, page 2-14
- Location Support, page 3-18
- Configuring the PMC End-User Interface, page 5-1
- Troubleshooting Voice Quality Issues, page 8-14

Using the PMC Application

This chapter provides information about using the PMC, including logging in and logging out of the application, channel and user interactions, associated caveats, accessing menus, and using end-user features.

This chapter includes the following sections:

- Logging In to the PMC Application, page 4-1
- Using the PMC Application, page 4-12
- Logging Out of the PMC Application, page 4-39

Logging In to the PMC Application

As a PMC user, you initially log in to the PMC application by logging through the application in to the Cisco IPICS server. (The first login requires availability of the Cisco IPICS server.) The server validates the user login credentials so that subsequent PMC logins can be performed without the server.

See the "Launching the PMC Application" section on page 2-14 for more information about launching and logging in to the PMC.

This section provides information about logging in to the PMC and includes the following topics:

- PMC Usage Guidelines, page 4-2
- License Information, page 4-6
- Server-PMC Login Sequence Interaction, page 4-6

PMC Usage Guidelines

Note Cisco IPICS only supports the use of PMC release 2.0(1) with a Cisco IPICS server that also runs release 2.0(1).

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

- Tips for Using the PMC, page 4-2
- Connectivity Tips for Using the PMC, page 4-3
- Login Caveats, page 4-4
- PMC Password Caveats, page 4-5

Tips for Using the PMC

The following tips will help you to use the Cisco IPICS PMC most effectively:

- Use a high-quality microphone and check the placement and settings of your audio devices before you begin to use the PMC. For more information about optimizing your audio, see the "Optimizing Your Audio on the PMC" section on page 2-7.
- Your ability to use certain PMC features, such as latch, multiselect, alert tones, DTMF, and All Talk, depend on the configuration in the server. For more information, see the "End-user Features and Interactions" section on page 4-20.
- You can use only those voice channels that have been assigned to you and which are visible on your PMC.
- When a channel is activated, the PTT button highlights and changes color. (For more information, see the "Channels/States" section on page 4-18, "User Channel Activity Interaction" section on page 4-37, and the "Configurable Server Attributes" section on page 3-15.
- To talk on a channel, click and hold the push-to-talk (PTT) button before you speak.
- Talk in short bursts and monitor the receive indicator so that you do not talk over other Cisco IPICS users.

Tip Be sure to monitor the receive indicator on the PTT channel button for PMC traffic so that you do not talk over other Cisco IPICS users. When the receive indicator shows activity, you are receiving traffic. If you talk while you are receiving traffic, you are likely not being heard.

Connectivity Tips for Using the PMC

The following tips will help to ensure successful connection of the Cisco IPICS PMC:

- Before you launch the PMC, establish network connectivity to make sure that you have a valid IP address.
- For connections that use the remote location, make sure that the PMC can establish connectivity to the Router Media Service (RMS). For more information, see the "Troubleshooting PMC Connectivity Issues with the RMS" section on page 8-21.
- If the Cisco VPN Client is installed on your PMC client machine, disable the "Stateful Firewall (Always On)" option; otherwise SIP and multicast connections may not work correctly. For more information, see the "Troubleshooting VPN Connectivity" section on page 8-15.
- For the PMC to work properly with Windows XP, you may need to modify the firewall settings so the PMC can send and receive the required protocols. For more information, see the "Using the PMC with the Windows XP Firewall" section on page 8-18
- Network limitations may prevent some PMC client machines from sending audio. In this case, choose the remote location to connect to Cisco IPICS. For more information, see the "Troubleshooting Multicast Communications Issues" section on page 8-19.
- Monitor the server status connectivity indicator for and other connectivity indicators for connection information. For more information, see the "Support for Cisco IPICS Recovery" section on page 6-1.
- If you use a docking station or pluggable audio devices with your client machine, close the PMC client and unplug your audio devices before you undock your PC; otherwise, your PC may become unresponsive and require you to reboot.

- The Cisco IPICS server contains the location information to determine how the PMC should connect. For optimum connectivity and higher quality audio, use the most appropriate location for your connection type when you log in to the PMC. If you choose a location and you do not hear any voice traffic, choose a different location until you hear the audio on the channel. For more information, see the "Location Support" section on page 3-18.
- If both wired and wireless connections are active, and if you selected a location other than remote, either disable the wireless connection or make sure that the PMC uses the IP address that is assigned to the wired connection. For more information, see the "Resolving IP Address Changes" section on page 8-13.

Login Caveats

This section describes the login caveats that pertain to this release of Cisco IPICS and it includes password caveat information that is contained in the "PMC Password Caveats" section on page 4-5. For information about using the PMC in offline mode, see the "PMC Offline Mode Caveats" section on page 4-7.

- The Cisco IPICS system allows only one instance of the PMC application to be open and only one user to be logged in to the PMC application on the client machine at a given time.
- If you need to log in to a PMC on a given client machine that already has another PMC user logged in, the original user must first log out of the application.
- A PMC user can log in to an unlimited number of different PMC applications at the same time; however, Cisco IPICS supports only the most recent PMC instance for use with the direct two-way and direct dial channel features. For more information, see the "Communicating with PMC Users via Direct Two-Way Channels" section on page 4-28.
- Any number of valid Cisco IPICS users can use the same PMC application, but not concurrently. See the "License Information" section on page 4-6.
- The PMC application can log in to the server that has been configured as the default server and from which the PMC installation file has been downloaded. Or, the PMC can log in to an alternate server if your primary server becomes unavailable. For more information about logging in to alternate servers, see the "PMC Login Procedure" section on page 4-8.

PMC Password Caveats

The following caveats pertain to the PMC password that you use to log in to the system:

Invalid Login Attempts

The following guidelines apply to the account lockout features

- If you incorrectly enter your password multiple times, such that you exceed the maximum number of invalid login attempts as configured in the server, your user account may be locked. In this case, the PMC does not allow you to log in to the system. A message displays to alert you to contact your system administrator to unlock your user account.
- If the number of invalid login attempts has been exceeded while you are already logged in to the PMC, the PMC allows you to continue to use the password for your current session. The PMC does not allow additional logins, however, until your user account is unlocked or your password is reset.
- If the number of invalid login attempts has been exceeded while you are logged in to the PMC via offline mode, the PMC allows you to continue to use the password after it returns to online mode.The PMC does not allow additional logins, however, until your user account is unlocked or your password is reset.

Password Expiration

The following guidelines apply to the password expiration feature:

- If you attempt to log in to the PMC after your password has expired, the PMC displays a message to alert you. In this case, the PMC does not allow you to log in to the system until after you have changed your password. To change your password, you must log in to the Cisco IPICS server and navigate to **Home > My Profile** to enter your old and new passwords. If you cannot access the server, contact your system administrator for assistance.
- If your password expires while you are logged in to the PMC, the PMC allows you to continue to use the password for your current session. You must change your password before the next login.
- If your password expires while you are logged in to the PMC via offline mode, the PMC allows you to continue to use the password after the PMC returns to online mode. You must change your password before the next login.

License Information

The Cisco IPICS server uses the PMC ID to track the version number of the PMC and to verify and manage concurrent PMC usage for licensing requirements.

Cisco IPICS uses the following criteria to determine license consumption for PMC users:

- 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, your access to the system will be interrupted. If this situation occurs, make sure that you contact your system administrator to request that additional user licenses be purchased and installed immediately.

Server-PMC Login Sequence Interaction

When you log in to the PMC, and when the connection between the server and the PMC is operational, your login request flows over a secure web (HTTPS) connection for processing by the Cisco IPICS server.

Tip You can see if the connection to the server is active by looking at the server status connectivity indicator that displays on the PMC. When the PMC is connected to the server, a green indicator displays. When the PMC is not connected to the server, a red indicator and an alert icon displays to make you aware of the loss of connectivity. When you click this indicator, the Status menu opens and displays the IP address of your Cisco IPICS server. For more information about this connectivity indicator, see the "Using the Status Menu" section on page 5-6.

If the connection between the server and the PMC is not operational, the system allows you to log in locally on your PMC client machine and connect to the server in offline mode. See the "PMC Offline Mode Caveats" section on page 4-7.

Note Cisco IPICS does not prevent you from logging in to the PMC application if the connection to the server goes offline as long as you have had at least one successful login to the server.

The PMC reconnects when the server access is restored.

This section describes the initial login sequence for the PMC user; it includes the following topics:

- PMC Offline Mode Caveats, page 4-7
- PMC Login Procedure, page 4-8

PMC Offline Mode Caveats

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.

Note The PMC also provides visual indication of server status connectivity so that you can be alerted when the connectivity to the server has been lost.

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. (When the PMC cannot connect to the server, it uses the cached information that it obtained from its prior connection.)
- 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.
- When you use the PMC in offline mode, the Cisco IPICS server address that displays in the **Settings > Status** menu may show the IP address of the server that you were trying to connect to, and which is offline. In this situation, the server status may display as “disconnected” even though the configuration information reflects the last server that you successfully logged in to.

- 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 list of channels from the last online session. (Some channels 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.

For information about operations that require the server to be online, see the "The Role of the Cisco IPICS Server" section on page 3-8.

PMC Login Procedure

To log in to the PMC application, perform the following procedure:

Procedure

Step 1 Double-click the **PMC** icon on your desktop or navigate to **Start > Programs > Cisco IPICS > PMC** to launch the application.

The Cisco IPICS login prompt displays.

Step 2 To log in to the PMC, enter the following information:

a. Your **server IP address** or **server host name** (or choose your server IP address from the drop-down list box)

b. Your **user name**

c. Your **password**

d. Click **OK**

If you cannot connect to your primary server, proceed to Step 3.

Tip Be aware that login user names and server host names are case-insensitive; that is, you can enter either upper case or lower case characters for these names. However, passwords are case-sensitive.

The PMC logs in to the Cisco IPICS server and sends this login information over a secure HTTPS connection.

- If your login was successful, the server provides the ability for subsequent local logins.
- If your login was not successful and you receive a failure notification because the PMC application could not communicate with the server, you can log in to the PMC locally, as long as you have already successfully logged in to the Cisco IPICS server. Or, you can log in to an alternate server, if one is available.

Note If the PMC becomes disconnected from the Cisco IPICS server, it continues to operate in its existing state; that is, the PMC can continue with its existing voice channels but it is not informed of any changes to the channel list until server connectivity is re-established.

Step 3 If the primary server is not accessible, and if there are alternate servers to choose from, follow these steps to connect to an alternate server:

a. Enter the alternate **server IP address** or **host name** (or choose an alternate server IP address from the drop-down list box); then, enter your **user name** and **password**.

b. Click **OK**.

Tip The last server IP address that you successfully connected to displays as the default server when you next launch the PMC.

For more information about connecting to alternate servers, see the "Support for Cisco IPICS Recovery" section on page 6-1.

Note If you incorrectly enter your password multiple times, such that you exceed the maximum number of invalid login attempts as configured in the server, your user account may be locked. In this case, you must contact your system administrator to unlock your user account.

Step 4 After successful login, the Cisco IPICS server checks the PMC version number.

If a PMC update is available for download, a message displays to alert you. If the update is optional, you can choose to upgrade the PMC at a later time. See the "Performing an Optional Upgrade" section on page 2-23 for more information.

If the system detects an incompatible version of the PMC, a message displays to alert you that the system must perform an upgrade immediately. See the "Performing a Required Upgrade" section on page 2-25 for more information.

If the PMC version is current, the server sends the list of locations that have been associated with your user ID.

Step 5 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 compatible with the server. The location information that displays in the drop-down list box is configured in the Cisco IPICS server. Contact your system administrator if your location information does not display as an option.

Step 6 The PMC sends its location information to the server and requests its configuration updates.

Note The PMC sets the location once per login sequence, but the server may also process the location information through the updates that it receives from the PMC.

After the login has completed and the location has been set, the server maintains the PMC session information to ensure that only one session exists on the server for each PMC.

Step 7 The PMC retrieves the personalized list of visible channels/VTGs from the server.

Note You may see various channel states on the PMC. For instance, if your ability to transmit on a channel has been disabled by the server, the channel appears dimmed. For more information, see the "Configurable Server Attributes" section on page 3-15. For information about channel behavior and caveats that pertain to the touch screen skins, see the "Touch Screen Skin Caveats" section on page 4-18.

Step 8 Click the **Activate** button on the PMC application to directly join the channel or VTG and hear the audio stream.

Tip When you click the Activate button immediately after a SIP-based (unicast) channel becomes available on the PMC, you may hear a busy tone if the RMS has not completely configured the channel. If you encounter this situation, click the **Activate** button to deactivate the channel; then, wait a few seconds and click **Activate** again to reactivate the channel. For more information about channel activation issues, see the "Identifying Channel Activation Issues" section on page 8-23.

After the PMC connects with the server, the channel on the PMC application becomes activated and appears highlighted to indicate that it is in an active state.

Step 9 Click the **PTT** button and hold it to talk.

The channel highlights and changes color to indicate that you are transmitting traffic.

Note If the channel appears dimmed, the PMC is not transmitting traffic. For instance, if you mute the microphone and click the PTT button or if there is a network transmission problem, the channel appears dimmed on the PMC to indicate that transmission is not occurring.

Step 10 When you are done talking, release the left mouse button to return to listen-only mode.

The receive graphical indicator blinks green to indicate that you are receiving traffic. (This indicator remains illuminated for several seconds after the receive transmission has ended.)

Tip To talk on one or more channels at the same time, you can select the channels that you want to talk on and click and hold the **All Talk** channel. You can also use the PTT latch functionality. (You need user permissions for both of these features.) For more information about using the latch functionality, see the "Using the Latch Functionality" section on page 4-17.

Related Topics

- Architecture/Deployment, page 1-15
- Maintaining and Upgrading the PMC Application, page 2-16
- Performing an Optional Upgrade, page 2-23
- Performing a Required Upgrade, page 2-25
- License Information, page 4-6

Using the PMC Application

This section provides information about how to use the PMC application and describes the various interactions that occur; it includes the following topics:

- Accessing Online Help, page 4-13
- Activating the PMC Buttons, page 4-13
- Joining a VTG, page 4-14
- Dynamic Configuration, page 4-14
- Channel Interactions, page 4-15
- End-user Features and Interactions, page 4-20
- Traffic Activity, page 4-35

Accessing Online Help

To access online help for the PMC, follow this procedure:

Procedure

Step 1 Position your cursor over the PMC window that displays on your desktop.

Step 2 Take one of the following actions to access online help:

- Click the **Menu** button that displays on the PMC; then click **Help**.
- Right-click in the PMC interface and click **Settings**; then, click **Help**.
- Press **F1** to access online help.

The PMC online help information displays.

Activating the PMC Buttons

When you use the 18-channel advanced console, each channel contains a PTT channel button with send/receive feedback, an activation control button that toggles on and off, a channel select check box, voice replay controls, volume control, volume graphical indicator, and a latch control indicator (if the channel has been configured as latchable in the server and if you have permission). For more information about using the latch functionality, see the "Using the Latch Functionality" section on page 4-17.

See Figure 1-1 on page 1-8 for a description of the buttons that display on the 18-channel advanced console.

The PMC provides the ability to individually control the volume on each channel. The volume slide bar controls the level of audio output for the specified channel as mixed with all other channels.

The volume level that the volume graphical indicator bar displays may appear slightly different depending on the granularity of the specific PMC skin that you use.

If you configured key mapping, you can use the assigned key, which displays on each mapped channel, to transmit instead of using your mouse.

Joining a VTG

When you are logged in to the PMC and the dispatcher creates a new VTG for you to join, the PMC retrieves the channel list, which includes information about the VTG, from the Cisco IPICS server; the server automatically refreshes the PMC window to show the updated channels.

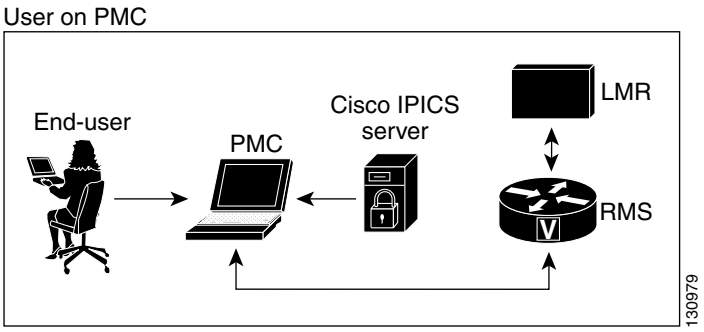
To join the VTG, click the **Activate** button. (The channel on the PMC application becomes activated and appears highlighted to show that it is in an active state as long as your ability to transmit has not been disabled by the server.)

Click the highlighted PTT channel button and hold it to talk; transmission becomes enabled on the multicast stream. When you are done talking, release the left mouse button to return to listen-only mode.

See the "End-user Channel Interaction" section on page 4-16 for information about the various channel states.

Figure 4-1 shows an illustration of the interaction with the PMC user.

Figure 4-1 Interaction with the PMC User



Dynamic Configuration

This section describes the dynamic configuration that the Cisco IPICS server performs for the PMC application. It also includes information about the PMC update procedure.

The Cisco IPICS server manages the configuration for the PMC so that you do not need to perform any configuration tasks. The server configuration includes information such as the system level PMC configuration, master skin distribution, user configuration, and channel definitions and authorized actions per channel.

In general, the PMC retrieves all configuration and channel connectivity data from the Cisco IPICS server, however, you can change the PMC skin by choosing from the available options that appear in the Settings menu. For more information about accessing the Settings menu, skin, see the "Configuring the PMC Skins" section on page 5-2.

The PMC includes the ability to check the Cisco IPICS server for configuration changes (when the server is online); if the application status changes, the PMC securely connects to the server to update its current state.

At regular intervals, the PMC sends a status request to the server for each PMC user. This status request determines if the user configuration needs an update and/or if the server has a request for the PMC to execute certain commands, such as an update. (The Cisco IPICS system performs a user level update only when a valid PMC user is logged in to the PMC application.)

Channel Interactions

This section describes the channel interactions on the PMC in the following topics:

This section includes the following topics:

- Support for Maximum Number of Channels, page 4-15
- End-user Channel Interaction, page 4-16

Support for Maximum Number of Channels

With this release, the PMC supports a maximum of eighteen channels. (The PMC allows the assignment of up to 50 channels, but only 18 channels may be active at the same time.) This support includes the ability to simultaneously receive and/or talk on one or multiple channels.

You can change the PMC skin to enable your own "look and feel," by choosing from one of the following skins as described in Table 5-1 on page 5-2.

The PMC modifies the PTT behavior on the touch screen skins. For more information, see the "Touch Screen Skin Caveats" section on page 4-18.

For more information and instructions about configuring the PMC skins, see the "Configuring the PMC End-User Interface" section on page 5-1.

Note

- Be aware that you may receive and transmit only on the channels that have been assigned to you and that are visible on the PMC client.
- If you have more than 18 channels assigned to you and you use the 18-channel advance console, the channels that are visible to you depend on whether or not the channel has already been visible on the PMC. That is, Cisco IPICS enables visibility of the last 18 channels that you saw. So, if a new channel has been assigned to you but it has not been previously visible, the channel will not display on the PMC when there are more than 18 channels assigned to you. If the channel is one that has been assigned and previously visible, it displays on the PMC.
- You can use the channel reordering functionality to move certain channels beyond the channel limit of the skin so that you can view the channels that you need. For more information about channel reordering, see the "Reordering Your Channels" section on page 4-28.

End-user Channel Interaction

As the Cisco IPICS standalone application, the primary goal of the PMC is to enable the PMC user to easily communicate on multiple PTT audio channels.

The PMC structure enables convenient and optimized interaction with multiple channels and different channel types. All channel types that the dispatcher has assigned and activated for your use appear on the PMC. You can selectively activate any of the assigned channels by clicking the **Activate** button on the PMC.

Channel Appearance on the PMC

- Channels that appear in blueprint mode on the PMC indicate that the channel/VTG is available and waiting for you to activate.
- If the channel has been disabled, you will not be able to activate the channel (none of the buttons will appear).

- If your ability to transmit on a channel has been disabled by the server, the channel appears dimmed on the PMC.
- When the channel appears dimmed, the PMC is not transmitting traffic. For instance, if you mute the microphone and click the PTT button or if there is a network transmission problem, the channel appears dimmed on the PMC to indicate that transmission is not occurring.

