Cisco IPICS PMC Installation and User Guide

Release 1.0(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-7698-01

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.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, 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. (0502R)

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface ix

- Introduction ix
- Audience x
- Organization x
- Related Documentation xi
  - Cisco CallManager Documentation xii
  - Cisco 7800 Series Media Convergence Servers Documentation xii
  - Cisco IP Phone Documentation xii
  - Cisco Land Mobile Radio over IP xiii
  - Cisco Security Agent xiii
  - Cisco IOS Documentation xiii
- Document Notes and Conventions xiii
- Obtaining Documentation xiv
  - Cisco.com xv
  - Product Documentation DVD xv
  - Ordering Documentation xv
- Documentation Feedback xvi
- Cisco Product Security Overview xvi
  - Reporting Security Problems in Cisco Products xvii
- Obtaining Technical Assistance xviii
  - Cisco Technical Support & Documentation Website xviii
  - Submitting a Service Request xix

Definitions of Service Request Severity xix
Obtaining Additional Publications and Information xx

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 1-4
About the PMC Application 1-6
Browser Support 1-9
Work Flow Activities 1-9
PMC Application Caveats 1-10
Architecture/Deployment 1-11
System Requirements for the PMC Application 1-13
Hardware Requirements 1-14
Software Requirements 1-14
System Interactions 1-15
Server Interactions 1-15
User Interactions 1-16

CHAPTER 2 **Installing and Upgrading the PMC Application 2-1**
PMC-Server Interactions 2-1
Installing the PMC Application 2-2
Installation Caveats 2-3
Downloading and Installing the PMC Application 2-3
Optimizing Your Audio on the PMC 2-11
Configuring the Audio Settings 2-11
Using a USB DSP Headset with the PMC 2-12
Using the Microphone with the PMC 2-14

Important Information about Using the Microphone 2-15
Checking the Microphone 2-15
Voice Quality Tips 2-16
Launching the PMC Application 2-17
Performing Additional PMC Tasks 2-19
Upgrading the PMC Application 2-20
Managing PMC Version Numbers 2-21
Checking for PMC Updates 2-23
Performing a Noncritical Upgrade 2-25
Downloading the PMC Update 2-25
Upgrading the PMC Application 2-26
Performing a Critical Upgrade 2-27
Reverting to a Previous Version of the PMC Application 2-28
Uninstalling the PMC Application 2-29

CHAPTER 3 **Using the PMC Application 3-1**
Scenarios for Using the PMC Application 3-1
Cisco IPICS Server-PMC Interaction Scenario 3-2
Incident Management Scenario 3-5
PMC User Interaction 3-6
Supported Features 3-7
Voice Interoperability 3-7
Channel Support 3-8
Channel Terminology 3-9
The Role of the Cisco IPICS Server 3-10
Implementing Policies 3-12
Location Support 3-13
Codec Support 3-15
Logging In to the PMC Application 3-16

Login Caveats 3-16
License Information 3-17
Server-PMC Login Sequence Interaction 3-17
PMC Offline Mode Caveats 3-18
PMC Login Procedure 3-19
Using the PMC Application 3-23
Accessing Online Help 3-23
Dynamic Configuration 3-24
Channel Interaction/Features 3-25
Cisco IPICS Server Commands 3-26
Support for Maximum Number of Channels 3-27
End-user Channel Interaction 3-28
Joining a VTG 3-30
Activating the PMC Buttons 3-30
Traffic Activity 3-33
Channel Traffic Activity Interaction 3-35
User Channel Activity Interaction 3-35
Logging Out of the PMC Application 3-36

CHAPTER 4 **Customizing the PMC Application 4-1**
Customizing the PMC End-User Interface 4-1
Configuring the PMC Skins 4-2
Skin Caveats 4-5
Configuring the Express and Channels Settings 4-6
Using the Optional Settings Menu 4-11

CHAPTER 5 **Recovering the PMC Application 5-1**
Support for Cisco IPICS Recovery 5-1
Recovering the PMC 5-2

Transparent Recovery Mechanism 5-2
System Recovery Caveats 5-3
PMC Recovery Scenarios 5-3
Cisco IPICS Server Down/PMC Up 5-4
Cisco IPICS Server and PMC Up/Communications Down 5-4
Cisco IPICS Server and PMC Up/Network Down 5-5
PMC Application Recovery 5-5

CHAPTER 6 **Using the PMC Application Logs 6-1**
Identifying the PMC Logs 6-1
Maintaining the PMC Log Files 6-1
Accessing the Logs Submenu Items 6-2
Accessing the PMC Logs 6-3
Using the PMC Logs 6-5
PMC Log Caveats 6-6
PMC Log Descriptions 6-7

CHAPTER 7 **Troubleshooting Tips for the PMC Application 7-1**
Troubleshooting PMC Application Problems 7-1
Resolving PMC Execution Issues 7-2
Generating a PMC Installation Log File 7-3
Making PMC Configuration File Changes 7-4
Using the PMC Optional Settings 7-5
Configuring the Audio Settings 7-5
Using a USB DSP Headset with the PMC 7-6
Checking the Microphone with the PMC 7-6
Using Cisco Security Agent with the PMC 7-7
PMC Coexistence with Other Voice Applications 7-8
Troubleshooting One-Way Audio 7-8

Using CLI Commands to Resolve Headset Issues 7-9
Resolving IP Address Changes 7-10
Troubleshooting Voice Quality Issues 7-11
Troubleshooting PMC Connectivity Issues 7-12
Troubleshooting VPN Connectivity 7-12
Using the PMC with the Windows XP Firewall 7-15
Troubleshooting Multicast Communications Issues 7-16
Troubleshooting Winsock Corruption Issues 7-17
Troubleshooting Offline Mode Issues 7-17
Resolving Name Resolution Failures 7-18
Identifying Channel Activation Issues 7-18
Resolving Codec Mismatch Issues 7-19
Support for Right-to-Left Languages 7-20
PMC Application Caveats 7-21
Analyzing PMC Error Conditions 7-22

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 IP reachability 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 x
- Organization, page x
- Related Documentation, page xi
- Document Notes and Conventions, page xiii
- Obtaining Documentation, page xiv

- Documentation Feedback, page xvi
- Cisco Product Security Overview, page xvi
- Obtaining Technical Assistance, page xviii
- Obtaining Additional Publications and Information, page xx

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 to 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, "Using the PMC Application"	This chapter provides information about using the PMC application.
Chapter 4, "Customizing the PMC Application"	This chapter provides information about customizing the PMC end-user interface.
Chapter 5, "Recovering the PMC Application"	This chapter provides information about the actions that you can take to recover the PMC application under specific circumstances.

Chapter 6, "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 7, "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 Guide, Release 1.0(1)*—This document provides tips and quick references for the most frequently used procedures that a user can perform on the Cisco IPICS PMC.
- *Cisco IPICS PMC Debug Reference Quick Start Guide, Release 1.0(1)*—This document provides a quick reference for troubleshooting and debugging the Cisco IPICS PMC.
- *Cisco IPICS Server Administration Guide, Release 1.0(1)*—This document contains information about the key configuration, operation, and management tasks for the Cisco IPICS server.
- *Cisco IPICS Server Installation Guide, Release 1.0(1)*—This document describes how to install and configure the Cisco IPICS server software and Linux operating system.
- *Cisco IPICS Troubleshooting Guide, Release 1.0(1)*—This document contains reference material about how to maintain and troubleshoot the Cisco IPICS system.
- *Cisco IPICS Backup and Restore Guide, Release 1.0(1)*—This document describes the administrative procedures that you use to backup and restore the database files on the Cisco IPICS server.
- *Cisco IPICS Command Line Interface, Release 1.0(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 1.0(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 1.0(1) Resources Card (Documentation Locator)*—This document provides a summary of the documentation that is available for this release of Cisco IPICS.
- *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 CallManager Documentation

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

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/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 IP Phone Documentation

For information about Cisco 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.
{**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. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

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

http://www.cisco.com/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

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

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

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

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

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

From this site, you can perform these tasks:

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

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

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

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

Reporting Security Problems in Cisco Products

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

- Emergencies—security-alert@cisco.com

  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.

- 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 to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one 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.

Obtaining Technical Assistance

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

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

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

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco 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)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

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

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

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

Obtaining Additional Publications and Information

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, 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

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help

solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

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

or view the digital edition at this URL:

http://ciscoiq.texterity.com/ciscoiq/sample/

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

  http://www.cisco.com/ipj

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

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

- Networking Professionals Connection is an interactive website for networking professionals to 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

- 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 1-13
- System Interactions, page 1-15

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 1-6
- Architecture/Deployment, page 1-11

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 the Cisco IP Phone models 7960 and 7970.

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 1-4

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 (based on Red Hat Linux) on selected Cisco Media Convergence Server (MCS) platforms. (Refer to the Cisco 7800 Series Media Convergence Servers data sheets, or contact your Cisco representative, for information about the servers that Cisco IPICS supports.) The Cisco IPICS server software includes the Cisco IPICS Administration Console, which is an incident management framework administration GUI that enables dynamic resource management for users, channels, and VTGs. (In Cisco IPICS, VTGs combine one or more channels and/or users.) By using this GUI, authorized Cisco IPICS users can manage the system configuration and authentication and security services, policies and privileges, and database information. In addition, the server enables control of the configuration of the media resources that are installed in the router and which are used for audio mixing capabilities. See the "Cisco IPICS User Roles" section on page 1-4 for more information about the various user roles that Cisco IPICS supports.

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 LMR 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 attach to based on specific incidents.) The PMC runs on the Microsoft Windows 2000 and Windows XP operating system. See the "System Requirements for the PMC Application" section on page 1-13 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.
Router Media Service	The Router Media Service (RMS) component enables the PMC to remotely attach to a VTG. It also provides support for remotely attaching (combining) two or more VTGs through its loopback functionality. The RMS provides support for mixing multicast channels in support of VTGs and for mixing remote PMC SIP-based (unicast) connections to a multicast channel or VTG. The RMS can be installed as a stand-alone component (RMS router) or as an additional feature that is installed in the LMR gateway.
Networking Components	The Cisco IPICS solution also includes various network components. Examples of these components include switches, routers, firewalls, mobile access routers, and wireless access points and bridges.
Cisco CallManager and VoIP Services	Cisco CallManager functionality and VoIP services help to extend the reach of PTT technology to the IP network. These services allow participation in VTGs through the use of the Cisco IP Phone 7960 and Cisco IP Phone 7970 by enabling these phones to work with Cisco IPICS as IP phone multicast client devices.

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, 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 3-2.

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.
Operator	The operator is responsible for setting up and managing users, configuring access privileges, and assigning user roles and ops views.
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 users, as necessary, and sets up system policies.
User	The Cisco IPICS user may set up personal login information, download the PMC application, customize the PMC skin, and specify communication preferences that are used to configure audio devices. By using a predefined user ID and profile, the user can participate in PTT channels and VTGs by using the PMC or a supported Cisco IP Phone model.

