CISCO SYSTEMS

Cisco IP Interoperability and Collaboration System (IPICS) Server Administration 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-8023-01

Cisco IP Interoperability and Collaboration System (IPICS) Server Administration Guide, Release 1.0(1)

Preface

Introduction

Cisco IP Interoperability and Collaboration System (IPICS) Server Administration Guide provides the information that you need to understand, configure, manage, and use the Cisco IP Interoperability and Collaboration System (IPICS) 1.0 application.

This preface contains the following sections:

Tip If you use Cisco IPICS solely for communicating with other users, and do not require any other introductory material, go to Chapter 5, "Administration Console: User Tasks," which provides information about logging into Cisco IPICS, downloading and setting up your PMC, and completing your user profile.

Audience

Cisco IPICS Server Administration Guide is intended for users who configure, operate, and manage tasks for the Cisco IPICS server. It also is intended for users who perform any of all of these Cisco IPICS roles: user, operator, dispatcher, or system administrator.

Organization

This document is organized as follows:

Chapter 1, "Introducing Cisco IPICS"	Provides an overview of Cisco IPICS and directs users to the appropriate sections in this document for their particular roles.
Chapter 2, "Administration Console: System Administrator Tasks"	Describes the tasks that the system administrator can perform in the Admin Console.
Chapter 3, "Administration Console: Operator Tasks"	Describes the tasks that the operator can perform in the Admin Console.
Chapter 4, "Administration Console: Dispatcher Tasks"	Describes the tasks that the dispatcher can perform in the Admin Console.
Chapter 5, "Administration Console: User Tasks"	Discusses how a user interacts with the Admin Console. Topics covered include logging in, downloading the PMC application, and setting up a user profile.
Chapter 6, "Operational Views"	Explains the Cisco IPICS operational view functions.
Appendix A, "RMS Configuration"	Describes how to configure and RMS so that you can use it with Cisco IPICS.
Appendix B, "Setting Up and Using the Cisco IP Phone with Cisco IPICS"	Describes how to set up and use supported Cisco IP Phones with Cisco IPICS.
Appendix C, "Frequently Asked Questions"	Provides answers to frequently asked questions regarding Cisco IPICS.

Related Documentation

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

- *Cisco IPICS Server Installation Guide, Release 1.0*—Describes how to install and configure the Cisco IPICS 1.0 server software and the Linux operating system
- *Cisco IPICS PMC Quick Start Guide, Release 1.0*—Provides tips and quick references for the most frequently used procedures that a user can perform on the Cisco IPICS PMC
- *Cisco IPICS PMC Installation and User Guide, Release 1.0*—Describes how to install, configure, manage, and operate the Cisco IPICS PMC application
- *Cisco IPICS PMC Debug Reference Quick Start Guide, Release 1.0(1)*—Provides a quick reference for troubleshooting and debugging the Cisco IPICS PMC
- *Cisco IPICS Troubleshooting Guide, Release 1.0*—Contains reference material about how to maintain and troubleshoot the Cisco IPICS system
- *Cisco IPICS Backup and Restore Guide, Release 1.0*—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*—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*—Contains a description of the new and changed features, important notes, caveats, and documentation updates for Cisco IPICS release 1.0
- *Cisco IPICS 1.0 Resources Card* (Documentation Locator)—Provides a summary of the documentation that is available for Cisco IPICS release 1.0
- *Cisco IPICS Compatibility Matrix*—Provides a list of compatible versions for all Cisco IPICS components

You can access Cisco IPICS documentation at this 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 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.

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.

Convention	Description
^ 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

Cisco IP Interoperability and Collaboration System (IPICS) provides voice interoperability among disparate systems. It offers an IP standards-based solution that interconnects voice channels, talk groups, and virtual talk groups, and that provides powerful and flexible management of personnel and media resources.

This chapter provides an overview of Cisco IPICS. It also introduces the Cisco IPICS Administration Console, which gives you complete control over Cisco IPICS operation and administration. Read this chapter if you are setting up Cisco IPICS for the first time or if you want to learn about the basic components and concepts of Cisco IPICS.

Tip If you use Cisco IPICS only for communicating with other users and you do not require any introductory material, go to Chapter 5, "Administration Console: User Tasks." That chapter describes how to log in to Cisco IPICS, download your Push-to-talk Management Center (PMC), set up push-to-talk (PTT) channels for the PMC and Cisco IP Phone, and complete your user profile

This chapter includes these sections:

- Getting Started, page 1-2—Provides a guide to the tasks that you perform when you set up Cisco IPICS
- Cisco IPICS Overview, page 1-3—Introduces the main hardware and software components of Cisco IPICS

- Cisco IPICS Roles, page 1-7—Explains the roles (user, system administrator, dispatcher, and operator) that a user of Cisco IPICS may have
- Cisco IPICS Administration Console, page 1-8—Describes how to access the Administration Console, the web interface that allows you to configure and monitor Cisco IPICS functions, access a variety of system tools, and perform many other administrative tasks

Getting Started

After you install Cisco IPICS, you perform a series of procedures in sequence to set up and configure Cisco IPICS for use. Table 1-1 lists these procedures and provides references to more information about each one.

Use this information as a guide when you set up Cisco IPICS for the first time.

For information about installing Cisco IPICS, refer to *Cisco IPICS Server Installation Guide*.

Table 1-1 Overview of Getting Started with Cisco IPICS

Procedure	Reference	Checkoff
Become familiar with Cisco IPICS		
1. Learn about the hardware and software components that are part of Cisco IPICS	Cisco IPICS Overview, page 1-3	❑
2. Learn about the roles that Cisco IPICS users can have	Cisco IPICS Roles, page 1-7	❑
3. Learn about the Cisco IPICS Administration Console, including how to access this application	Cisco IPICS Administration Console, page 1-8	❑
Set Up and Configure Cisco IPICS		
1. Configure RMSs	See the "Managing the RMS" section on page 2-2	❑
2. Configure locations	See the "Managing Locations" section on page 2-38	❑
3. Configure the multicast pool	See the "Managing the Multicast Pool" section on page 2-30	❑

Table 1-1 Overview of Getting Started with Cisco IPICS (continued)

Procedure	Reference	Checkoff
4. Create push-to-talk channels	See the "Managing PTT Channels and Channel Groups" section on page 2-17	❑
5. Determine user roles and add users	See the "Managing Users and User Groups" section on page 3-3	❑
6. Create VTG templates	See the "Managing VTG Templates" section on page 4-8	❑
7. Ensure that the server is hosting the current version of the PMC	See the "Managing PMC Automatic Updates" section on page 2-48	❑
8. Create policies, which activate and deactivate virtual talk groups	See the "Managing Policies" section on page 4-26	❑
9. Create operational views, if needed	See Chapter 6, "Operational Views"	❑
10. Set up Cisco IP Phones, if needed	See Appendix B, "Setting Up and Using the Cisco IP Phone with Cisco IPICS"	❑

Cisco IPICS Overview

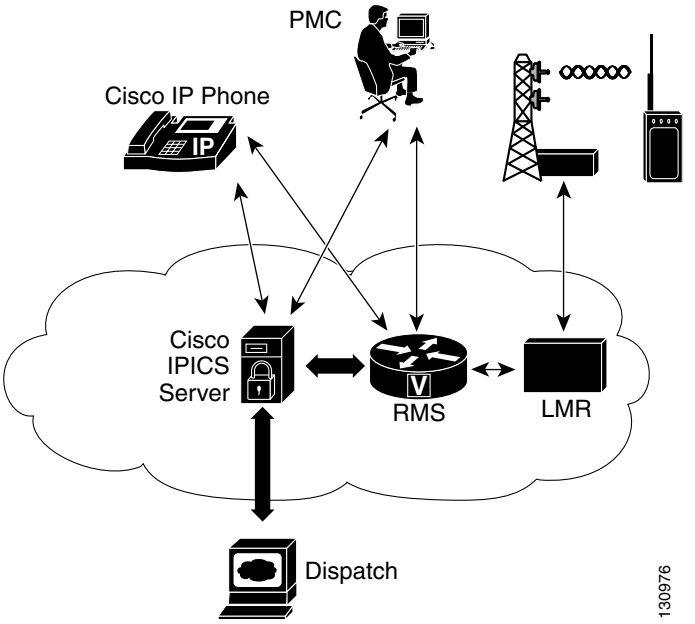
Cisco IPICS can be deployed in a variety of configurations. Your configuration will depend on the types of communications devices that users will employ, the media types that will be used, your interoperability requirements, and so on. A Cisco IPICS deployment will include various hardware and software components to provide the functionality that you require, including some or all of the following:

- Cisco IPICS Server, page 1-5—Provides the core functionality of the Cisco IPICS system
- Push-to-Talk Management Center, page 1-5—Standalone PC-based software application that provides push-to-talk (PTT) functionality for end-users, dispatch personnel, and administrators
- LMR Gateways, page 1-6—Provide radio network interoperability and application integration

- RMS, page 1-6—Enables a PMC to remotely attach to a VTG or channel, enables channels to be brought together in VTGs, and performs other mixing functions
- Networking Components, page 1-7—Include switches, routers, firewalls, mobile access routers, and wireless access points and bridges
- Cisco CallManager Functionality and Voice over IP Services, page 1-7—Provide voice interoperability between radio and non-radio networks
- Audio Clients, page 1-7—Devices such as LMRs and Cisco IP Phones that let users participate in VTGs

Figure 1-1 illustrates a typical Cisco IPICS deployment.

Figure 1-1 Cisco IPICS Components in a Typical Deployment



Cisco IPICS Server

Every Cisco IPICS deployment includes a Cisco IPICS server, which is the center of all Cisco IPICS activity. The Cisco IPICS server software runs on the Cisco Linux operating system. It performs the following functions:

- Hosts the Administration Console, which gives you control over operation and administration of Cisco IPICS
- Provides Cisco IPICS authentication and security services
- Stores data that is required for operation
- Enables integration with various media resources, such as RMSs, PMCs, and Cisco IP Phones
- Hosts the Policy Engine, which provides a set of rules for selected operations of Cisco IPICS

Push-to-Talk Management Center

The Push-to-Talk Management Center (PMC) is a PC-based software application that enables end-users, dispatch personnel, and administrators to participate, via an IP network, in one or more talk groups or VTGs at the same time. The PMC acts as a land mobile radio (LMR) or push-to-talk (PTT) audio application. Through an intuitive interface, the PMC application lets users monitor and participate in one or multiple PTT channels or VTGs at the same time.

The PMC runs on Microsoft Windows 2000 and Windows XP operating systems.

You install the PMC application on your PC after downloading the software from the Cisco IPICS server. For more information, see the "Downloading the PMC" section on page 5-6. After you install the application the first time, Cisco IPICS automatically upgrades your PMC with new versions when they become available.

The Cisco IPICS operator sets up user access to the PMC. The operator also assigns specific PTT channels that PMC users can monitor and use to participate in conferences with other Cisco IPICS users.

Figure 1-2 shows an example of the PMC application user interface. You can change the look of the PMC user interface by choosing another Cisco-provided or custom skin, as explained in *Cisco IPICS PMC Installation and User Guide*.