This section also includes information about the following topics:

- Using the Latch Functionality, page 4-17
- Touch Screen Skin Caveats, page 4-18
- Channels/States, page 4-18

Using the Latch Functionality

Your ability to latch a channel is configured in the server. If enabled, you can use the PTT latch functionality to talk on multiple channels at the same time. To latch, or lock in, the PTT channel button, click the latch indicator that displays to the right of the channel. Alternatively, you can position your cursor over the PTT button and then press the **Shift** key while you click the left mouse button.

When the channel has been latched, the PMC displays the highlighted latch indicator to the right of the channel. Follow this procedure for each channel that you want to talk on. To clear the latch, click the **PTT** button without holding the Shift key.

Latch functionality is not affected when the PMC loses focus, or is no longer the active application. In this situation, a latched channel remains latched even if the PMC loses focus.

Note Cisco IPICS does not support latching of the All Talk channel on the PMC.

When you latch a channel, the channel remains latched until one of the following activities occurs on the PMC:

- Alert tones are sent and complete
- DTMF tones are sent
- The All Talk channel is pressed and released
- The channel is deactivated, unassigned or not enabled for latch

- The PTT button for the channel is pressed and released
- The latch indicator is pressed and released

Caution Use the latch functionality with caution. Be aware that when you latch the PTT button, this action blocks transmissions from half-duplex radios when these devices are attached to the channel or VTG via an LMR gateway.

Touch Screen Skin Caveats

When you use the touch screen skins, the PMC modifies the PTT behavior in the following ways:

- The transmit graphical indicator blinks red to indicate that you are transmitting traffic.
- If your ability to transmit on a channel has been disabled by the server, the PTT button will not highlight.
- If the channel has been disabled by the server, you will not be able to activate the channel.

Channels/States

Table 4-1 shows the channel/VTG states that Cisco IPICS supports for user interaction.

If a name, or label, has been configured in the server for the PTT button, that name displays in the channel area as part of the PTT button on the PMC. You may also see channel type indicators, along with other visual indicators that have been configured in the server.

For more information, see the "Channel Information" section on page 3-13.

Tip When the channel appears dimmed, the PMC is not transmitting traffic.

Table 4-1 End-User Channel Interaction States

VTG/Channel State	PMC Button Indication	Description
Activating	The Activate button appears highlighted	This state becomes effective when you click the **Activate** button. The other PMC buttons remain in an inactive state as the system attempts to activate and connect. **Note** If your ability to transmit on a channel has been disabled by the server, the channel appears dimmed (none of the buttons appear on the PMC).
Activated	The PTT channel button and volume indicator appear highlighted	This state indicates that the SIP (unicast) or multicast channel is fully operational. When a channel is enabled and activated, all of the PMC buttons are operational.
Not Activated	No PMC buttons appear highlighted	This state becomes effective when you click the **Activate** button again (to deactivate the channel) or if the connection terminates. When a channel is enabled but not activated, the PTT channel button appears in blueprint mode but you may click the **Activate** button to activate the channel.
Disabled	No PMC buttons appear highlighted and you cannot activate the channel	When a channel is disabled, the channel appears dimmed and none of the PMC buttons appear so that you cannot activate the channel. However, you can still view the channel or VTG label, if one was configured in the server.
Unassigned	No PMC buttons appear highlighted and you cannot activate the channel	A channel that is unassigned appears on the PMC as completely empty, with no buttons and no channel name. You cannot activate or use an unassigned channel.

Table 4-1 End-User Channel Interaction States (continued)

VTG/Channel State	PMC Button Indication	Description
Listen-only	The PTT channel appears dimmed	When a channel is configured for listen-only mode, the channel appears dimmed on the PMC. In this case, you may listen in to the channel but you may not transmit.
Secure	All PMC buttons are functional	The PMC provides a visual indication of secure channels by displaying an icon in the lower left corner of the PTT channel. **Note** Cisco IPICS supports the configuration of secure channels, but does not provide support for secure VTGs.

End-user Features and Interactions

This section contains information about the following PMC end-user features and interactions. (Some of these features may be available only with the 18-channel PMC advanced console.) This section includes the following topics:

- Using Keyboard Mapping, page 4-21
- Using DTMF to Generate Tones, page 4-24
- Selecting One or More Channels and Using the All Talk Channel, page 4-25
- Playing out Alert Tones, page 4-26
- Reordering Your Channels, page 4-28
- Communicating with PMC Users via Direct Two-Way Channels, page 4-28
- Communicating with Phone Users via Direct Dial Channels, page 4-30
- Using the Voice Replay Feature, page 4-32

Using Keyboard Mapping

Cisco IPICS allows you to use keyboard mapping to assign specific keys to each of your channels. This feature provides transmit functionality by allowing you to press and hold the assigned key, to transmit on a channel, by using the keys on your keyboard. This control maps to specific channels on your PMC.

Cisco IPICS also supports the use of a device that simulates key down and key up events, such as a footswitch or other USB device. (Refer to the product documentation that you received with your USB device for details about how to configure it to generate the proper key; this device must be capable of simulating key held events as if you were holding down a key on a keyboard.)

Note

- Cisco IPICS provides support for devices that behave exactly like a keyboard and require no special support for the PMC to recognize it.
- To use these devices, the PMC must already be the active application (in focus) or the footswitch/USB device must be able to cause the PMC to be in focus.
- The device must be capable of generating key down events when you hold down the footswitch pedal followed by a key up event when you release the pedal (to simulate pressing and holding a key on a keyboard and then releasing it).
- The device and support applications must be able to send key down and key up events that correspond to keys “e” through “z” and/or the “Tab” and “space” keys.

To map your channels, you choose from a list of letters that range from “e” to “z.” The PMC displays only those keys that have not been previously used to map to a channel.

Tip Cisco IPICS does not allow you to map the same key to multiple channels, so any key that has already been mapped to a channel cannot be used to map to another channel until you unmap it.

If you have mapped a key to a channel that gets deleted from your PMC, the key that you mapped becomes available for you to map to another channel.

To configure the keys for each channel, navigate to the **Settings > Channels** menu. For detailed information, see the "Configuring the Channels and Advanced Settings" section on page 5-7.

After you define the key mappings for your channels, the PMC displays the assigned key on each channel that you configured. When you want to transmit on that channel, you can press and hold the assigned key instead of using your mouse. When you are done talking, release the key.

Note The key mapping that you configure is stored locally on the PMC client machine and applies only to the individual user who configured the key mapping assignments on the PMC client machine that you logged in to. If you use another PMC client machine, be aware that you must reconfigure your key mapping assignments.

Keyboard Mapping Caveats

The use of keyboard mapping may interact with the following PMC features:

- Certain Windows events and applications may change the focus from the PMC; that is, the PMC may no longer be the active application on the desktop. A change in focus may occur when a pop-up message displays and interferes with the expected operation of the PMC.
  - Under normal conditions, transmission continues until the method that you used to initiate the transmission has been ended, such as releasing the PTT button. However, if the focus changes when you are using a mouse, keyboard, or USB device to transmit on a channel, the transmission stops when the PMC detects that it is no longer the active application (or has lost focus). In this case, the PTT button changes color to indicate that it is no longer transmitting; this break in transmission occurs even if you continue to hold down the mouse or mapped key. After the PMC regains focus, you can begin transmitting again.
  - You may also encounter a loss of focus when you press and hold a mapped key and right-click the mouse in the PMC interface at the same time. If the key does not perform a valid PMC function, you may hear a "ding" or "beep" sound when you release the key or while the key is held. You may also hear these sounds when you press a key that performs a valid PMC function, such as the "s" key, which is a shortcut for the Settings menus. In these situations, the window that has the focus tries to

interpret the key that you pressed. These behaviors, as part of the standard operation of the Windows operating system, occur when the focus has been removed from the PMC.

Note Be aware that the PMC must be the active application when you press the All Talk channel or the PTT channel button. If the PMC loses focus (and is no longer the active application), the PMC stops transmitting. The PMC continues to transmit, however, if the channel is latched.

- You can transmit audio in several ways: by clicking or pressing the PTT button on a channel, checking the multiselect check box along with your mouse or touch screen client or mapped key, pressing a key that is mapped to the specific channel, using a device that simulates entry of a mapped key (such as a footswitch), or by entering the CLI **play** command from the Windows command line of the PMC.

  By using any of these methods, the transmission should continue until the method that you used to initiate the transmission has been ended. That is, if you press a mapped key and also click the PTT button with the mouse at the same time, releasing only the PTT button does not stop the transmission. You must also release the key that is mapped to the channel for the transmission to stop. Exceptions can occur when you simultaneously perform functions that may cause the PMC to behave in different ways. For example, if you press a mapped key, then click the PTT button with your mouse and then release the mapped key, the transmission stops.

- The keys that you can use for dual-tone multifrequency (DTMF) tone generation and the keys that you can assign to your channels by using keyboard mapping are mutually exclusive. That is, on an ASCII keyboard, Cisco IPICS supports the use of the number keys, the letter keys from ‘a’ through ‘d’ and the ‘*’ and ‘#’ symbols for DTMF use. The letter keys from ‘e’ through ‘z’ are reserved for PTT keyboard mapping. For more information about DTMF tone generation, see the “Using DTMF to Generate Tones” section on page 4-24.

Using DTMF to Generate Tones

You can use this feature to transmit DTMF tones for a fixed time duration to any specific channel. Cisco IPICS supports DTMF tone generation by using inband signaling. That means, when you press a key that supports DTMF tone generation, Cisco IPICS sends these tones as part of the normal voice transmission.

To generate DTMF tones, follow these steps:

1. Check the channel select check box for all channels that you want to transmit on. The channel select check box displays in the lower left corner of the channel on the PMC. Alternatively, you can select all channels by checking the Select All (or multiselect) check box, which is located at the bottom of the 18-channel PMC skin.
2. Then, press one of the supported keys, which include the number keys from ‘0 through 9, letter keys from ‘a’ through ‘d’ and the ‘*’ and ‘#’ symbols, on your keyboard.

   DTMF tones are generated inband for the duration of time that you press and hold the key.

DTMF Tone Generation Caveats

The following caveats pertain to the use of DTMF tones:

- Cisco IPICS supports the use of the number keys, the letter keys from ‘a’ through ‘d’ and the ‘*’ and ‘#’ symbols for DTMF use.
- Cisco IPICS sends DTMF tones only to the selected channels.
- To transmit DTMF tones, the PMC must be in focus; that is, it must be the active application that appears on your desktop. If the PMC loses focus while you are transmitting DTMF tones, the transmission stops and the PTT button changes color to indicate that it is no longer transmitting. After the PMC regains focus, transmission begins again.
- The G.729 codec cannot appropriately transmit DTMF tones and alert tones; for more information, see the “Playing out Alert Tones” section on page 4-26.
- When you use spatial positioning on the PMC, the DTMF tone that you play out is audible only on the highest position channel on the PMC. Check the **Settings > Channels** menu for the positioning information of your channels on the PMC.

- If your permission to transmit is revoked on the highest position channel, you will no longer hear the DTMF tone that is being played out, although the PMC continues to transmit the tone via other selected channels.
- If you attempt to transmit a DTMF tone while the network is down, the DTMF tone is audible to the sender even though it is not actually being transmitted. In this case, the DTMF tone that the sender hears is a confirmation of the request and not an indication that the tone is being sent. When this situation occurs, the PTT channel button appears dimmed, and the transmit indicator on the touch screen skin does not blink, to indicate that transmission is not occurring. For more information about the appearance of channels in various states, see the "Channels/States" section on page 4-18.

Selecting One or More Channels and Using the All Talk Channel

Cisco IPICS allows you to select one or more channels on the PMC for audio transmission. You can select a single channel or multiple channels by checking the channel select check box that displays in the lower left corner of the channel on the PMC. When you use this feature, a check mark displays in the check box of each channel that you have selected.

Alternatively, you can select all channels by clicking the Select All (or multiselect) button, which is located in the bottom portion of the 18-channel PMC skin and use the All Talk channel to talk.

Check the channel select check box or click the multiselect button to select channels that you want to use to send audio transmissions or alert tones. For more information about alert tones, see the "Playing out Alert Tones" section on page 4-26.

Multiselect Caveats

The following caveats pertain to the use of the multiselect feature:

- The multiselect button may reset under the following conditions:
  - Reconfiguration of the PMC skin
  - Stopping and restarting the channel
  - Channel reconfiguration to the listen-only or disabled state
  - Removal or reassociation of the channel

- Channel audio quality may degrade when multiple channels simultaneously send the same transmission. This situation is most noticeable to recipients when you play alert tones. To help resolve this issue, lower the volume or deactivate the channels that you seldom use and avoid sending the same alert tone to more than 3 channels at the same time.
- If the focus changes on the PMC while you are using the All Talk button to transmit, the transmission stops when the PMC detects that it has lost focus. After the PMC regains focus, you can begin transmitting again.

Playing out Alert Tones

In this release, Cisco IPICS provides the capability for the PMC to broadcast .wav files that contain alerting tones (hereafter referred to as alert tones) to a variety of Cisco IPICS users at the same time. Cisco IPICS stores alert tones in a set on the server. An alert tone set is associated with an ops view; therefore, each PMC user can see only one tone set based on the ops view association. For more information about ops views, refer to the *Cisco IPICS Server Administration Guide.*

If your PMC includes alert tones, you can play out these tones on one channel or multiple channels on the PMC. The PMC plays out alert tones only on the channel(s) that you select.

To play out an alert tone, you must first select a channel (or multiple channels) by checking the channel select check box that displays in the lower left corner of the channel on the PMC. Then, click the tone that you want to play out. The PTT channel highlights to indicate that transmission is occurring. Alert tone playout is not affected when the PMC loses focus; that is, alert tones continue to play out even if the PMC loses focus.

Tip Alert tone buttons do not actively display on the PMC until you select at least one channel by checking the channel select or multiselect check box.

The alert tone playout continues until it completes or you click another tone to play. To stop alert tone playout, deactivate and then reactivate the channel or click the stop tone if it is included in your list of alert tones.

Note The PMC alert tone feature requires the use of compatible alerting tone files. These files must be .wav files that are encoded in Pulse Code Modulation (PCM), which is a sampling technique that digitizes analog signals. These .wav files must

be encoded in PCM format with 8 bits monaural samples at 8000 Hz sampling rate, for a total of 64 kbps. While higher and lower bit rates may seem to work, Cisco IPICS does not support the use of any other encoding or bit rates, as they may produce inferior sound quality. (Any file that is used with the G.729 codec may sound inferior due to its encoding algorithms; for more information, see the "Codec Support" section on page 3-22.) In addition, all alerting tones should be encoded to a nominal value of -20 decibels relative to one milliwatt (dBm) and begin and end with zero deflection to eliminate or minimize "popping" or "clicking" sounds.

Alert Tone Playout Caveats

Be aware of the following caveats when you use alert tones on the PMC:

- When you select a channel and click a tone to play out, the tone begins to play out on that channel. If you want to transmit on the same channel while the tone is playing out, Cisco IPICS mixes your voice with the tone.
- If you deselect one of the channels after you selected multiple channels for transmission and click and hold the All Talk channel, Cisco IPICS terminates the transmission on the channel that you deselected but continues it on the channel that is still selected.
- While tone playout is occurring, if you deselect one of the channels after you selected multiple channels for transmission, Cisco IPICS continues to play out the tone on all channels that you originally selected.
- The PMC allows the use of either the alert tone playout feature, DTMF input, or the **Play** command at one time. That is, if an alert tone is currently playing and you invoke the **PMC.EXE -Play** *file* [**-line** *#]* command to the same channel, the alert tone on that channel stops playout immediately and is replaced with the output of the **-Play** command. If you press a DTMF digit, the alert tone or the -Play output stops immediately and the system sends the DTMF digit.
- Cisco IPICS allows you to talk over tones that are being played out by supporting the simultaneous use of the PTT channel button or the All Talk channel button.
- If you do not have permission to use any of the alert tones, the server does not download these tones to the PMC client machine. In this case, the alert tone buttons either do not display or appear disabled on the PMC.
- If your access to alert tones has been restricted by the server, your access to the All Talk channel button is similarly restricted.

- If the server assigns more alert tones that your PMC skin can display, the PMC pops up a message to alert you.
- Channel audio quality may degrade when multiple channels simultaneously send the same transmission. This situation is most noticeable to recipients when you play alert tones. To help resolve this issue, lower the volume or deactivate the channels that you seldom use and avoid sending the same alert tone to more than three channels at the same time.
- When you use spatial positioning on the PMC, the alert tone that you play out is audible only on the highest position channel on the PMC. Check the **Settings > Channels** menu for the positioning information of your channels on the PMC.
- If your permission to transmit is revoked on the highest position channel, you will no longer hear the alert tone that is being played out, although the PMC continues to transmit the tone via other selected channels.

Reordering Your Channels

The server designates the initial order in which the channels display on the PMC. However, you may reorder or reposition the channels that display on your PMC by accessing the **Settings > Channels** menu.

The ability to reorder your channels allows you to place channels in the order that you want to see them. For example, you can rearrange your channels so that the channels that you use most often appear at the top of the PMC and the ones that you use infrequently appear at the bottom of the PMC. This feature helps to optimize the space on your PMC skin so that you may be able to use a skin that includes fewer channels.

For more information about reordering your channels, see the "Configuring the Channels Menu Options" section on page 5-8.

Communicating with PMC Users via Direct Two-Way Channels

Cisco IPICS supports the use of direct, point-to-point PTT connections between online PMC users. This type of PMC communication operates similarly to other PMC channels, however, the direct two-way channels allow PMC users to talk directly from one user to another by using the PMC. (There is no capability to connect to other third parties when you use direct two-way channels.)

To enable this support, a direct two-way, bidirectional association is configured in the server on a per-user basis. The PMC then displays the direct two-way channel on your PMC by using the name of the user with whom you have an association in the server configuration. The channel may also include an indication of the channel type, such as 2-way.

Either online PMC user can activate the direct two-way channel. After one of the PMC users activates the channel, Cisco IPICS automatically activates the channel at the other end of the connection, as long as the channel is visible on the PMC skin. (If the channel is not visible, you may be able to reorder the channels on your skin; for more information, see the "Reordering Your Channels" section on page 4-28.) When the connection has been established, the PTT button highlights to signal the capability to transmit.

When one of the PMC users deactivates the channel, the other end of the connection becomes deactivated as well.

Direct Two-way Caveats

The following caveats pertain to the use of direct two-way channel connections on the PMC:

- Direct two-way channels are associated and disassociated in the server, so you do not have the ability to permanently deactivate or disconnect this channel. If you deactivate a direct two-way channel, the associated PMC user at the other end of the connection can reactivate it. This action causes the PMC to automatically reactivate the channel on your PMC. If you do not want to listen in to this channel, you can lower the volume.
- A single PMC user may have more than one direct two-way channel on the PMC to communicate on a one-to-one basis with different associated PMC users.
- Users must be logged in to Cisco IPICS to use PMC direct two-way channel connections. If both PMC users are online, the PMC displays the channel in an active state for all associated users. If one of the PMC users is not online, the PMC displays the channel in a disabled state for all associated users. (If your PMC client machine goes offline, the PMC notifies the associated PMC user by disabling the channel.)
- If a single PMC user logs in to Cisco IPICS multiple times by using the same login information, the system creates only one direct two-way channel for that user and links it to the most recent user login.

Note If previous direct two-way channels were established for the user, Cisco IPICS disables all direct two-way channels except for the most recent user login. If the PMC is not connected to the server when the simultaneous login occurs, the previous PMC instance maintains its login to the server (the PMC does not get logged out until it reestablishes connectivity with the server).

- The PMC does not attempt to retry the channel activation if the connection to the associated PMC user cannot be established. In this case, a warning indicator displays next to the channel and a busy tone plays out on the PMC. Connection failure may be caused by situations such as a network interruption or reset/restart activity at the remote end, if the PMC user does not have available channels to use, or if the online status of the user is undetermined by the Cisco IPICS server. When this situation occurs, you must deactivate the direct two-way channel; then, reactivate the channel to try the call again.
- If a direct two-way channel is associated to your user ID but your PMC client has no available channels, the PMC displays a message to inform you and request that you choose another skin. If you do not choose another higher-capacity skin, the associated PMC user at the other end of the connection hears a busy tone upon attempting to activate the channel.

Communicating with Phone Users via Direct Dial Channels

Cisco IPICS supports the use of direct, point-to-point connections that enable a PMC user to directly dial a phone number that is connected via the PSTN or an IP phone that is reachable via the customer network. (Similar to the two-way direct connection, there is no capability to connect to other third parties when you use direct dial channels.)