Related Topics

- About the PMC Application, page 1-6
- PMC Application Caveats, page 1-10
- Architecture/Deployment, page 1-11
- System Requirements for the PMC Application, page 1-13
- System Interactions, page 1-15
- Cisco IPICS Server-PMC Interaction Scenario, page 3-2

About the PMC Application

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

- Browser Support, page 1-9
- Work Flow Activities, page 1-9
- PMC Application Caveats, page 1-10

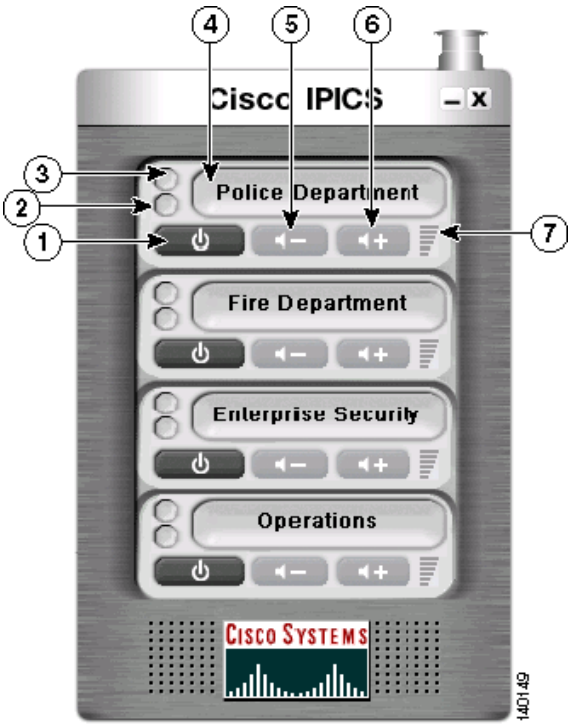
The PMC application provides the interface for users to host push-to-talk audio communications. By using a simplified GUI, the PMC allows simultaneous monitoring and participation in one or more talk groups or VTGs at the same time.

The 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 2-3.

You can customize the appearance of the PMC user interface by choosing another Cisco-provided or custom skin. For more information, see the "Customizing the PMC End-User Interface" section on page 4-1.

See Figure 1-1 for an illustration of the PMC application. This example shows the PMC configured for mouse-based use with the 4-channel skin.

Figure 1-1 PMC with 4-Channel Mouse Skin



1	Activation/ Deactivation button	Click this button to activate a channel (to call out); click again to deactivate. For more information about the PMC buttons, see the "Activating the PMC Buttons" section on page 3-30.
2	Transmit indicator	This indicator blinks red when the PMC is transmitting traffic. For more information about traffic activity indicators, see the "Traffic Activity" section on page 3-33.
3	Receive indicator	This indicator blinks green when the PMC is receiving traffic.

4	PTT Channel button	This is the PTT button and the PMC receive (green) and transmit (red) indicators. Click with your mouse, or push, the **PTT** button and hold it to talk. When you are done talking, release the left mouse button to return to listen-only mode. You can also latch this button to talk on one or more channels at the same time. To clear the latch, click the **PTT** button to release and return to listen-only mode.
5	Volume Down button	Click this button to decrease the volume on the channel.
6	Volume Up button	Click this button to increase the volume on the channel.
7	Volume level indicator bar	This bar shows the current volume level on the channel in a graphical format.

The PMC GUI includes buttons that allow you to interact with the Cisco IPICS server. It also includes various indicators to 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 buttons to activate the channel and control the volume level. It also includes indicators that blink when you receive and transmit traffic. See the "Traffic Activity" section on page 3-33 for more information about these indicators.
- 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 customize the PMC

GUI skins for mouse-based or touch screen-based display. Based on your preference, you can use the mouse or touch screen to select and control functions on the PMC application.

Note See Chapter 4, "Customizing the PMC Application," for additional information about customizing the end-user interface.

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 access to the server via the Internet by using the following supported browser:

- Internet Explorer 6.0.2 or later

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 dispatcher sets up the necessary VTGs and channel definitions on the server.
2. The PMC then retrieves the personalized list of channels 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 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 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 3-17 for more information about these licensing requirements.
- Each PMC application connects to only one Cisco IPICS server.
- The dispatcher assigns the voice channels that you can use on your PMC application, as they are needed. (The voice channels that the dispatcher assigns to you display a channel name on the PMC.) The dispatcher also creates, 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 channel(s) that were created to support the VTG(s).
- The PMC application does not provide support for the creation of ad hoc VTGs; that is, there is no support for direct PMC-to-PMC connectivity.

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. To latch, or lock in, the PTT button, 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.

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.

See Chapter 3, "Using the PMC Application" and Chapter 4, "Customizing the PMC Application" for detailed information about using and customizing the PMC application.

Related Topics

- Installing the PMC Application, page 2-2
- Launching the PMC Application, page 2-17
- Upgrading the PMC Application, page 2-20
- Logging In to the PMC Application, page 3-16
- License Information, page 3-17
- Using the PMC Application, page 3-23
- Customizing the PMC End-User Interface, page 4-1

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 through a wired or wireless network. The additional components, such as routers and gateways, enable interoperability and additional capabilities. (See Figure 3-1 on page 3-8 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.

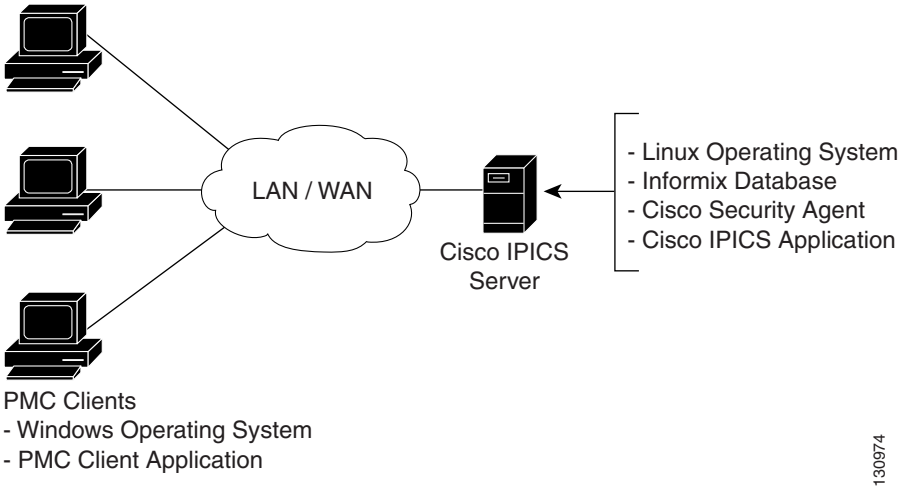
As a part of the login process, all user configuration information is downloaded and stored in conjunction with the login credentials. If the PMC becomes disconnected from the Cisco IPICS server, a user with a valid login may continue to use the application in offline mode.

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 the user with the tools 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 performs a drag-and-drop operation to include 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 Cisco IPICS server. 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 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 appropriate 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 3-13.
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 3-1
- Location Support, page 3-13

System Requirements for the PMC Application

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

- Hardware Requirements, page 1-14
- Software Requirements, page 1-14

Hardware Requirements

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

The PMC application requires the following minimum requirements:

- 300 MHz Pentium III class, including Mobile Pentium
- 256 MB RAM
- 16 MB free space
- Network interface card

Software Requirements

Table 1-3 shows the software and applications that you install on your PMC system.

Table 1-3 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 1-15
- User Interactions, page 1-16

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 frequency 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 "Upgrading the PMC Application" section on page 2-20 and "Dynamic Configuration" section on page 3-24 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 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 3-12 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. See Table 3-3 on page 3-27 for a list of the PMC skins that this release of Cisco IPICS supports.

For more information about configuring the PMC skins, see the "Configuring the PMC Skins" section on page 4-2.

End-User Channel Interaction

The VTG channel is the most fundamental type of channel option; it may display on the PMC in one of the states that are described in Table 1-4.

For more information about using the PMC application, see Chapter 3, "Using the PMC Application."

Table 1-4 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 PTT button will not highlight.
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 grayed-out but you may press the Activate button to activate the channel.

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

VTG/Channel State	PMC Button Indication	Description
Disabled	No PMC buttons appear highlighted and you cannot activate the channel	When a channel is disabled, all of the PMC buttons are grayed-out or muted so that you cannot activate the channel. However, you can still view the channel or VTG label, if one was configured in the server.
Unassigned	No PMC buttons appear highlighted and you cannot activate the channel	A channel that is unassigned appears on the PMC with all of the buttons grayed-out and no channel name. You cannot activate or use an unassigned channel.

Related Topics

- PMC-Server Interactions, page 2-1
- Upgrading the PMC Application, page 2-20
- Implementing Policies, page 3-12
- Dynamic Configuration, page 3-24
- Using the PMC Application, page 3-23
- Channel Interaction/Features, page 3-25
- Configuring the PMC Skins, page 4-2

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 2-11
- Launching the PMC Application, page 2-17
- Performing Additional PMC Tasks, page 2-19
- Upgrading the PMC Application, page 2-20
- Reverting to a Previous Version of the PMC Application, page 2-28
- Uninstalling the PMC Application, page 2-29

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 provide the Cisco IPICS server information along with skin and user configuration data. (The skin information specifies the "look and feel" of the PMC end-user interface.) For more information about the PMC skin, see the "Customizing the PMC End-User Interface" section on page 4-1.
- Upon login to the PMC, 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 2-21 for more information about version management. PMC upgrades can be in the form of noncritical or critical upgrades. See the "Performing a Noncritical Upgrade" section on page 2-25 and the "Performing a Critical Upgrade" section on page 2-27 for more information.

Related Topics

- System Interactions, page 1-15
- Configuring the PMC Skins, page 4-2

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 1-13 for information about hardware and software requirements.

This section includes the following topics:

- Installation Caveats, page 2-3
- Downloading and Installing the PMC Application, page 2-3

Installation Caveats

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 default skins, from the Cisco IPICS server.
- The PMC installation program automatically runs the PMC installation file to install the PMC software on your client machine.
- The PMC performs preinstallation version checks to ensure compatibility.
- During the installation process, the PMC may be offline.
- The installation automatically adds an entry to the Windows Start menu for "Cisco IPICS PMC" along with a desktop shortcut.
- The system retains a copy 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 2-21 for information about the number of versions that may be retained.)
- The PMC retrieves your configuration data from the Cisco IPICS server, which maintains the most current information.

Downloading and Installing the PMC Application

The PMC application uses Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS) to ensure secure communications between the browser on 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 1-6 for more information about supported browsers.)

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:

http://<*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.

Figure 2-1 shows an illustration of the Cisco IPICS server login window.

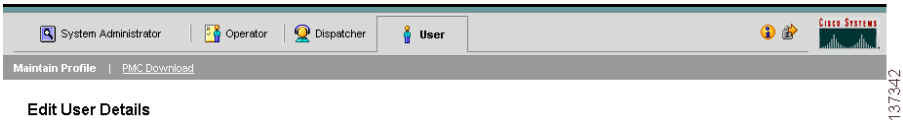
Figure 2-1 Cisco IPICS Server Login Window

The User menu on the Cisco IPICS server displays.

Step 4 Click the **PMC Download** link that displays near the top of the User menu window.

Figure 2-2 shows an illustration of the Cisco IPICS User window that displays the PMC Download link.

Figure 2-2 PMC Download on the Cisco IPICS User Window

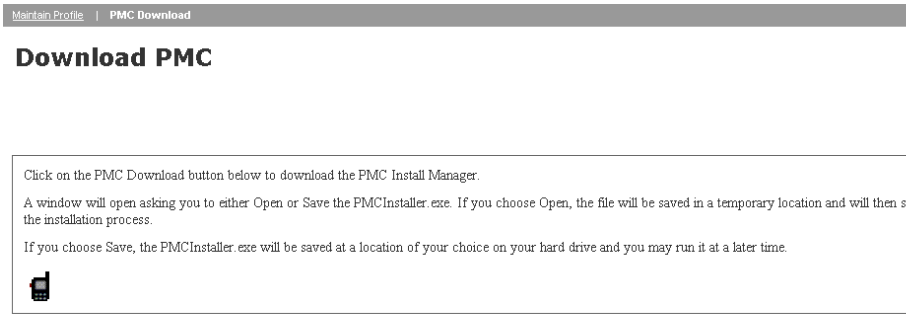


The Download PMC dialog box displays.