Figure 1-2 4-channel PMC

LMR Gateways

Gateways provide radio network interoperability using the Cisco IOS Hoot ‘n’ Holler feature. They provide a bridge between radio frequencies and IP multicast streams. The LMR gateway functionality is often installed as an additional feature in a router.

RMS

A router media service (RMS) provides a variety of functions for Cisco IPICS, including:

- Support through its loopback function for combining two or more VTGs
- Mixing of multicast channels to support VTGs

- Mixing of remote PMC unicast connections to a multicast channel or a VTG
- Support for unicast M1:U12:M2 connection trunks

Networking Components

Networking Components include switches, routers, firewalls, mobile access routers, and wireless access points and bridges.

Cisco CallManager Functionality and Voice over IP Services

Cisco CallManager and VoIP services enable selected Cisco IP Phone models to participate in channels and VTGs.

Audio Clients

Audio clients are devices through which users participate in VTGs. They include LMRs and the Cisco IP Phone models 7960G and 7970G.

Cisco IPICS Roles

Every person who uses Cisco IPICS is assigned one or more roles. Roles define what Cisco IPICS features a user can access and what functions that user can perform. In this way, roles help provide system security.

Table 1-2 describes the Cisco IPICS roles.

Table 1-2 Cisco IPICS Roles

Role	Description	Reference
User	Has the ability to maintain personal information, download the PMC client application, and specify communication preferences that are used to configure audio devices. Each Cisco IPICS user is assigned the user role. The user may have additional roles	See Chapter 5, "Administration Console: User Tasks."
System administrator	Responsible for installing and setting up Cisco IPICS resources, such as servers, routers, multicast addresses, locations, and PTT channels. 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.	See Chapter 2, "Administration Console: System Administrator Tasks."
Operator	Responsible for setting up and managing users, granting access to Cisco IPICS and the PMC, and assigning user channels, roles and operational views (ops views).	See Chapter 3, "Administration Console: Operator Tasks."
Dispatcher	Responsible for setting up system policies and setting up VTG templates, activating VTGs to begin conferences, and adding or removing participants in VTG templates and active VTGs. Also monitors active VTGs and events and can mute and unmute users, as necessary.	See Chapter 4, "Administration Console: Dispatcher Tasks."

Cisco IPICS Administration Console

The Cisco IPICS server provides a web-based application called the Administration Console. You use the Administration Console to manage Cisco IPICS activities. A user uses the Administration Console to maintain personal information and update the PMC. A system administrator and operator use the Administration Console to set up system resources and participants. A dispatcher uses the Administration Console to view and manage active and stored VTGs.

This section includes these topics.

Browser Guidelines

When you access the Cisco IPICS Administration Console by using a browser, follow these guidelines:

- Windows in the Administration Console do not refresh automatically. As a best practice, make sure that you update your browser window often and before you perform any server administration functions to ensure that you are working with the most current information. If you attempt to perform an administration update in a window that does not display the most current data, the update will not succeed and Cisco IPICS will display an error. If this situation occurs, update your browser window and retry the operation.
- To ensure that a current window displays the most up-to-date information, refresh it by clicking the button or tab that you used to display it. Cisco IPICS does not support the use of the browser **Refresh** button to refresh a window in the Administration Console.
- The Cisco IPICS Administration Console uses browser pop-up windows for certain functionality. If you have any browser pop-up blocker software installed on your machine, you may be prevented from performing certain actions. To ensure that you are not blocked from performing administration tasks, disable any pop-up blocker software that is installed on your machine before you use the Administration Console.
- Cisco IPICS does not support the use of more than one browser session at a time, on the same machine, for accessing the Administration Console. If you use multiple browser sessions to access the Administration Console, you may

experience unexpected results. To ensure proper server operational behavior, do not open more than one browser session at a time on the same machine for Administration Console functions.

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

Accessing the Administration Console

After you install Cisco IPICS, you can access the Administration Console from any computer that meets these requirements:

- Has IP connectivity to the Cisco IPICS server
- Running either of these operating systems:
  - Windows 2000 SP4 or higher
  - Windows XP SP2 or higher
- Running Internet Explorer version 6.0.2 or higher

To access the Cisco IPICS Administration Console, perform these steps:

Procedure

Step 1 Start Internet Explorer and enter the IP address or the host name of the server on which Cisco IPICS is running.

The Authentication window displays.

Step 2 In the Authentication window, take one of these actions:

- If you are accessing Cisco IPICS for the first time, enter these Cisco IPICS default login credentials:
  - User Name: **ipics**
  - Password: **cisco123**
- If you have been configured as a Cisco IPICS user, enter your user name and password in the User Name and Password fields.

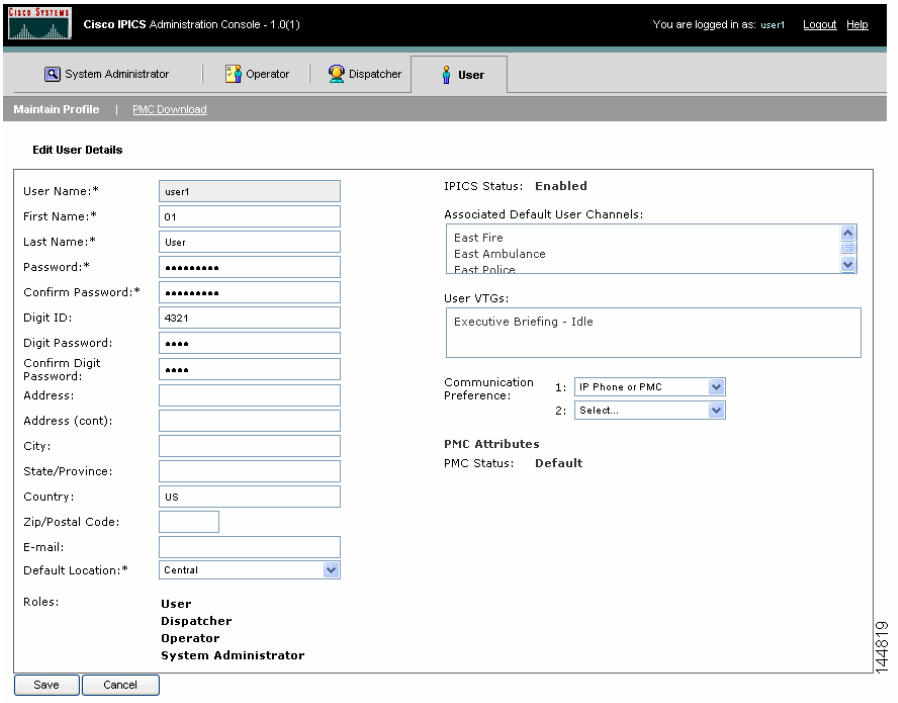
User names and passwords are case-sensitive, so make sure to enter them exactly as they are configured.

Note To help maintain the security of your Cisco IPICS system, change the default Cisco IPICS login credentials, and change your user name and password regularly.

Step 3 Click **Log In**.

The User Details window displays, as shown in Figure 1-3. This example shows tabs for each of the Cisco IPICS user roles. The tabs that appear in your window will correspond to your roles, so you may not see all four tabs in your window.

Figure 1-3 User Details Window



You can perform a variety of activities in the User Details window. Table 1-3 describes these activities.

Table 1-3 User Details Window Activities

Activity	Reference
Update your user information	See the "Managing Your User Profile" section on page 5-2
Access the Download PMC window (when the User tab is selected)	See the "Downloading the PMC" section on page 5-6
Choose a tab to access additional windows for its corresponding role (if you have a role other than user)	See the appropriate chapter: • Chapter 2, "Administration Console: System Administrator Tasks" • Chapter 3, "Administration Console: Operator Tasks" • Chapter 4, "Administration Console: Dispatcher Tasks" • Chapter 5, "Administration Console: User Tasks"
Obtain online help	See the "Getting Help in the Administration Console" section on page 1-14
Log out and exit from the Administration Console	See the "Exiting the Administration Console" section on page 1-13

Exiting the Administration Console

You can exit the Administration Console from any window within the application. To do so, follow these steps:

Step 1 Click **Logout** in any Administration Console window.

Step 2 Click **OK** in the pop-up window that prompts you to confirm that you want to log out.

Entering Required Information in Administration Console Windows

Many of the Administration Console windows let you enter a variety of information. You might enter information by typing in fields, choosing from drop-down lists, checking check boxes, or clicking radio buttons, depending on the window.

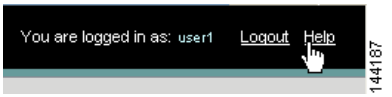
An asterisk (*) next to a field, drop-down list, check box, or radio button indicates required information. You must provide this information before you can save your changes and exit the window.

Getting Help in the Administration Console

You can access the Cisco IPICS help system from any window in the Administration Console. The help system provides online access to the information that is in this *Cisco IPICS Server Administration Guide*.

To access Cisco IPICS online help, click **Help** in any Administration Console window, as shown in Figure 1-4.

Figure 1-4 Accessing Cisco IPICS Help



Administration Console Timeout

For increased system security, the Administration Console will time out after 30 minutes of non use. In this situation, the current Administration Console window remains displayed, but Cisco IPICS will prompt you to log back in when you attempt to perform a function. To log back in, enter your user name and password, and then click **Log In**.

Administration Console: System Administrator Tasks

The Cisco IPICS system administrator is responsible for installing Cisco IPICS and for setting up Cisco IPICS resources, including servers, routers, multicast addresses, locations, and PTT channels. The system administrator also manages the Cisco IPICS licenses and PMC versions, monitors the status of the system, reviews log files as needed, and creates operational views.

In addition, the system administrator often manages backing up and restoring Cisco IPICS data. For more information, refer to *Cisco IPICS Backup and Restore Guide*.

You perform most Cisco IPICS system administrator activities from the System Administrator window in the Administration Console. To access this window, log in to the Administration Console as described in the "Accessing the Administration Console" section on page 1-10, then choose the **System Administrator** tab.

Note You must be assigned the system administrator role to access the System Administrator window.

The following sections describe many of the activities that you can perform from the System Administrator window:

- Managing Locations, page 2-38
- Managing Activity Logs, page 2-41
- Managing Licenses, page 2-45
- Managing PMC Automatic Updates, page 2-48
- Managing the PMC Installer, page 2-51

For information about managing operational views in the Ops Views window, see Chapter 6, "Operational Views."

For information about managing system information in the System Status window, refer to *Cisco IPICS Troubleshooting Guide*.

For information about managing backups in the Database window, refer to *Cisco IPICS Backup and Restore Guide*.

For information about managing options in the Options window, refer to *Cisco IPICS Troubleshooting Guide*.

Managing the RMS

A Router Media Service (RMS) enables a variety of functionality for Cisco IPICS. For details, see the "RMS" section on page 1-6.

Note Before you perform the RMS management procedures that are described in the following sections, you must configure the RMS. For more information see Appendix A, "RMS Configuration."