This direct dial feature allows a PMC user to use the PMC PTT features to speak directly with a telephone user. The destination telephone can be any phone that is reachable by the SIP provider. (The SIP provider routes the call to the number that you dial.) As SIP-based calls, direct dial calls route from the PMC through the RMS to the SIP provider.

To enable this support, a direct dial phone number is configured in the server, on a per-user basis, where the dial phone number is associated to a PMC user. Every phone that may be called by the PMC direct dial feature must have its destination

number configured in the server and assigned a label. Then, users are associated with these phones; each phone association appears on the PMC as a channel, with the unique identification of direct dial.

For more information about SIP providers and the direct dial configuration, refer to the "Configuring and Managing the Cisco IPICS Policy Engine" chapter in the *Cisco IPICS Server Administration Guide*.

After the configuration is completed, the PMC displays the direct dial channel on your PMC by using the description that was configured in the server, along with an indication of the direct dial channel type.

To use the direct dial channel, you must first click the **Activate** button to activate the channel and dial out to the PSTN or IP phone user. The PTT button highlights to signal the capability to transmit and the PMC automatically dials the phone number that was configured in the server.

Note As the call is being placed through the PSTN or customer network, you may hear a ringing tone on the PMC channel. If the call cannot be completed, you may hear a busy tone or an error message that provides additional information. (The PSTN user hears the usual ring tone, if the PSTN phone is not busy.)

After your call is connected, you can talk to the PSTN or IP phone user by clicking and holding the PTT channel button or by latching the direct dial channel, if you have permission to use the latch functionality. For more information about the latch functionality, see the "Using the Latch Functionality" section on page 4-17.

The call terminates when the PMC user deactivates the channel or the PSTN or IP phone user hangs up.

Direct Dial Caveats

The following caveats pertain to the use of direct dial channel connections on the PMC:

- The PMC does not attempt to retry the call if the PSTN or IP phone user does not answer the phone, if the PSTN or IP phone is busy, or if the call fails for any reason. In this case, a warning indicator displays next to the channel and a busy tone plays out on the PMC. When this situation occurs, you must deactivate the direct dial channel; then, reactivate the channel and try the call again.

- The dial destinations that you are allowed to call depend on the configuration in the Cisco IPICS server and your specific telephony deployment.
- Cisco IPICS does not support the call transfer feature when you use direct dial. If a PSTN or IP phone user attempts to transfer a direct dial call, the Cisco IPICS system terminates the call.

Using the Voice Replay Feature

Cisco IPICS supports the ability for the PMC to maintain a rolling history of voice transmissions, on a per-channel basis. With this feature, the PMC constantly records the aggregate inband voice transmissions that are played out on a channel. It then buffers the audio in talk spurts that are based on detected aggregate silence; this buffering occurs on a per-channel basis so that each channel maintains its own recording buffer. (A talk spurt occurs after a period of silence.) If two or more PMC users talk at the same time, the system detects silence only after both users stop talking.

In playback mode, the PMC mixes live and buffered (recorded) audio so that you can talk and play audio on the same channel at the same time. In this mixed audio mode, the PMC records only live audio.

When the PMC replays buffered audio, it simultaneously receives and buffers new audio. The new audio gets added to the buffer and the existing audio get pushed toward the end of the buffer. The PMC mixes the new audio with the buffered playback.

Note The PMC compresses and buffers these voice transmissions in the memory of the PMC client machine. The size of the voice replay buffer is 60 seconds per channel (the playback window size is not configurable; it is the same for all channels). Be aware that Cisco IPICS does not provide support for these voice transmissions to be saved to a file.

To enable this feature, the PMC includes the following voice replay controls that allow you to choose to jump back (rewind) or jump ahead (fast forward) to available recorded transmissions for playback on one or more channels.

Note Upon activation of a channel, the voice replay controls display on the lower half of the PMC channel when there is audio in the buffer; when there is no audio in the buffer, the voice replay controls appear dimmed on the PMC.

- Jump back—Click this button to enter voice replay mode. The PMC rewinds the voice transmission 7 seconds or to the beginning of the current talk spurt, whichever number is less. The PMC mixes the audio so that it plays out the buffered audio at the same time that it plays out live audio. You can click this button again to jump back an additional 7 seconds from the current playback position or you can continue to click this button until the PMC reaches the end of the voice buffer.

  When you click the jump back button, the voice replay indicator displays the amount of the replay buffer that remains and the jump ahead button becomes enabled so that you can click it to fast forward to another point in the buffer.

Tip You must click the jump back, or rewind, button to enter voice replay mode and play out the available, recorded audio.

- Jump ahead—Click this button to fast forward the voice buffer by 5 seconds or to the beginning of the next talk spurt, whichever is less. Each click of this button, fast forwards the recording by another 5 seconds. If there is no available recorded audio to play, the PMC exits voice replay mode.

Tip When you click the jump back, or rewind, button, the PMC starts playout of the recorded audio and enables the jump forward button. Because the voice recording buffer contains only a small amount of data (60 seconds per channel), the PMC quickly reaches the end of the buffer and automatically disables the jump forward button. Therefore, the jump forward button may appear enabled for a limited amount of time. When you continuously and repetitiously click the jump back button, you may see the jump forward button flash as the PMC continues to enable and disable this button.

- Voice replay indicator—This indicator displays as an illuminated line that progresses during voice replay mode.
- Graphical display of buffered talk spurts—The PMC displays a graph that indicates that audio is being recorded.

Voice Replay Caveats

The following caveats pertain to the voice replay feature:

- The voice replay feature may stop playing if you change the spatial position setting while you are using this functionality. Therefore, make sure that you do not change the spatial position setting at the same time that you are using the voice replay feature.
- The PMC detects aggregate silence; it does not record audio during periods of silence.
- The PMC does not buffer individual audio streams. Instead, the PMC buffers the aggregate voice transmission (per channel) that is being played out to the speaker or headphone so that each channel maintains its own recording buffer.
- The total buffered audio is comprised of the last one minute of actual, incoming traffic that occurred on the channel.
- The PMC uses dynamically allocated memory to temporarily store the buffered audio. The PMC does not support saving the buffered audio to disk or other permanent storage.
- Because the PMC stores the voice replay buffers in memory on the PMC client machine, you lose access to your original voice replay buffers when you change PMC client machines. If the PMC client machine that you use has less than the required amount of memory, the voice replay feature may not be available or each voice replay buffer may be smaller (with a shorter voice replay time period). If you close your PMC or deactivate your channels and then restart the PMC, the voice replay buffer is emptied and no longer available.
- Any live audio that is received while the PMC is in voice replay mode will move the earlier audio toward the back of the audio buffer, where it will be eventually discarded when the maximum buffer size has been reached.
- The voice replay feature records only inband audio packets; it does not buffer DTMF tones or other tones that are not inband.
- Your ability to hear buffered audio while transmitting depends on the “RX Mute on PTT” setting on the channel. If you latched multiple channels or if you clicked the All Talk channel, the most restrictive “RX Mute on PTT” setting prevails for all channels. For more information about this setting, see the “Configuring the Channels Menu Options” section on page 5-8.

Traffic Activity

This section provides information about traffic and channel traffic activity interactions; it includes the following topics:

- Channel Traffic Activity Interaction, page 4-37
- User Channel Activity Interaction, page 4-37

The PMC supports the display of channel traffic activity (receive and transmit) along with the ability to tune in and tune out of the channel itself.

Note To show traffic activity, the PMC provides graphical indicators, depending on the skin that you use. For instance, the touch screen skins include a transmit graphical indicator that blinks red to indicate that you are transmitting traffic. For information about caveats that pertain to the touch screen skins, see the "Touch Screen Skin Caveats" section on page 4-18

See Figure 1-1 on page 1-8 for an illustration of the 18-channel advanced console and the location of the graphical indicators.

Although the PMC skins may be configured to define the actual colors that are used, the Cisco standard defines the following conventions for the receive and transmit indicators:

Table 4-2 Channel Traffic Activity Indicators

Channel Traffic Activity Indicator	Description
Receive indicator	This graphical indicator illuminates and blinks green when you are receiving traffic. This indicator 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. **Note** Be sure to monitor the receive indicator for PMC traffic so that you do not talk over other Cisco IPICS users. When the receive indicator shows activity, you are receiving traffic. If you talk while you are receiving traffic, you are likely not being heard.
Transmit indicator	The PTT channel button highlights and changes color to indicate that you are transmitting traffic. The touch screen skins include a graphical indicator that blinks red when you are transmitting traffic. **Note** If you mute your microphone after you have clicked or latched the PTT button, the PTT channel button returns to a dimmed state; this change indicates that you are not transmitting traffic. When you unmute your microphone, the PTT channel button changes color to indicate that you are once again in transmit mode.

These graphical indicators provide useful visual aids that enable clear identification of the PMC traffic streams. When you are talking, you should monitor the receive indicator to see if it is blinking. If the receive indicator is blinking, you may be talking over another user. If you encounter this situation, release the PTT button to listen to the user who is talking. (To be sure that a user has stopped talking, wait for the receive indicator to display in a solid color format for a few seconds before you start to talk.)

Examples of how these indicators may appear are shown below:

- The channel may blink green when it receives traffic from the network.
- The channel may change color when there is PTT transmission while the PTT control is activated. (Or, if there is a graphical indicator for transmit activity, the channel may blink red when there is PTT transmission while the PTT control is activated.)
- When receive traffic activity displays, a graphical indicator reveals that traffic has occurred in the past on this channel; this feedback clears after five seconds.

Channel Traffic Activity Interaction

The following information describes the channel traffic activity interaction:

- Both the channel name and the traffic activity feedback can be mapped to the PTT button in the server. This allows both of these indicators to display as part of the PTT button itself.
- Cisco IPICS supports implicit floor control; that is, when the PMC wants to have the floor, the PMC assumes that the user will wait until there is no incoming traffic to enter transmit mode.
- The Cisco IPICS server has the ability to administratively stop the transmission of traffic onto a channel on a per-channel basis; in this situation, all transmission terminates immediately.

User Channel Activity Interaction

Your ability to view and use channels on the PMC depends on your user status.

- 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.
- If you activate and deactivate channels on the PMC while you are actively using one of the channels, the audio on the channel that you are actively using may become distorted.
- Channels that appear in blueprint mode on the PMC indicate that the channel/VTG is available and waiting for you to activate.
- If your ability to transmit on a channel has been disabled by the server, you will not be able to activate the channel (none of the buttons will appear) and the channel appears dimmed. (When the channel appears dimmed, the PMC is not transmitting traffic.)
- When a channel is disabled, the channel appears dimmed and none of the PMC buttons appear 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 as completely empty, with no buttons and no channel name. You cannot activate or use an unassigned channel.
- If there is no traffic activity after a 30 minute interval, channels that are activated via a SIP-based remote connection may be deactivated by the system. The PMC will automatically reactivate the connection after 30 seconds. Alternatively, you can reactivate the channel by clicking the **Activate** button on the PMC.

Note When SIP-based remote connections fail, the PMC displays a visual indicator in the form of a yellow triangle next to the channel. For more information, see the "Identifying Channel Activation Issues" section on page 8-23.

- To connect your PMC via a SIP-based remote connection, make sure that the PMC can establish connectivity to the RMS. (The PMC connects to the RMS by using the IP address of the Loopback0 interface that is assigned to the RMS.) 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, see the "Configuring the Channels and Advanced Settings" section on page 5-7. For more information about troubleshooting the RMS, see the "Troubleshooting PMC Connectivity Issues with the RMS" section on page 8-21.

Related Topics

- Configuring the PMC Skins, page 5-2
- Skin Caveats, page 5-4

Logging Out of the PMC Application

You can log out of the PMC application in either of the following ways:

- Click the **Menu** button; then, click **Exit**.
- Right-click in the PMC interface; then, from the PMC menu, click **Exit**.
- Click the "**X**" that is located at the top right corner of the PMC to close the application.

Where to Find More Information

- *Cisco IPICS Server Administration Guide*

CHAPTER 5

Configuring the PMC Application

This chapter provides information about modifying some of the PMC configuration elements to personalize the PMC application end-user interface.

This chapter includes the following sections:

- Configuring the PMC End-User Interface, page 5-1
- Using the Optional Settings Menu, page 5-15

Configuring the PMC End-User Interface

The Cisco IPICS server manages the configuration for the PMC. However, as a PMC end-user, you may personalize some of the PMC configuration elements, such as the PMC skin, view and configure settings (such as key mapping), and set up the PMC logs, if necessary.

For information about using the PMC logs, see "Identifying the PMC Logs" section on page 7-1.

This section describes how to change the PMC skin setting and certain caveats that you should be aware of when you configure the PMC skin. It also includes information about using the Status, Skin, Channels, and Advanced settings that appear in the Settings menu. This section describes the following topics:

- Configuring the PMC Skins, page 5-2
- Skin Caveats, page 5-4
- Using the Status Menu, page 5-6
- Configuring the Channels and Advanced Settings, page 5-7

Configuring the PMC Skins

Cisco IPICS supports a maximum of eighteen channels and several different skins that you can use for the PMC. (The PMC allows the assignment of up to 50 channels, but only 18 channels may be active at the same time.) See the "Support for Maximum Number of Channels" section on page 4-15 for more information about Cisco IPICS channel support.

The Cisco IPICS administrator creates and configures the skins that are available for the PMC. Your system administrator has the option to allow you to use only selected PMC skins. If you cannot configure your PMC skin, contact your system administrator for additional information and assistance.

The ability to change the PMC skin allows you to individualize your own PMC "look and feel." You may choose a different skin to create your own individualized interface by accessing the **Settings > Skin** menu in the PMC application. The PMC stores the skin locally on the PMC client machine. For information about accessing the Settings menu, see the "Procedure" section on page 5-4.

Tip Right-click in the PMC interface, or click the **Menu** button, to access the options that allow you to view and configure settings, choose skins, access online help, find version information, and exit the PMC.

You can change the PMC skin by choosing from one of the following skins as described in Table 5-1. The 4-channel, 6-channel, and 18-channel skins may be available in lighter and darker versions.

Table 5-1 Cisco IPICS PMC Skins

Skin Label	Skin Description
4-Channel Mode	This PMC client displays 4 channels that you control with your mouse. It includes the standard set of Cisco IPICS features.
6-Channel Mode	This PMC client displays 6 channels that you control with your mouse.

Table 5-1 Cisco IPICS PMC Skins (continued)

Skin Label	Skin Description
4-Channel Touch Screen Mode	This PMC client displays 4 channels in a low resolution touch screen format. It includes the standard set of Cisco IPICS features. (For information about using the touch screen low resolution skins, see the "Configuring the PMC Skins" section on page 5-2.)
8-Channel Touch Screen Mode	This PMC client displays 8 channels in a low resolution touch screen format. It includes the standard set of Cisco IPICS features. (For information about using the touch screen low resolution skins, see the "Configuring the PMC Skins" section on page 5-2.)
18-Channel Advanced Console	This PMC console displays 18 channels that you control with your mouse. It includes the advanced set of Cisco IPICS features. See Figure 1-1 on page 1-8 for an illustration of the 18-channel advanced console.

The PMC modifies the PTT behavior on the touch screen skins. For more information, see the "Touch Screen Skin Caveats" section on page 4-18.

Caution If you change the PMC skins while you are actively using the PMC, you may experience degraded audio quality and/or a temporary halt in your transmission.

Note When you configure your PMC to use one of the supported skins, you may need to adjust your desktop display screen area resolution to view all of the channels. (The Cisco IPICS minimum supported screen size is 1024x768.) To adjust your screen area resolution, right-click on your desktop and then click **Properties**. Or, navigate to **Start > Settings > Control Panel > Display > Settings**. The Display Properties dialog box displays. Use the slide bar to increase the screen area (for Windows 2000 machines) or the screen resolution (for Windows XP machines). If you cannot increase your screen area resolution to view the entire skin, choose another skin from the **Settings > Skin** menu.

To display the Settings menu, take one of the following actions:

- Click the **Menu** button that is located next to the All Talk button on the 18-channel PMC skin.
- Or, right-click in the PMC interface and then click **Settings**.

To access the skin configuration in the PMC Settings menu, perform the following procedure:

Procedure

Step 1 Position your cursor over the PMC GUI that displays on your desktop.

Step 2 Click the **Menu** button or right-click in the PMC interface; then, click **Settings**.

The Status, Skin, Channels, and Advanced tabs appear in the PMC GUI.

Step 3 To view the various skin options, click the **Skin** tab.

The Skin menu displays the available PMC skins.

Step 4 To change the skin, choose a different skin from that which you have currently configured.

Step 5 Click **OK**.

The PMC skin changes to reflect the new setting.

If you reconfigure your PMC skin and your association to channels and VTGs is greater than what has been specified, you may encounter a skin mismatch condition. For more information about skin mismatch conditions, see the "Skin Caveats" section on page 5-4.

Skin Caveats

Note For information about channel modifications that pertain to the touch screen skin, see the "Touch Screen Skin Caveats" section on page 4-18.

The following caveats pertain to the PMC skins:

- When you upgrade the PMC from one version to the next, the PMC provides support for only the most current version of the skins, as displayed in the **Settings > Skin** menu. However, the PMC does not remove the obsolete skins from the Skins directory that resides on the PMC client machine hard drive.
- If you change the PMC skin and use a different number of channels than that which has been configured in the Cisco IPICS server, you may encounter a mismatch condition.
- When you have a mismatch condition and the server tries to download more channels than the PMC can display, the PMC processes only the channels that it can support and ignores the rest.

  For example, if you configure the 4-channel skin on the PMC and the Cisco IPICS server tries to download eight channels based on the assignment by the dispatcher, the PMC enables visibility only of the first four channels; you can reorder the remainder of the channels so that they appear on the skin, if needed. For more information about reordering your channels, see the "Configuring the Channels Menu Options" section on page 5-8.

  If the PMC displays more than four channels and you attempt to change to the 4-channel skin, the PMC performs the following actions to warn you about the mismatch:

  - If channel 5, 6, 7, or 8 is configured and active (currently on a call), the PMC displays a pop-up message to warn you that switching to the 4-channel skin would hide active channels. The PMC does not allow this change to occur.
  - If channel 5, 6, 7, or 8 is configured but not active, the PMC displays a pop-up message to warn you that switching to the 4-channel skin will hide the configured channels and requests your input to proceed.
- If you attempt to switch from an 8-channel skin to a 4-channel skin when five or more channels are assigned, a dialog box displays to inform you and ask if you want to switch to a skin that displays fewer channels.
  - If you click **Yes** to proceed with the change, the PMC allows the skin change to occur.
  - If you click **No**, the PMC does not allow the skin change to occur.
- If the server tries to assign more than the maximum number of supported channels, a pop-up message displays to inform you.
- To support urgent communications when skin mismatches occur, Cisco IPICS provides the following functionality:

- If an emergency situation exists and the PMC does not have sufficient channels configured, the dispatcher may be able to alert the PMC user through the always open policy channel if this channel was defined. (This multicast channel may be the first channel that the dispatcher pushes to each PMC user so that all users can listen in on this channel.)
- The dispatcher can also assign a channel to the PMC user on an ad hoc basis and initiate communications in that manner.

See the "Implementing Policies" section on page 3-10 for more information about policies.

Using the Status Menu

The Status menu provides information about your PMC and its connectivity to the server. This menu also includes buttons that allow you to easily connect to the server to access and change your user information or download the PMC.

You can access the Status menu by navigating to **Settings > Status** in the PMC application.

To access the Status menu in the PMC Settings menu, perform the following procedure:

Procedure

Step 1 Position your cursor over the PMC GUI that displays on your desktop.

Step 2 Click the **Menu** button that displays on the PMC or right-click in the PMC interface and then click **Settings**.

The Status, Skin, Channels, and Advanced tabs appear in the PMC GUI.

Step 3 To view the Status menu, click the **Status** tab.

The Status menu displays the following fields:

Table 5-2 Status Menu Fields

Field	Description
Product Name	This field displays the name of the product, Cisco IPICS PMC.
Version	This field specifies the version of the PMC that you are using.
Cisco IPICS Server Address	This field displays the IP address of the server that your PMC is connected to.
Server Status and Connectivity Indicator	This field specifies your connectivity status with the server. • When your PMC is connected to the server, this field displays a green connectivity indicator along with the word "Connected." • When your PMC is not connected to the server, this field displays a red connectivity indicator and an alert icon, along with the word "Disconnected." **Note** The PMC updates its connectivity status dynamically based on the status of its connectivity with the server.
Access the Server via Web	Click this button to use your browser to connect to the Cisco IPICS server and access your profile information or download the PMC. **Note** For information about browsers that are supported for use with Cisco IPICS, see the "Browser Support" section on page 1-12.
User	This field specifies the user ID that you entered when you logged in to the PMC. For more information, see the "PMC Login Procedure" section on page 4-8.
Location	This field specifies the location that you selected as part of your login to the PMC. For more information, see the "PMC Login Procedure" section on page 4-8.