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

Figure 2-3 shows an illustration of the download PMC dialog box.

Figure 2-3 Download PMC Dialog Box



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**.

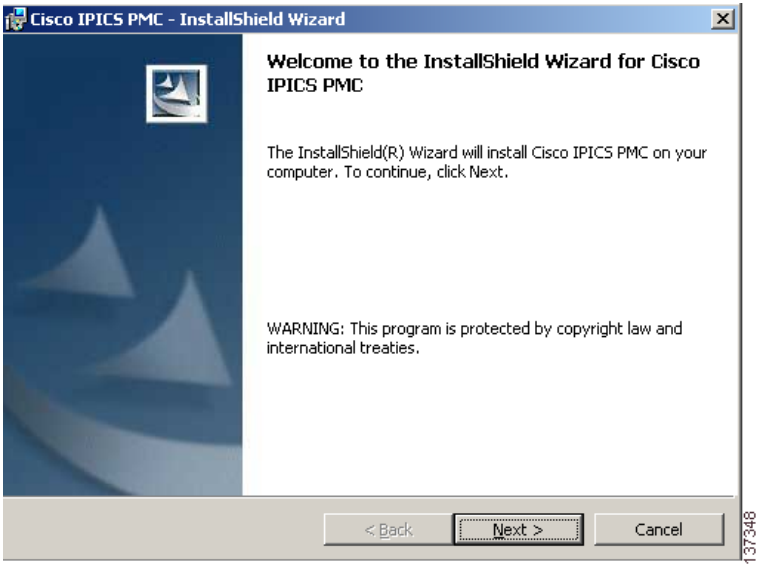
Step 8 Navigate to the directory where you saved the PMC installation program and double-click **pmcsetup.exe** to extract the PMC installation file and the PMC configuration file, and to automatically run the installation executable to install the PMC on your client machine.

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 7-3.

The Cisco IPICS PMC InstallShield Wizard displays.

Figure 2-4 shows an illustration of the Cisco IPICS PMC InstallShield Wizard.

Figure 2-4 PMC InstallShield Wizard



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**.

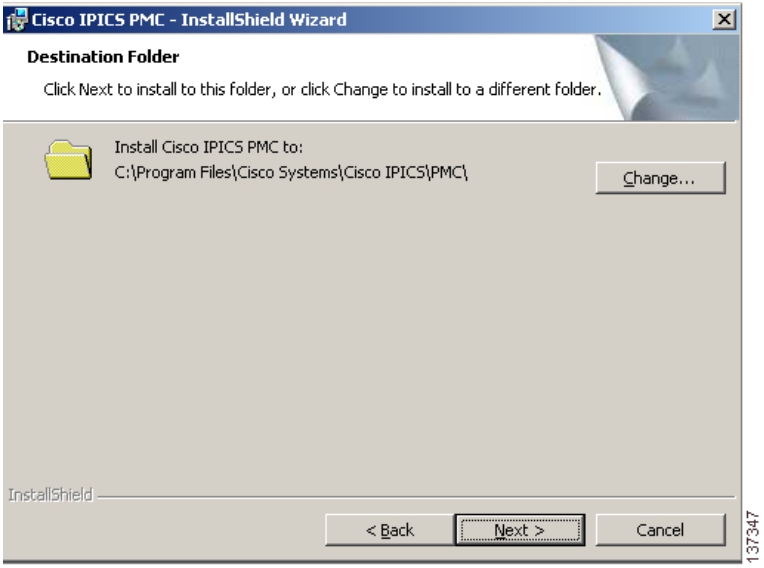
The destination folder window displays.

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.

Figure 2-5 shows an illustration of the PMC destination folder window.

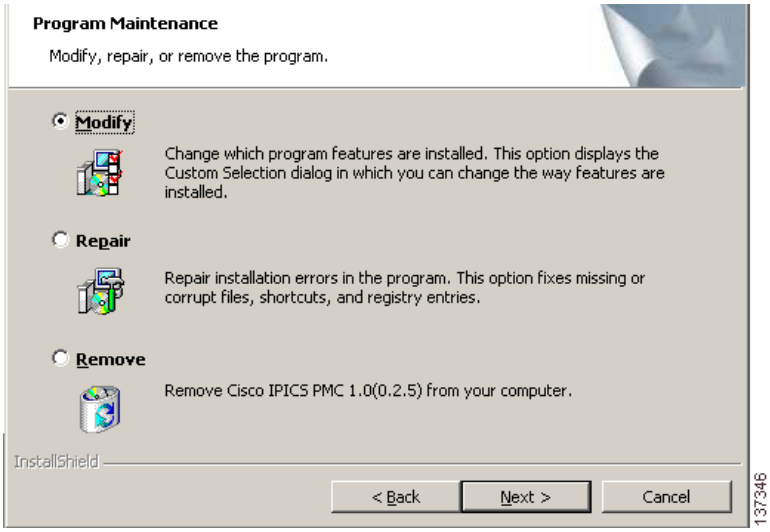
Figure 2-5 PMC Installation Destination Folder



Note 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.

Figure 2-6 is provided as a reference to show an illustration of the PMC program maintenance window. This window only displays if you have the same version of the PMC already installed on your client machine.

Figure 2-6 PMC Program Maintenance Window



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

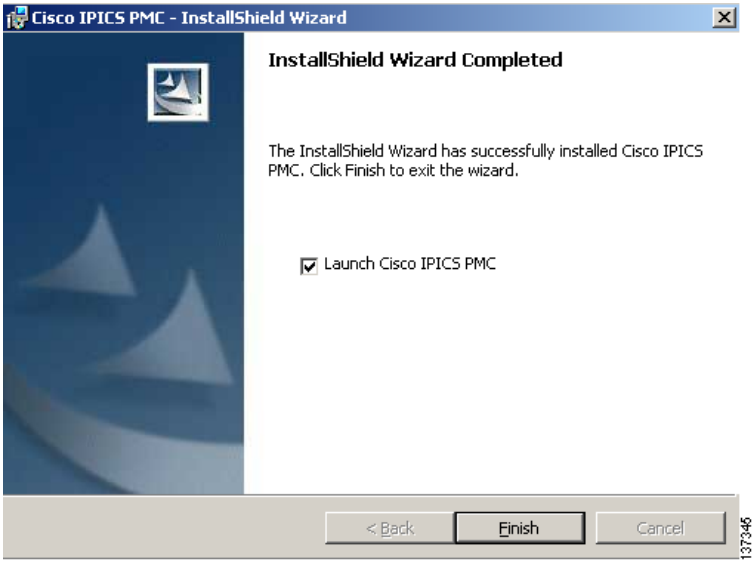
Step 13 Click **Finish** to exit the Cisco IPICS PMC InstallShield Wizard.

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\IPICS PMC\PMC**.

Figure 2-7 shows an illustration of the PMC installation completion window.

Figure 2-7 PMC Installation Complete



Tip The installation process places a shortcut on the Start menu, along with a desktop shortcut. 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 2-11
- Using a USB DSP Headset with the PMC, page 2-12
- Using the Microphone with the PMC, page 2-14
- Voice Quality Tips, page 2-16

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 On Windows 2000 client machines, navigate to **Start > Settings > Control Panel > Sounds and Multimedia**.

The Sounds and Multimedia Properties window displays.

a. Click the **Audio** tab.

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

c. Click **OK**.

Step 2 On Windows XP client machines, 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**.

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 7-8 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.

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

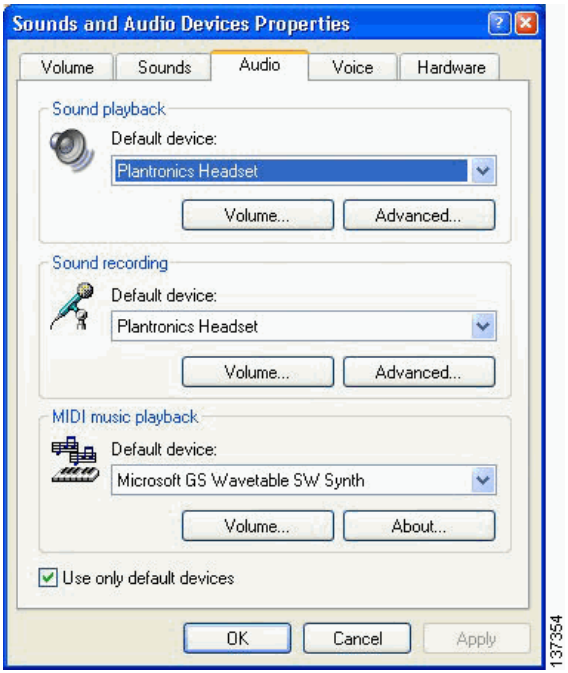
a. Configure the Windows audio settings to set the USB DSP headset as the default device by choosing the device from the drop-down list box.

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

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

Figure 2-8 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 2-8 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 2-15
- Checking the Microphone, page 2-15

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 uses 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 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.

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.
- For enhanced voice quality, make sure that you plug your USB headset or audio device into a dedicated USB port instead of a USB hub. The use of USB hubs, which multiplex data from USB devices into one data stream, can result in timing issues and impact voice quality.
- Check your audio settings to make sure that the volume is not set too low. If the volume is set low, increase the input gain on your microphone by sliding the bar up on the volume controls to increase the volume.

- For optimum connectivity, use the most appropriate location for your connection type when you log in to the PMC. For example, if you are using a wireless connection, choose the location that correlates to wireless connectivity for your organization. You can ensure higher quality audio by choosing the appropriate connection type.
- Make sure that you always use the most recent version of the PMC. Newer versions of software often contain voice quality updates that enhance functionality.
- Be aware that a slow-speed connection, such as a digital subscriber line (DSL) connection or any slow wired link, may affect voice quality. If possible, try to use a high-speed connection when you use the PMC.
- Try to limit the use of high-bandwidth applications on the PMC client machine at the same time that you use the PMC. If your CPU is overburdened by other programs that are running at the same time, there may insufficient CPU cycles for the PMC to run properly. Check the CPU activity on your PMC client machine and close any programs that do not need to be open.

For more information about voice quality issues and tips, see Chapter 7, "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 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

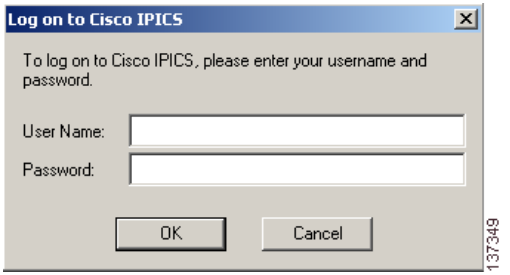
(microphone). If the "Don't ask me again" check box displays as an option, you may check it to instruct CSA not to prompt you again in the future.

Note Be aware that if you allow CSA to time-out based on its default value of No, the PMC 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.

The Cisco IPICS login dialog box displays.

Figure 2-9 shows an illustration of the Cisco IPICS login dialog box.

Figure 2-9 Cisco IPICS Login Dialog Box



Step 2 Enter your **user name** and **password**; then, click **OK**.

Tip Be aware that user names and passwords are case-sensitive.

The location selection dialog box displays.

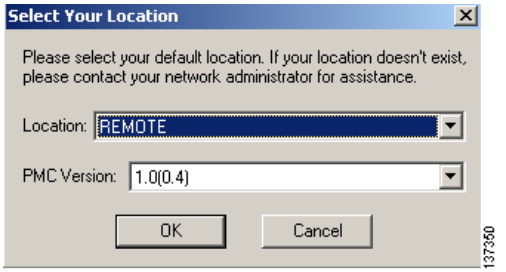
Step 3 Choose your default location and your PMC version from the drop-down list boxes; then, click **OK**.

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

Note 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.