As a Cisco IPICS system administrator, you can perform these RMS management tasks:

- Viewing and Editing RMS Details, Activating an RMS, and Deactivating an RMS, page 2-4
- Adding an RMS, page 2-9
- Viewing and Configuring Loopbacks, page 2-11
- Deleting an RMS, page 2-14
- Merging RMS Configuration, page 2-14

- Updating RMS Configuration, page 2-15
- Viewing RMS Configuration, page 2-16

You perform the RMS management tasks in the Administration Console Manage RMS window. For more information about this window, including how to access it, see the "Manage RMS Window" section on page 2-3.

Note Cisco IPICS is not intended to provide complete management capabilities for an RMS. Cisco IPICS manages only the voice-specific parameters that are necessary to set up audio services for Cisco IPICS. For additional information about setting up, configuring, and managing an RMS, refer to the documentation for the RMS.

Manage RMS Window

The Manage RMS window lists the RMSs that are available in your Cisco IPICS network. It also lets you perform the RMS management functions.

To open the Manage RMS window, click the **RMS** link in the Administration Console System Administrator tab.

The Routers area in the Manage RMS window displays the name of each RMS that is installed in your Cisco IPICS network. An icon next to each router name indicates the status of the router, as described in Table 2-1.

Table 2-1 RMS Status Icons

Icon	Meaning
	RMS is operating.
	RMS is deactivated. It might be turned off, unreachable, not configured, or deactivated through Cisco IPICS.

Viewing and Editing RMS Details, Activating an RMS, and Deactivating an RMS

You can view and edit information for any RMS in your Cisco IPICS network. You can also deactivate an RMS, which makes it unavailable for use by Cisco IPICS, or reactivate an RMS. You perform these tasks in the Edit Router Details area.

By default, Cisco IPICS polls the RMS every 10 minutes and updates information in the Edit Router Details area if information has changed. (You can change this default polling period by entering a new value in the RMS Polling Frequency field in the System Administrator Options window. For more information, refer to *Cisco IPICS Troubleshooting Guide*.) To ensure that you see current information, redisplay the Edit Router Details area if it has been displayed for longer than the default polling period.

Note The Edit Router Details displays information for items that have been configured in Cisco IPICS. You can obtain other RMS configuration information from the router as described in the documentation for the router, and by using the Show Configuration feature as described in the "Viewing RMS Configuration" section on page 2-16.

Editing or Viewing RMS Details

You can edit or view a variety of information for an RMS. To do so, perform the following steps.

For information about accessing the Manage RMS window, see the "Manage RMS Window" section on page 2-3.

Procedure

Step 1 In the Manage RMS window Routers area, take either of these actions:

- Click the RMS for which you want to view or change information and then click **Details**
- Double-click the RMS for which you want to view or change information

The Edit Router Details area for the selected RMS displays.

Note If you choose another RMS when the Edit Router Details area is displayed, the information in this area does not change for the new RMS until you click **Details** again or double-click the new RMS.

Step 2 If you want to change any RMS information, except updating the name, configuring loopbacks, or reserving or unreserving DS0s, click **Deactivate**.

This action makes the RMS temporarily unavailable to Cisco IPICS.

Before you make changes, wait until all RMS resources are not in use, or manually disable the channel or deactivate any VTG that involves this RMS.

Step 3 View or update the information that is described in Table 2-2

Table 2-2 Router Details Area Fields

Field	Description
Identification	
Name	Name of the RMS. The name can include alphanumeric characters, spaces, and any of these characters: . , – ‘ # ( ) / :.
Location	Multicast domain that contains the multicast addresses that can be accessed by this RMS. An RMS must be configured with the same location that is configured for the channels that it serves. When the Location is set to All, this RMS can access multicast addresses that have been configured for accessibility in every location (multicast domain). The location name can include alphanumeric characters, spaces, and any of these characters: . , – ‘ # ( ) / :.

Table 2-2 Router Details Area Fields (continued)

Field	Description
Status—*Display only*	• Operational—RMS has at least one loopback configured and that is operating. • Unconfigured—RMS has no loopbacks. • Stopping—RMS has been deactivated but has at least one DS0 in use by Cisco IPICS. The RMS will become deactivated when Cisco IPICS no longer uses any of its voice ports. • Deactivated— RMS has been deactivated and has no DS0s in use. **Note** You can change the user name, password, multicast address, or location of the RMS only when it is in the Deactivated state. • Unreachable—RMS cannot be reached by the Cisco IPICS server.
Connection Properties	
IP Address—*Display only*	Loopback IP address of the RMS.
Host Name—*Display only*	Host name of the RMS.
User Name—*Display only*	User name that Cisco IPICS uses to access the RMS. This name must have administrator privileges on the RMS.
Password	Password that Cisco IPICS uses to access the RMS.
Type—*Display only*	Model number of the RMS.

Table 2-2 Router Details Area Fields (continued)

Field	Description
Controllers—*Display only*	T1 connections on the RMS. The number in parentheses is the number of ports on the corresponding controller.
Loopbacks	Mappings between two controllers that are physically connected. To change a loopback, choose a pair of controllers from the two Loopback drop-down lists and click **Add**. A controller appears in gray if it is in use. Each configured loopback appears in a list near the bottom of this area. To see detailed information about a loopback, click the right arrow next to its name. To see detailed information about all loopbacks, click **Expand All**. To collapse an expanded view of a loopback, click the down arrow next to its name. To collapse detailed information about all loopbacks, click **Collapse All**. For an explanation of the detailed loopback information, see the "Viewing and Configuring Loopbacks" section on page 2-11.

Step 4 If you changed information in the IP Address, User Name, or Password fields, make the corresponding change in the router using the configuration application of the router.

Step 5 Click **Save** to save your changes.

To exit without saving changes, click **Cancel**.

Step 6 If you deactivated the router, click **Activate** to reactivate it.

After you change information for an RMS, it can take up to 10 minutes (by default) for Cisco IPICS to recognize the changes. If you want to cause Cisco IPICS to recognize the changes immediately, see the "Updating RMS Configuration" section on page 2-15.

Note You can change the default time that Cisco IPICS takes to recognize an RMS by entering a new value in the RMS Polling Frequency field in the System Administrator Options window. For more information, refer to *Cisco IPICS Troubleshooting Guide*.

Deactivating or Activating an RMS

When you deactivate an RMS, it goes into the Deactivated state and becomes unavailable for use by Cisco IPICS until you activate it. You should deactivate an RMS when you make certain changes to it, as described in the "Editing or Viewing RMS Details" section on page 2-4.

If you deactivate an RMS that has one or more voice ports in use by Cisco IPICS, the RMS goes into the Stopping state. A router that is in stopping state will not serve additional PMC SIP connections or additional channels that are participants in active VTGs. Existing connections and channels that are served by the RMS are not affected. The RMS will become deactivated when Cisco IPICS no longer uses any of its voice ports.

When you activate an RMS, it becomes available for use by Cisco IPICS.

To deactivate or activate an RMS, perform the following steps.

For information about accessing the Manage RMS window, see the "Manage RMS Window" section on page 2-3.

Procedure

Step 1 In the Manage RMS window Routers area, take either of these actions:

- Click the RMS that you want to deactivate or activate and then click **Details**
- Double-click the RMS that you want to deactivate or activate

The Edit Router Details area for the selected RMS displays.

Step 2 Click **Deactivate** to deactivate an active RMS, or click **Activate** to activate a deactivated RMS.

Adding an RMS

When you add an RMS, you make it available to Cisco IPICS. Before you add an RMS, make sure that these conditions are met:

- The router must exist on the Cisco IPICS network and it must be configured as described in Appendix A, "RMS Configuration"
- At least one location must be defined, as described in the "Managing Locations" section on page 2-38

To add a new RMS in Cisco IPICS, perform the following steps.

For information about accessing the Manage RMS window, see the "Manage RMS Window" section on page 2-3.

Procedure

Step 1 In the Manage RMS window, click **Add**.

The Add New Router Media Service area displays at the bottom of the Manage RMS window.

Step 2 In the Add New Router Media Service area:

a. In the IP Address field, enter a loopback address.

The loopback access must be configured to support SIP calls.

b. In the User Name field, enter the user name required to log in to the RMS that you are adding.

c. In the Password field, enter the password required to log in to the RMS that you are adding.

d. From the Location drop-down list, choose a location that is defined by the IP address that you entered for the router.

e. Click **Save**.

If you do not want to add this RMS, click **Cancel**.

When you click **Save**, Cisco IPICS determines whether it can access the RMS. This process can take up to one minute. If the RMS is accessible, Cisco IPICS displays the Router Details area for the RMS. If the router is not accessible, a message informs you of the possible reason.

The Router Details area displays this information for the router that you are adding:

- Location—Location defined for this RMS
- Status—Displays Unconfigured because you have not yet saved the changes that you made
- IP Address—Loopback IP address that you entered for this router
- Host Name—Host name configured on the router
- User Name—Information that you entered for this router
- Password—Information that you entered for this router
- Type—Model number of the router that you are adding
- Controllers—T1 connections that the router has available for loopback

Step 3 In the Name field, enter a name for the RMS, if you want to change the name that displays in the list or routers in the Manager Routers window.

The name that displays by default is the router host name. You might find it useful to give the RMS a descriptive name. A name that you enter is for IPICS use only, it does not change the router host name.

Step 4 In the adjacent Loopbacks drop-down lists, create a loopback by choosing two controllers that are physically connected on the router, and then click **Add**.

Repeat this step as needed to create additional loopbacks.

Step 5 Configure DS0s for each loopback as described in the "Viewing and Configuring Loopbacks" section on page 2-11.

Step 6 Click **Save** to save the configuration for this RMS.

If you do not want to add this RMS, click **Cancel**.

After you add an RMS, it can take up to 10 minutes (by default) for Cisco IPICS to recognize the addition. If you want to cause Cisco IPICS to recognize the addition immediately, see the "Updating RMS Configuration" section on page 2-15.

Viewing and Configuring Loopbacks

Each loopback that you create in Cisco IPICS appears in a list near the bottom of the Edit Router Details area. You can perform the following tasks related to loopbacks:

- Viewing Detailed Information about a Loopback, page 2-11
- Enabling DS0s in a Loopback, page 2-12
- Disabling DS0s in a Loopback, page 2-13
- Removing a Loopback, page 2-13

Viewing Detailed Information about a Loopback

To see detailed information about a loopback, click the right arrow next to its name. To collapse an expanded view of a loopback, click the down arrow next to its name.

To see detailed information about all loopbacks, click **Expand All**. To collapse detailed information about all loopbacks, click **Collapse All**.

An expanded view of a loopback provides this information for each time slot in the loopback:

- Number—DS0 in the loopback
- State—One of the following:
  - Enabled—DS0 can be used by Cisco IPICS
  - Disabled—DS0 cannot be used by Cisco IPICS
- DS0 Status—One of the following:
  - In Use—DS0 is being used to add a channel to a VTG, add a VTG to a VTG, or add a SIP connection for a channel for a user
  - Unavailable—DS0 is reserved for non-Cisco IPICS use
  - Available—DS0 can be used by Cisco IPICS
  - Error—DS0 is misconfigured
- DS0 Source and DS0 Destination—Connections that the loopback is making. Port Source can be a channel or a VTG. Port Destination can be a channel, a VTG, or a user.