Configuring the Channels and Advanced Settings

You can personalize your PMC by changing the settings that appear under the Channels and Advanced tabs.

This section includes information about each of these menus:

- Configuring the Channels Menu Options, page 5-8
- Configuring the Advanced Menu Options, page 5-14

Configuring the Channels Menu Options

You can access the Channels menu by navigating to **Settings > Channels** in the PMC application. The Channels menu provides the option for you to configure certain settings, such as spatial positioning, key mapping, and channel reordering.

To access the Channels menu in the PMC Settings menu, perform the following procedure:

Procedure

Step 1 Position your cursor over the PMC GUI that displays on your desktop.

Step 2 Click the **Menu** button or right-click in the PMC interface; then, click **Settings**.

The Status, Skin, Channels, and Advanced tabs appear in the PMC GUI.

Step 3 To view the Channels menu, click the **Channels** tab.

The Channels menu displays information about the channels that have been assigned to you, along with the following channel properties, as shown in Table 5-3 on page 5-9:

Table 5-3 Channels Menu Fields

Field	Description
Channel Label	The channel label that displays corresponds to the channel that you select in the top window pane. The PMC also displays any key mapping assignments that you have defined for each channel. From this menu, you can also rearrange the appearance of your channels by using the Move Down and Move Up buttons. To rearrange or reorder the appearance of the channels on your PMC, follow these steps: 1. Click to select and highlight the channel that you want to reposition. 2. Click the **Move Up** button to move the channel position up on the PMC, or click the **Move Down** button to move the channel position down on the PMC. The Position field specifies the position of the channel on the PMC. **Note** Make sure that you do not move an active channel beyond the last available channel position in the skin that you are using. If you move a channel beyond the last position, the PMC can no longer display the channel. Alternatively, you can use this feature to move channels that you do not use beyond the boundaries of the skin. 3. Repeat these steps for each channel that you want to move. 4. To save your changes, click **Apply**; then click **OK**. **Note** The PMC does not save your channel ordering on a per-skin basis. That is, if you change skins, you may need to reorder your channels again, as needed.
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.

Table 5-3 Channels Menu Fields (continued)

Field	Description
Connection Type	This option specifies the type of connection that Cisco IPICS uses for the associated channel. If your connection type specifies SIP, the following fields display: • Local Chan ID—This field specifies a unique channel identifier for the type of channel that you are using for your connection. For example, the Local Chan ID for a channel displays as “chan<uid>” where uid represents the unique identifier for that channel; for a VTG, the Local Chan ID displays as “vtg<uid>” where the uid is the unique identifier for that VTG. • Dialed Number—This number specifies the number that your PMC dials to connect on the corresponding channel. • SIP Proxy—This IP address specifies the preconfigured address and port of the SIP proxy that Cisco IPICS uses for this connection. (The PMC uses this IP address to connect to the RMS component to enable SIP-based remote connections.) If your connection type specifies multicast, the following fields display: • Recv Addr—This IP address specifies the multicast address and port that has been configured for your PMC to receive traffic. • Send Addr—This IP address specifies the multicast address and port that has been configured for your PMC to send traffic.
Preferred Codec	This field specifies the preferred codec that the PMC uses for the corresponding channel. • If your connect type specifies SIP, the Preferred Codec field displays. • If your connection type specifies multicast, the Preferred Codec RX and Preferred Codec TX fields display to signify the receive and transmit channels.

Table 5-3 Channels Menu Fields (continued)

Field	Description
RX Mute During PTT	This option specifies the transmission duplex settings for all channels or only one channel; it controls the audio from the active channels while you are transmitting. (This attribute is defined in the server but it may be overridden on the PMC.) From the drop-down list box, choose one of the following options: • **None**—When you choose this option, you are able to hear audio while the PTT channel is depressed because the PMC does not mute any of the received traffic. • **This channel only**—When you choose this option, you will not be able to hear audio on the selected channel while the PTT channel is depressed. This option, as the default value, simulates the behavior of a true PTT device. • **All channels**—When you choose this option, you will not be able to hear audio on any of the active channels while the PTT channel(s) are depressed.
Use VAD	This option enables voice activity detection (VAD). When you enable VAD, the PMC only sends voice traffic when it detects your voice. (Although this attribute is defined in the server and it may be overridden on the PMC, Cisco recommends that you do not change the default setting.) **Note** VAD is disabled by default. You should not edit this field unless you are instructed to do so by your system administrator or Cisco support personnel as part of your troubleshooting efforts.

Table 5-3 Channels Menu Fields (continued)

Field	Description
Key Mapping	This option allows you to assign specific keys to each of your channels and provides transmit functionality when you press and hold the assigned key.To use this feature, highlight a channel to select it; then, from the drop-down list box, choose one of the available letters. • You can choose letters that range from e to z. To save your changes, click **Apply**; then, **OK**. • You can create new key map assignments or change current mappings by choosing another letter for the channel. • The keys that are currently mapped to channels display in the table next to the channel names. • When you map new channels, you can choose from the letters that have not already been assigned. • If you want to map a key that has already been assigned to another channel, you must first unmap the key before you can reassign it. To unmap the key, highlight the channel to select it; then, from the drop-down list box, choose **None**. • The PMC does not allow you to map the same key to more than one channel at a time. The PMC displays the key map on each channel that you configured. When you want to transmit on that channel, you can press and hold the assigned key instead of using your mouse. This feature also provides support for devices that simulate key down and key up events, such as a footswitch or other USB device. Refer to the product documentation that you received with your USB device for details about how to configure your USB device to generate the proper key sequence. **Note** Be aware that the key mapping that you configure applies only to the PMC client machine that you logged in to. If you use another PMC client machine, you must reconfigure your key mapping assignments.

Table 5-3 Channels Menu Fields (continued)

Field	Description
Optimize for low bandwidth	This option allows you to optimize your audio quality, on a per-channel basis, when you are connected via a low bandwidth and/or high latency (high delay) link, such as when you use a satellite connection. To use this feature, follow these steps: 1. From the channel list that displays at the top of this menu, click to select and highlight a low bandwidth channel. 2. Check the **Optimize for low bandwidth** check box to enable this feature on the selected channel. 3. Repeat these steps for all channels that require optimization. By using this feature, you should notice an improvement in voice quality when you use a low bandwidth and/or high latency channel. In some cases, you may experience delay that ranges from 200 ms to 2 seconds on the incoming audio from other Cisco IPICS users. **Note** Upon the first PMC login, an error message displays to inform you that the channels are being disabled. This error occurs because of the time delay to connect. To recover from this error, click **OK**. After the server completes its tasks, the channels display on the PMC (this timing varies based on latency). For more information about using the PMC over a low bandwidth and/or high latency link, refer to the *Solution Reference Network Design (SRND) for Cisco IPICS Release 2.0(1)*. If you are not sure whether you should enable this option, contact your system administrator for assistance. **Note** When you enable this feature, the PMC does not upload any logs to the server. For information about troubleshooting this type of connection, see the "Troubleshooting PMC Connectivity Issues with a High Latency, Low Bandwidth Link" section on page 8-22.

Step 4 To save your changes, click **OK**.

Configuring the Advanced Menu Options

You can access the Advanced menu by navigating to **Settings > Advanced** in the PMC application. The Advanced menu provides the option for you to modify certain settings, such as the All Talk key mapping and VPN settings.

To access the Advanced menu in the PMC Settings menu, perform the following procedure:

Procedure

Step 1 Position your cursor over the PMC GUI that displays on your desktop.

Step 2 Click the **Menu** button or right-click in the PMC interface; then, click **Settings**.

The Status, Skin, Channels, and Advanced tabs appear in the PMC GUI.

Step 3 To view the Advanced menu, click the **Advanced** tab.

The Advanced menu displays the following fields:

Table 5-4 Advanced Menu Fields

Field	Description
All Talk Key Mapping	Choose one of the following options to configure key mapping for the All Talk channel: • **None**—Choose this option if you do not want to map any key to the All Talk channel. • **Space**—This option, as the default value, specifies that the space bar maps to the All Talk channel. • **Tab**—Choose this option to map the tab key to the All Talk channel.

Table 5-4 Advanced Menu Fields (continued)

Field	Description
VPN Settings	Choose one of the following options to configure your VPN settings, if necessary: • **Use Default IP Address**—Click this radio button to use the default IP address that the PMC has configured. Cisco IPICS specifies this option as the default. At startup, the PMC attempts to determine the best IP address to use for connection to the server; that is, the default IP address. Under most conditions, this default IP address requires no reconfiguration. • **Use VPN Address**—Click this radio button to override the default IP address option and to specify a VPN address that the PMC should use for connectivity to the Cisco IPICS server; then, enter your IP address. Contact your system administrator if you are not sure about whether you need to choose the Use VPN Address option for your connection.

Step 4 To save your changes, click **OK**.

Using the Optional Settings Menu

The optional settings menu provides access to additional submenus, such as the PMC log files. This section describes how to access and use the optional settings submenus.

Caution You should only use these optional settings to aid troubleshooting and debugging efforts as directed by your system administrator or Cisco support personnel. To ensure system integrity, make sure that you contact your system administrator before you use any of these optional settings submenus.

To access the PMC optional settings, perform the following procedure:

Procedure

Step 1 Position your cursor so that it is over the PMC GUI that displays on your desktop.

Step 2 Hold down the left **Shift** key and right-click in the PMC interface.

The following submenu items display:

- Settings—Click **Settings** to see the Settings menu.
- Logs—Click **Logs** to access the log submenus.

  From here, you can manually turn on and turn off logging, as well as set the debug log levels.

Note Be aware that logging for these log files should only be turned on when you need help in isolating and resolving problems with the PMC and as directed by your system administrator or Cisco support personnel. To ensure system integrity, be sure to contact your system administrator before you use any of the available logs.

See "Identifying the PMC Logs" section on page 7-1 for more information about using the PMC log files.

- Help—Click **Help** to display online help information for the PMC.
- About—Click **About** to display version information for the PMC.

Note Alternatively, you can access the **Settings > Status** menu to see version information for the PMC. For more information, see the "Using the Status Menu" section on page 5-6.

- Exit—Click **Exit** to close the PMC application.

Step 3 Click the submenu that you need to access.

Note If you are configuring changes to the PMC settings when the PMC retrieves an update from the server, the server may overwrite your changes and redisplay the channel information. If this situation occurs, you may need to reenter any changes that you want to make.

Related Topics

- Identifying the PMC Logs, page 7-1
- Channel Support, page 3-11
- Implementing Policies, page 3-10
- Dynamic Configuration, page 4-14

Where to Find More Information

- *Cisco IPICS Server Administration Guide*

Recovering the PMC Application

This chapter provides information about recovering the PMC application under specific circumstances.

This chapter includes the following sections:

- Support for Cisco IPICS Recovery, page 6-1
- Recovering the PMC, page 6-3
- PMC Recovery Scenarios, page 6-4
- PMC Application Recovery, page 6-9

Support for Cisco IPICS Recovery

This release of Cisco IPICS allows the connection of a PMC to only one Cisco IPICS server at a time. The PMC GUI displays a server status connectivity indicator. When you click this indicator, the Status menu opens and displays the IP address of your Cisco IPICS server. For more information about the Status menu, see the "Using the Status Menu" section on page 5-6.

Cisco IPICS provides support for connection to an alternate server if your primary server goes offline. When the primary server becomes inaccessible, you may enter the IP address or host name of an alternate server or choose an alternate server from the drop-down list box in the PMC login dialog box.

Note Be aware that when you connect to an alternate server, it is logically the same as your primary server. That is, you receive the same list of channels as if you connected to your primary server.

To choose an alternate server when your primary server is not available, perform the following procedure:

Procedure:

Step 1 Enter your alternate **server IP address** or **server host name** (or choose your alternate server IP address from the drop-down list box)

Step 2 Enter your **user name** and **password**

Step 3 Click **OK**

The last server IP address that you successfully connected to becomes your default server when you next launch the PMC.

Note The PMC displays its connectivity status with the server. If connectivity with the server is lost, a red indicator and an alert icon displays to make you aware of the loss of connectivity. When you click this indicator, the Status menu opens and displays the IP address of your Cisco IPICS server. For more information about this connectivity indicator, see the "Using the Status Menu" section on page 5-6.

When SIP-based remote connections fail, the PMC displays a visual indicator in the form of a yellow triangle next to the channel. For more information, see the "Identifying Channel Activation Issues" section on page 8-23.

If a system failure occurs and the PMC application cannot connect to the Cisco IPICS server, the PMC may continue to operate in offline mode, which is a disconnected state. A failure may be the result of a network failure, a hardware failure, or extreme latency.

Note When the PMC becomes disconnected from the Cisco IPICS server, it continues to operate in its existing state; that is, the PMC can continue with its existing voice channels but it cannot connect to additional, new channels until it reconnects to the server.

After the system recovers and resumes normal operations, the PMC automatically attempts to reconnect to the Cisco IPICS server. The Cisco IPICS server enables recovery of the PMC application by retaining the necessary PMC-related configuration and session information, and by doing so, it provides an efficient recovery mechanism for the PMC.

For more information, see the"Server-PMC Login Sequence Interaction" section on page 4-6 and the "System Recovery Caveats" section on page 6-4.

Related Topics:

- Server-PMC Login Sequence Interaction, page 4-6
- System Recovery Caveats, page 6-4

Recovering the PMC

This section provides information about recovering the PMC application after a system failure occurs. It also provides information about recovery caveats and includes the following topics:

- Transparent Recovery Mechanism, page 6-3
- System Recovery Caveats, page 6-4

Transparent Recovery Mechanism

The Cisco IPICS server provides a transparent recovery mechanism for the PMC end-user by maintaining in its database any PMC-specific session information that the server needs to communicate with the PMC.

The Cisco IPICS PMC login process requires that the PMC end-user log in to the PMC application, which in turn logs in to the Cisco IPICS server. If you attempt to log in to the PMC application and the PMC cannot communicate with the

server, you receive notification that the login to the server has failed. When this failure occurs, the PMC automatically enters offline mode so that you can log in to the PMC locally.

Tip You can only login to the PMC locally if you have already successfully logged in to the Cisco IPICS server once before. For more information, see the "Logging In to the PMC Application" section on page 4-1.

By allowing local login to the PMC application, Cisco IPICS ensures uninterrupted communications by providing the ability for the PMC to continue to operate in its existing state even when the server becomes unreachable.

After you log in to the PMC, the PMC automatically attempts to reconnect to the Cisco IPICS server.

System Recovery Caveats

When a system failure occurs, the PMC maintains functionality by allowing you to continue participation in existing VTGs, even if the PMC cannot connect to the Cisco IPICS server. However, you cannot connect to new, additional VTGs until the system recovers.

When the server recovers from a communications failure and resumes normal operations, the server automatically refreshes the channels that are running on the PMC.

Related Topics:

- Logging In to the PMC Application, page 4-1
- Dynamic Configuration, page 4-14

PMC Recovery Scenarios

The following information describes how the PMC recovers in certain scenarios:

- Cisco IPICS Server is Unavailable, page 6-5
- Cisco IPICS Server and PMC are Up/Communications are Down, page 6-8

- Cisco IPICS Server and PMC are Up/Network is Down, page 6-8

Cisco IPICS Server is Unavailable

If Cisco IPICS server fails, either at startup or during the middle of an operation, the PMC displays a message to inform you that connectivity has been lost. The PMC continues to operate in its existing state, and polls the server during this time, but the system does not allow changes to channels or configurations to be made while the server is down.

Note Cisco IPICS does not prevent you from logging in to the PMC application if the connection to the server goes offline.

This section includes information about the following scenarios:

- Cisco IPICS Server is Down/RMS and PMC are Up, page 6-5
- Cisco IPICS Server and RMS are Down/PMC is Up, page 6-6
- Cisco IPICS Server Resumes Operation, page 6-7

Cisco IPICS Server is Down/RMS and PMC are Up

If Cisco IPICS server fails, either at startup or during the middle of an operation, the PMC displays a message, along with a server status connectivity indicator on the PMC, to inform you that connectivity has been lost. The PMC continues to operate in its existing state but no changes to channels or configuration parameters can be made while the server is down. (The PMC continues to poll the server during this time.)

In the following scenarios, the server becomes inaccessible but the PMC maintains communications with the RMS (except where noted):

- The server is offline when the PMC starts up

  Because the PMC stores the user and configuration data on the local machine, Cisco IPICS uses this information to enable PMC communications when the server is unavailable.

  - In this situation, the PMC clients who are in the same location can continue to use the multicast connection information that was previously configured.
  - SIP users may continue to use the SIP connection information unless the PMC successfully logged out of Cisco IPICS. (Upon successful logout, Cisco IPICS reclaims the resources and invalidates the SIP connections.)

  When the PMC starts up, the server allocates the necessary RMS resources for all assigned channels, whether or not the channels are activated or visible on the PMC. This functionality enables the PMC to communicate by using data that has been configured.

Note The exception exists when RMS modifications, which are unknown to the PMC, occur. In this situation, RMS availability becomes unpredictable.

- The server goes offline after successful user login

  When this situation occurs, the PMC displays a message to notify the user that communications with the server have been interrupted. By using the stored configuration, the PMC sets up its SIP and multicast connections. All channels again become operable unless the RMS is modified by server or RMS activity.

- The server is online but the PMC has lost connectivity to the server

  The PMC displays a message to notify the user that communications with the server have been interrupted. The PMC uses the last known configuration to set up its SIP and multicast connections, but in this situation, some of the SIP connections may not be accurate if the server had modified the RMS during the time when the PMC lost connectivity.

Cisco IPICS Server and RMS are Down/PMC is Up

When both the server and RMS become unavailable, the following scenarios may occur:

- The PMC cannot connect to either the server or the RMS at PMC startup

  In this situation, the PMC user can log in to the PMC by using the stored information. When the PMC tries to set up a SIP connection, it detects the loss of connectivity to the RMS.

  - If the PMC had not previously logged out, all SIP connections and VTGs that are stored in the last known configuration may appear to be available on the PMC (but they are really unavailable).
  - Upon successful logout, Cisco IPICS marks all SIP resources as unavailable and displays the channels as disabled on the PMC.
  - When the PMC user tries to activate a SIP resource that it not in service, a busy tone is heard.
  - Multicast connections that are stored in the configuration remain operable for the same location.

Note Be aware that the location information is also stored in the last known configuration. Therefore, if the PMC user logs in to a different location while both the server and the RMS are offline, the multicast connection may no longer be operable.

- The PMC loses connectivity to both the server and the RMS while the PMC is operational
  - When the PMC detects that it has lost connectivity with the RMS, Cisco IPICS marks all SIP connections on the RMS as disabled.
  - Multicast connections remain operable if the PMC user location does not change, as described above.

Cisco IPICS Server Resumes Operation

When the Cisco IPICS server resumes normal operations, the following activities occur:

1. When the server recovers from a failure, it returns to its last known state and resumes normal operations. The server initializes the PMC sessions and commands by using the information that it has stored in the database.
2. After connectivity is reestablished between the server and the PMC, new sessions may be created on the server. The server checks for concurrent license usage, and if the number of concurrent users exceeds the maximum, the system displays a warning message. For more information about license requirements, see the "License Information" section on page 4-6.

3. The PMC login state is recovered from the server database when the server restarts. If the PMC session had been in an inactive state during the communications interruption, the system may prompt you to log in to the PMC again.

Note Cisco IPICS does not prevent you from logging in to the PMC application if the connection to the server goes offline.

Cisco IPICS Server and PMC are Up/Communications are Down

In this scenario, the Cisco IPICS server is operational but the communications between the server and the PMC are down. The PMC retains the ability to login locally and it continues to operate in its existing state and poll the server.

When communications resume, the server manages the licensing and sessions as shown below:

1. After communications resume, the Cisco IPICS server checks the licenses for the PMC that had been locally logged in.
2. The PMC sessions that were inactive with the server become active and communications with those sessions proceed as normal.
3. If the PMC session became inactive, the Cisco IPICS server may prompt you to log in to the PMC application again.

Cisco IPICS Server and PMC are Up/Network is Down

When the network fails and communications go offline, you can still log in to the PMC application by using the local login process. When normal operations resume, the same process, as described in the "Cisco IPICS Server and PMC are Up/Communications are Down" section on page 6-8, occurs.