Figure 2-10 shows an illustration of the location selection dialog box.

Figure 2-10 Location Selection Dialog Box



The PMC application opens on your desktop. For information about using the PMC application, see Chapter 3, "Using the PMC Application."

Related Topics

- About the PMC Application, page 1-6
- System Requirements for the PMC Application, page 1-13
- Location Support, page 3-13
- Using the PMC Application, page 3-23

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 a noncritical update at a later time.	Downloading the PMC Update, page 2-25
Upgrade the PMC application	This task upgrades the PMC application when you choose to perform a noncritical upgrade at a later time.	Upgrading the PMC Application, page 2-26
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 2-28

Related Topics

- Downloading the PMC Update, page 2-25
- Upgrading the PMC Application, page 2-26
- Reverting to a Previous Version of the PMC Application, page 2-28

Upgrading the PMC Application

This section describes the upgrade process for the PMC application and includes the following topics:

- Managing PMC Version Numbers, page 2-21
- Checking for PMC Updates, page 2-23
- Performing a Noncritical Upgrade, page 2-25
- Performing a Critical Upgrade, page 2-27

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.

Managing PMC Version Numbers

Because the Cisco IPICS server maintains information about version compatibility, the system supports the ability to perform version upgrades to the next release of software, along with the ability to revert to an earlier compatible version.

To ensure version compatibility, the Cisco IPICS server regularly provides information to the PMC about version availability. The system then performs a version check of major and minor version upgrades.

- The PMC client system can maintain multiple versions, current and previous, of the PMC application. (The system retains the previous versions in the event that you need to revert to an earlier installed version.)
- Upon login, the server communicates the following version information to the PMC, as described in Table 2-2:

Table 2-2 Cisco IPICS Server -PMC Version Information

Version Information	Description
Minimum version	This version represents the minimum software version that is required to run on the PMC.
Maximum version	This version represents the maximum software version that is available to run on the PMC.
Recommended version	This version represents the recommended software version that should be run on the PMC.
Current version	This version represents the most current software version on the PMC, which is the most recent software version that the PMC downloaded from the server.
Number of versions	This number signifies the number of PMC versions that the PMC should maintain.
Polling rate	This number signifies the polling rate (time interval) at which the PMC checks the server for changes that need to be downloaded.

- When the PMC starts up, it applies this version information to the existing versions that are installed on the PMC client machine hard drive. The PMC automatically deletes all versions prior to the minimum version. The PMC

then deletes additional previous versions until the number of versions to maintain matches the information that is configured in the server. For example, if the server configures the number of versions to maintain as two, then the last two most recent versions of the PMC are retained.

- If the PMC has deleted all versions from the PMC client machine, a pop-up dialog box displays to inform you that you do not have a valid version of the PMC and asks if you would like to download and run the latest version of the PMC software.
- If your PMC client machine does not have a version of the PMC software that is greater than or equal to the recommended version, a pop-up dialog box displays to inform you that your version is not the recommended version and asks if you would like to download the recommended version.
  - When you click **Yes** to this prompt, the PMC.DLL file for the recommended version downloads to the following directory on the PMC client machine:

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

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

- When new upgrades become available, and based on version compatibility, the PMC may be forced to download and upgrade a new version immediately (critical upgrade) if the system detects version incompatibility. Alternatively, an option may be provided to download and upgrade a new version at a later time (noncritical upgrade).

Note The current version of the PMC application continues to operate when a new version becomes available as long as the upgrade is not critical.

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 application.

Step 2 Position your cursor so that it is located inside the PMC window; then right-click inside this window.

A list of options displays.

Step 3 Click **About**.

The version information for your PMC application displays.

Step 4 Click **OK** to exit the window.

Note Cisco IPICS does not support automatic downgrades of the PMC application when you have downloaded noncumulative versions from the server. (You can identify noncumulative versions by the release numbers, which appear out of sequence.) If you need to downgrade to a PMC version that is earlier than the currently installed version, and if you have been running noncumulative versions, you must uninstall the current PMC before you can install a downgraded version. For information about how to uninstall the PMC application, see the "Uninstalling the PMC Application" section on page 2-29.

Checking for PMC Updates

At regular intervals, the PMC receives update information from the server. When updates become available, the Cisco IPICS server automatically notifies the PMC and a pop-up message displays to alert you.

For information about PMC automatic updates, see the "Managing PMC Version Numbers" section on page 2-21.

Cisco IPICS supports the following types of upgrades:

- Noncritical upgrades
- Critical upgrades

Note When a critical upgrade must be installed, the system automatically downloads the PMC application update immediately and upgrades the software in the background; you do not need to take any action. Be aware that network performance might be impacted during this time.

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
Noncritical Upgrades	If the upgrade is considered noncritical, you can 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 a Noncritical Upgrade" section on page 2-25.
Critical Upgrades	There may be situations where the system detects a version incompatibility or another emergency situation. In these cases, the PMC application must be upgraded immediately; a warning message displays to alert you of the necessity to download the critical update. The download and upgrade procedures then run automatically.	For more information, see the "Performing a Critical Upgrade" section on page 2-27.

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 you need are enabled. For more information about how to identify, access, and use these logs, see Chapter 6, "Using the PMC Application Logs."

Performing a Noncritical Upgrade

This section describes the process that you need to follow to perform a noncritical upgrade of the PMC and includes the following topics:

- Downloading the PMC Update, page 2-25
- Upgrading the PMC Application, page 2-26

When you log in to the PMC, the Cisco IPICS server sends information about the minimum, maximum, recommended, and current PMC versions, as described in the "Managing PMC Version Numbers" section on page 2-21. If the currently-installed PMC version is newer than the minimum version but older than the latest version, the system prompts you to download and install the upgrade. When you choose to download and install the upgrade, the system performs this activity automatically. After the installation has completed, you will have the option to choose the new version.

Upgrade tasks for the PMC involve the following steps:

1. Downloading the PMC update files from the Cisco IPICS server to the PMC client machine—For more information, see the "Downloading the PMC Update" section on page 2-25.
2. Upgrading the PMC software on the PMC client machine—For more information, see the "Upgrading the PMC Application" section on page 2-26.

Downloading the PMC Update

When a noncritical update becomes available for the PMC, you have the option 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 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 In addition, the PMC will prompt 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:

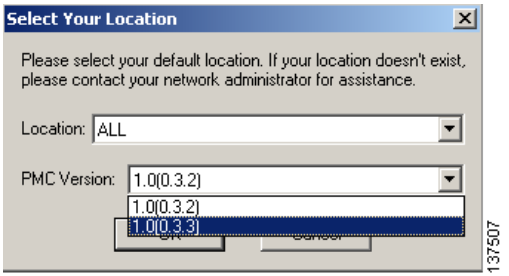
- **Yes**—Choose this option to instruct the PMC application to upgrade.
- **No**—Choose this option to instruct the PMC application to not upgrade now and to prompt you at a later time.

Note In addition, the PMC will prompt you to perform the upgrade every time that you log in.

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

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

Figure 2-11 PMC Version Dialog Box



Tip 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.

Note 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.

Performing a Critical Upgrade

The system typically requires an immediate upgrade of the PMC application when the Cisco IPICS application has been upgraded to a version that is not compatible with the PMC application or in other emergency situations.

If an immediate upgrade of the PMC is required, a message alerts you. The critical 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 and you can choose your default location and the upgraded PMC version from the location selection dialog box. (The system ensures that the new version maintains the same state as the previous version.)

Related Topics

- Identifying the PMC Logs, page 6-1
- Using the PMC Logs, page 6-5

Reverting to a Previous Version of the PMC Application

When you upgrade the PMC application, the PMC maintains a copy 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 current Cisco IPICS application.

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 2-17.

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 2-17

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*

Using the PMC Application

This chapter provides information about using the PMC, including logging in and logging out of the application. It also includes information about supported features and specific terminology that the Cisco IPICS solution uses.

This chapter includes the following sections:

- Scenarios for Using the PMC Application, page 3-1
- Supported Features, page 3-7
- Logging In to the PMC Application, page 3-16
- Using the PMC Application, page 3-23
- Logging Out of the PMC Application, page 3-36

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 3-2
- Incident Management Scenario, page 3-5
- PMC User Interaction, page 3-6

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 2-3.

   The Cisco IPICS server checks the license count for concurrent license usage. See the "License Information" section on page 3-17 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 2-17.

   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 2-21.

6. The PMC sends a request to the server to authenticate the user. See the "Server-PMC Login Sequence Interaction" section on page 3-17.
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, and 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 customization information, including the order preference for displaying the channels. See the "Channel Interaction/Features" section on page 3-25.

9. The PMC user may perform minimal PMC customization, such as setting the PMC skin. For more information about customizing the PMC, see the "Customizing the PMC End-User Interface" section on page 4-1.

   After the PMC changes are saved, the PMC sends the updated configuration settings to the server.

10. The PMC user can use only the voice channels that the dispatcher assigns. The PMC user can choose to activate any of the assigned channels.

Note The PMC only displays those channels that have been assigned by the dispatcher. 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.

   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 3-12.

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 Cisco IPICS server. 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.)

    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 3-13 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 The PTT latch functionality provides the ability to talk on multiple channels at the same time. To latch, or lock in, the PTT button, 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, press the **PTT** button without holding the Shift key.

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.

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.

Note Based on the updates from the server, the PMC display refreshes automatically to reflect the changes that were made by the dispatcher (such as the activation of a new VTG or the deactivation of a VTG that has ended).

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 6-5 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 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. With a simple drag-and-drop operation on 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, with a simple drag-and-drop operation on 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 order of the channels, as they display on the PMC, is determined by the server. (The PMC display refreshes automatically based on the configuration that it retrieves from the Cisco IPICS server. If a channel has been disabled by the server, you will not be able to activate the channel.)
2. 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 Cisco IPICS server. After the connection has been established, the remaining PMC buttons, including the PTT 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.)
4. The PMC user clicks the **PTT** button to talk and releases the button to invoke listen-only mode.
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 1-11
- Launching the PMC Application, page 2-17
- Location Support, page 3-13
- Server-PMC Login Sequence Interaction, page 3-17
- Channel Interaction/Features, page 3-25
- Joining a VTG, page 3-30
- Activating the PMC Buttons, page 3-30

Supported Features

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

- Voice Interoperability, page 3-7
- Channel Support, page 3-8
- Location Support, page 3-13
- Codec Support, page 3-15

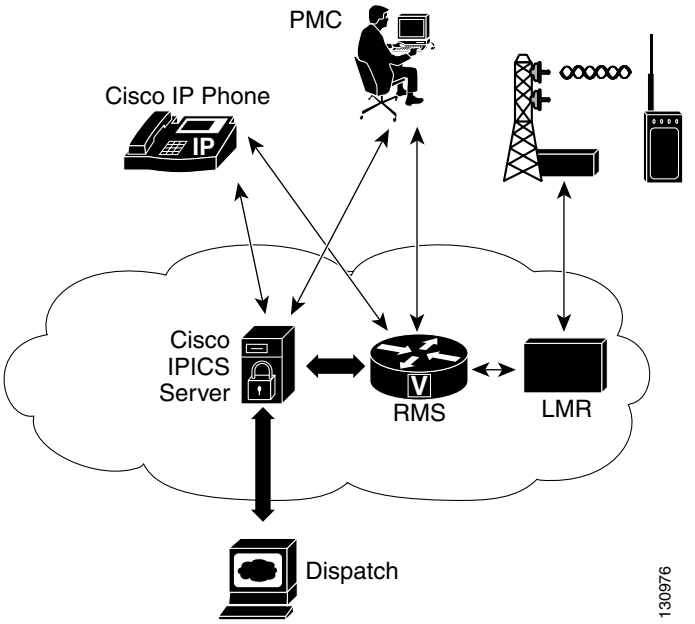
Voice Interoperability

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

As a PC-based software application, the PMC comprises a stand-alone LMR 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 1-11.