Enabling DS0s in a Loopback

After you create a loopback, you must enable the DS0s that can be used by Cisco IPICS. You can enable DS0s in one loopback at a time, or in several loopbacks at a time.

To enable DS0s in a loopback, perform these steps:

Procedure

Step 1 Expand each loopback in which you want to enable DS0s by clicking the right arrow next to its name or by clicking **Expand All**.

Step 2 Check the check box next to each DS0 that you want to enable.

If you want to enable all DS0s in a loopback, check the check box next to Number at the top of the list of DS0s for that loopback.

If you want to uncheck check boxes, take one of these actions:

- Uncheck specific check boxes, or uncheck the check box next to Number at the top of the list of DS0s to clears all check boxes for that loopback.
- Click **Clear** to clear all check boxes for all loopbacks.

Step 3 Click **Enable DS0s**.

The state for the DS0 displays **Enabled** in green text.

Step 4 Click **Save**.

If you do not want to enable the DS0 or DS0s, click **Cancel**.

Disabling DS0s in a Loopback

If you disable a DS0 in a loopback, it cannot be used by Cisco IPICS. You can disable DS0s in one loopback at a time, or in several loopbacks at a time.

To disable DS0s in a loopback, perform these steps:

Procedure

Step 1 Expand each loopback in which you want to disable DS0s by clicking the right arrow next to its name or by clicking **Expand All**.

Step 2 Check the check box next to each DS0 that you want to disable.

If you want to disable all DS0s in a loopback, check the check box next to Number at the top of the list of DS0s for that loopback.

If you want to uncheck check boxes, take one of these actions:

- Uncheck specific check boxes, or uncheck the check box next to Number at the top of the list of DS0s to clears all check boxes for that loopback.
- Click **Clear** to clear all check boxes for all loopbacks.

Step 3 Click **Disable DS0s**.

The state for the DS0 displays **Disabled** in red text.

Step 4 Click **Save**.

If you do not want to disable the DS0 or DS0s, click **Cancel**.

Removing a Loopback

To remove a loopback, click **Remove** next to its name, and then click **Save**.

If you decide not to remove the loopback, click **Add** next to its name or click **Cancel** instead of clicking **Save**.

Deleting an RMS

Deleting an RMS removes all of its resources from Cisco IPICS and makes the RMS unavailable to Cisco IPICS.

You cannot delete an RMS if any of its DS0s are in use by Cisco IPICS.

To delete an RMS, perform the following steps.

For information about accessing the Manage RMS window, see the "Manage RMS Window" section on page 2-3.

Procedure

Step 1 In the Manage RMS window Routers area, click the RMS that you want to delete.

The RMS becomes highlighted in blue.

Step 2 Click **Delete**.

A dialog box prompts you to confirm the deletion.

Step 3 To confirm the deletion, click **OK**.

If you do not want to delete this RMS, click **Cancel**.

Merging RMS Configuration

The Merge RMS configuration procedure updates Cisco IPICS with this router information:

- Host name
- Router type
- Controllers

Use this procedure if you add or remove controllers on the router or if you change its host name, and you want Cisco IPICS to recognize the change.

To update RMS configuration, perform the following steps.

For information about accessing the Manage RMS window, see the "Manage RMS Window" section on page 2-3.

Procedure

Step 1 In the Manage RMS window Routers area, click the name of the RMS with the configuration that you want to merge.

The RMS name becomes highlighted.

Step 2 Click **Merge Configuration**.

Cisco IP displays changes in the Edit Router Details area.

Step 3 Click **Save** to update the Cisco IPICS RMS configuration with the changes.

If you do not want to save the changes, click **Cancel**.

Updating RMS Configuration

Updating the configuration of an RMS applies the RMS configuration that is specified in Cisco IPICS to the RMS. This procedure can be useful in these situations:

- You have changed information for an RMS as described in the "Viewing and Editing RMS Details, Activating an RMS, and Deactivating an RMS" section on page 2-4 and you do not want to wait for Cisco IPICS to recognize the changes, which can take up to 10 minutes (by default).
- You have added an RMS as described in the "Adding an RMS" section on page 2-9 and you do not want to wait for Cisco IPICS to recognize the addition, which can take up to 10 minutes (by default).
- You have restarted an RMS and are having voice connectivity or voice quality issues. Updating the configuration of the RMS can help eliminate the router configuration as the source of the problem.
- The RMS has restarted but Cisco IPICS has not yet updated the router configuration with the configuration that is specified in Cisco IPICS. (An RMS that shuts down returns to its default configuration when it restarts. Within 10 minutes—by default—after it restarts, Cisco IPICS compares the current RMS configuration with the RMS configuration in the Cisco IPICS database. If there is a discrepancy, Cisco IPICS refreshes the RMS configuration to match the configuration in the database.)

Note Manually updating the configuration for an RMS disconnects all users that are connected to the RMS through a SIP connection and may interrupt any active VTG participant that is hosted on that RMS.

To manually update the configuration for an RMS, perform the following steps.

For information about accessing the Manage RMS window, see the "Manage RMS Window" section on page 2-3.

Procedure

Step 1 In the Manage RMS window Routers area, click the RMS with the configuration that you want to reload.

The RMS name becomes highlighted.

Step 2 Click **Update Configuration**.

Viewing RMS Configuration

You can view the configuration file for any router that is configured for use with the Cisco IPICS network and that is operating. Configuration information can be helpful if you need to troubleshoot a problem with an RMS.

To view the RMS configuration, perform the following steps.

For information about accessing the Manage RMS window, see the "Manage RMS Window" section on page 2-3.

Procedure

Step 1 In the Manage RMS window Routers area, click the RMS for which you want to update the configuration.

The router becomes highlighted.

Step 2 Click **Show Configuration**.

Cisco IPICS displays the configuration in a new window.

Tip You can use the **Show Configuration** button to update information that displays in the Router Details area.

Managing PTT Channels and Channel Groups

A PTT channel, also called a *channel*, is a multicast communications path that allows users to communicate with each other.

A channel group is a logical grouping of PTT channels. Channel groups allow Cisco IPICS dispatchers to work with multiple PTT channels efficiently. For example, instead of dragging individual PTT channels one at a time to set up a VTG, a Cisco IPICS dispatcher can drag a channel group to move all PTT channels in the group. A PTT channel can be in as many channel groups as you require.

As a Cisco IPICS system administrator, you can perform these PTT channel and channel group management tasks:

Channel group management tasks

- Viewing and Editing Channel Group Details, page 2-20
- Creating a Channel Group, page 2-21
- Deleting a Channel Group, page 2-22
- Adding a PTT Channel to a Channel Group, page 2-23
- Removing a PTT Channel from a Channel Group, page 2-24

Channel management tasks

- Viewing and Editing Channel Details, page 2-25
- Adding a PTT Channel, page 2-28
- Deleting a PTT Channel, page 2-29

You perform the PTT channel management tasks in the Administration Console Manage Channels window. For more information about this window, including how to access it, see the "Manage Channels Window" section on page 2-18.

Manage Channels Window

The Manage Channels window lists the channel groups and the channels that are available in your Cisco IPICS network. It also lets you perform the PTT channels and channel groups management functions.

To open the Manage Channels window, click the **Channels** link in the Administration Console System Administrator tab.

The Channels Group area in the Manage Channels window displays the name of each channel group that is configured in Cisco IPICS. To see the channels that are in a channel group, expand the group by clicking the right arrow next to the group name. Click the down arrow next to a group name to collapse an expanded group.

The Channels area displays the name of each channel that is configured in Cisco IPICS.

For information about the icons and colors that appear in the Manage Channels window, see these sections:

- Manage Channels Window Icons, page 2-18
- Manage Channels Window Color Coding, page 2-19

Manage Channels Window Icons

Icons in the Manage Channels window provide information about each channel group and channel name, as described in Table 2-3.

Table 2-3 Channel Group and Channel Icons

Icon	Meaning
	PTT channel.
	Channel group.
	Busy PTT channel. A channel is busy when it is use by an active VTG.
	Secure PTT channel. You can designate a PTT channel as secure when you add the channel.
	Unavailable PTT channel. A channel is unavailable when it is disabled.

Manage Channels Window Color Coding

Information in the Manage Channels window is color coded as described in Table 2-4.

Table 2-4 Color Coding in Manage Channels Window

Color	Meaning
Green channel name in Channel Groups area	You have dragged the channel to the channel group but have not yet clicked **Save**. For more information, see the "Adding a PTT Channel to a Channel Group" section on page 2-23.
Red channel name in Channel Groups area	You have dragged the channel from the channel group but have not yet clicked **Save**. For more information, see the "Removing a PTT Channel from a Channel Group" section on page 2-24.

Table 2-4 Color Coding in Manage Channels Window

Color	Meaning
Blue highlighted channel group or channel name	Channel group or channel is selected in preparation for clicking **Details**, **Add**, or **Delete**.
Orange highlighted channel group or channel name	You have clicked another channel group or channel while the Details area for this channel group or channel is displayed.

Viewing and Editing Channel Group Details

You can view information for and change the name of any channel group in your Cisco IPICS network. You do so in the Edit Channel Groups Details area.

To edit or view channel group details, perform the following steps.

For information about accessing the Manage Channels window, see the "Manage Channels Window" section on page 2-18.

Procedure

Step 1 In the Manage Channels window Channel Groups area, take either of these actions:

- Click the channel group for which you want to view or change information and then click **Details**
- Double-click the channel group for which you want to view or change information

The Edit Channel Group Details area for the selected channel group displays.

Note If you choose another channel group when the Edit Channel Group Details area is displayed, the information in this area does not change for the new channel group until you click **Details** again or double-click the new channel group.

Step 2 View or update the information that is described in Table 2-5.

Note If Operational Views is enabled, additional ops views fields appear in this area. For more information, see Chapter 6, "Operational Views."

Table 2-5 Edit Channel Group Details Area Fields

Field	Description
Static Attributes	
Channel Group Name	Name of the channel group. The name can include alphanumeric characters, spaces, and any of these characters: . , – ‘ # ( ) / :_ .
Runtime Attributes	
Associated VTGs—*Display only*	VTG or VTGs in which channel group is a member. Includes one of these designations: • Active—Channel group is a participant in an active VTG • Idle—Channel group is a member of a VTG template

Step 3 Click **Save** to save your changes.

To exit without saving changes, click **Cancel**.

Creating a Channel Group

A channel group provides a a way to organize channels. You may find it useful to create and name channel groups according to location (for example, South Area PTT Channels) or function (for example, Executive PTT Channels).

To create a channel group, perform the following steps.

For information about accessing the Manage Channels window, see the "Manage Channels Window" section on page 2-18.

Procedure

Step 1 In the Manage Channel Groups window Channel Groups area, click **Add**.

The Edit Channel Group Details area for a new channel group displays.

Step 2 In the Channel Group Name field, enter a name for the new channel group.