For more information about logging in to the PMC application, see the "Logging In to the PMC Application" section on page 4-1.

Related Topics:

- Logging In to the PMC Application, page 4-1
- License Information, page 4-6

PMC Application Recovery

The Cisco IPICS server provides the basic PMC configuration, skin, and XML definitions.

If Cisco IPICS cannot locate your chosen PMC skin, or if your skin has been misconfigured, a message displays to prompt you to check the configuration and the Skin directory to make sure that it has not been deleted.

If, at startup, Cisco IPICS detects that your PMC skin has been corrupted, the system prompts you with a skin selection dialog box so that you can choose a PMC skin to use.

If you encounter a configuration, skin, or XML loss, you can quickly recover from these failures by uninstalling and reinstalling the PMC application on your client machine or by choosing another compatible version to run at login.

For information about uninstalling the PMC application, see the "Uninstalling the PMC Application" section on page 2-28.

For information about installing the PMC application, see the "Installing the PMC Application" section on page 2-2.

For information about choosing a compatible version to run at login, see the "Launching the PMC Application" section on page 2-14, and the "Managing PMC Version Numbers" section on page 2-18.

Related Topics

- Installing the PMC Application, page 2-2
- Launching the PMC Application, page 2-14
- Managing PMC Version Numbers, page 2-18
- Reverting to a Previous Version of the PMC Application, page 2-27
- Uninstalling the PMC Application, page 2-28
- Logging In to the PMC Application, page 4-1

Where to Find More Information

- *Cisco IPICS Server Administration Guide*

Using the PMC Application Logs

This chapter provides information about how to use the PMC application logs. It includes information about turning on and turning off logging for each of the individual log files and setting up levels for the debug log.

This chapter includes the following topics:

- Identifying the PMC Logs, page 7-1
- Accessing the PMC Logs, page 7-3
- Using the PMC Logs, page 7-5

Identifying the PMC Logs

This section identifies the PMC log files and describes how to access the Logs submenu items. It contains the following topics:

- Maintaining the PMC Log Files, page 7-1
- Accessing the Logs Submenu Items, page 7-2

Maintaining the PMC Log Files

The PMC maintains the following log files, plus the debug log, to help aid your troubleshooting efforts:

- Authentication.log
- ChannelActivity.log

- ChannelStatistics.log
- UserInterface.log
- DebugLog.txt

Caution Logging for these log files should only be turned on when you need help in isolating and resolving problems with the PMC and as directed by your system administrator or Cisco support personnel. To ensure system integrity, be sure to contact your system administrator before you use any of these logs.

The Cisco IPICS system allows you to turn on or turn off logging for these individual PMC log files, as well as set the debug log levels, by using the PMC optional settings menu. Logging is turned off by default.

Accessing the Logs Submenu Items

You can access the PMC Logs submenu items by using the PMC optional settings menu.

To access the PMC optional settings menu, follow this procedure:

Procedure

Step 1 Position your cursor over the PMC window that appears on your desktop.

Step 2 Hold down the left **Shift** key and right-click the mouse anywhere inside the PMC window.

Step 3 Click **Logs**.

The list of Logs submenu items displays.

Step 4 Navigate to the log that you want to turn on or turn off the logging functionality.

For information about turning on and turning off logging, and accessing the individual log files, see the "Procedure" section on page 7-3.

See the "Using the PMC Logs" section on page 7-5 for a description of each of the PMC logs.

Accessing the PMC Logs

From the PMC Logs submenu, you can choose to turn on or turn off logging to the PMC log files that are shown, as well as set or clear the debug log.

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.

To turn on and turn off logging for the individual logs, and to set or clear the debug log, follow this procedure:

Procedure

Step 1 Access the PMC optional settings menu, as described in the "Using the Optional Settings Menu" section on page 5-15.

Step 2 Click **Logs** to access the logs submenu items.

Step 3 To turn on logging for a log file, click the specific log name.

A check mark appears next to the log name to indicate that the logging functionality has been turned on.

Note You can choose to turn on logging for all of the log files or only individual log files.

Step 4 To set the debug log, choose **Debug > Set All** from the Logs menu.

A check mark appears next to all of the options that are listed in the debug submenu to indicate that they have been set.

Note Cisco recommends that you only set the specific debug options that you need to use for your troubleshooting efforts; this approach helps to minimize the amount of hard disk space that the debug logs may consume. You can choose which debug options to set by clicking each individual option that you want to turn on; alternatively, these debug options may be set in the Cisco IPICS server. Be aware that some debug options may not be available until at least one PMC channel has been activated.

Step 5 To turn off logging for a log file, click the specific log name.

The check mark no longer appears next to the log name to indicate that logging has been turned off.

Step 6 To turn off the debug settings, choose **Debug > Clear All** from the Logs menu.

The check marks no longer appear next to the debug log options to indicate that the options have been cleared.

You can also choose to clear only certain debug options by clicking each individual option that you want to clear.

Step 7 To override the server log settings, click **Override Server Log Settings**.

A check mark appears next to this setting to indicate that the override option has been enabled. When you enable this option, the PMC ignores all server requests to modify your log and debug log settings.

To disable the override option, click **Override Server Log Settings** again to toggle it off; the check mark no longer appears next to the option to indicate that it has been turned off.

Note Cisco recommends that you only enable this override setting as directed by your system administrator or Cisco support personnel.

Tip Be aware that the system may reset your debug log settings after you perform installation activities (such as install, upgrade, or repair) on the PMC. Check your debug log settings to make sure that the options that you need are enabled. For more information about installing and upgrading the PMC, see Chapter 2, "Installing and Upgrading the PMC Application."

Note When the PMC writes to any of the log files (*.log or DebugLog.txt) and the recording files (*.raw in the User recording directory), the application checks to make sure that available disk space exists to capture this data. If the amount of free disk space falls below a predefined level, logging and recording activities stop and data that can no longer be written to the disk is lost. When the free disk space increases to sufficient levels, the PMC automatically resumes logging and recording activities.

Using the PMC Logs

The PMC application stores all of the log files, with the exception of the Authentication log, in the following directory on the PMC client machine:

C:\Program Files\Cisco Systems\Cisco IPICS\PMC\Users\<*username*>\Logs

where <*username*> is the user name of the PMC user who is currently logged in to the application.

The PMC application stores the Authentication.Log file in the following directory on the PMC client machine:

C:\Program Files\Cisco Systems\Cisco IPICS\PMC\Components\Logs

Note The ChannelActivity.log, ChannelStatistics.log, UserInterface.log, and DebugLog.txt files are all user-specific. The Authentication.log is not user-specific, but rather, contains information for all users based on the PMC installation. See the "PMC Log Descriptions" section on page 7-7 for additional information.

The PMC stores all of the log and debug files in the Logs folders to enable PMC serviceability when the PMC does not have a connection to the Cisco IPICS server.

This section includes the following topics:

- PMC Log File Caveats, page 7-6
- PMC Log Descriptions, page 7-7

PMC Log File Caveats

The following caveats pertain to the PMC log files:

- All of the logs, except for the debug log, are based on size; that is, the system creates a new log when the predefined limit has been reached.
- To use the logging functionality, Cisco IPICS requires sufficient free disk space on the PMC client machine; that is, when the PMC detects only 100 MB of free disk space, it displays a warning message to alert you and when the PMC detects 50 MB of free disk space, it stops logging data to the log files.
- The debug log (DebugLog.txt) file starts a fresh log each time you start the PMC; when this activity occurs, the system moves the information that was contained in DebugLog.txt to DebugLog_archive.txt.
- By default, the Cisco IPICS system retains one current active copy (DebugLog.txt) and one archive copy (DebugLog_archive.txt) of the debug log.
- By default, the Cisco IPICS system writes all error messages to the debug log
- The PMC specifies the number of logs and debug files to maintain per log file type.
- At predefined intervals, the Cisco IPICS server may retrieve the log files from the PMC. (The server may also request the PMC to upload any of the log files on demand.)
- The server may request that a log file be uploaded from the PMC whenever a new log file is created based on file size rollover.
- When you check the **Optimize for low bandwidth** check box in the PMC Channels menu, the PMC does not upload logs to the server in an effort to conserve bandwidth.

  - When that activity occurs, the system renames the uploaded log file to reflect an archive copy. For example, when the server requests a log file upload of the UserInterface.log file, the system renames the file to reflect UserInterface.1, which signifies the first archive copy.
  - Multiple log archives may be maintained to allow for multiple upload requests by the server.
  - All archive files are automatically deleted after they have been uploaded to the server.
  - If the server does not request log file upload on rollover, the system does not create these archive log files.
- All of the logs appear in Greenwich Mean Time (GMT).
- The DebugLog.txt appears in text format.
- The Authentication.log, ChannelActivity.log, ChannelStatistics.log, and UserInterface.log appear in XML format. The Cisco IPICS server parses them and turns them into syslog format; the server then sends the syslog messages to the router for collection.

PMC Log Descriptions

This section provides a description and a sample format for each of the PMC log files.

Note The PMC timestamps all log entries in GMT format, however, it does not synchronize its clock to any central source. Therefore, Cisco recommends that the PMC client machine and the Cisco IPICS server synchronize their clocks to a central source using Network Time Protocol (NTP) or another similar solution.

Table 7-1 describes each of the PMC log files.

Table 7-1 PMC Log File Descriptions

PMC Log File Name	PMC Log File Description
Authentication.log	This log file contains a history of all user login and logout attempts per PMC installation. This log appears in XML format.

Table 7-1 PMC Log File Descriptions (continued)

PMC Log File Name	PMC Log File Description
ChannelActivity.log	This log contains a history of channel activation and deactivation and the PTT status of each channel within the PMC. This log appears in XML format.
ChannelStatistics.log	At regular and predefined intervals, this log records the statistics for each channel, including data for both sent and received transmissions over the network. This log appears in XML format.
UserInterface.log	This log contains a history of the user interactions with the PMC application. This log appears in XML format.
DebugLog.txt	This log contains detailed debugging information that is relevant to how the PMC operates. Several different debug levels can be enabled. This log appears in text format; it is rotated each time that you execute the PMC application.

An example of the formatting and the type of information that is contained in each log file is shown below.

Authentication.log

```
<log-msg><time>Thu Jun 09 16:16:44
2005</time><facility>AUTH</facility><msg-id>SUCCESS</msg-id><args><arg
id="0">user1</arg></args></log-msg>
<log-msg><time>Thu Jun 09 18:52:34
2005</time><facility>AUTH</facility><msg-id>FAILURE</msg-id><args><arg
id="0">user2</arg></args></log-msg>
<log-msg><time>Thu Jun 09 18:52:37
2005</time><facility>AUTH</facility><msg-id>FAILURE</msg-id><args><arg
id="0">user1</arg></args></log-msg>
<log-msg><time>Thu Jun 09 18:52:38
2005</time><facility>AUTH</facility><msg-id>FAILURE</msg-id><args><arg
id="0">user1</arg></args></log-msg>
<log-msg><time>Thu Jun 09 18:52:40
2005</time><facility>AUTH</facility><msg-id>SUCCESS</msg-id><args><arg
id="0">user1</arg></args></log-msg>
```

ChannelActivity.log

```
<log-msg><time>Wed, 06 Apr 2005 17:33:41
GMT</time><facility>CHANNEL</facility><msg-id>Activate</msg-id><args><
arg id="0">LINE1</arg></args></log-msg>
<log-msg><time>Wed, 06 Apr 2005 17:34:28
GMT</time><facility>CHANNEL</facility><msg-id>Deactivate</msg-id><args
><arg id="0">LINE1</arg></args></log-msg>
```

ChannelStatistics.log

```
<log-msg><time>Wed, 06 Apr 2005 22:02:12
GMT</time><facility>STATS</facility><msg-id></msg-id><args><arg
id="0">Sent Packets</arg><arg id="1">0</arg><arg id="2">Sent
Bytes</arg><arg id="3">0</arg><arg id="4">Rcvd Packets</arg><arg
id="5">0</arg><arg id="6">Rcvd Bytes</arg><arg
id="7">0</arg></args></log-msg>

<log-msg><time>Wed, 06 Apr 2005 22:03:13
GMT</time><facility>STATS</facility><msg-id></msg-id><args><arg
id="0">Sent Packets</arg><arg id="1">0</arg><arg id="2">Sent
Bytes</arg><arg id="3">0</arg><arg id="4">Rcvd Packets</arg><arg
id="5">0</arg><arg id="6">Rcvd Bytes</arg><arg
id="7">0</arg></args></log-msg>
```

UserInterface.log

```
<log-msg><time>Thu, 07 Apr 2005 19:05:03
GMT</time><facility></facility><msg-id>LButtonDown</msg-id><args><arg
id="0">exit</arg><arg id="1">0000</arg></args></log-msg>

<log-msg><time>Thu, 07 Apr 2005 19:05:03
GMT</time><facility></facility><msg-id>LButtonUp</msg-id><args><arg
id="0">exit</arg><arg id="1">006c</arg></args></log-msg>
```

Note For detailed information about using PMC CLI command options, refer to the *Cisco IPICS PMC Command Line Interface* for your version of Cisco IPICS.

Related Topics

- Maintaining and Upgrading the PMC Application, page 2-16
- Using the Optional Settings Menu, page 5-15

Where to Find More Information

- *Cisco IPICS Server Administration Guide*
- *Cisco IPICS PMC Command Line Interface*

Troubleshooting Tips for the PMC Application

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

This chapter includes the following sections:

- Troubleshooting PMC Application Problems, page 8-1
- Analyzing PMC Error Conditions, page 8-28

Troubleshooting PMC Application Problems

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

- Resolving PMC Execution Issues, page 8-2
- Generating a PMC Installation Log File, page 8-3
- Using the PMC Installer with an Encrypted File System, page 8-5
- Making PMC Configuration File Changes, page 8-6
- Using the PMC Optional Settings, page 8-6
- Resolving Footswitch/USB Device Issues, page 8-7
- Configuring the Audio Settings, page 8-7
- Using Cisco Security Agent with the PMC, page 8-9
- PMC Coexistence with Other Voice Applications, page 8-10

- Troubleshooting One-Way Audio, page 8-10
- Troubleshooting Voice Quality Issues, page 8-14
- Resolving Unknown Publisher Errors with Windows XP SP2, page 8-14
- Troubleshooting PMC Connectivity Issues, page 8-15
- Resolving Name Resolution Failures, page 8-23
- Identifying Channel Activation Issues, page 8-23
- Resolving Codec Mismatch Issues, page 8-24
- Support for Right-to-Left and Double-Byte Languages, page 8-25
- PMC Application Caveats, page 8-28

Resolving PMC Execution Issues

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

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

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

Procedure

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

Step 2 Click **Task Manager**.

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

Step 3 Click the **Processes** tab.

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

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

Step 5 Click **PMC.exe** to highlight or right-click **PMC.exe**; then, click **End Process**.

A warning message displays to ask if you are sure that you want to terminate this process.

Step 6 Click **Yes**.

Step 7 Close Windows Task Manager by clicking the "**X**" in the upper right corner.

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

Generating a PMC Installation Log File

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

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

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

To generate the PMC installation log file, follow this procedure:

Procedure

Step 1 Create a **C:\temp** directory in Windows, if this directory does not already exist.

Step 2 Use Windows Explorer to navigate to the location where you saved the pmcsetup.exe file, as described in the "Downloading and Installing the PMC Application" section on page 2-4.

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

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

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

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

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

pmcsetup.exe -log

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

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

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

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

Using the PMC Installer with an Encrypted File System

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

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

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

Procedure

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

A command line window displays.

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

C:\ **echo %temp%**

The location of the TEMP folder displays.

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

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

C:\ **set TEMP=**<*new location*>

where:

<*new location*> specifies the new, nonencrypted folder for the %temp% environment variable.

The new location of the TEMP folder displays.

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

C:\ **set TMP=**<*new location*>

where:

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

Step 5 Rerun the PMC installation by entering the following command:

C:\ **run pmcsetup.exe**

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

For more information about the Encrypted File System, refer to the Microsoft support site at http://support.microsoft.com/

Making PMC Configuration File Changes

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

Using the PMC Optional Settings

The optional settings menu can aid your troubleshooting efforts by providing access to additional submenus that are not normally viewable or editable, such as the PMC log files. For example, you can manually turn on and turn off logging for individual PMC log files and you can also set debug levels.

These submenu items become available by using the PMC optional settings. See the "Using the Optional Settings Menu" section on page 5-15 for additional information and caveats about using the PMC optional settings.

Caution You should only use these optional settings to aid troubleshooting and debugging efforts in emergency situations, such as not being able to connect to the server, and as directed by your system administrator or Cisco support personnel. To ensure system integrity, make sure that you contact your system administrator before you use any of these optional settings submenus.

Resolving Footswitch/USB Device Issues

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

If you use a footswitch or similar USB device, and you encounter a situation where the All Talk channel button flickers between orange and yellow, you may not have properly configured the device.

Make sure that the device can generate key down events when you hold down the footswitch pedal followed by a key up event when you release the pedal (to simulate pressing and holding a key on a keyboard and then releasing it).

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

For more information about using a footswitch or other USB device, see the "Using Keyboard Mapping" section on page 4-21.

Configuring the Audio Settings

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

- Using a USB DSP Headset with the PMC, page 8-8
- Checking the Microphone with the PMC, page 8-8

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

Tip If you change your audio settings while you are running the PMC, you may need to restart the PMC for the changes to become effective.

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

For tips about how to ensure the best possible voice quality when you use the PMC, see the "Voice Quality Tips" section on page 2-12.

Using a USB DSP Headset with the PMC

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

If you launch the PMC after you plug the headset into your PMC client machine, the PMC does not automatically remember the audio setting for the USB DSP headset; instead, the PMC reverts to the Windows operating system's default audio settings. See the "Using a USB DSP Headset with the PMC" section on page 2-9 for more information about checking and reconfiguring the Windows audio settings for use with a USB DSP headset.

Note If you use the microphone on a USB headset for an extended period of time, your voice may become unintelligible. If this problem occurs, close the PMC and unplug the USB headset from the PMC client machine. Then, plug the USB headset back into the PMC client machine and restart the PMC.

Checking the Microphone with the PMC

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

- Make sure that you use a high-quality microphone with the PMC; otherwise, the Cisco IPICS system may not be able to accurately detect your voice and properly register transmit and/or receive traffic.
- If the Cisco IPICS system cannot detect your voice when you transmit, the system may squelch the transmission; in this situation, another Cisco IPICS user may start speaking over your transmission because your voice cannot be heard and the PMC receive indicator may not display any indication of the transmission.

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

See the "Configuring the Audio Settings" section on page 2-7, the "Using a USB DSP Headset with the PMC" section on page 2-9 and "Using the Microphone with the PMC" section on page 2-10 for detailed information about the audio setting configuration and sound recording capability.

Using Cisco Security Agent with the PMC

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

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

CSA may prompt you for permission in the following instances:

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

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

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

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

PMC Coexistence with Other Voice Applications

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

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

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

Troubleshooting One-Way Audio

You may encounter one-way audio issues (such as, you may be able to send audio but you may not be able to hear audio) under various situations when you use the PMC. The following topics provide information about how to resolve these one-way audio issues:

- Using CLI Commands to Resolve Audio and Headset Issues, page 8-11
- Resolving IP Address Changes, page 8-13

Note Be aware that multicast issues may also contribute to problems with one-way audio. For more information, see the "Troubleshooting Multicast Communications Issues" section on page 8-19.

Tip Check the network connectivity for your PMC client machine to make sure that you have a valid IP address and that you can connect to the network before you start using the PMC. If you use SIP-based remote connections, make sure that the PMC can establish connectivity to the RMS. (The PMC connects to the RMS by using the IP address of the Loopback0 interface that is assigned to the RMS.) For more information, see the "Resolving IP Address Changes" section on page 8-13.

Using CLI Commands to Resolve Audio and Headset Issues

You can verify and isolate audio issues that you may experience by using CLI command options on the PMC. This section describes the CLI commands that you can use to help resolve audio issues.

Using CLI Commands to Resolve Headset Issues

If you encounter a situation where you cannot hear audio on the PMC, the problem may be due to the headset that you are using. You can verify and isolate one-way audio problems by using CLI command options on the PMC.

Be aware of the following caveats when you use CLI commands:

- Make sure that the PMC to which you are issuing the command is running; the command has no effect if the PMC is not running.
- Issue the command from the Windows command line on the PMC client machine; the command affects only that PMC.