Channel Support

This section includes information about the types of channels that Cisco IPICS supports. It describes the following topics:

- Channel Terminology, page 3-9
- The Role of the Cisco IPICS Server, page 3-10
- Implementing Policies, page 3-12

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 send/receive feedback, volume control, and an activation control button that toggles on and off.

Table 3-1 describes the terminology that Cisco IPICS uses.

Table 3-1 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. The name may change, based on the configuration in the Cisco IPICS server.
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

Table 3-1 Cisco IPICS Terminology (continued)

Term	Description
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 3-13 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 Cisco IP Phone 7960 or Cisco IP Phone 7970.

The Role of the Cisco IPICS Server

Cisco IPICS authorized personnel register, assign, activate, and deactivate channels in the Cisco IPICS server. These activities affect the channel, configuration, and connection information for your PMC in addition to the level of your user privileges.

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 the administrator assigns to the channel and defines in the server.

Note If the channel name includes more characters than what the PMC can display, the PMC truncates the name and adds an ellipsis (...) next to the name.

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 is determined by the server.

The system administrator performs most of the configuration tasks for the PMC application; however, you may customize the PMC skin for your own "look and feel." To customize the PMC skin, navigate to the **Settings > Skin** menu on the PMC.

Note To access the Skin submenu, move your cursor so that it is positioned over the PMC that displays on your desktop; then, right-click anywhere inside the PMC window and click **Settings > Skin**. For more information about customizing the PMC skin, see the "Customizing the PMC End-User Interface" section on page 4-1.

The Cisco IPICS server 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.

Note Be sure to pre-qualify 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 7-16.

- 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 3-13.

For more information about the multicast technology, refer to the following URL: http://www.cisco.com/warp/public/732/Tech/multicast/.

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 obtain privileges to all channels in that VTG for the duration of the VTG.
- After the dispatcher deactivates a VTG that has ended, the PMC display refreshes automatically, based on the updates that it receives from the server, and removes the VTG from your PMC.

Implementing Policies

Cisco IPICS 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
- 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 VTGs.

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

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.

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 specifies 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 specifies a location whenever a new channel, VTG, or user is added to the system.

1. 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 that channel.

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

   a. 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.

      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.

   b. 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 7-16 for information about troubleshooting multicast communications.

3. 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. See the "Launching the PMC Application" section on page 2-17 for more information about choosing your location.

   This prompt occurs only one time per PMC instance and immediately after your initial login.

4. You choose a location that corresponds to the type of connection that you will use on that channel.

   a. The server uses this location to specify the type of channel communication (SIP-based unicast or multicast) that is appropriate for the location.

   b. 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.

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 7-19.

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 1-11
- Launching the PMC Application, page 2-17
- Location Support, page 3-13
- Customizing the PMC End-User Interface, page 4-1
- Troubleshooting Voice Quality Issues, page 7-11

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 2-17 for more information and an illustration of the login prompt window.

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

- Login Caveats, page 3-16
- License Information, page 3-17
- Server-PMC Login Sequence Interaction, page 3-17
- Related Topics, page 3-23

Login Caveats

The following login caveats apply to this release of Cisco IPICS:

- 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.
- Any number of valid Cisco IPICS users can use the same PMC application, but not concurrently. See the "License Information" section on page 3-17.
- The PMC application always logs in to the same Cisco IPICS server; that is, the server that has been configured as the default server and from which the PMC installation file has been downloaded. To change servers, you must reinstall the PMC application from a different Cisco IPICS server.

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. 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.

Note Cisco IPICS does not prevent you from logging in to the PMC application if the connection to the server goes offline.

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

- PMC Offline Mode Caveats, page 3-18
- PMC Login Procedure, page 3-19

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. The following caveats apply to the PMC offline mode:

- You must have at least one successful login to the server before you can use the PMC in offline mode.
- If the server goes offline while you are running the PMC, the system displays a message to alert you that the server is not available. The PMC enters offline mode with the current list of channels.
- If the server is offline when you start the PMC, the system displays a message to alert you. The PMC enters offline mode with the last online session's list of channels. (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.

PMC Login Procedure

To log in to the PMC application, follow this procedure:

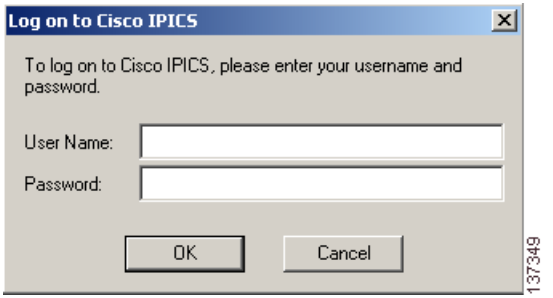
Procedure

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.

Figure 3-2 shows an illustration of the Cisco IPICS login window.

Figure 3-2 Cisco IPICS Login Window



Step 2 To log in to the PMC, enter your **user name** and **password**; then, click **OK**.

Tip Be aware that user names and 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.

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 cannot connect to other channels until it reconnects to the server.

Step 3 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 not critical, you can choose to upgrade the PMC at a later time. See the "Performing a Noncritical Upgrade" section on page 2-25 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 Critical Upgrade" section on page 2-27 for more information.
- If the PMC version is current, the server sends the list of locations that have been associated with your user ID.

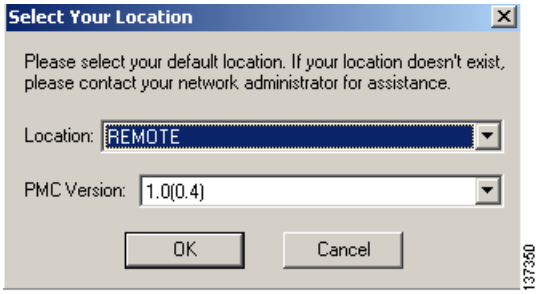
Step 4 Choose your default location and your PMC version from the drop-down list boxes; then, click **OK**.

Note The PMC version drop-down list box includes the PMC versions that are compatible with the server.

Note 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.

Figure 3-3 shows an illustration of the location selection dialog box.

Figure 3-3 Location Selection Dialog Box



Step 5 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 6 The PMC retrieves the personalized list of visible channels/VTGs from the server.

- A channel displays on the PMC when it has been assigned to you by the dispatcher. The server determines the order in which the channels appear.
- A VTG displays on the PMC after it has been activated by the dispatcher; this activation begins the talk group and, at this point, you are placed into the active VTG.

Note 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. Channels that appear grayed-out 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, the PTT button will not highlight.

Step 7 Click the **Activate** button on the PMC application to directly join the 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 7-18.

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

Step 8 Click the **PTT** button and hold it to talk.

The transmit graphical indicator blinks red to indicate that you are transmitting traffic.

Step 9 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.)

To talk on one or more channels at the same time, you can use the PTT latch functionality. To latch, or lock in, the PTT channel, 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. (The receive graphical indicator blinks green for the duration of the latch, whether you are talking or not.) To clear the latch, click the **PTT** button without holding the Shift key.

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.

Related Topics

- Architecture/Deployment, page 1-11
- Upgrading the PMC Application, page 2-20
- Performing a Noncritical Upgrade, page 2-25
- Performing a Critical Upgrade, page 2-27
- License Information, page 3-17

Using the PMC Application

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

- Accessing Online Help, page 3-23
- Dynamic Configuration, page 3-24
- Channel Interaction/Features, page 3-25
- Traffic Activity, page 3-33

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 Right-click anywhere inside the PMC window; then, click **Settings**.

Step 3 Click **Help**. Alternatively, you can press **F1** to access help.

The PMC online help information displays.

Figure 3-4 shows the Help link on the Cisco IPICS Mouse 4-Channel skin.

Figure 3-4 PMC 4-Channel Mouse Skin with Menu

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. (See the "PMC Updates" section on page 3-25.)

The Cisco IPICS server manages the configuration for the PMC so 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, including a default theme and a skin/XML definition that is configured by the system administrator.

You can, however, customize the PMC skin by choosing from the available options that appear in the Settings menu. For more information about accessing the Settings menu to change the PMC skin, see the "Configuring the PMC Skins" section on page 4-2.

Note The Cisco IPICS server saves and stores all user configuration settings for use with each login.

PMC Updates

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). If the user's configuration settings have changed, the PMC creates a secure HTTPS connection to the server for transmission of the updated information.

Note The Cisco IPICS system performs a user level update only when a valid PMC user is logged in to the PMC application.

Channel Interaction/Features

This section describes the channel interactions and features on the PMC; it also provides information about joining a VTG and using the PMC buttons.

This section includes the following topics:

- Cisco IPICS Server Commands, page 3-26
- Support for Maximum Number of Channels, page 3-27
- End-user Channel Interaction, page 3-28
- Joining a VTG, page 3-30
- Activating the PMC Buttons, page 3-30

Cisco IPICS Server Commands

Table 3-2 describes the commands that can be sent from the Cisco IPICS server to the PMC in XML format.

Table 3-2 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 the case of channel mismatch, the dispatcher receives a warning message when the PMC user may not be able to view all of the assigned channels/VTGs. See the "Skin Caveats" section on page 4-5 for more information
Disable User	This command disables the PMC user from accessing the Cisco IPICS system. If the user is disabled while the PMC is online (communicating with the server), Cisco IPICS logs the user off the PMC 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. (The system displays a pop-up message, along with a grayed out PTT channel button, to alert the user that permission to transmit has been revoked; if your ability to transmit on a channel has been disabled by the server, the PTT button will not highlight on the PMC).

Support for Maximum Number of Channels

With this release, the PMC supports a maximum of eight channels. This support includes the ability to simultaneously receive and/or talk on one or multiple channels.

You can use the PTT latch functionality to talk on one or more channels at the same time. To latch, or lock in, the PTT button, 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.

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.

You can customize the PMC skin to enable your own "look and feel," by choosing from one of the following skins as described in Table 3-3.

Table 3-3 Cisco IPICS PMC Skins

Skin Label	Skin Description
Cisco IPICS Mouse 4-Channel	This skin displays 4 channels that you control with your mouse.
Cisco IPICS Mouse 8-Channel	This skin displays 8 channels that you control with your mouse.
Cisco IPICS Touch 4-Channel	This skin displays 4 channels in a touch screen format.
Cisco IPICS Touch 4-Channel Low Res	This skin displays 4 channels in a low resolution touch screen format. (For information about using the touch screen low resolution skins, see the "Configuring the PMC Skins" section on page 4-2.)
Cisco IPICS Touch 8-Channel	This skin displays 8 channels in a touch screen format.
Cisco IPICS Touch 8-Channel Low Res	This skin displays 8 channels in a low resolution touch screen format.

For more information and instructions about customizing the PMC skins, see the "Customizing the PMC End-User Interface" section on page 4-1.

See Figure 1-1 on page 1-7 for an illustration of the Cisco IPICS Mouse 4-Channel skin.

See Figure 4-2 on page 4-4 for an illustration of the Cisco IPICS Touch 4-Channel skin.

See Figure 4-5 on page 4-12 for an illustration of the Cisco IPICS Mouse 4-Channel skin with the optional settings menu.

End-user Channel Interaction

As the Cisco IPICS stand-alone 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. (Channels that appear grayed out 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.)

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

Channels/States

Table 3-4 shows the VTG/channel 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. The name may change, based on the configuration in the Cisco IPICS server.