The name can include alphanumeric characters, spaces, and any of these characters: . , – ‘ # ( ) / :_ .

Step 3 Optional. If Operational Views is enabled, enter appropriate information in the Ops View Attributes fields.

For more information, see Chapter 6, “Operational Views.”

Step 4 Click **Save** to save the new channel group

If you do not want to create this channel group, click **Cancel**.

Deleting a Channel Group

When you delete a channel group, it is no longer available to Cisco IPICS. Deleting a channel group does not affect the channels that are contained in the channel group.

You cannot delete a channel group that is a participant in an active VTG or that is a member of a VTG template. You must remove the channel group from the VTG before you can delete it.

To delete a channel group, perform the following steps.

For information about accessing the Manage Channels window, see the “Manage RMS Window” section on page 2-3.

Procedure

Step 1 In the Manage Channels window Channel Groups area, click the channel group that you want to delete.

The channel group becomes highlighted in blue.

Step 2 Click **Delete** in the Channel Groups area.

A dialog box prompts you to confirm the deletion.

Step 3 To confirm the deletion, click **OK**.

If you do not want to delete this channel group, click **Cancel**.

Adding a PTT Channel to a Channel Group

Adding a PTT channel to a channel group makes the channel part of that group. You can add the same PTT channel to multiple channel groups.

You cannot add a channel to a channel group that is a participant in an active VTG or that is a member of a VTG template. You must first remove the channel group from the active VTG or from the VTG template.

For information about creating channels, see the "Adding a PTT Channel" section on page 2-28.

To add a PTT channel to a channel group, perform the following steps.

For information about accessing the Manage RMS window, see the "Manage Channels Window" section on page 2-18.

Procedure

Step 1 In the Manage Channels window Channel Groups area, display the channel group to which you want to add the PTT channel.

Step 2 Drag the PTT channel name that you want to add from the Channels area to the desired channel group.

When you release the mouse button, the PTT channel is added to the group. If the channel group is expanded, you will see the newly added PTT channel displayed in green.

Repeat this step as needed to add other channels to channel groups.

Step 3 Click **Save** to complete the additions that you have made.

If you want to undo the changes that you made since you last clicked **Save**, click **Revert**.

Removing a PTT Channel from a Channel Group

When you remove a PTT channel from a channel group, the channel is no longer a part of that group. Removing a PTT channel from a channel group does not remove the channel itself from Cisco IPICS, nor does it remove the channel from any other channel group to which it belongs.

You cannot remove a PTT channel from a channel group that is a participant in an active VTG or that is a member of a VTG template. You must first remove the channel group from the active VTG or from the VTG template.

To remove a PTT channel from a channel group, perform the following steps.

For information about accessing the Manage RMS window, see the "Manage Channels Window" section on page 2-18.

Procedure

Step 1 In the Manage Channels window Channel Groups area, display the channel group from which you want remove a PTT channel.

Step 2 If the PTT channels in the channel group are not visible, click the right arrow next to the group name to expand it.

Step 3 Locate the channel that you want to remove and drag it out of the Channel Groups area.

When you release the mouse button, the channel name changes to red.

Repeat this step as needed to remove other channels from the channel group.

Step 4 Click **Save** to complete removing the channels.

If you want to undo the changes that you made since you last clicked **Save**, click **Revert**.

Viewing and Editing Channel Details

You can view and edit information for any channel. You do so in the Edit Channel Details area.

To edit or view channel details, perform the following steps.

For information about accessing the Manage Channels window, see the "Manage Channels Window" section on page 2-18.

Procedure

Step 1 In the Manage Channels window Channel area, take either of these actions:

- Click the channel for which you want to view or change information and then click **Details**
- Double-click the channel for which you want to view or change information

The Edit Channel Details area for the selected channel displays.

Note

- If Operational Views is enabled, additional ops views fields appear in this area. For more information, see Chapter 6, "Operational Views."
- If you choose another channel when the Edit Channel Details area is displayed, the information in this area does not change for the new channel until you click **Details** again or double-click the new channel group.

Step 2 View or update the information that is described in Table 2-6

Table 2-6 Edit Channel Details Area Fields

Field	Description
Static Attributes	
Channel Name	Name of the channel. The name can include alphanumeric characters, spaces, and any of these characters: . , – ‘ # ( ) / :_ .
Preferred Codec	Codec (G.711 or G.729) used by this channel. Use G.711 if this channel should be available to Cisco IP Phone users or will be part of a VTG. Use G.711 or G.729 if this channel will be available to PMC users. G.729 uses less bandwidth but consumes more PMC resources and router resources than G.711.
Secure Flag	Indicates whether this channel is a secure channel. This field is for reference only and should be set to reflect the configuration of the channel in your network. Changing this setting does not affect the security configuration of the channel.
Status—*Display only*	Displays one the following states: • Active—Channel is an active participant in an active VTG • Idle—Channel is available for use in a VTG • Pending—A VTG in which this channel is a participant has been activated and the channel is being initialized • Disabled—Channel is disabled

Table 2-6 Edit Channel Details Area Fields (continued)

Field	Description
Connection Attributes	
Location	Users from the specified locations can access this channel without using additional network resources. Users from other locations can only access this channel through a SIP connection. If the network is configured so that the channel can be accessed by users in every location, set this value to **All**.
Type	Type of connection that Cisco IPICS and devices use to connect to this channel when connecting from the corresponding location.
Address	Multicast address, in the corresponding location, that is used to connect to this channel. The first octet in this address must be 224, 232, 233, 238, 239. Each subsequent octet must be in the range of 0 through 255. Two channels in the same location cannot have the same multicast address.
Port	Multicast address port number, in the corresponding location, that is used to connect to this channel. This value must be an even number in the range of 21000 through 65534.
Runtime Attributes	
Associated VTGs—*Display only*	VTGs that are associated with this channel.
Associated Users—*Display only*	Users that are associated with this channel.

Step 3 Click **Save** to ave any changes that you have made.

To exit without saving changes, click **Cancel**.

Adding a PTT Channel

Adding a PTT channel makes it available for use by Cisco IPICS.

Before you add a PTT channel, configure locations as described in the "Managing Locations" section on page 2-38.

To add a new channel, perform the following steps.

For information about accessing the Manage Channels window, see the "Manage Channels Window" section on page 2-18.

Procedure

Step 1 In the Manage Channels window Channel area, click **Add**.

The Edit Channel Details area for a new channel displays.

Step 2 In the Edit Channel Details area for a new channel:

a. In the Channel Name field, enter a name for the channel.

Choose a unique and recognizable name that accurately describes the PTT channel. It is often helpful to name the PTT channel according to the department or organization that will use it, or for a particular geographic region (for example *Fire Department* or *North Area*).

b. From the Preferred Codec drop-down list, choose a codec for the channel:

- Choose G.711 if the channel will be available to Cisco IP Phone users or will be part of a VTG.
- Choose G.711 or G.729 if this channel will be available to PMC users.

  G.729 uses less bandwidth but consumes more PMC resources and router resources than G.711.

c. From the Secure Flag drop-down list, choose whether this channel is a secure channel (**Yes**) or is not a secure channel (**No**).

This field is for reference only and should be set to reflect the configuration of the channel in your network. The setting that you make does not affect the security configuration of the channel.

d. Optional. If Operational Views is enabled, enter appropriate information in the Ops View Attributes fields.

For more information, see Chapter 6, "Operational Views."

e. From each Location drop-down list, choose the multicast domain that contains a multicast address that you want to connect to this channel.

   If there is only one multicast domain, choose the location **All**.

f. From each Type drop-down list, choose the type of connection that Cisco IPICS and devices use to connect to this channel when connecting from the corresponding location.

g. In each Address field, enter the multicast address, in the corresponding location that is used to connect to this channel.

   The first octet in this address must be 224, 232, 233, 238, 239. Each subsequent octet must be in the range of 0 through 255.

   Cisco recommends that addresses be in the range of 239.192.0.0 through 239.251.255.255 to conform to IANA specifications. Cisco IPICS does not check an address that you enter for conflicts with reserved or special addresses. If you add an address that is outside of the recommended range, make sure that there are no conflicts.

h. In each Port field, enter the port number for the corresponding multicast address.

   This value must be an even number in the range of 21000 through 65534.

Step 3 Click **Save** to save the information for this channel.

If you do not want to add this channel, click **Cancel**.

Deleting a PTT Channel

If a PTT channel is no longer needed, you can delete it from Cisco IPICS.

You cannot delete a PTT channel that has an active VTG associated with it. You must remove the channel from the VTG before deleting it.

Tip To see the VTGs associated with a PTT channel, click the channel in the Channels list and then click **Details**. Cisco IPICS displays the VTG names in the Associated VTGs field of the Edit Channel Details area.

To delete a channel, perform the following steps.

For information about accessing the Manage RMS window, see the "Manage RMS Window" section on page 2-3.

Procedure

Step 1 In the Manage Channels window Channels area, click the channel that you want to delete.

The channel becomes highlighted.

Step 2 Click **Delete**.

A dialog box prompts you to confirm the deletion.

Step 3 To confirm the deletion, click **OK**.

If you do not want to delete this channel, click **Cancel**.

Managing the Multicast Pool

Cisco IPICS stores multicast addresses in the multicast pool. When you activate a VTG, Cisco IPICS automatically assigns an available multicast address from the multicast pool to that VTG. (A multicast address is available when it is not assigned to an active VTG or to a channel). When a VTG deactivates, its multicast address is released for use by another VTG.

Note You cannot activate more VTGs than there are multicast addresses in the multicast pool.

As a Cisco IPICS system administrator, you can perform these multicast pool management tasks:

- Viewing and Editing Multicast Address Information, page 2-32
- Adding Individual Multicast Addresses, page 2-34
- Adding a Sequence of Multicast Addresses, page 2-36
- Deleting a Multicast Address, page 2-38

You perform the multicast pool management tasks in the Administration Console Manage Multicast Pool window. For more information about this window, including how to access it, see the "Manage Multicast Pool Window" section on page 2-31.

Manage Multicast Pool Window

The Manage Multicast Pool window displays information about the multicast addresses that are in the multicast pool. It also lets you perform the multicast pool management functions.

To open the Manage Multicast Pool window, click the **Multicast** link in the Administration Console System Administrator tab.

Each multicast address in the multicast pool window appears on its own row with related information displayed in various columns. By default, rows of information appear in ascending order by multicast address. You can toggle the display so that rows appear in ascending or descending order by any column heading. To do so, click the name in a column heading. An up arrow in a column indicates that activities are in ascending order by that column, and a down arrow indicates that activities are in descending order by that column.

You can resize any column by dragging the border to the right of its name.

For each multicast address in the multicast pool, the Manage Multicast Pool window displays the information that is described in Table 2-7.