To enter a CLI command on the PMC, follow this procedure:

Procedure

Step 1 On the PMC that has encountered the problem, open the Windows command line by following these steps:

a. Choose **Start > Run**.

The Windows dialog box displays.

b. Enter **cmd** in the Open field.

c. Press **Enter** or click **OK**.

The Windows command line window displays.

Step 2 In the Windows command line window, change the current directory to the folder in which the PMC is installed.

The following example shows the directory structure in which the PMC folder may appear:

C:\Program Files\Cisco Systems\Cisco IPICS\PMC

Step 3 Enter the desired CLI command and press **Enter**.

For a description of each CLI command, refer to Chapter 2, "Command Line Interface Commands" in the *Cisco IPICS Command Line Interface*.

Using the CLI Play Command to Resolve One-Way Audio Issues

To verify that the one-way audio problem is not a PMC application issue, you can enter the CLI **play** command from the Windows command line of the PMC.

The play command outputs a wave audio file to the specified PTT channel. This command latches the PMC PTT button, plays the designated wave file, and then unlatches the PTT button. The syntax of the play command appears below:

PMC.EXE -Play *file* [**-line #**]

- The *file* argument specifies the path and file name of the wave file to play.
- The **-line #** option, where # is a number between 1 and 18, specifies the PTT channel line to which this command applies. (If you omit this option, the command applies to channel 1.)

The following command shows an example of the play command:

PMC.EXE -Play C:\aud1.wav -line 2

In this example, this command plays the aud1.wav file to PTT channel 2.

When you successfully execute this command, you can hear audio from one PMC to another PMC and eliminate the PMC as the source of the one-way audio problem. When this situation occurs, the problem can be isolated to a faulty headset. In that case, replace the headset and try again.

Note For detailed information about using PMC CLI command options, refer to the *Cisco IPICS Command Line Interface*.

Resolving IP Address Changes

The following section provides information about resolving IP address changes on the PMC client machine; it includes the following topics:

- Changing IP Addresses on the PMC Client Machine, page 8-13
- IP Address Change Notifications, page 8-13

Changing IP Addresses on the PMC Client Machine

If you change the IP address on your PMC client machine (for example, when switching from a wired to a wireless network), and the PMC is open, you may encounter one-way audio on the PMC. To resolve this issue, close and then restart the PMC.

If you change the IP address on your PMC client machine when the PMC is not open, the PMC should not be affected by the change. You should always establish network connectivity to make sure that you have a valid IP address before you open the PMC.

IP Address Change Notifications

Under normal conditions, the PMC chooses the first network connection that allows it to communicate with the server. If that network connection becomes unusable, the PMC chooses another network connection for its communications.

Cisco IPICS provides notification to the PMC user when the PMC changes the source IP address that it uses for communications with the server. However, on PMC client machines that include more than one network connection, the PMC may not provide this notification. In these instances, there is no impact to functionality; Cisco IPICS continues to operate normally when notification of the IP address change is not sent to the user.

Troubleshooting Voice Quality Issues

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

For detailed information about voice quality problems and symptoms, refer to the Recognizing and Categorizing Symptoms of Voice Quality Problems documentation, which can be found at the following URL: http://www.cisco.com/en/US/tech/tk652/tk698/technologies_white_paper09186a00801545e4.shtml.

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

This document also includes a link to the TAC Case Collection Tool, which provides solutions by interactively identifying and troubleshooting common technology or product problems.

You can access the TAC Case Collection Tool at the following URL: http://www.cisco.com/en/US/customer/support/tsd_tac_case_collection.html

Resolving Unknown Publisher Errors with Windows XP SP2

As part of the browsing security enhancements that were implemented in Microsoft Windows XP Service Pack 2 (SP2), you may encounter an "Unknown Publisher" error when you use the Internet Explorer (IE) browser to download the PMC from the Cisco IPICS server.

This problem may occur when you try to run an executable file or an add-in program that contains an invalid signature and that you downloaded by using the IE version that is installed with Windows XP (SP2).

To resolve this issue, Microsoft recommends that you unblock the publisher and then try to save or run the file that you downloaded. Alternatively, you can modify the security settings on your PMC client machine, although this workaround is not recommended.

For detailed information about how to resolve this issue, refer to the Microsoft support site at http://support.microsoft.com/ and search for Article ID 843022.

Troubleshooting PMC Connectivity Issues

The following topics provide information about troubleshooting PMC connectivity issues:

- Troubleshooting VPN Connectivity, page 8-15
- Using the PMC with the Windows XP Firewall, page 8-18
- Troubleshooting Multicast Communications Issues, page 8-19
- Troubleshooting Winsock Corruption Issues, page 8-20
- Troubleshooting Offline Mode Issues, page 8-21
- Troubleshooting PMC Connectivity Issues with the RMS, page 8-21
- Troubleshooting PMC Connectivity Issues with a High Latency, Low Bandwidth Link, page 8-22

Troubleshooting VPN Connectivity

If the Cisco Systems VPN Client is installed on your PMC client machine, you must ensure that the settings for the integrated stateful firewall feature are correctly set to enable PMC remote connectivity. This section includes the following topics to describe the Cisco Systems VPN Client and how to ensure it is correctly set on the PMC client machine:

- About the VPN Client Stateful Firewall, page 8-16
- Enabling and Disabling the Stateful Firewall on the PMC Client Machine, page 8-16

Be aware of the following caveats that apply to specific versions of the Cisco Systems VPN Client.

Cisco Systems VPN Client Version Interoperability Caveats

When you use the Cisco Systems VPN Client version 3.6.3(x) with the PMC, the PMC may not be able to detect the IP address and route change after you establish or disconnect a VPN tunnel. This problem occurs when the Cisco Systems VPN Client does not communicate the IP address and route change information to the operating system. When this problem occurs, the channels on the PMC may not be able to receive audio.

To resolve this problem, access the **Settings > Advanced** menu in the PMC application after you have established or disconnected the VPN tunnel on your PMC client machine. When you access this menu, the PMC probes the Cisco Systems VPN Client to determine its activity and tunnel status and, from this menu, it can also detect an IP address change. For more information about the Express menu, see the "Configuring the Channels and Advanced Settings" section on page 5-7.

When you use the Cisco VPN Client version 4.0x, the SIP-based remote connection may not become activated. In this situation, you may need to deactivate and then reactivate the channel after you establish the VPN tunnel. To deactivate the channel, click the **Activate** button. Click the **Activate** button again to reactivate the channel.

About the VPN Client Stateful Firewall

The VPN Client integrated stateful firewall provides protection when split tunneling is in effect by safeguarding from Internet attacks while the VPN client is connected to a VPN concentrator through an IPSec tunnel.

When enabled, this "Stateful Firewall (Always On)" feature enforces more robust security by disallowing inbound sessions from all networks, regardless of whether a VPN connection is being used. This firewall is active for both encrypted and unencrypted traffic, except when you use the following protocols:

- Dynamic Host Configuration Protocol (DHCP)—The stateful firewall allows inbound traffic because requests to the DHCP server are sent out one port and responses are received through a different port.
- Encapsulating Security Payload (ESP)—The stateful firewall permits this traffic from the secure gateway because ESP rules are packet filters and not based on sessions.

For more information about exceptions, refer to the release notes for the VPN Client documentation at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/vpn/client/index.htm

Enabling and Disabling the Stateful Firewall on the PMC Client Machine

To ensure PMC connectivity, check the VPN Client Options menu to verify that the "Stateful Firewall (Always On)" feature is disabled. (If a check mark does not appear next to this option, then it is disabled.) The "Stateful Firewall (Always On)" option enables and disables the integrated stateful firewall.

Note Be sure that the "Stateful Firewall (Always On)" option is not enabled on your PMC client machine. If this option is enabled, you must disable it; otherwise, SIP and multicast connections may not work correctly.

Tip The "Stateful Firewall (Always on)" feature affects only Internet traffic; when this feature is enabled, it disallows inbound sessions from all networks, regardless of whether a VPN connection is being used. This is true for the VPN Client on any operating system.

To enable or disable the stateful firewall, and manage this setting on your Cisco Systems VPN Client PMC machine, perform the following procedure:

Procedure

Step 1 Double-click the VPN Client icon to launch the application.

Step 2 From the VPN Client main dialog box, click the Options drop-down menu button and scroll down to the "Stateful Firewall (Always On)" option. Alternatively, you can right-click the **lock icon** in the system tray and choose **Stateful Firewall**.

Note When the stateful firewall is enabled, a check mark displays next to this option. The stateful firewall feature is disabled by default.

a. If a check mark appears next to this option, the option is enabled. Click "**Stateful Firewall (Always On)**" to remove the check mark and disable the internal stateful firewall.

b. If a check mark does not appear next to this option, the option is already disabled. You do not need to take any action.

To view the status of the stateful firewall, right-click the **lock icon** in the system tray during a VPN connection.

Step 3 Close the VPN client.

For additional information about the Cisco Systems VPN Client, refer to the VPN Client documentation for your specific version at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/vpn/client/index.htm

Using the PMC with the Windows XP Firewall

The Microsoft Windows XP operating system includes an integrated firewall to provide additional security. Windows XP and Windows XP Service Pack 1 (SP1) include the Internet Connection Firewall (ICF) while Windows XP SP2 includes the Windows Firewall, as a replacement to the ICF.

For the PMC application to work properly with Windows XP, you may need to modify your firewall settings to ensure that the PMC can send and receive the required protocols.

To modify your firewall settings, perform the following procedure:

Procedure

Step 1 On your Windows XP PMC client machine, navigate to **Start > Control Panel > Network and Internet Connections**.

The Network and Internet Connections window displays.

Step 2 Click the **Change Windows Firewall settings** link.

The Windows Firewall window displays.

Step 3 Click the **Exceptions** tab.

A list of programs and services displays.

Step 4 If you have already installed the PMC, check the **Cisco IPICS PMC** check box to add this program to the list of exceptions in the Windows Firewall; then, proceed to Step 6.

Step 5 If you have not yet installed the PMC, install and then launch the PMC.

For information about installing and launching the PMC, see the "Installing the PMC Application" section on page 2-2 and the "Launching the PMC Application" section on page 2-14.

a. After you launch the PMC, a Windows Security Alert displays to inform you that Windows XP has blocked the PMC.

b. Click **Unblock** to add this program to the list of exceptions in the Windows Firewall.

Step 6 Click **OK**.

Windows XP now allows the PMC to function properly.

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

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

Troubleshooting Multicast Communications Issues

Certain PMC client machines that are running the Windows 2000 and Windows XP operating systems may not be able to send multicast communications because of an issue with the operating system; in these situations, PMC multicast users may experience one-way audio where they can hear, but they may not be heard by, other Cisco IPICS users.

Tip To ensure identification of this specific problem, please check to make sure that the microphone mute options on the headset and in the Windows operating system are not enabled. For more information about using the microphone with the PMC, see the "Using the Microphone with the PMC" section on page 2-10.

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

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

1. Run the sniffer on the affected PMC client machine and filter for outgoing multicast UDP packets.

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

To fully resolve this problem, you must perform a fresh installation of the Windows 2000 or Windows XP operating system on the PMC client machine.

Troubleshooting Winsock Corruption Issues

If you encounter connectivity problems, such as the inability to send and/or receive IP traffic or if you receive an error when you try to release and renew the IP address on your PMC client machine, you may be experiencing a problem with damaged or corrupted Windows Winsock registry keys.

When the Winsock registry is damaged or corrupted, the PMC client machine may unexpectedly lock up and not accept any additional input.

To fully resolve this problem, you must fix the malfunctioning network components in your Windows installation. To fix the malfunctioning network components, perform one of the following tasks:

- Remove and reinstall the Windows TCP/IP stack
- Issue a command to fix the Winsock corruption (this command is applicable to Windows XP systems only)
- Perform a fresh installation of the Windows operating system

For additional information, access the Microsoft support site at http://support.microsoft.com and search for the Microsoft knowledge base article 811259 entitled “How to determine and recover from Winsock2 corruption.” This bulletin contains information about the symptoms and causes of Winsock corruption issues and the procedures that you can follow to resolve these problems.

To help identify problems with the Winsock registry keys and avoid application issues, Cisco recommends that you validate that your Windows Winsock library is not corrupted before you install the PMC application on your client machine.

Troubleshooting Offline Mode Issues

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

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

For detailed information about the situations that apply to offline mode based on interactions between the PMC and the server, see the "PMC Offline Mode Caveats" section on page 4-7.

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

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

Note Be sure that the "Work Offline" option in your IE browser settings is not enabled on your PMC client machine. If this option is enabled, you must disable it; otherwise, you may not be able to connect to the server.

Troubleshooting PMC Connectivity Issues with the RMS

To connect the PMC via a SIP-based remote connection, make sure that the PMC can establish connectivity to the RMS. (The PMC connects to the RMS by using the IP address of the Loopback0 interface that is assigned to the RMS and configured in the Cisco IPICS server.)

To determine the IP address of the RMS, access the **Settings > Channels** menu in the PMC application. Click a remote connection channel to highlight it; then, scroll through the Channel Properties pane to the SIP Proxy field to find the IP address of the RMS for the associated channel. (If you cannot determine the IP address of the RMS, contact your System Administrator for assistance.)

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

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

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

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

Troubleshooting PMC Connectivity Issues with a High Latency, Low Bandwidth Link

When you first log in to a PMC that is connected via a high latency and/or low bandwidth link, such as when you use a satellite connection, an error message displays to inform you that the channels are being disabled. This error occurs because of the time delay to connect over this type of link. To recover from this error, click **OK**.

If the Cisco IPICS server times out while it is waiting for a response from one or more resources, the server does not have complete information to send to the PMC. In this case (after about one minute), the server sends an incomplete list of channels to the PMC while it waits for a response.

The server marks each channel that does not respond within the timeout interval as “unavailable” until the operation completes. When this situation occurs, the PMC displays a message that states that the “RMS resources may not be available.”

You do not need to take any action to resolve this issue. After the server completes its tasks, the channels display on the PMC.

Note Be aware that the amount of time that it takes for the server to complete its tasks will vary depending on the amount of latency in the network.

For information about configuring the PMC for use with a high latency and/or low bandwidth link, see the "Configuring the Channels Menu Options" section on page 5-8.

Resolving Name Resolution Failures

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

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

Identifying Channel Activation Issues

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

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

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

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

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

- Network connectivity issues that prevent connection to the RMS.
- The RMS may be in an offline or invalid state.
- The RMS may be misconfigured in the server.

- The dial peers may not have been configured or the dial peers and/or the voice ports may be misconfigured in the RMS.
- The RMS may not have yet created the dial peers because of a delay between the server configuration and RMS dial peer creation. In this case, you should wait a couple of minutes and then restart the PMC to try again.

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

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

- The PMC will automatically reactivate the connection after 30 seconds. Alternatively, you can reactivate the channel by clicking the **Activate** button on the PMC.

Resolving Codec Mismatch Issues

When the protocol type or codec type is misconfigured in the RMS LMR gateway, the PMC has the ability to detect this codec type mismatch (such as G.729 versus G.711) and thereby, preserve system resources and PMC functionality.

If the misconfiguration includes a specific codec type that Cisco IPICS supports (that is, G.729 or G.711), the PMC adapts the codec decoding to enable handling of the different version of that specific codec type. For example, the PMC can adapt to different versions of G.711, such as G.711 ulaw and G.711 alaw, and decode either version automatically to maintain functionality.

If the codec type mismatch is caused by the configuration of an incorrect or unsupported codec type, the PMC will drop the incorrect or unsupported encoded samples because it cannot decode them. In this case, the PMC user will not hear any audio.

For more information about the codecs that Cisco IPICS supports, see the "Codec Support" section on page 3-22.

Support for Right-to-Left and Double-Byte Languages

Note Although this version of Cisco IPICS does not support localization, it does provide support for the PMC to display channel/VTG names that are configured in the server in certain right-to-left (RTL) and double-byte (character-based) languages. This support allows for the input of Arabic and Hebrew characters (RTL languages) and Chinese and Japanese characters (double-byte languages) for names and descriptions in the Cisco IPICS server.

To use a right-to-left language or a double-byte language in Windows 2000 and Windows XP, you need to configure the operating system to enable support for the specific language that you use.

Note If you try to use the Arabic or Hebrew language without enabling support for RTL, your text will display in reverse.

Procedure

To enable RTL support for the Arabic and Hebrew languages for use with Cisco IPICS, and to enable support for double-byte languages, perform the following procedure:

Procedure:

Step 1 If your client machine runs Windows 2000, follow this step. Otherwise, proceed with Step 2. On Windows 2000 client machines, navigate to **Start > Settings > Control Panel > Regional Options**.

The Regional Options dialog box displays. In this dialog box, you can specify system settings such as locale, languages, currency, time, and date.

a. From the **General** tab, you can add support for the languages that you need to use:

- To add support for the Arabic language, check the **Arabic** check box in the Language Settings for the System area.
- To add support for the Hebrew language, check the **Hebrew** check box in the Language Settings for the System area.

- To add support for the Chinese language, check the **Traditional Chinese** or the **Simplified Chinese** check box in the Language Settings for the System area.
- To add support for the Japanese language, check the **Japanese** check box in the Language Settings for the System area.

b. Click **OK**.

c. Restart your PMC client machine for your changes to become effective.

Note After your PMC client machine restarts, your operating system will be enabled for the languages that you chose.

d. After the language files have been installed, navigate to Regional Options, as described above, and click the **Input Locales** tab to add the language input options that you want to use; then, click the **Change** button from the Input Languages and Methods pane.

e. From the Installed Services pane, click **Add**.

The Add Input Language dialog box displays.

f. From the Input Language drop-down list box, click to select and highlight the input language for one of the supported languages.

g. Check the **Keyboard Layout / IME** check box; from the drop-down list box, choose the keyboard layout to use.

h. Click **OK**.

The Text Services dialog box displays your selection in the Installed Services pane.

i. Click **Apply**; then, click **OK**.

j. Repeat Step d. to Step i. for each supported language that you want to add.

Step 2 On Windows XP client machines, navigate to **Start > Control Panel > Regional and Language Options**.

The Regional and Language Options dialog box displays. In this dialog box, you can specify options for regional and language settings on your system.

a. Click the **Languages** tab.

- To add support for supplemental languages, check the **Install files for complex script and right-to-left languages (including Thai)** check box in the Supplemental Language Support area.
- To add support for Chinese and Japanese languages, check the **Install Files for East Asian languages** check box.

  A pop-up message displays to inform you that the installation of supplemental language support requires a defined amount of available disk space.

b. Click **OK** to accept.

c. From the Regional and Language Options dialog box, click **Apply**; then, click **OK**.

d. If you are prompted, restart your PMC client machine for your changes to become effective.

Note After your PMC client machine restarts, your operating system will be enabled for the languages that you chose.

e. After the language files have been installed, navigate to Regional and Language Options, as described above, and click the **Details** button in the Text Services and Input Languages pane.

f. From the Installed Services pane, click **Add**.

   The Add Input Language dialog box displays.

g. From the Input Language drop-down list box, click to select and highlight the input language for one of the supported languages; then, click **OK**.

h. Check the **Keyboard Layout / IME** check box; from the drop-down list box, choose the keyboard layout to use.

i. Click **OK**.

   The Text Services and Input Languages dialog box displays your selection in the Installed Services pane.

j. Click **Apply**; then, click **OK**.

k. Repeat Step e. to Step i. for each supported language that you want to add.

PMC Application Caveats

The following caveats pertain to the PMC application:

- Only one instance of the PMC application can be open and each PMC supports only one user ID login on a given PC at one time.
- A PMC end-user can log in to an unlimited number of different PMC applications at the same time.
- Any number of valid Cisco IPICS users can use the same PMC application, but not concurrently, based on PMC licensing requirements.
- The PMC application can log in to the server that has been configured as the default server and from which the PMC installation file has been downloaded. If the primary server is not accessible, and if there are alternate servers to choose from, you can log in to a different server. For more information about connecting to alternate servers, see the "Support for Cisco IPICS Recovery" section on page 6-1.
- See the "PMC Usage Guidelines" section on page 4-2 for information about using the PMC.
- See the "PMC Offline Mode Caveats" section on page 4-7 for information about using the PMC in offline mode.
- See the "Skin Caveats" section on page 5-4 for information about PMC skin caveats.
- If you use a docking station with your PMC client machine, make sure that you close the PMC application before you undock your PC; otherwise, your PC may become unresponsive and require you to reboot.

Analyzing PMC Error Conditions

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

In some situations, the PMC may display an error message. In other situations, you may experience certain issues, such as audio quality issues, where a message does not display.