Table 3-4 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 PTT button will not highlight.
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 grayed-out but you may press the Activate button to activate the channel.
Disabled	No PMC buttons appear highlighted and you cannot activate the channel	When a channel is disabled, all of the PMC buttons are grayed-out or muted so that you cannot activate the channel. However, you can still view the channel or VTG label, if one was configured in the server.
Unassigned	No PMC buttons appear highlighted and you cannot activate the channel	A channel that is unassigned appears on the PMC with all of the buttons grayed-out and no channel name. You cannot activate or use an unassigned channel.

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.

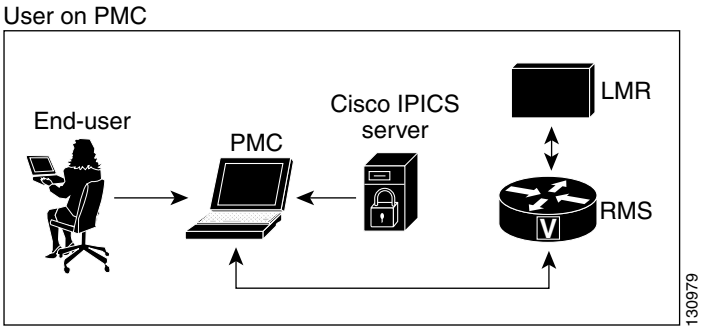
A corresponding alerting channel flashes on the PMC to let you know that you need to click the **Activate** button to join the VTG. (The channel on the PMC application becomes activated and appears highlighted to show that it is in an active state as long as your ability to transmit has not been disabled 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 3-28 for information about the various channel states.

Figure 3-5 shows an illustration of the interaction with the PMC user.

Figure 3-5 Interaction with the PMC User



Activating the PMC Buttons

Each channel contains a PTT channel button with send/receive feedback, volume control, volume graphical indicator, and an activation control button that toggles on and off.

Table 3-5 describes the buttons that display on the PMC. Use your mouse to click, or push, these buttons to perform the corresponding function.

Table 3-5 PMC Button Icons

Button Icon	Button Function	Button Description
	PTT Channel	This is the PTT channel button and the PMC receive (green) and transmit (red) indicators. Click with your mouse, or push, the **PTT** button and hold it to talk. You can also latch this button to talk on one or more channels at the same time. To clear the latch, click the **PTT** button to release and return to listen-only mode.
	Activation and Deactivation	Click this button to activate a channel (to call out); click again to deactivate a channel.
	Volume Down	Click this button to decrease the volume on the channel.
	Volume Up	Click this button to increase the volume on the channel.

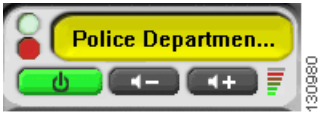
Tip To latch, or lock in, the PTT button, position your cursor over the PTT button and then press the **Shift** key while you click the left mouse button. Follow this procedure for each channel that you want to talk on. To clear the latch, click the **PTT** button without holding the Shift key.

Caution Use the latch functionality with caution. 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.

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.

Figure 3-6 shows an illustration of the PMC buttons and the volume indicator bar as they appear on the application.

Figure 3-6 PMC Buttons



Note 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.

You can also use key assignments to quickly access these same buttons, and other features, by pressing keystroke sequences to activate the corresponding function.

Table 3-6 lists these keystrokes and the function that each one provides in Cisco IPICS release 10.

Table 3-6 PMC Button Accelerated Keystroke Assignments

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

Table 3-6 PMC Button Accelerated Keystroke Assignments (continued)

Channel Number on the PMC	Keystroke to Activate or Deactivate the Channel	Keystroke to Latch (lock in) or Unlatch the PTT Button	Keystroke to Increase the Volume	Keystroke to Decrease the Volume
Channel 7	Shift-7	7	u	j
Channel 8	Shift-8	8	i	k

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

Note These keystroke assignments may be customized in the Cisco IPICS server; contact your administrator if the keystroke sequences that are shown in Table 3-6 do not function.

Traffic Activity

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

- Channel Traffic Activity Interaction, page 3-35
- User Channel Activity Interaction, page 3-35

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. To show traffic activity, the PMC provides graphical indicators. (See Figure 1-1 on page 1-7 for an illustration of the PMC and the location of the graphical indicators.)

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

Table 3-7 Channel Traffic Activity Indicators

Channel Traffic Activity Indicator	Description
Receive indicator	This graphical indicator blinks green when you are receiving traffic. This indicator remains illuminated for several seconds after the receive transmission has ended to let you know that the user has stopped talking. **Note** When you latch the PTT button, the receive indicator blinks green for the duration of the latch whether you are talking or not.
Transmit indicator	This graphical indicator blinks red when you are transmitting traffic.

Tip 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 release it and 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 blink red when there is PTT transmission while the PTT control is activated.
- Indicators for glare, a condition when a channel receives traffic while the PTT is active, may blink a different color.
- A separate color may blink for situations where the bearer traffic is lost because of a system transmit/receive overflow.

- 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 Cisco IPICS wants to have the floor, the system assumes that the user will wait to generate traffic. The Cisco IPICS server considers the reception of traffic as a floor request.
- 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 grayed-out 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, the PTT button will not highlight.

- 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.
- When a channel is disabled, all of the PMC buttons are grayed-out or muted so that you cannot activate the channel. However, you can still view the channel or VTG label, if one was configured in the server.
- A channel that is unassigned appears on the PMC with all of the buttons grayed-out and no channel name. You cannot activate or use an unassigned channel.

Note If you activate and deactivate channels while you are actively using one of the channels on the PMC, the audio on the channel that you are actively using may become distorted.

Related Topics

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

Logging Out of the PMC Application

You can log out of the PMC application by either clicking **Exit** from the PMC menu or by clicking the "**X**" that is located at the top right corner of the PMC application.

Figure 3-7 shows an illustration of the Cisco IPICS Mouse 4-Channel skin. It displays the Exit option on the Settings menu and the "X" on the PMC.

Figure 3-7 4-Channel PMC Skin

Where to Find More Information

- *Cisco IPICS Server Administration Guide*

Customizing the PMC Application

This chapter provides information about customizing the PMC application end-user interface.

This chapter includes the following sections:

- Customizing the PMC End-User Interface, page 4-1
- Using the Optional Settings Menu, page 4-11

Customizing the PMC End-User Interface

The Cisco IPICS server manages the configuration for the PMC. However, as a PMC end-user, you may customize the PMC skin, reconfigure the Express and Channels settings, and set up the PMC logs.

For information about using the PMC logs, see "Identifying the PMC Logs" section on page 6-1.

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 Express and Channels settings that appear in the Settings menu. This section describes the following topics:

- Configuring the PMC Skins, page 4-2
- Skin Caveats, page 4-5
- Configuring the Express and Channels Settings, page 4-6

Configuring the PMC Skins

With this release, Cisco IPICS supports a maximum of eight channels and four skins for the PMC. See the "Support for Maximum Number of Channels" section on page 3-27 for more information about Cisco IPICS channel support.

The Cisco IPICS administrator creates and configures the skins that are available for the PMC, including the default skin configuration for each channel and the number of channels that the PMC retrieves from the Cisco IPICS server.

The ability to customize the PMC skin allows you to individualize your own PMC "look and feel." You may choose a different skin to create your own customized look 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 4-3.

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 Your system administrator has the option to allow you to use only selected PMC skins. In addition, the Cisco IPICS server can be configured so that the PMC skin is preselected for you. If you cannot customize your PMC skin, contact your system administrator for additional information and assistance.

Note Cisco IPICS supports 4-channel and 8-channel high and low resolution touch screen skins. When you configure your PMC to use the 8-channel touch screen skin, 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 anywhere 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 the low resolution touch screen skin or choose another skin from the **Settings > Skin** menu.

Figure 4-1 shows an illustration of the Cisco IPICS Touch 4-Channel skin with the Settings menu. The Settings menu displays on the PMC application when you position your cursor over the PMC window and then right-click anywhere inside the window.

Figure 4-1 PMC 4-Channel Touch Skin with Settings Menu

To access the skin configuration in the PMC Settings menu, follow this procedure:

Procedure

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

Step 2 Right-click anywhere inside the PMC window; then, click **Settings**.

The Express, Skin, and Channels tabs appear in the PMC window.

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

The Skin menu displays the available options for 4-channel and 8-channel mouse and touch screen formats.

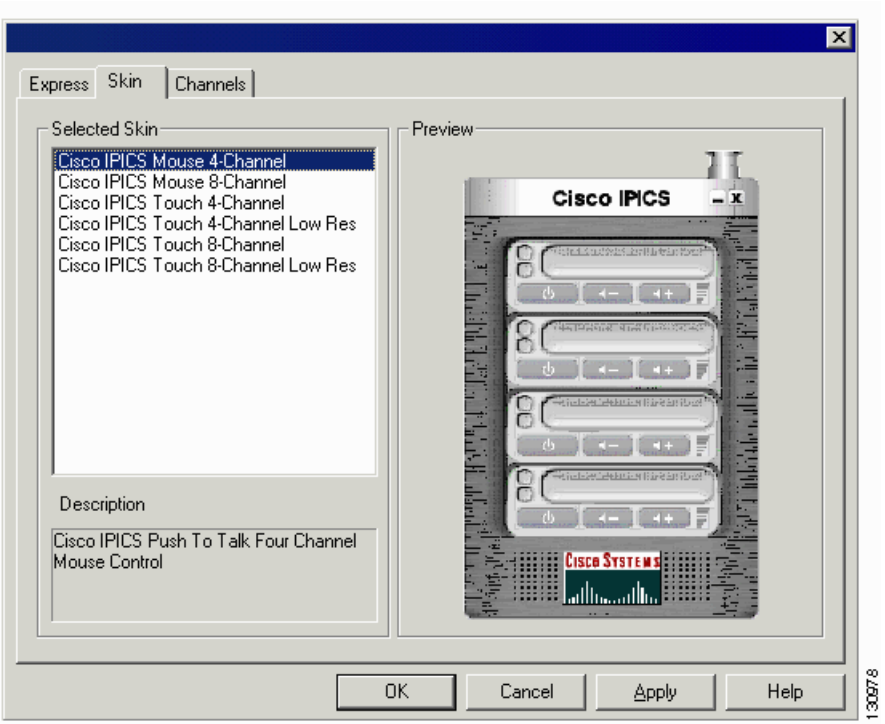
Step 4 To change the skin, choose a different option from that which you have currently configured.

Step 5 Click **OK**.

The PMC skin changes to reflect the new setting.

Figure 4-2 shows an illustration of an example of the PMC Skin menu with the Cisco IPICS Mouse 4-Channel skin shown in the display.

Figure 4-2 PMC Skin Menu



If you reconfigure your PMC skin and your association to channels and VTGs is greater than what has been specified, the Cisco IPICS dispatcher receives an error message that states that the maximum number of channels is already in use and some channels must be disassociated before adding a new channel.

For more information about skin mismatch conditions, see the "Skin Caveats" section on page 4-5.

Note When you reconfigure the PMC skin, the PMC reports the number of channels that are visible in the skin to the Cisco IPICS server. The PMC sends this information to the server each time the skin changes as well as whenever it requests a channel list.

Skin Caveats

The configuration in the Cisco IPICS server defines the default skin for the PMC. This definition also determines the number of channels that the PMC retrieves from the Cisco IPICS server.

Note If you customize 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 processes the first four channels and ignores the other four channels.

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.

When 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.

In addition, the PMC reports the number of channels that are visible in the skin to the Cisco IPICS server. Therefore, if the dispatcher attempts to assign additional channels for the PMC user when the 4-channel skin is configured, a warning message displays to notify the dispatcher that the PMC user can only view four channels.

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 3-12 for more information about policies.