Table 2-7 Manage Multicast Pool Window Fields

Field	Description
Address	Multicast address and port.
Location	Location that is assigned to this multicast address. The location name can include alphanumeric characters, spaces, and any of these characters: . , – ‘ # ( ) / :_ .
Status	Either of these designations: • Active—Address is assigned to an active VTG • Idle—Address is not assigned to an active VTG

Table 2-7 Manage Multicast Pool Window Fields (continued)

Field	Description
Connection Type	Either of these designations: • Used by Channel—Multicast address is assigned to a PTT channel. • Used by VTG—Address is reserved for use or is in use by a VTG. Cisco IPICS assigns an available multicast address to a VTG automatically. When the VTG ends, the address becomes available for another VTG. **Note** If you remove a PTT channel connection (the multicast address you assign to a PTT channel) from a PTT channel, Cisco IPICS disassociates that address from the PTT channel and removes the address from the multicast pool.
Used By	Name of the active channel or VTG that is using the multicast address, if applicable.

Viewing and Editing Multicast Address Information

You can view information for any multicast address, and you can change a multicast address and port number. You do so in the Edit Multicast Address Details area.

To edit or view multicast address information, perform the following steps.

For information about accessing the Manage Multicast Pool window, see the "Manage Multicast Pool Window" section on page 2-31.

Procedure

Step 1 In the Manage Multicast Pool window, take either of these actions:

- Click the multicast address for which you want to view or change information and then click **Details**, which appears under the list of multicast addresses
- Double-click the multicast address for which you want to view or change information

The Edit Multicast Address Details area for selected channel displays.

Note If you choose another multicast address when the Edit Multicast Address Details area is displayed, the information in this area does not change for the new multicast address until you click **Details** again or double-click the new address.

Step 2 View or update the information that is described in Table 2-8.

Table 2-8 Multicast Address Details Area Fields

Field	Description
Address	Multicast address. When adding an address, enter a valid multicast address, which must begin with 224, 232, 233, 238, or 239. Also, make sure to enter all 4 parts, or octets, of the address. Each octet must be in the range of 0 through 255. Cisco recommends that addresses be in the range of 239.192.0.0 through 239.251.255.255 to conform to IANA specifications. Cisco IPICS does not check an address that you enter for conflicts with reserved or special addresses. If you add an address that is outside of the recommended range, make sure that there are no conflicts.
Port	Multicast address port number This value must be an even number in the range of 21000 through 65534.

Table 2-8 Multicast Address Details Area Fields (continued)

Field	Description
Connection Type—*Display only*	Either of these designations: • Used by Channel—Address is assigned to a PTT channel. • Used by VTG—Address is reserved for use or is in use by a VTG. Cisco IPICS assigns an available multicast address to a VTG automatically. When the VTG ends, the address becomes available for another VTG.
Last Released—*Display only*	Date at time at which the address was last released from an active VTG.
Status—*Display only*	Either of these designations: • Active—Address is assigned to an active VTG • Idle—Address is not assigned to an active VTG
Location—*Display only*	Location that is assigned to this multicast address. An address for a PTT channel has a specific location, either location All or another location name. Regardless of the location in this field, a VTG can contain only channels that are in the same multicast domain as the RMS that is used to mix the channels.
Used By—*Display only*	Name of the active channel or VTG that is using the multicast address, if applicable.

Step 3 Click **Save** to save your changes.

To exit without saving changes, click **Cancel**.

Adding Individual Multicast Addresses

When you add a multicast address to the multicast pool, it becomes available for use by active VTGs.

If you later assign the address to a channel, it will no longer be available for use by active VTGs.

Before you add a multicast address, configure locations as described in the "Managing Locations" section on page 2-38.

For information about adding a sequence of multicast addresses simultaneously, see the "Adding a Sequence of Multicast Addresses" section on page 2-36.

To add one or more multicast addresses to the multicast pool individually, perform the following steps.

For information about accessing the Manage Multicast Pool window, see the "Manage Multicast Pool Window" section on page 2-31.

Procedure

Step 1 In the Manage Multicast Pool window, click **Add**, which appears under the list of multicast addresses.

The Add One area displays under the Multicast Pool.

Step 2 In the Address field, enter the multicast address that you want to add.

Make sure to enter a valid multicast address, which must begin with 224, 232, 233, 238, or 239. Also, make sure to enter all 4 parts, or octets, of the address.

Cisco recommends that addresses be in the range of 239.192.0.0 through 239.251.255.255 to conform to IANA specifications. Cisco IPICS does not check an address that you enter for conflicts with reserved or special addresses. If you add an address that is outside of the recommended range, make sure that there are no conflicts

Step 3 In the Port field, enter the port number for this address.

This value must be an even number in the range of 21000 through 65534.

Step 4 Click **Save**.

If you choose not to add this address, click **Cancel**.

Step 5 If you want to add another individual address, repeat Step 2 through Step 4.

Adding a Sequence of Multicast Addresses

Cisco IPICS can generate a list of multicast addresses and add them to the multicast pool. This feature can be useful when you need to add several multicast addresses.

For information about adding multicast addresses individually, see the "Adding Individual Multicast Addresses" section on page 2-34.

When you choose to have Cisco IPICS generate a sequence of multicast addresses, you specify the first address and the number of addresses that you want. Cisco IPICS returns the number of addresses you specify, starting with the first address that you specified and incrementing the fourth part, or octet, of each additional address by one. You can generate a sequence of up to 255 multicast addresses at a time.

For example, if you request five addresses and specify the first address to be 239.195.5.1, Cisco IPICS generates this sequence of addresses:

```
239.195.5.1
239.195.5.2
239.195.5.3
239.195.5.4
239.195.5.5
```

When you generate multicast addresses in this way, Cisco IPICS assigns the port number that you designate to each address.

After Cisco IPICS generates the list of addresses, you can change the number or port for any address, and you can delete any addresses that you do not want in the multicast pool. For more information, see the "Viewing and Editing Multicast Address Information" section on page 2-32 and see the "Deleting a Multicast Address" section on page 2-38.

To generate and add a sequence of multicast addresses to the multicast pool individually, perform the following steps.

For information about accessing the Manage Multicast Pool window, see the "Manage Multicast Pool Window" section on page 2-31.

Procedure

Step 1 In the Manage Multicast Pool window, click **Many**, which appears under the list of multicast addresses.

The Add Many area displays under the Multicast Pool.

Step 2 In the Initial Address field the four parts, or octets, of the first IP address in the sequence that you want.

Make sure to enter a valid multicast address, which must begin with 224, 232, 233, 238, or 239. Also, make sure to enter all 4 parts, or octets, of the address. Each octet must be in the range of 0 through 255. Each octet must be in the range of 0 through 255.

Cisco recommends that addresses be in the range of 239.192.0.0 through 239.251.255.255 to conform to IANA specifications. Cisco IPICS does not check an address that you enter for conflicts with reserved or special addresses. If you add an address that is outside of the recommended range, make sure that there are no conflicts

Step 3 In the Number of Addresses field, enter the number of IP addresses that you want Cisco IPICS to generate.

You can enter a number between 1 and 255.

Step 4 In the Port field, enter the port number to be used for each generated multicast addresses.

This value must be an even number in the range of 21000 through 65534.

Step 5 Click **Save**.

If you choose not to generate these addresses, click **Cancel**.

If you click **Save**, Cisco IPICS generates the IP addresses and displays them in the Multicast Pool pane.

If the generated list contains addresses that you do not want, you can edit or delete them. See the "Viewing and Editing Multicast Address Information" section on page 2-32 and see the "Deleting a Multicast Address" section on page 2-38.

Deleting a Multicast Address

You can delete a multicast address when it is no longer needed.

You cannot delete a multicast address that is assigned to an active VTG. You must deactivate the VTG before you can delete the address.

You also cannot delete a multicast address that is assigned to a channel. To delete the address in this case, delete the channel, which automatically removes the multicast address from the multicast pool.

To delete a multicast addresses from the multicast pool, perform the following steps.

For information about accessing the Manage Multicast Pool window, see the "Manage Multicast Pool Window" section on page 2-31.

Procedure

Step 1 In the Manage Multicast Pool window, click the multicast address that you want to delete.

The multicast address becomes highlighted in blue.

Step 2 Click **Delete**, which appears under the list of multicast addresses.

A dialog box prompts you to confirm the deletion.

Step 3 To confirm the deletion, click **OK**.

If you choose not to delete this address, click **Cancel**.

Managing Locations

A location is a multicast domain that contains multicast addresses that can be accessed by a designated RMS. Users who are associated with the same location can communicate with each other without additional network configuration.

As a Cisco IPICS system administrator, you can perform these locations management tasks:

- Changing a Location Name, page 2-39
- Adding a Location, page 2-40
- Deleting a Location, page 2-41

You perform the locations management tasks in the Administration Console Manage Location window. For more information about this window, including how to access it, see the "Manage Location Window" section on page 2-39.

Manage Location Window

The Manage Location window displays the locations that are configured in your Cisco IPICS network. It also lets you perform the locations management functions.

To open the Manage Location window, click the **Locations** link in the Administration Console System Administrator tab.

By default, location names appear in ascending alphanumeric order. You can toggle the display between ascending and descending order. To do so, click the Location Name column heading. An up arrow indicates that location names are in ascending order, and a down arrow indicates that location names are in descending order.

Changing a Location Name

Edit Location Details area lets you change any location name.

To change the name of a location, perform the following steps.

For information about accessing the Manage Location window, see the "Manage Multicast Pool Window" section on page 2-31.

Procedure

Step 1 In the Manage Location window, take either of these actions:

- Click the location name that you want to change and then click **Details**
- Double-click the location name that you want to change

The Edit Location Details area for the selected location displays.

Step 2 Enter the new location name.

The location can include alphanumeric characters, spaces, and any of these characters: . , – ‘ # ( ) / :_ .

Step 3 Click **Save** to save your changes.

To exit without saving changes, click **Cancel**.

Adding a Location

You can add location to Cisco IPICS as needed.

To add a location, perform the following steps.

For information about accessing the Manage Location window, see the “Manage Location Window” section on page 2-39.

Procedure

Step 1 In the Manage Location window, click **Add**, which appears under the list of location names.

The Add Location area displays.

Step 2 In the Location Name field, enter a name for the location.

The location can include alphanumeric characters, spaces, and any of these characters: . , – ‘ # ( ) / :_ .

Step 3 To add the location, Click **Save**.

If you choose not to add this location, click **Cancel**.

Deleting a Location

You can delete a location when it is no longer needed.

You cannot delete a location if it is associated with a channel or if it is set as the default location for a user. In these cases, you must disassociate the location from the channel or set another default location for the user before you can delete the location.

To delete a location from Cisco IPICS, perform the following steps.

For information about accessing the Manage Location window, see the "Manage Location Window" section on page 2-39.

Procedure

Step 1 In the Manage location window, click the location name that you want to delete.

The location name becomes highlighted in blue.

Step 2 Click **Delete**, which appears under the list of location names.

A dialog box prompts you to confirm the deletion.

Step 3 To confirm the deletion, click **OK**.

If you choose not to delete this location, click **Cancel**.

Managing Activity Logs

The Cisco IPICS logs store a variety of information about activities relating to VTGs. You can review this information at any time.