Table 8-1 describes some of these error conditions and audio quality issues and how to resolve them.

Table 8-1 PMC Error Conditions

Problem	Solution
You cannot connect to the server. Or, you may see error messages that state you cannot connect to the server but you can connect by using Internet Explorer.	Invalid entries in the pmc.ini file may be the cause of this problem. To check this file, perform the following steps: 1. Navigate to **C:\Program Files\Cisco Systems\Cisco IPICS\PMC**. 2. Search for the **pmc.ini** file. 3. Right-click **pmc.ini** and click **Open With**. 4. Click **Notepad**; then, click **OK**. 5. Delete all entries in this file except the following fields: server_host, server_port, and server_port_ssl. 6. Validate that the configured values in these fields are correct. **Note** Contact your system administrator if you are not sure of these values or if these values are correct and you still cannot connect.
You can hear other users but they cannot hear you.	Check your audio settings to make sure that your microphone is not set to mute. See the "Configuring the Audio Settings" section on page 2-7 for more information about audio settings. **Note** If you are using a hardware DSP headphone, such as the Plantronics DSP, check to make sure that the external microphone mute button is not switched to the "on" position.
When you attempt to download the PMC application from the server, you may receive an error message to inform you that the PMC is not available for download at this time.	This problem may occur if the pmcsetup.exe file was erroneously modified, moved, renamed, or deleted from the server. Contact your system administrator for assistance.

Table 8-1 PMC Error Conditions (continued)

Problem	Solution
When you talk, other users tell you that your voice sounds choppy and breaks up at times during a conversation.	If VAD is enabled, disable the setting in the Channels menu. See the "Configuring the Channels and Advanced Settings" section on page 5-7 for more information about VAD. If voice quality still sounds choppy, check the CPU activity on your client machine. If your CPU is overburdened by other programs that are running at the same time, there may insufficient CPU cycles for the PMC to run properly. You can check the CPU usage by opening Windows Task Manager and clicking on the **Performance** tab. If your CPU utilization appears high, check the applications that are running by clicking the **Applications** tab and then close any programs that do not need to be open.
When you talk, other users tell you that your voice sounds low.	Check the placement of your microphone so that it is positioned between 2 and 6 inches from your mouth. If necessary, reposition the microphone for optimum use. If your microphone gain is set too low, VAD may be interfering with and disabling output; this activity can result in choppy voice quality. Check your audio settings to make sure that the volume is not set too low. If the volume is set low, increase the input gain on your microphone by sliding the bar up on the volume controls to increase the volume.
When you talk, other users tell you that they hear a persistent or intermittent noise, such as a hum.	The existence of a persistent or intermittent noise, such as a hum, when you talk may be due to defective headset hardware. In this situation, Cisco recommends that you isolate the source of the audio quality issue by replacing the defective headset with a new, high-quality headset. For more information about voice quality, see the "Voice Quality Tips" section on page 2-12.

Table 8-1 PMC Error Conditions (continued)

Problem	Solution
When you attempt to log in to the PMC, you see an error message that states "invalid user or password."	This error may display because the password that was entered is incorrect for the specified user name or because the user name does not exist on the Cisco IPICS server. To remedy this situation, log in to the PMC by using a correct user name and password combination. If this action does not resolve the problem, contact your system administrator to request that a new user account be added to the server for the specified user.
When you start the PMC after a new installation, the PMC displays an error message to alert you that the PMC cannot register with the Cisco IPICS server and to check your network connection.	Upon initial connection to the server, the PMC must be able to register with the Cisco IPICS server to obtain its unique PMC ID. This error message may display when the PMC tries to connect to a server that is offline and has not yet assigned the PMC ID. When you see this error dialog box, click **OK** to exit; then, restart the PMC to try again. If the PMC continues to display this error message, contact your system administrator for assistance.
The PMC displays a security alert dialog box that prompts you to approve the server certificate.	The PMC has been designed to automatically approve the Cisco IPICS server certificate for secure communications; however, this functionality may not work under certain circumstances. When this functionality does not work properly, the PMC displays a security alert dialog box to inform you that the page requires a secure connection which includes server authentication. To proceed, you must approve the server certificate. On affected PMC client machines, this dialog box appears each time that you run the PMC, once per PMC session (usually during login). When you see this dialog box, you must click **Yes** to run the PMC. If you click No, the PMC will exit.

Table 8-1 PMC Error Conditions (continued)

Problem	Solution
When you try to launch the PMC, an error message displays because the PMC cannot access the media device.	The PMC application may coexist with other voice applications depending on the operating system that you use. Windows XP allows multiple applications to run concurrently and open and use the microphone at the same time. Windows 2000, however, does not provide support for this same capability. You may encounter this error if you are using Windows 2000 and try to open the PMC application while you are running another voice application, such as Microsoft NetMeeting conferencing software, on your PMC client machine. To resolve this issue, close NetMeeting and then launch the PMC. You can then restart NetMeeting.

Related Topics

- Configuring the Audio Settings, page 2-7
- Skin Caveats, page 5-4
- Configuring the Channels and Advanced Settings, page 5-7
- Using the Optional Settings Menu, page 5-15

Where to Find More Information

- *Cisco IPICS Server Administration Guide*
- *Cisco IPICS Command Line Interface*

A

action — A discrete function that is performed through a policy. Discrete functions include activate VTG, notification, VTG add participant, dial-out, and invite to VTG.

activate VTG — An action that activates a preconfigured VTG; can also specify a duration. At the end of the specified duration, the VTG is deactivated. If no duration is specified, the VTG must be manually deactivated by the dispatcher from the VTG Management drawer in the Cisco IPICS administration console.

activated — A state that indicates that the SIP (unicast) or multicast channel is fully operational. When a channel/VTG on the PMC is enabled and activated, all of the PMC buttons are operational.

activating — A state that becomes effective when you click the **Activate** button on the PMC. The Activate button appears highlighted while the other PMC buttons remain in an inactive state as the system attempts to activate and connect.

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

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

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

alert tone buttons Buttons on the PMC that can play out alert tones on one channel or multiple channels.

all talk button Allows you to simultaneously talk on all of the channels that you selected.

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

B

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

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

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

C

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

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

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

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

CAS channel associated signaling. The transmission of signaling information within the voice channel. CAS signaling often is referred to as robbed-bit signaling because user bandwidth is being robbed by the network for other purposes.

channel A communication path that is wide enough to permit a single RF transmission. Multiple channels can be multiplexed over a single cable in certain environments. *See* PTT channel.

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

channel folder A logical grouping of channels

channel select check box Provides the ability to select or deselect the specified channel on the PMC for audio transmission.

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

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

Cisco IPICS Cisco IP Interoperability and Collaboration System. The Cisco IPICS system provides an IP standards-based solution for voice interoperability by interconnecting voice channels, talk groups, and VTGs to bridge communications amongst disparate systems.

Cisco IPICS policy engine Integrated with the Cisco IPICS server, this component enables telephony dial functionality and is responsible for the management and execution of policies and user notifications.

Cisco IPICS server Provides the core functionality of the Cisco IPICS system. The Cisco IPICS server software runs on the Linux operating system on selected Cisco Media Convergence Server (MCS) platforms. The server software includes an incident management framework administration GUI that enables dynamic resource management for users, channels, and VTGs. The server also includes the Cisco IPICS policy engine, which enables telephony dial functionality and is responsible for the management and execution of policies and user notifications.

Cisco Unified IP Phone A full-featured telephone that provides voice communication over an IP network. A user can participate in a PTT channel or VTG by using a Cisco Unified IP Phone as a PTT device.

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

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

codec coder-decoder.

1. Integrated circuit device that typically uses pulse code modulation to transform analog signals into a digital bit stream and digital signals back into analog signals.

2. In Voice over IP, Voice over Frame Relay, and Voice over ATM, a DSP software algorithm that is used to compress/decompress speech or audio signals.

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

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

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

coverage In radio communications, the geographical area that is within the range of, or that is covered by, a wireless radio system to enable service for radio communications. Also referred to as service delivery area.

D

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

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

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

dial engine scripts Scripts that the Cisco IPICS dial engine executes to provide the telephony user interface (TUI) for interaction with incoming and outgoing phone calls.

dial-in A phone call that is dialed in to the policy engine.

dial-in floor control A feature that allows one dial-in user, at a time, to talk in a VTG or a channel. The telephony user interface provides this dial-in floor control feature to support dial-in users. It does not provide support for floor control for other PTT users.

dial number The phone number that is used by the policy engine and the SIP provider and configured in the Dial Information pane in the Ops Views window. Dialing this number provides user access to the telephony user interface.

dial out invite An action that invites selected user(s) to the selected VTG.

A phone call that is dialed out by the policy engine to a phone user to invite the user in to a talk group.

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

digit ID A numeric identifier that is chosen by a Cisco IPICS user and stored in the user profile. Cisco IPICS uses this ID and a numeric password to authenticate a Cisco Unified IP Phone user.

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

dispatcher The Cisco IPICS dispatcher is responsible for setting up the VTG templates, activating the VTGs to begin conferences, and adding and/or removing participants in VTG templates and active VTGs. The dispatcher also monitors the active VTGs and events, can mute and unmute PMC users, as necessary, and manages policies, which activate/deactivate VTGs based on specific criteria and designated intervals. Policy management activities include create/modify/delete policies, view policies, execute policies, and activate privileges.

DS0 digital service zero (0). Single timeslot on a DS1 (also known as T1) digital interface—that is, a 64-kbps, synchronous, full-duplex data channel, typically used for a single voice connection on a PBX.

dynamic regrouping A trunking system feature that allows multiple radios to be placed upon a specific talk group without manual manipulation of the programming of the radios. Dynamic regrouping is initiated through a system control console and transmitted to the radio via the trunking systems control channel.

E

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

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

2. A type of signaling that is traditionally used in the telecommunications industry. Indicates the use of a handset that corresponds to the ear (receiving) and mouth (transmitting) component of a telephone.

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

encode To modify information into the required transmission format.

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

event An active VTG in the Cisco IPICS solution.

F

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

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

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

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

frame A logical grouping of information sent as a data link layer unit over a transmission medium. Often refers to the header and the trailer, used for synchronization and error control, that surround the user data contained in the unit. The terms cell, datagram, message, packet, and segment also describe logical information groupings at various layers of the OSI reference model.

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

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

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

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

frequency sharing The assignment to or use of the same radio frequency by two or more stations that are separated geographically or that use the frequency at different times.

G

gateway Device that performs an application-layer conversion of information from one protocol stack to another. In Cisco IPICS, the gateway component includes LMR gateways, which functionality is usually installed as an additional feature in a supported Cisco router. LMR gateways provide voice interoperability between radio and non-radio networks by bridging radio frequencies to IP multicast streams.

GRE generic routing encapsulation. Tunneling protocol that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP internetwork. By connecting multiprotocol subnetworks in a single-protocol backbone environment, IP tunneling that uses GRE allows network expansion across a single-protocol backbone environment. GRE is generally used to route multicast traffic between routers.

H

H.323 Defines a common set of codecs, call setup and negotiating procedures, and basic data transport methods to allow dissimilar communication devices to communicate with each other by using a standardized communication protocol.

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

Hoot ‘n’ Holler (Hootie) A communications system where the loudest and most recent talker or talkers are mixed into one multicast output stream. Also known as hootie, these networks provide “always on” multiuser conferences without requiring that users dial in to a conference.

Cisco enables the Cisco Hoot 'n' Holler feature in specific Cisco IOS versions.

i

I

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

incident management framework A software framework that includes an adaptable GUI to facilitate resources, such as users, radio channels, cameras, and sensor information, for delivery that is based upon policy or incident needs.

informix linux group Members of this group have full permission to Cisco IPICS server folders, files, and scripts that are related to the Informix database application. Members of this group include the informix and ipicsdba users. In addition, the informix user has full administrative permissions to the Informix database instance.

informix user ID The Cisco IPICS Linux user that belongs to both the informix linux group, which includes full permission to the Cisco IPICS database server folders, files, and scripts, and the ipics linux group, which includes permission to Cisco IPICS application-related folders, files, and scripts. In addition, this user has full administrative permission to the Informix database instance. Cisco IPICS creates this Linux system user ID and generates the password during the software installation process. The password for this user ID never expires.

To access the informix user, log in to the Cisco IPICS server by using the root user ID; then, enter **su - informix** (superuser from root).

interference The effect of unwanted energy due to one or a combination of emissions, radiation, or inductions upon reception in a radio communication system, manifested by any performance degradation, misinterpretation, or loss of information, which could be extracted in the absence of such unwanted energy.

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

invitation policy A policy that can be invoked only through the telephony user interface and can include only the invite to VTG action. After joining a talk group, a user can access the breakout menu and invoke invitation policies. The talk group that this user has joined is the talk group that the invited users join.

invite to VTG A version of the dial out invite action where users to be invited are preconfigured but the VTG that they are invited to depends on which VTG the invoker of the policy is dialed into.

ipicsadmin user ID The Cisco IPICS Linux user that, as part of the ipics linux group, has full permission to the Cisco IPICS server folders, files, and scripts that are related to the Cisco IPICS application and database backup and restore operations. In addition, the ipicsadmin user has permission to read and write data from and/or to the Informix database. Cisco IPICS creates this Linux system user ID during the software installation process. The password for this user ID never expires.

ipicsdba user ID The Cisco IPICS Linux user that belongs to both the informix linux group, which includes full permission to the Cisco IPICS database server folders, files, and scripts, and the ipics linux group, which includes permission to Cisco IPICS application-related folders, files, and scripts. In addition, the ipicsdba user has permission to read data, write data, create tables, and create databases in the Informix database instance. Cisco IPICS creates this Linux system user ID and generates the password during the software installation process. The password for this user ID never expires.

To access the ipicsdba user, log in to the Cisco IPICS server by using the root user ID; then, enter **su - ipicsdba** (superuser from root).

ipics linux group Members of this group have full permission to Cisco IPICS server folders, files, and scripts that are related to the Cisco IPICS application and database backup and restore operations. Members of this group include the ipicsadmin, ipicsdba, and informix users.

ipics user ID The Cisco IPICS application-level user ID that can perform all administration-related tasks via the Cisco IPICS Administration Console. Cisco IPICS creates this web-based user ID during the software installation process.

IPSec IP Security. A framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer. IPSec uses IKE to handle the negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPSec. IPSec can protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

K

keepalive A message that is sent by one network device to inform another network device that the virtual circuit between the two devices is still active.

key The parameter that defines an encryption code or method.

kilohertz (kHz) A unit of frequency that denotes one thousand Hz.

L

latch The PMC functionality that allows a Cisco IPICS user to lock in a PTT channel.

linear modulation A radio frequency transmission technique that provides the physical transport layer of a radio system. This technology is compatible in digital and analog system environments and supports channel bandwidths of 5 kHz to 50 kHz.

LMR Land Mobile Radio. A Land Mobile Radio (LMR) system is a collection of portable and stationary radio units that are designed to communicate with each other over predefined frequencies. They are deployed wherever organizations need to have instant communication between geographically dispersed and mobile personnel.

Cisco IPICS leverages the Cisco Hoot 'n' Holler feature, which is enabled in specific Cisco IOS versions, to provide radio integration into the Cisco IPICS solution. LMR is integrated by providing an ear and mouth (E&M) interface to a radio or other PTT devices, such as Nextel phones. Configured as a voice port, this interface provides the appropriate electrical interface to the radio. You configure this voice port with a connection trunk entry that corresponds to a voip dial peer, which in turn associates the connection to a multicast address. This configuration allows you to configure a corresponding channel in Cisco IPICS, using the same multicast address, which enables Cisco IPICS to provide communication paths between the desired endpoints.

location In Cisco IPICS, location signifies reachability; meaning, channels or users who are associated with the same location can communicate with each other without additional network configuration. Location may refer to a physical or virtual location, as defined in the server.

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

M

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

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

multicast Single packets that are copied by the network and sent to a specific subset of network addresses. Multicast refers to communications that are sent between a single sender and multiple recipients on a network.

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

multicast address/port Cisco IPICS uses this type of connection to enable the PMC to directly tune in to the multicast channel. Multicast address/port combinations are also used by gateways and RMS components.

multicast pool Multicast IP addresses that are defined as part of a multicast pool. Cisco IPICS allocates a multicast address from this pool of resources when a dispatcher activates a VTG.

multiplexing The combination of two or more information channels on to a common transmission medium. In electrical communications, the two basic forms of multiplexing are time-division multiplexing (TDM) and frequency-division multiplexing (FDM).

multipurpose policy A policy that can include any of the supported actions; may be invoked through the telephony user interface or the Cisco IPICS administration console.

multiselect buttons Provides the ability to select or deselect all channels on the PMC for audio transmission.

mute The functionality that enables a dispatcher to mute a PMC user from talking or transmitting voice on one or more channels. The dispatcher can mute the microphone of the user or both the microphone and the speaker.

mutual aid channel A national or regional channel that has been set aside for use only in mutual aid interoperability situations. Restrictions and guidelines governing usage usually apply.

N

narrowband channels Channels that occupy less than 20 kHz.

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

National Telecommunication and Information Administration — The United States executive branch agency that serves as the principal advisor to the president on telecommunications and information policies and that is responsible for managing the federal government's use of the radio spectrum.

network — An interconnection of communications entities.

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

not activated — A VTG state that becomes effective when the Activate button is clicked a second time (to deactivate the channel) or if the connection terminates. No PMC buttons appear highlighted.

notification — An action that notifies selected user(s) via email, SMS, pager, or phone. The necessary IDs and phone numbers are configured in the communication preferences for each user. Notifications that are sent via the phone require user authentication before the notification prompt is heard.

An email, SMS, pager, or phone call that is placed to a user for the purpose of sending a notification message.

O

offline mode — When the connection to the server goes offline, the PMC enters offline mode. Offline mode enables continuous communication during periods of server downtime. Using offline mode requires at least one successful login to the server.

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

ops view operational view. A Cisco IPICS feature that provides the ability to organize users, user groups, channels, channel groups, VTGs, and policies into different user-definable views across multiple organizations or agencies that normally would not share resources. While ops views are maintained separately by the Cisco IPICS system administrator and/or ops view administrator, this functionality also allows multiple entities to use one Cisco IPICS server to enable resource sharing across multiple ops views, according to business need.

ops view administrator The ops view administrator capabilities include managing and monitoring the activity logs that are filtered by ops views and accessible in the Administration Console (**Administration > Activity Log Management**) window.

OTAR over-the-air re-keying. Provides the ability to update or modify over radio frequency the encryption keys that are programmed in a mobile or portable radio.

P

packet A logical grouping of information that includes a header that contains control information. Usually also includes user data.

packet switching The process of routing and transferring data by using addressed packets so that a channel is occupied during the transmission of the packet only. Upon completion of the transmission, the channel is made available for the transfer of other traffic.

PIM Protocol Independent Multicast. Multicast routing architecture that allows the addition of IP multicast routing on existing IP networks. PIM is unicast routing protocol independent and can be operated in two modes: PIM dense mode and PIM sparse mode.

PIM dense mode One of the two PIM operational modes. PIM dense mode is data-driven and resembles typical multicast routing protocols. Packets are forwarded on all outgoing interfaces until pruning and truncation occurs. In dense mode, receivers are densely populated, and it is assumed that the downstream networks want to receive and will probably use the datagrams that are forwarded to them. The cost of using dense mode is its default flooding behavior. Sometimes called dense mode PIM or PIM DM.

PIM sparse mode One of the two PIM operational modes. PIM sparse mode tries to constrain data distribution so that a minimal number of routers in the network receive it. Packets are sent only if they are explicitly requested at the RP (rendezvous point). In sparse mode, receivers are widely distributed, and the assumption is that downstream networks will not necessarily use the datagrams that are sent to them. The cost of using sparse mode is its reliance on the periodic refreshing of explicit join messages and its need for RPs. Sometimes called sparse mode PIM or PIM SM.

PMC Push-to-Talk Management Center. A standalone PC-based software application that simulates a handheld radio to enable PTT functionality for PC users. This application enables Cisco IPICS PMC end-users, dispatch personnel, and administrators to participate in one or more VTGs at the same time.