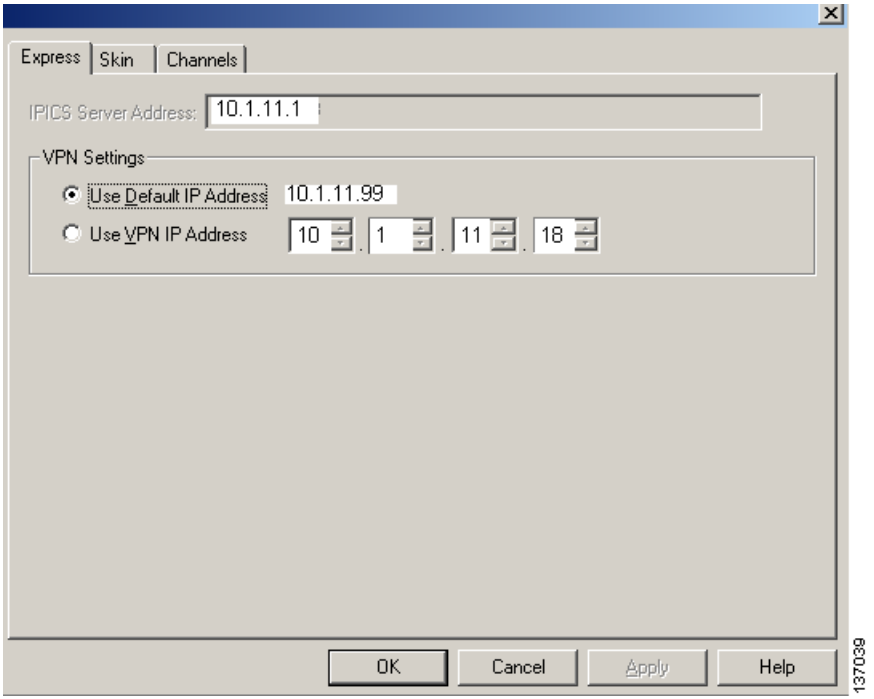
Configuring the Express and Channels Settings

You can change the settings that appear under the Express and Channels tabs.

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

Figure 4-3 shows an illustration of the PMC Express menu.

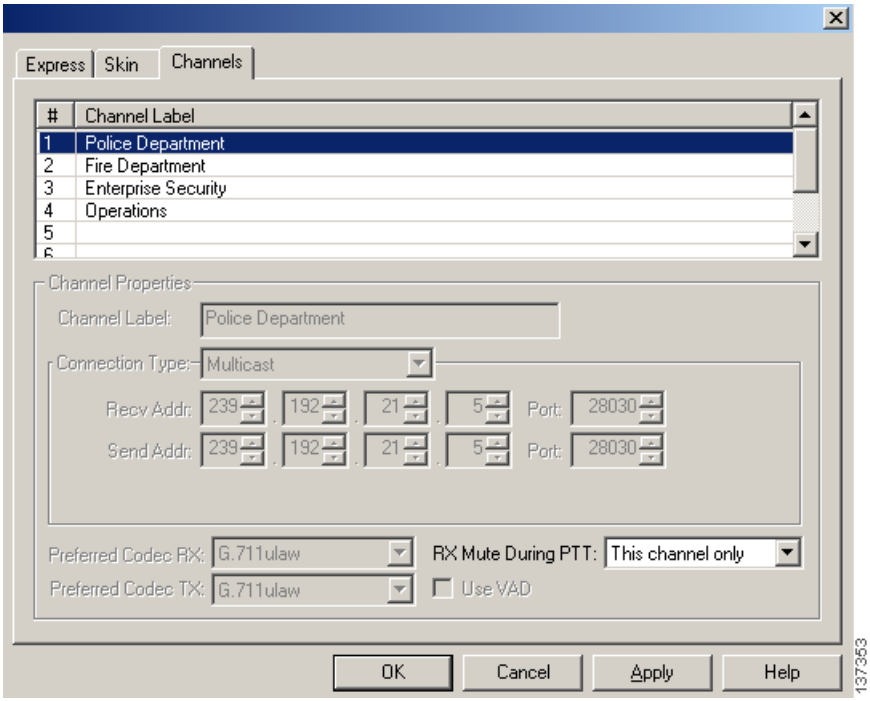
Figure 4-3 PMC Express Menu



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

Figure 4-4 shows an example of the fields that display in the PMC Channels menu.

Figure 4-4 PMC Channels Menu



To access the Express and Channels configuration menus in the PMC Settings menu, follow this procedure:

Procedure

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

Step 2 Right-click anywhere inside the PMC window; then, click **Settings**.

The Express, Skin, and Channels tabs appear in the PMC window.

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

The Express menu displays the following fields:

- Cisco IPICS Server Address—This field specifies the IP address of the Cisco IPICS server that your PMC connects to.

- 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**.

Step 5 To view the Channels menu, click the **Channels** tab.

The Channels menu displays the channel number and the associated channel name, along with the following channel properties:

- Channel Label—The channel label that displays corresponds to the channel that you select in the top window pane.
- 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 fields 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.
  - 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.
- 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. From the drop-down list box, choose one of the following options:
  - **None**—This option sets the transmission to full duplex; that is, you hear audio while the PTT channel is depressed because the PMC does not mute any of the received traffic.
  - **This channel only**—This option sets the transmission to half duplex for the specified channel; that is, you will not 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**—This option sets the transmission to half duplex for all channels; that is, you will not hear audio on any of the channels.
- Use VAD—This option enables voice activity detection (VAD). When you enable VAD, the PMC only sends voice traffic when it detects your voice.

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.

Step 6 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, follow this procedure:

Procedure

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

Step 2 Hold down the left **Shift** key and right-click the mouse anywhere inside the PMC window.

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 6-1 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.
- 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.

Figure 4-5 shows an illustration of the PMC optional settings submenus as they appear on the PMC window.

Figure 4-5 PMC Optional Settings Submenus

Related Topics

- Identifying the PMC Logs, page 6-1
- Channel Support, page 3-8
- Implementing Policies, page 3-12
- Dynamic Configuration, page 3-24

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 5-1
- Recovering the PMC, page 5-2
- PMC Recovery Scenarios, page 5-3
- PMC Application Recovery, page 5-5

Support for Cisco IPICS Recovery

With this release, Cisco IPICS allows the connection of a PMC to only one Cisco IPICS server. Therefore, this release does not include support for load balancing or redundancy functionality.

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.

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.

For more information, see the"Server-PMC Login Sequence Interaction" section on page 3-17 and the "System Recovery Caveats" section on page 5-3.

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.

Related Topics:

- Server-PMC Login Sequence Interaction, page 3-17
- System Recovery Caveats, page 5-3

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 5-2
- System Recovery Caveats, page 5-3

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 system presents you with the option of logging 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 3-16.

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. For more information about the status checks that Cisco IPICS performs, see the "PMC Updates" section on page 3-25.

Related Topics:

- Logging In to the PMC Application, page 3-16
- Dynamic Configuration, page 3-24
- PMC Updates, page 3-25

PMC Recovery Scenarios

The following information describes how the PMC recovers in certain scenarios:

- Cisco IPICS Server Down/PMC Up, page 5-4
- Cisco IPICS Server and PMC Up/Communications Down, page 5-4
- Cisco IPICS Server and PMC Up/Network Down, page 5-5

Cisco IPICS Server Down/PMC Up

When the Cisco IPICS server fails, the PMC continues to operate in its existing state but no changes to channels or configuration can be made while the server is down. (The PMC continues to poll the server during this time.)

In this scenario, the following activities occur when the server resumes normal operations:

1. When the Cisco IPICS 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 3-17.
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 Up/Communications Down

In this scenario, the Cisco IPICS server is operational but the communications between the server and the PMC is 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 Up/Network 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 Up/Communications Down" section on page 5-4, occurs.

For more information about logging in to the PMC application, see the "Logging In to the PMC Application" section on page 3-16.

Related Topics:

- Logging In to the PMC Application, page 3-16
- License Information, page 3-17

PMC Application Recovery

The Cisco IPICS server provides the basic PMC configuration, skin, and XML definitions.

If you encounter a configuration, skin, or XML loss, you can quickly recover from this failure 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 2-29.

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 2-17, the "Managing PMC Version Numbers" section on page 2-21, the "Reverting to a Previous Version of the PMC Application" section on page 2-28, and the "Logging In to the PMC Application" section on page 3-16.

Related Topics

- Installing the PMC Application, page 2-2
- Launching the PMC Application, page 2-17
- Managing PMC Version Numbers, page 2-21
- Reverting to a Previous Version of the PMC Application, page 2-28
- Uninstalling the PMC Application, page 2-29
- Logging In to the PMC Application, page 3-16

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 6-1
- Accessing the PMC Logs, page 6-3
- Using the PMC Logs, page 6-5

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 6-1
- Accessing the Logs Submenu Items, page 6-2

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 6-3.

Figure 6-1 shows an illustration of the PMC window that displays the Logs submenu items.

Figure 6-1 PMC with Logs Submenu Items

See the "Using the PMC Logs" section on page 6-5 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.

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 4-11.

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.

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.

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 clear the debug log, 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 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 6-7 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. (Under most normal conditions, the log and debug files will be obtained from the server.)

This section includes the following topics:

- PMC Log Caveats, page 6-6
- PMC Log Descriptions, page 6-7

PMC Log 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 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.

Table 6-1 describes each of the PMC log files.

Table 6-1 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.
ChannelActivity.log	This log contains a history of channel activation and deactivation within the PMC. This log appears in XML format.
ChannelStatistics.log	At regular and predefined intervals, this log records each channel's statistics, 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 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 information about using Command Line Interface (CLI) command options for the PMC log files, refer to the *Cisco IP Interoperability and Collaboration System Software Development Kit Guide*.

Related Topics

- Upgrading the PMC Application, page 2-20
- Using the Optional Settings Menu, page 4-11

Where to Find More Information

- *Cisco IPICS Server Administration Guide*
- *Cisco IP Interoperability and Collaboration System Software Development Kit Guide*

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 7-1
- Analyzing PMC Error Conditions, page 7-22

Troubleshooting PMC Application Problems

The following sections describe how to resolve problems with the PMC application:

- Resolving PMC Execution Issues, page 7-2
- Generating a PMC Installation Log File, page 7-3
- Making PMC Configuration File Changes, page 7-4
- Using the PMC Optional Settings, page 7-5
- Configuring the Audio Settings, page 7-5
- Using Cisco Security Agent with the PMC, page 7-7
- PMC Coexistence with Other Voice Applications, page 7-8
- Troubleshooting One-Way Audio, page 7-8
- Troubleshooting Voice Quality Issues, page 7-11

- Troubleshooting PMC Connectivity Issues, page 7-12
- Resolving Name Resolution Failures, page 7-18
- Identifying Channel Activation Issues, page 7-18
- Resolving Codec Mismatch Issues, page 7-19
- Support for Right-to-Left Languages, page 7-20
- PMC Application Caveats, page 7-21

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 2-3.

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.

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 4-11 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.

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 7-6
- Checking the Microphone with the PMC, page 7-6

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.

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 2-16.

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 2-12 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 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 2-11, the "Using a USB DSP Headset with the PMC" section on page 2-12 and "Using the Microphone with the PMC" section on page 2-14 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 Headset Issues, page 7-9
- Resolving IP Address Changes, page 7-10

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.

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 IP Interoperability and Collaboration System Software Development Kit Guide*.

Using the CLI Play Command to Resolve 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 8, 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 IP Interoperability and Collaboration System Software Development Kit Guide*.