Cisco IPICS tracks and logs the date and time that following activities occur:

- User is assigned to, or release from, a PTT channel
- PMC user is enabled or disabled
- PMC user starts or stops listening to a channel
- PMC user is muted
- PMC user is unmuted

- PMC user pushes the **PTT** button
- PMC user releases the **PTT** button
- Channel is added to a VTG
- Channel is removed from a VTG
- VTG is added to another VTG
- VTG is removed from another VTG
- User is added to a VTG
- User is removed from a VTG
- VTG is activated
- VTG is deactivated

You can choose how to view activity logs:

- By channel—Users and VTGs that used that PTT channel
- By user—PTT channels and VTGs in which that user was involved
- By VTG—Users and PTT channels that were participants in that VTG

As a Cisco IPICS system administrator, you can perform these activity log management tasks:

- Downloading Activity Logs, page 2-43
- Viewing an Activity Log, page 2-43

You display activity logs from the Administration Console Activity Logs Pool window. For more information about this window, including how to access it, see the "Activity Logs Window" section on page 2-42.

Activity Logs Window

The Activity Logs window displays each channel, user, or VTG that is configured in Cisco IPICS, depending on the information that you choose to view. It also lets you perform the activity logs management functions

To open the Activity Logs window, click the **Activity Logs** link in the Administration Console System Administrator tab.

Downloading Activity Logs

To perform detailed analysis of activities, you can download activity logs. When you download activity logs, Cisco IPICS takes these actions:

- Creates a .csv file that contains all activity logs in the period that you designate
- Downloads the .csv file to the location that you specify on the computer from which you are accessing the Administration Console

You can open the downloaded file with Microsoft Excel.

To download activity logs, perform the following steps.

For information about accessing the Activity Logs window, see the "Activity Logs Window" section on page 2-42.

Procedure

Step 1 In the Activity Logs window:

a. In the From drop-down lists, specify the beginning date and time of the period for which information should be included in the activity logs that you are downloading.

b. In the To drop-down lists, specify the ending date and time of the period for which information should be included in the activity logs that you are downloading.

Step 2 Follow the on-screen prompts to download the file.

Viewing an Activity Log

You can view activity logs for any channel, user, or VTG. To view an activity log, perform the following steps.

For information about accessing the Activity Logs window, see the "Activity Logs Window" section on page 2-42.

Note Because a log maintains historical data, if you delete or rename a channel, user, or VTG, that name will appear in an activity list but will not be listed in the channel, user, or VTG management windows.

Procedure

Step 1 If the Activity Logs window does not display a list that contains the item (channel, user, or VTG) for which you want to view an activity log, take these actions:

a. Click the **By Channel**, **By User**, or **By VTG** radio button to indicate the list of items that you want.

b. Click **Find**.

The Activity Logs window displays a list of channels, users, or VTGs, depending on the radio button that you choose.

Step 2 Take either of these actions:

- Click the channel, user, or VTG for which you want to view an activity log and then click **Details**, which appears under the list of items
- Double-click the channel, user, or VTG for which you want to view an activity log

An activity log displays. The information in the log depends on whether you are viewing a log for channel, a user, or a VTG as follows:

- An activity log for a channel displays a list of user activities and a list of VTG activities that involve the specified channel
- An activity log for a user displays a list of channel activities and a list of VTG activities that involve the specified user
- An activity log for a VTG displays a list of channel activities a list of user activities that involve the specified VTG

Each activity in a log appears on its own row with information in these columns:

- Time—Date and time that an activity started
- Channel, User, or VTG—Name of the channel, user, or VTG
- Action—Brief description of the activity

You can resize any column by dragging the border to the right of its name.

By default, the activities in a log appear in ascending order by time. You can toggle the display so that activities appear in ascending or descending order by any column heading. To do so, click the name in a column heading. An up arrow in a column indicates that activities are in ascending order by that column, and a down arrow indicates that activities are in descending order by that column.

Note If you click another channel, user, or VTG when an activity log is displayed, Cisco IPICS highlights in orange the item for which the log information is displayed. The log information does not change for the new selection until you click **Details** again or double-click the new selection.

Managing Licenses

License files determine number of Cisco IPICS ports, the number of concurrent PMC users, and the number of concurrent Cisco IP Phone users that your Cisco IPICS system supports, and whether Operational Views is enabled.

If your requirements exceed the limits of your current license, you can obtain additional licenses. For detailed information about licenses and how to obtain them, refer to *Cisco IPICS PMC Installation and User Guide*.

As a Cisco IPICS system administrator, you can upload new license files to the Cisco IPICS server so that the new licenses take effect. For instructions, see the "Uploading a License File" section on page 2-47.

You perform the license management tasks in the Administration Console License Management window. For more information about this window, including how to access it, see the "License Management Window" section on page 2-45.

License Management Window

The License Management window provides information about the licenses that are configured for your Cisco IPICS installation. It also lets you upload new licenses to the Cisco IPICS server.

To open the License Management window, click the **License** link in the Administration Console System Administrator tab.

The Configured License area in the License Management window provides the information that is described in Table 2-9.

Note The License Management window displays of available licenses and current usage information does not reflect real-time data. The data that displays in this window shows the usage at the time that the license window was last accessed. To make sure that you are viewing the most current license information, update your browser window.

Table 2-9 License Management Window Configured License Area

Field	Description
Cisco IPICS Ports	Total Ports—Number of voice interoperability ports that are licensed for your system. Each port corresponds to a unique multicast address in a particular location. Current Usage—Number of voice ports in use.
Concurrent PMC Users	Total Ports—Number of users that can access this Cisco IPICS server through PMCs at one time. Current Usage—Number of users currently accessing this server through PMCs. **Note** If a user accesses this server through multiple PMCs at the same time, each PMC counts as 1 user.
Concurrent IP Phone Users	Total Ports—Number of users that can access this Cisco IPICS server through Cisco IP Phones at one time. Current Usage—Number of users currently accessing this server through Cisco IP Phones. **Note** If a user accesses this server through multiple Cisco IP Phones at the same time, each phone counts as 1 user.

Table 2-9 License Management Window Configured License Area (continued)

Field	Description
Cisco IPICS Ops View	Displays Licensed when Operational Views is enabled. Displays Not Licensed when Operational Views is not enabled.

Uploading a License File

When you obtain a new Cisco IPICS license file, you must upload it to the Cisco IPICS server before it will take effect. This procedure copies a licence file from the server on which you stored it when you obtained it to the Cisco IPICS server.

To upload a license, perform the following steps.

For information about accessing the License Management window, see the "License Management Window" section on page 2-45.

Procedure

Step 1 In the License Management window License File field, enter the path name and file name of the license file to upload to the Cisco IPICS server.

To locate this file in a Choose File window, click **Browse**.

Step 2 Click **Upload** to upload the file to the Cisco IPICS database.

If you choose not to upload this file, click **Cancel**.

Step 3 Click **Apply** to cause the new license to take effect.

Cisco IPICS updates the information in the Configured License area to reflect the new license.

Managing PMC Automatic Updates

Cisco provides updates of the PMC application to add features and resolve issues. Users can upgrade their PMCs at their convenience by downloading the current version of the PMC Installer, as described in the "Downloading the PMC" section on page 5-6.

In addition, each PMC client polls the Cisco IPICS server regularly. As part of this process, the PMC client determines whether there is a PMC version to which the it can or must update. You use the automatic update feature to designate the PMC version that is available for this update, and to designate whether an update is required or recommended.

When a PMC performs an automatic update, it installs the pmc.dll file only. This process does not update PMC skins or the PMC help file. To update skins and the help file, you must download the current version of the PMC Installer from the Administration Console Download PMC window in the User tab, and install the PMC as described in *Cisco IPICS PMC Installation and User Guide*.

As a Cisco IPICS system administrator, you can perform these PMC version management tasks:

- Specifying PMC Versions for Automatic Updates, page 2-49
- Uploading pmc.dll Files, page 2-50

You perform the PMC automatic update tasks in the Administration Console PMC Auto Update window. For more information about this window, including how to access it, see thee "PMC Auto Update Window" section on page 2-48.

PMC Auto Update Window

The PMC Auto Update window lets you specify information about PMC versions to use for automatic updates. It also lets you upload to the Cisco IPICS server the new PMC versions that are used for these updates.

To open the PMC Auto Update window, click the **PMC Auto Update** link in the Administration Console System Administrator tab.

The Last Uploaded Version field in this window displays the version number of the PMC that was last uploaded to the Cisco IPICS server.

The other fields in this window contain information used for the automatic update, as described in the "Specifying PMC Versions for Automatic Updates" section on page 2-49.

A field displays Uninitialized if Cisco IPICS has no value for that field.

Specifying PMC Versions for Automatic Updates

The PMC Versions area in the PMC Auto Update window lets you designate the PMC versions that are used for an automatic update. When you specify PMC version for the automatic update, be aware of this information:

- If you want to force PMCs to update as soon as possible, enter PMC version numbers in the Maximum Available Version field and in the Minimum Supported Version field. When you enter values in these fields, the next time that a PMC client polls the server, it compares the PMC version that it is running with the minimum supported PMC version. If the PMC client is not running the minimum supported version, it automatically downloads the PMC version that is specified in the Maximum Available Version field, automatically updates to that version, and then automatically restarts.

Caution Forcing a PMC automatic update shuts down and then restarts a PMC without warning a user, regardless of what the PMC is in use for. For this reason, it is recommended that you force an update only when it is absolutely necessary.

- If you want to prompt PMC users to update their PMCs when it is convenient for them, enter a PMC version number in the Recommended Download Version field. In this case, the next time that a PMC polls the server, it receives instructions to prompt PMC users to update. When a user decides to update, the PMC automatically downloads the PMC version that is specified in the Recommended Download Version field, automatically updates to that version, and then automatically restarts.
- You must upload a PMC version to the Cisco IPICS server before it becomes available in any of the fields in the PMC Version area in the PMC Auto Update window

To specify PMC versions for automatic updates, perform the following steps.

For information about accessing the PMC window, see the "PMC Auto Update Window" section on page 2-48.

Procedure

Step 1 In the PMC Auto Update window:

- If you want to force an automatic update, take these actions:
  a. From the Maximum Available Version drop-down list, choose the PMC version to which PMCs should be updated.
  b. From the Minimum Supported Version drop-down list, choose the minimum version of the PMC that is acceptable to run.

  PMC clients that are running a PMC version that is earlier than the version in the Minimum Supported Version field will automatically update to the version in the Maximum Available Version field.
- If you want to prompt users to perform an automatic update, from Recommended Download Version drop-down list, choose the PMC version to which PMCs should be updated.

Step 2 Click **Save** to save changes that you have made.

If you do not want to save your changes, click **Cancel**.

Uploading pmc.dll Files

A pmc.dll file contains the version of the PMC that is installed during the automatic update process. Before selections appear in the Maximum Available Version, Minimum Supported Version, or Recommended Download Version drop-down lists in the PMC Versions area in the PMC Auto Update window, you must upload the corresponding pmc.dll file or files to the Cisco IPICS server.

When you upload a pmc.dll file, the file is copied from the PC on which you stored it to the Cisco IPICS server.