PMC ID The unique ID that the Cisco IPICS server generates for each PMC to track requests between the PMC and the server and to verify and manage concurrent PMC usage for licensing requirements.

policy Policies include one or more actions that execute sequentially and can be manually activated via the Cisco IPICS administration console or the telephony user interface. Cisco IPICS provides support for multiple policy types.

policy channel A channel that can be set up by the dispatcher and configured as a designated channel; that is, a channel that is always open to enable your interaction with the dispatcher.

policy execution status An indicator of policy execution success or failure. The Cisco IPICS administration console provides a status for each action under a policy,

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

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

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

PTT channel A channel consists of a single unidirectional or bidirectional path for sending and/or receiving signals. In the Cisco IPICS solution, a channel represents one LMR gateway port that maps to a conventional radio physical radio frequency (RF) channel.

PTT channel button The button on the PMC that you click with your mouse, or push, and hold to talk. You can use the latch functionality on this button to talk on one or more channels at the same time.

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

Q

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

queue Represents a set of items that are arranged in sequence. Queues are used to store events occurring at random times and to service them according to a prescribed discipline that may be fixed or adaptive.

queuing delay In a radio communication system, the queuing delay specifies the time between the completion of signaling by the call originator and the arrival of a permission to transmit to the call originator.

R

radio channel Represents an assigned band of frequencies sufficient for radio communication. The bandwidth of a radio channel depends upon the type of transmission and its frequency tolerance.

radio equipment Any equipment or interconnected system or subsystem of equipment (both transmission and reception) that is used to communicate over a distance by modulating and radiating electromagnetic waves in space without artificial guide. This equipment does not include microwave, satellite, or cellular telephone equipment.

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

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

RF radio frequency. Any frequency within the electromagnetic spectrum that is normally associated with radio wave propagation. RF generally refers to wireless communications with frequencies below 300 GHz.

RF repeater An analog device that amplifies an input signal regardless of its nature (analog or digital). Also, a digital device that amplifies, reshapes, retimes, or performs a combination of any of these functions on a digital input signal for retransmission.

RMS router media service. Component that enables the Cisco IPICS PMC to remotely attach to a VTG. It also provides support for remotely attaching (combining) two or more VTGs through its loopback functionality.

The RMS mixes multicast channels in support of VTGs and it also mixes PMC SIP-based (unicast) connections to a multicast channel or VTG. The RMS can be installed as a stand-alone component (RMS router) or as an additional feature that is installed in the LMR gateway.

root user ID The Cisco IPICS Linux user that has access to all files in the Cisco IPICS server. Strong passwords are enforced and Linux operating system password expiration rules apply to this user ID.

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

S

scanning A subscriber unit feature that automatically allows a radio to change channels or talk groups to enable a user to listen to conversations that are occurring on different channels or talk groups.

script prompts The audio prompts that the dial engine scripts play out during execution and which callers hear when they are interacting with the telephony user interface.

secure channel A channel that is connected to a radio that provides secure (encrypted or scrambled) communications on the Common Air Interface (CAI) side of the radio. (The level of security that is configured in the data network determines the security of the communications between the LMR gateway and a network attached device, such as a PMC or Cisco Unified IP Phone.)

An attribute that is set in the server to indicate that a channel is secure. A PTT channel that is configured as secure cannot be combined with unsecure channels in a VTG.

service delivery area *See* coverage.

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

skin Skins form the appearance of the PMC. In Cisco IPICS, skins are customizable and available in various options, including 4-channel and 8-channel mouse and touch screen formats.

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

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

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

spoken names The recorded names that are used for entities, such as channels, channel groups, VTGs, users, user groups, ops views, and policies. The names can be recorded through the policy engine or externally-recorded .wav files that can be uploaded into the system.

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

stored VTG Also referred to as inactive VTG.

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

system administrator The Cisco IPICS system administrator is responsible for installing and setting up Cisco IPICS resources, such as servers, routers, multicast addresses, locations, and PTT channels. The system administrator also creates ops views, manages the Cisco IPICS licenses and PMC versions, and monitors the status of the system and its users via the activity log files.

system architecture The design principles, physical structure, and functional organization of a land mobile radio system. Architectures may include single site, multi-site, simulcast, multicast, or voting receiver systems.

T

T1 Digital WAN carrier facility. T1 transmits DS-1-formatted data at 1.544 Mbps through the telephone-switching network, using alternate mark inversion (AMI) or binary 8 zero suppression (B8ZS) coding.

T1 loopback Allows mapping from multicast to unicast so that unicast phone calls can be patched into an LMR or into other multicast audio streams. A loopback is composed of two of the available T1 interfaces.

talk group A VTG or a channel.

A subgroup of radio users who share a common functional responsibility and, under normal circumstances, only coordinate actions among themselves and do not require radio interface with other subgroups.

TCP Transmission Control Protocol. A connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack.

TDMA time division multiple access. Type of multiplexing where two or more channels of information are transmitted over the same link by allocating a different time interval (“slot” or “slice”) for the transmission of each channel; that is, the channels take turns to use the link.

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

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

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

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

transmit indicator On some of the PMC skins, this indicator blinks red when traffic is being transmitted.

trigger A time-based event that invokes a policy on a scheduled basis, without manual intervention.

trunk A physical and logical connection between two switches across which network traffic travels. In telephony, a trunk is a phone line between two central offices (COs) or between a CO and a PBX.

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

trunked radio system Integrates multiple channel pairs into a single system. When a user wants to transmit a message, the trunked system automatically selects a currently unused channel pair and assigns it to the user, decreasing the probability of having to wait for a free channel.

TUI telephony user interface. The telephony interface that the dial engine provides to enable callers to perform tasks, such as joining talk groups and invoking policies.

U

user The Cisco IPICS user may set up personal login information, download the PMC application, customize the PMC skin, and specify communication preferences that are used to configure audio devices. By using a predefined user ID and profile, the user can participate in PTT channels and VTGs by using the PMC, supported models of Cisco Unified IP Phones, and the Public Switched Telephone Network (PSTN) via the telephony dial functionality of the Cisco IPICS IP policy engine. Users may have one or more Cisco IPICS roles, such as system administrator, ops view administrator, operator or dispatcher.

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

V

VAD Voice Activity Detection. When VAD is enabled on a voice port or on a dial peer, only audible speech is transmitted over the network. When VAD is enabled on Cisco IPICS, the PMC only sends voice traffic when it detects your voice.

virtual channel A virtual channel is similar to a channel but a radio system may not be attached. By creating a virtual channel, participants who do not use physical handheld radios to call into a VTG become enabled by using the PMC application or a supported Cisco Unified IP Phone model.

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

voice replay A feature that allows the PMC user to replay buffered audio on a per channel basis.

VoIP Voice over Internet Protocol. By digitalizing and packetizing voice streams, VoIP provides the capability to carry voice calls over an IP network with POTS-like functionality, reliability, and voice quality.

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

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

VOX Voice-operated transmit. A keying relay that is actuated by sound or voice energy above a certain threshold and sensed by a connected acousto-electric transducer. VOX uses voice energy to key a transmitter, eliminating the need for push-to-talk operation.

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

VTG add participant An action that adds selected participant(s) to the selected VTG.

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

W

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

wideband channel Channels that occupy more than 20 kHz.

A

activating the PMC buttons 1-8, 4-13
advanced PMC permissions 3-17
alert tones
  caveats 4-27
  names 3-14
  playing out 4-26
  privileges 3-16
  upgrades 2-26
All Talk button
  focus changes 4-26
  functionallity 4-12
  latching 4-17
  using with alert tone playout 4-27
  using with multiselect 4-25
application recovery 6-9
audio quality 2-7
audio settings configuration 2-7
automatic updates 2-21

B

browser support 1-12

C

caution, described xvi
caveats
  alert tones 4-27
  application troubleshooting 8-28
  application usage 1-13
  CLI commands 8-11
  direct dial channels 4-31
  direct two-way channels 4-29
  DTMF tone generation 4-24
  end-user interface configuration 5-1
  installation 2-3
  keyboard mapping 4-22
  login 4-4
  logs 7-6
  multiselect 4-25
  offline mode 4-7
  password 4-5
  skins 5-4
  system recovery 6-4
  touch screen skin 4-18
  troubleshooting 8-28
  voice replay 4-33
  VPN client 8-15

channel appearances 4-16
channel interactions
  activated 4-19
  activating 4-19
  disabled 4-19
  listen-only 4-20
  not activated 4-19
  secure 4-20
  unassigned 4-19
channel mapping 4-21
channels
  connectivity failure indicator 8-24
  customized color indicators 3-15
  direct dial 3-12
  direct two-way 3-12
  disable audio 3-16
  dispatcher policy channel 3-11
  indicators 3-14
  interactions 4-15
  labels 3-14
  latch 4-17
  latch permission 3-15
  listen-only mode 3-15
  locations 3-18
  maximum channel support 4-15
  names 3-14
  policies 3-10
  secure indicators 3-15
  terminology 3-12
  traffic activity indicators 4-35
  transmission settings 3-16
  truncating names 3-14
  types 3-14
  using direct dial connections 4-30
  using direct two-way connections 4-28
  visual indicators
    connectivity failure 8-24
    types 3-14
  voice activity detection 3-16
  VTGs 1-7
channel states 4-18
channel traffic activity
  administratively stopping transmission 4-37
  implicit floor control 4-37
  indicators 4-35
  interaction 4-37
  receive and transmit indicators 4-35
checking the microphone 2-11
Cisco CallManager
  documentation xiv
Cisco CallManager Express
  documentation xv
Cisco IOS
  documentation xvi
Cisco IPICS
  benefits 1-2
  browser support 1-12
  components 1-3

deployment 1-15
overview 1-2
server 1-3
server interactions 1-19
user interactions 1-20
Cisco IPICS user roles 1-5
Cisco IP Phones
documentation xv
Cisco IP Phone support 1-5
Cisco Land Mobile Radio (LMR)
documentation xv
Cisco Security Agent
documentation xv
codec support 3-22
communications
multicast 3-17
unicast 3-17
communications interruptions 6-5
components
Cisco IPICS server 1-3
Cisco IP Phone 1-5
gateways 1-4
PMC 1-4
router media service 1-5
configuring audio settings 2-7
configuring key mapping 5-12
configuring the PMC application 5-1
connection support 3-17
connectivity indicators
server connection status 4-6, 6-2
SIP-based remote connections 3-19, 6-2, 8-24
conventions, document xvi
customized skin downloads 2-21

D

direct dial
caveats 4-31
channels 4-30
direct two-way
caveats 4-29
channels 4-28
disable audio 3-16, 3-17
disconnected mode 4-9
dispatcher role 1-6
documentation
Cisco CallManager xiv
Cisco CallManager Express xv
Cisco IOS xvi
Cisco IP Phones xv
Cisco Land Mobile Radio (LMR) xv
Cisco Security Agent xv
conventions xvi
MCS servers xv
double-byte language support 8-25
downloading the PMC update 2-23
DTMF tone generation
caveats 4-24

focus changes 4-24
supported keys 4-23
using 4-24
dynamic configuration 4-14

E

echo 3-5
encrypted file system 8-5
end-user channel interactions 4-16
end-user features 4-20
error messages 8-28

F

feature support
channels 3-11
end-user features 4-20
implementing policies 3-10
interoperability 3-1
locations 3-18
PMC skin 1-8
focus changes
alert tone playout 4-26
All Talk channel 4-23
DTMF tone generation 4-24
mapped key 4-22
multiselect 4-26
PTT channel 4-23
USB devices 4-21
while transmitting 4-22
footswitch
key mapping 4-21
troubleshooting 8-7
forced upgrades 2-23

G

gateways
LMR 1-4
router media service 1-5

H

headset
audible hum 2-13
checking audio settings 2-13
connecting to PMC client machine 2-12
resolving headset issues 8-11
using a high-quality headset 2-12
using a USB DSP headset 2-9
using the microphone 2-10
voice quality tips 2-12
high latency, low bandwidth connections 5-13
HTTPS 2-4
Hypertext Transfer Protocol over Secure Sockets Layer
See HTTPS

I

IE publisher error 8-14
implementing policies 3-10
incident management scenario 3-6
installation log file 8-3
installing the PMC application 2-2
interactions
  channels 4-15
  channel states 4-18
  Cisco Security Agent 2-6
  client-server 2-1
  end-user features and interactions 4-20
  PMC user 3-7
  scenarios 3-3
  server 1-19
  server-PMC interaction 3-8
  server-PMC login sequence 4-6
  system 1-19
  user 1-20

J

joining a VTG 4-14

K

key assignments 4-21
keyboard mapping
  caveats 4-22
  configuring 4-21
  focus changes 4-22
  footswitch 4-21

L

Land Mobile Radio
  See LMR
latch functionality
  latching a channel 3-5
  latching the PTT button 1-14
  using the PMC latch 4-17
license requirements 4-6
listen-only channels 3-15
LMR
  channel representation 3-12
  gateway 1-4
location 3-18
log files 7-1
logging in to the PMC
  information 4-1
  local login 4-9
  login caveats 4-4
logging out of the PMC 4-39
loss of focus 4-22

M

managing alert tone upgrades 2-26
managing PMC upgrades 2-22
managing version numbers 2-18
MCS servers
  documentation xv
microphone setup 2-11
multicast
  communications 3-17
  connection type 3-19
  maximum allowable voice streams 3-19
  PMC behavior when exceeding the maximum allowable voice streams 3-19
multiselect
  caveats 4-25
  focus changes 4-26
  functionality 4-25

N

note, described xvi

O

one-way audio issues 8-11
operator role 1-6
ops view administrator role 1-6
optimizing audio for low bandwidth use 5-13
optimizing for high latency, low bandwidth connections 5-13
optimizing your audio on the PMC 2-7
optional settings submenus 5-15
optional upgrades 2-23
overview
  Cisco IPICS 1-2
  PMC 1-7

P

passwords
  caveats 4-5
  expiration 4-5
  invalid login attempts 4-5, 4-10
PMC
  alert tones 4-26
  All Talk button 4-25
  application recovery 6-9
  automatic updates 2-21
  buttons 1-8, 4-13
  caveats
    alert tones 4-27
    application troubleshooting 8-28
    application usage 1-13
    CLI commands 8-11
    direct dial channels 4-31
    direct two-way channels 4-29
    DTMF tone generation 4-24

high latency, low bandwidth connections 5-13
installation 2-3
keyboard mapping 4-22
login 4-4
logs 7-6
multiselect 4-25
offline mode 4-7
password 4-5
skins 5-4
system recovery 6-4
touch screen skin 4-18
voice replay 4-33
VPN client 8-15
channels
appearance on PMC 4-16
customized color indicators 3-15
direct dial 3-12
direct two-way 3-12
focus 4-22
interactions 4-15
latch 4-17
latch permission 3-15
listen-only mode 3-15
reordering 4-28
secure indicator 3-15
states 4-18
support 3-11
terminology 3-12
traffic activity indicators 4-35
truncating names 3-14
using direct dial connections 4-30
using direct two-way connections 4-28
visual indicators 3-14
voice activity detection 3-16
checking for updates 2-22
client application 1-4
communications interruptions 6-5
configuration customization 1-12
configuring the application 5-1
disconnected mode 4-9
downloading the update 2-23
DTMF tone generation 4-24
end-user features 4-20
GUI 1-11
illustration 1-8
installation
caveats 2-3
installing the application 2-2
interactions
Cisco Security Agent 2-6
client-server 2-1
interface 1-7
interoperability features 3-1
joining a VTG 4-14
key assignments 4-21
key mapping 5-12
license requirements 4-6
locations

support 3-18
truncating names 3-18
logging in
caveats 4-4
local login 4-9
logging out 4-39
login information 4-1
logs
accessing the logs 7-3
accessing the submenu 7-2
caveats 7-6
describing the logs 7-7
examples 7-8
files 7-1
identifying the logs 7-1
using the logs 7-5
maintaining the application
process 2-16
maintaining version compatibility 2-17
managing alert tone upgrades 2-26
managing skin downloads 2-21
managing upgrades 2-22
managing version numbers 2-18
multiselect channels 4-25
offline mode 4-7
optimize audio for low bandwidth use 5-13
passwords
caveats 4-5
expiration 4-5
invalid login attempts 4-5
quality of service 2-13
recovering the system 6-1
recovery caveats 6-4
recovery scenarios 6-4
communications are down 6-8
network is down 6-8
server and RMS down 6-6
server down 6-5
server resumes operation 6-7
reverting to a previous version 2-27
scenarios
incident management 3-6
interactions 3-2
PMC user interaction 3-7
selecting channels 4-25
server status connection indicator 4-6
skin
caveats 5-4
mismatch 5-5
touch screen caveats 4-18
system requirements 1-17
troubleshooting
application 8-1
audio and headset issues 8-11
audio settings 8-7
caveats 8-28
channel activation issues 8-23
Cisco Security Agent 8-9

codec misconfiguration 8-24
coexistence 8-10
configuration file changes 8-6
connectivity issues 8-15
DNS issues 8-23
error messages 8-28
execution 8-2
footswitch device 8-7
generating a PMC installation log file 8-3
headset 8-8
headset issues 8-11
high latency, low bandwidth links 8-22
microphone 8-8
multicast connections 8-19
offline mode 8-21
one-way audio 8-10
one-way audio issues 8-12
optional settings menu 8-6
publisher error 8-14
resolving IP address changes 8-13
right-to-left and double-byte language support 8-25
RMS connectivity 8-21
satellite connectivity 8-22
using an encrypted file system 8-5
voice quality 8-14
VPN issues 8-15
Windows XP firewall 8-18
winsock corruption 8-20
uninstalling the application 2-28
upgrading the application
forced upgrades 2-23
messages 2-24
optional upgrades 2-23
process 2-16
types of upgrades 2-22
usage guidelines 4-2
USB devices
focus 4-21
footswitch 4-21
user privileges 3-16
using the logs 7-1
using the optional settings 5-15
version number management 2-18
voice quality tips 2-12
voice replay 4-32
PMC ID 1-19
PMC installation caveats 2-3
PTT latch 1-14
Push-to-Talk Management Center
See PMC

Q

quality of service 2-13

R

recovery scenarios 6-4

remote connection 3-19
reordering channels 4-28
reverting to a previous version of the PMC 2-27
right-to-left language support 8-25
RMS
  channel interaction 4-11
  connectivity 4-38
  description 1-5
  entries 4-8
  IP address 4-39
  PMC connectivity to the RMS 8-11
  SIP-based connectivity 8-23
  troubleshooting connectivity issues 8-21
router media service
  See RMS

S

satellite connectivity 5-13
scenarios 3-2
secure channel indicator 3-15
selecting channels 4-25
server
  commands 3-9
  connection status indicator 4-6
  dynamic configuration 4-14
  location support 3-18
  role 3-8
server commands
  channel list 3-9
  disable channel 3-10
  disable user 3-10
  mute user 3-10
  retrieve logs 3-10
  set logging level 3-10
server connection status indicator 4-6
server-PMC login sequence 4-6
SIP-based connection
  connection failure 8-24
  maximum allowable voice streams 3-19
  remote connection 3-19
  visual indicator for connection failures 3-19
skin caveats 5-4
skin mismatch 5-5
sorting channels 4-28
supported codecs 3-22
supported features 3-11
supported user roles 1-5
system administrator role 1-6
system interactions 1-19
system recovery 6-1
system recovery caveats 6-4

T

TAC Case Collection Tool 8-14
tips
  login caveats 4-4

optimizing your audio on the PMC 2-7
password caveats 4-5
PMC connectivity 4-3
using the PMC 4-2
using the PMC in offline mode 4-7
voice quality 2-12
touch screen skin caveats 4-18
traffic activity indicators 4-35
transmitting DTMF tones 4-24
troubleshooting the PMC application 8-1
truncating
channel names 3-14
location names 3-18

U

unicast
communications 3-17
connection 3-19
uninstalling the PMC application 2-28
updating the PMC application 2-22
upgrading the PMC
optional upgrade 2-23
required upgrade 2-25
types of upgrades 2-22
upgrade management 2-22
usage guidelines 4-2
USB devices 4-21
user channel activity interaction 4-37
user names 4-9
user permissions
advanced PMC permissions 3-17
allow latch 3-17
disable audio 3-17
listen-only 3-17
user privileges 3-16
user role 1-7
using PMC end-user features 4-20
using the headset 2-9
using the latch functionality 4-17
using the microphone 2-10
using the PMC buttons 1-8, 4-13
using USB devices with keyboard mapping 4-21

V

VAD 5-11
version compatibility 2-17
version number management 2-18
Virtual Talk Groups
See VTGs
visual indicators
connectivity status for SIP-based remote connections 3-19
server connectivity status 4-6
voice activity detection
See VAD
voice quality

issues 8-14
tips 2-12
voice replay
caveats 4-33
using 4-32
VTGs
channel 1-7
server-PMC interaction 4-14
states 1-21
user interaction states 4-18