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 7-11

- IP Address Change Notifications, page 7-11

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

Troubleshooting PMC Connectivity Issues

The following topics provide information about troubleshooting PMC connectivity issues:

- Troubleshooting VPN Connectivity, page 7-12
- Using the PMC with the Windows XP Firewall, page 7-15
- Troubleshooting Multicast Communications Issues, page 7-16
- Troubleshooting Winsock Corruption Issues, page 7-17
- Troubleshooting Offline Mode Issues, page 7-17

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 7-13
- Enabling and Disabling the Stateful Firewall on the PMC Client Machine, page 7-14

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 > Express** 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 Express and Channels Settings" section on page 4-6.

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 following protocols:

- Internet Control Message Protocol (ICMP) type 8 (echo request) / ICMP type 0 (echo reply)
- Hypertext Transfer Protocol (HTTP) GET port 80 / HTTP/1.1 (response version 1.1)
- Hypertext Transfer Protocol Secure (HTTPS) port 443 and port 443 setup
- Standard Session Initiation Protocol (SIP) call setup

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 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 2-14.

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 transmit traffic indicator LED blinks.)
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 3-18.

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.

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, the PTT button will not highlight.

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.

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 3-15.

Support for Right-to-Left Languages

Cisco IPICS supports the use of languages that are written right-to-left (RTL), such as Arabic and Hebrew. To use a right-to-left language in Windows 2000 and Windows XP, you need to configure the operating system to enable RTL 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, perform the following procedure:

Step 1 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 Arabic and Hebrew languages.
   - 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.

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 Arabic and Hebrew language support.

Step 2 On Windows XP client machines, navigate to **Start > Settings >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.

b. 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.

   A pop-up message displays to inform you that the installation of supplemental language support requires a defined amount of available disk space.

c. Click **Ok** to accept.

d. From the Regional and Language Options dialog box, click **Apply**.

e. 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 RTL language support, including the Arabic and Hebrew languages.

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 always logs in to the same Cisco IPICS server that has been configured as the default server and from which the PMC was downloaded as part of the installation. To change servers, the PMC application must be reinstalled from a different Cisco IPICS server.
- See the "PMC Offline Mode Caveats" section on page 3-18 for information about using the PMC in offline mode.
- See the "Skin Caveats" section on page 4-5 for information about PMC skin caveats.

Analyzing PMC Error Conditions

This section includes information about identifying and resolving errors that you may encounter when you use the PMC.

Table 7-1 describes the error conditions that may display on your PMC client machine and how to resolve these errors.

Table 7-1 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 2-11 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 7-1 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 Express and Channels Settings" section on page 4-6 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.	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 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.

Table 7-1 PMC Error Conditions (continued)

Problem	Solution
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.
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 2-11
- Skin Caveats, page 4-5
- Configuring the Express and Channels Settings, page 4-6
- Using the Optional Settings Menu, page 4-11

Where to Find More Information

- *Cisco IPICS Server Administration Guide*
- *Cisco IP Interoperability and Collaboration System Software Development Kit Guide*

A

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

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

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

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

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

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

B

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

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

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

C

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

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

call setup time The time that is required to establish a circuit-switched call between users or terminals.

carrier A wave that is suitable for modulation by an information-bearing signal.

CAS channel associated signaling. The transmission of signaling information within the voice channel. CAS signaling often is referred to as robbed-bit signaling because user bandwidth is being robbed by the network for other purposes.

channel A communication path that is wide enough to permit a single RF transmission. Multiple channels can be multiplexed over a single cable in certain environments. *See* PTT channel.

channel capacity The maximum possible information transfer rate through a channel, subject to specified constraints.

channel folder A logical grouping of channels

channel spacing The distance from the center of one channel to the center of the next-adjacent-channel. Typically measured in kilohertz.

Cisco CallManager The software-based call-processing component of the Cisco IP telephony solution. Cisco CallManager functionality extends enterprise telephony features and functions to packet telephony network devices, such as Cisco 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 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.

Cisco 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 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 peer Addressable call endpoint. In Voice over IP, there are two kinds of dial peers: POTS and VoIP.

digital 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 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 users, as necessary, and sets up system policies.

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.

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.

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.

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.

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 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).

mute This 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 Telecommunications 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.

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. While ops views are maintained separately by the Cisco IPICS system administrator, this functionality also allows multiple entities to use one Cisco IPICS server to enable resource sharing across multiple ops views, according to business need.

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 An association of events or triggers to an action. Policies can include a set sequence of actions, such as activating VTGs.

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.

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 mixes remote PMC SIP-based (unicast) connections to a multicast channel or VTG. The RMS can be installed as a stand-alone component (RMS router) or as an additional feature that is installed in the LMR gateway.

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.

SDM Security Device Manager. A web-based integrated router application, provides a user-friendly GUI for configuring security features in Cisco routers. Cisco IPICS uses SDM to configure voice ports and LMR functions on LMR gateways.

secure flag A PTT channel indicator that identities a channel as a secure PTT channel.

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.

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 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 The indicator on the PMC that blinks red when traffic is being transmitted.

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.

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 or a supported Cisco IP Phone model. Users may have one or more Cisco IPICS roles, such as system 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 Cisco IP Phone 7960 or Cisco IP Phone 7970.

voice interoperability Voice interoperability enables disparate equipment and networks to successfully communicate with each other.

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 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 3-30
activation button 3-31
application recovery 5-5
audio quality 2-11
audio settings configuration 2-11
automatic update process 2-22

B

browser support 1-9

C

CallManager
  documentation xii
caution, described xiv
channel interaction 1-17
channel name 3-10
channels
  activated 1-8
  dispatcher policy channel 3-12
  interactions 3-25
  latch 3-4
  locations 3-13
  maximum channel support 3-27
  policies 3-12
  terminology 3-9
  traffic activity indicators 3-33
  VTGs 1-6
channel states 3-28
channel traffic activity
  administratively stopping transmission 3-35
  implicit floor control 3-35
  indicators 3-33
  interaction 3-35
  receive and transmit indicators 3-33
checking the microphone 2-15
Cisco IOS
  documentation xiii
Cisco IPICS
  benefits 1-2
  browser support 1-9
  components 1-3
  deployment 1-11
  overview 1-2
  server 1-3
  server interactions 1-15
  user interactions 1-16

Cisco IPICS user roles 1-4
Cisco IP Phones
  documentation xii
Cisco IP Phone support 1-4
Cisco Land Mobile Radio (LMR)
  documentation xiii
Cisco Security Agent
  documentation xiii
codec support 3-15
communications
  multicast 3-11
  unicast 3-11
communications interruptions 5-4
components
  Cisco IPICS server 1-3
  Cisco IP Phone 1-4
  gateways 1-4
  PMC 1-4
  router media service 1-4
configuring audio settings 2-11
conventions, document xiii
critical upgrades 2-24
customizing the PMC application 4-1

D

disconnected mode 3-20
dispatcher role 1-5
documentation
  CallManager xii
  Cisco IOS xiii
  Cisco IP Phones xii
  Cisco Land Mobile Radio (LMR) xiii
  Cisco Security Agent xiii
  conventions xiii
  MCS servers xii
downloading the PMC update 2-25
dynamic configuration 3-24

E

echo
  multiple channels 3-4
error messages 7-22

F

feature support
  channels 3-8
  implementing policies 3-12
  interoperability 3-7
  locations 3-13

G

gateways
  LMR 1-4
  router media service 1-4

H

HTTPS 2-3

Hypertext Transfer Protocol over Secure Sockets Layer

See HTTPS

I

implementing policies 3-12

incident management scenario 3-5

installing the PMC application 2-2

interactions

- Cisco Security Agent 2-9
- client-server 2-1
- server 1-15
- system 1-15
- user 1-16

J

joining a VTG 3-30

L

Land Mobile Radio

- *See* LMR

latching the PTT button 1-10

license requirements 3-17

LMR

- channel representation 3-9
- gateway 1-4
- PTT audio application 3-7

location 3-13

log files 6-1

logging in to the PMC

- local login 3-19
- login caveats 3-16
- login information 3-16

logging out of the PMC 3-36

M

MCS servers

- documentation xii

microphone setup 2-15

multicast communications 3-11

multicast connection 3-13

N

non-critical upgrades 2-24

note, described xiii

O

operator role 1-5

optimizing audio 2-11

optional settings submenus 4-11

overview
Cisco IPICS 1-2
PMC 1-6

P

PMC
application recovery 5-5
automatic update process 2-22
buttons 3-30
caveats 1-10
channels
interactions 3-25
latch 3-4
states 3-28
support 3-8
terminology 3-9
traffic activity indicators 3-33
checking for updates 2-23
client application 1-4
communications interruptions 5-4
configuration customization 1-8
customizing the application 4-1
disconnected mode 3-20
downloading the update 2-25
GUI 1-8
illustration 1-6
installation
caveats 2-3
installing the application 2-2
interactions
Cisco Security Agent 2-9
client-server 2-1
interface 1-6
interoperability features 3-7
joining a VTG 3-30
key assignments 3-32
license requirements 3-17
locations 3-13
logging in
caveats 3-16
local login 3-19
logging out 3-36
logs
accessing the logs 6-3
accessing the submenu 6-2
caveats 6-6
describing the logs 6-7
examples 6-8
files 6-1
identifying the logs 6-1
using the logs 6-5
managing version numbers 2-21
offline mode 3-18
recovering the system 5-1
recovery caveats 5-3
recovery scenarios 5-3
reverting to a previous version 2-28

scenarios
incident management 3-5
interactions 3-1
PMC user interaction 3-6
skin
caveats 4-5
mismatch 4-5
system requirements 1-13
troubleshooting
application 7-1
audio settings 7-5
caveats 7-21
channel activation issues 7-18
Cisco Security Agent 7-7
codec misconfiguration 7-19
coexistence 7-8
configuration file changes 7-4
connectivity issues 7-12
DNS issues 7-18
error messages 7-22
execution 7-2
headset 7-6
headset issues 7-9
microphone 7-6
multicast connections 7-16
offline mode 7-17
one-way audio 7-8
optional settings menu 7-5
resolving IP address changes 7-10
right-to-left language support 7-20
voice quality 7-11
VPN issues 7-12
winsock corruption 7-17
uninstalling the application 2-29
upgrading the application
critical upgrades 2-24
messages 2-26
non-critical upgrades 2-24
process 2-20
types of upgrades 2-23
user privileges 3-11
using the logs 6-1
using the optional settings 4-11
version number management 2-21
voice quality tips 2-16
PMC ID 1-15
PMC installation caveats 2-3
PTT button 3-31
Push-to-Talk Management Center
See PMC

R

recovery scenarios 5-3
remote connection 3-13
reverting to a previous version of the PMC 2-28
right-to-left language support 7-20

S

scenarios 3-1
server
  commands 3-26
  dynamic configuration 3-24
  location support 3-13
  role 3-10
server commands
  channel list 3-26
  disable channel 3-26
  disable user 3-26
  mute user 3-26
  retrieve logs 3-26
  set logging level 3-26
server-PMC login sequence 3-17
skin caveats 4-5
skin mismatch 4-5
supported codecs 3-15
supported features 3-7
supported user roles 1-4
system administrator role 1-5
system interactions 1-15
system recovery 5-1
system recovery caveats 5-3

T

TAC Case Collection Tool 7-12
traffic activity indicators 3-33
troubleshooting the PMC application 7-1

U

unicast communications 3-11
unicast connection 3-13
uninstalling the PMC application 2-29
updating the PMC application 2-23
upgrading the PMC
  critical upgrade 2-27
  non-critical upgrade 2-25
  types of upgrades 2-23
user channel activity interaction 3-35
user privileges 3-11
user role 1-5
using the microphone 2-14
using the PMC buttons 3-30

V

version number management 2-21
Virtual Talk Groups
  See VTGs
voice quality issues 7-11
voice quality tips 2-16
volume down button 3-31
volume up button 3-31
VTGs
  channel 1-6

server-PMC interaction 3-30

states 1-17

user interaction states 3-28