To upload a pmc.dll file to the Cisco IPICS server, perform the following steps from the PC on which you have stored the file.

For information about accessing the PMC window, see the "PMC Auto Update Window" section on page 2-48.

Procedure

Step 1 In the PMC Auto Update window PMC File field, enter the full path name and file name (pmc.dll) of the pmc.dll file that your obtained from Cisco.

To locate this file in a Choose File window, click **Browse**.

Step 2 In the Version of Upload field, enter the PMC version number of pmc.dll file.

Enter the version number in this format, where each # is a number: #.#(#.#.#). Only the first two numbers are required.

The PMC version number that you enter will appear in the Maximum Available Version, Minimum Supported Version, and Recommended Download Version drop-down lists.

Step 3 Click **Upload**.

Cisco IPICS uploads the file from your PC to the Cisco IPICS server. A status bar displays the progress of the upload as it proceeds. When the upload completes, Cisco IPICS updates information in the Last Uploaded Version field.

Managing the PMC Installer

The PMC Installer, pmcsetup.exe, installs the PMC on PMC client machines. This file downloads to a PMC client when a PMC user clicks the **PMC Download** link in the Administration Console User tab, as described in the "Downloading the PMC" section on page 5-6.

Managing the PMC installer involves these processes:

1. Upload the pmcinst.exe file to the Cisco IPICS server.

   The pmcinst.exe file contains the PMC binary files, including the .exe, pmc.dll, help, and skins files.

2. Generate the PMC Installer.

   This process creates the pmc.ini file, which contains the IP address that PMCs use to communicate with the Cisco IPICS server, and bundles the pmc.ini file and the pmcinst.exe file into a single file, called pmcsetup.exe.

As a Cisco IPICS system administrator, you can upload the pmcinst.exe file and generate the pmcsetup.exe file as described in the "Generating a PMC Installer" section on page 2-52.

You perform these tasks in the Administration Console Manager PMC Installer window. For more information about this window, including how to access it, see thee "Manage PMC Installer Window" section on page 2-52.

Manage PMC Installer Window

The Manage PMC Installer window displays information about the PMC Installer and lets you generate a PMC installer.

To open the Manage PMC Auto Update window, click the **PMC Installer** link in the Administration Console System Administrator tab.

The Installer Status field displays the date and time that a pmcsetup.exe files was last generated, and displays the IP address defined by the bundled pmc.ini file.

The pmcinst.exe field displays the version number of the pmcinst.exe file that was last uploaded to the Cisco IPICS server.

The other fields in this window contain information used when you generate a pmcsetup.exe file, as described in the "Generating a PMC Installer" section on page 2-52.

Generating a PMC Installer

Generating a PMC Installer creates a new pmcsetup.exe file, and makes it available for download from the **PMC Download** link in the Administration Console User tab.

To generate a PMC Installer, perform the following steps from the PC on which you stored the pmcinst.exe file.

For information about accessing the Manage PMC Installer window, see the "Manage PMC Installer Window" section on page 2-52.

Procedure

Step 1 From the System Administrator tab, click the **PMC Installer** link.

The Manage PMC Installer window displays.

Step 2 In the Upload pmcinst.exe field, enter the full path name and file name (pmcinst.exe) of the pmcinst.exe that your obtained from Cisco.

To locate this file in a Choose File window, click **Browse**.

Step 3 In the Version field, enter the PMC version number of the pmcinst.exe file.

Enter the version number in this format, where each # is a number: #.#(#.#.#). Only the first two numbers are required.

Step 4 Click **Upload**.

Cisco IPICS uploads the pmcinst.exe file from your PC to the Cisco IPICS server.

Step 5 From the Server IP Address drop-down list, choose the IP address that PMCs use to communicate with the Cisco IPICS server.

Step 6 Click **Generate PMC Installer**.

Cisco IPICS creates the pmc.ini file, which contains the IP address that you specified, bundles it with pmcinst.exe that you downloaded, and creates the mcsetup.exe file.

Now you can instruct PMC users download a new PMC application, as described in the "Downloading the PMC" section on page 5-6.

CHAPTER 3

Administration Console: Operator Tasks

The Cisco IPICS operator is responsible for setting up and managing Cisco IPICS users and user groups, granting access to Cisco IPICS and to the PMC, and assigning user channels, roles, and operational views (ops views).

A user is someone who can participate in an active VTG or channel to communicate with other VTG or channel participants. A user group is a logical grouping of users. User groups allow you to work with multiple users efficiently. For example, instead of dragging individual users to a VTG one at a time, you (as a dispatcher) can drag a user group to move all users in the group to the VTG. A user can be in an unlimited number of user groups.

For information about operational views, see Chapter 6, “Operational Views.”

This chapter includes these sections:

Manage Users Window

The Manage Users window lists the user groups and the users that are configured in Cisco IPICS. It also lets you perform the users and user groups management functions.

To access this window, log in to the Administration Console as described in the "Accessing the Administration Console" section on page 1-10, then choose the **Operator** tab.

Note You must be assigned the operator role to access the Operator window.

The User Group area in the Manage Users window displays the name of each user group that is configured in Cisco IPICS. To see the members of a user group in this list, expand the group by clicking the right arrow next to the user group name. Click the down arrow next to a user group name to collapse an expanded group.

The Users area displays the name of each user that is configured in Cisco IPICS.

For information about the icons and colors that appear in the Manage Users window, see these sections:

- Manage Users Window Icons, page 3-2
- Manage Users Window Color Coding, page 3-3

Manage Users Window Icons

Icons in the Manage Users window provide information about each user group and user name, as described in Table 3-1.

Table 3-1 User Group and User Icons

Icon	Meaning
	User
	User group

Manage Users Window Color Coding

Information in the Manage Users window is color coded as described in Table 3-2.

Table 3-2 Color Coding in Manage Users Window

Color	Meaning
Green user name in User Group area	You have dragged the user to the user group but have not yet clicked **Save**. For more information, see the "Adding a User to a User Group" section on page 3-6.
Red user name in User Group area	You have dragged the user from the user group but have not yet clicked **Save**. For more information, see the "Removing a User from a User Group" section on page 3-7.
Blue highlighted user group or user name	User group or user is selected in preparation for clicking **Details**, **Add**, or **Delete**.
Orange highlighted user group or user name	You have clicked another user group or user while the Details area for this user group or user is displayed.

Managing Users and User Groups

As a Cisco IPICS operator, you can perform these user and user group management tasks:

- Editing User Group Details, page 3-4
- Creating a User Group, page 3-5
- Deleting a User Group, page 3-6
- Adding a User to a User Group, page 3-6
- Removing a User from a User Group, page 3-7
- Viewing and Editing User Details, page 3-8
- Adding a User, page 3-16
- Specifying the PTT Channels that are Associated with a User, page 3-20

- Muting or Unmuting a User in the Edit User Details Window, page 3-22
- Removing a Role from a User, page 3-24
- Deleting a User, page 3-25

You perform the user and user group management tasks in the Administration Console Manage Users window. For more information about this window, including how to access it, see the "Manage Users Window" section on page 3-1.

Editing User Group Details

You can change the name of any user group that is configured in Cisco IPICS. You do so in the Edit User Groups Details area.

To change a user group name, perform the following steps.

For information about accessing the Manage Users window, see the "Manage Users Window" section on page 3-1.

Procedure

Step 1 In the Manage Users window User Groups area, take either of these actions:

- Click the user group name that you want to change and then click **Details**
- Double-click user group name that you want to change

The Edit User Group Details area for the selected user group displays. If Operational Views is enabled, additional ops views fields appear in this area. For more information, see Chapter 6, "Operational Views."

Note If you choose another user group when the Edit User Group Details area is displayed, the information in this area does not change for the new user group until you click **Details** again.

Step 2 Enter the new user group name.

The name can include alphanumeric characters, spaces, and any of these characters: . , – ' # ( ) / :_.

Step 3 Click **Save** to exit the Edit User Group Details area and save any changes that you have made.

To exit without saving changes, click **Cancel**.

Creating a User Group

Creating a user group makes it available to Cisco IPICS.

You may find it useful to create and name user groups according to location (for example, South Side users) or function (for example, Translators).

To create a user group, perform the following steps.

For information about accessing the Manage Users Window, see the "Manage Users Window" section on page 3-1.

Procedure

Step 1 In the Manage User window User Group area, click **Add**.

The Edit User Group Details area for a new user group displays. If Operational Views is enabled, additional ops views fields appear in this area. For more information, see Chapter 6, "Operational Views."

Step 2 In the User Group Name field, enter a name for the new User group.

The name can include alphanumeric characters, spaces, and any of these characters: . , – ' # ( ) / :_.

Step 3 (Optional) If Operational Views is enabled, enter appropriate information in the Ops View Attributes fields.

For more information, see Chapter 6, "Operational Views."

Step 4 Click **Save** to save the new user group.

If you do not want to create this use group, click **Cancel**.

Deleting a User Group

You can delete a user group when you no longer need it to organize users.

You cannot delete a user group that is a participant in an active VTG or that is a member of a VTG template. You must remove the user group from the VTG before you delete it.

To delete a user group, perform the following steps.

For information about accessing the Manage Users Window, see the "Manage Users Window" section on page 3-1.

Procedure

Step 1 In the Manage Users window User Groups area, click the user group that you want to delete.

The user group becomes highlighted in blue.

Step 2 Click **Delete** in the User Group area.

A dialog box prompts you to confirm the deletion.

Step 3 To confirm the deletion, click **OK**.

If you do not want to delete this user group, click **Cancel**.

Adding a User to a User Group

Adding a user to a user group makes the user a part of the user group. You can add the same user to an unlimited number of user groups.

You cannot add a user to a user group that is a participant in an active VTG. You must remove the user group from the VTG before you add a user to it.

For information about creating users, see the "Adding a User" section on page 3-16.

To add a user to a user group, perform the following steps.

For information about accessing the Manage Users Window, see the "Manage Users Window" section on page 3-1.

Procedure

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

Step 2 Drag the user name that you want to add from the Users area to the desired user group.

When you release the mouse button, if the user group is expanded, the newly added user name displays in green.

Repeat this step as needed to add other users to user groups.

Step 3 Click **Save** to complete the additions that you have made.

If you want to undo the changes that you made since you last clicked **Save**, click **Revert**.

Removing a User from a User Group

You can remove a user from a user group when the user is no longer needed in that group.

You cannot remove a user from a user group that is a participant in an active VTG. You must remove the user group from the VTG before you remove the user from the user group.

Removing a user from a particular user group does not remove the user itself from Cisco IPICS, nor does it remove the user from any other user group to which it belongs.

To remove a user from a user group, perform the following steps.

For information about accessing the Manage Users Window, see the "Manage Users Window" section on page 3-1.

Procedure

Step 1 In the Manage Users window User Groups area, display the user group from which you want remove a user.

Step 2 If the users in the user group are not visible, click the right arrow next to the group name to expand it.

Step 3 Locate the user that you want to remove or move and drag it out of the User Groups area.

When you release the mouse button, the user name changes to red.

Repeat this step as needed to remove other users from the user group.

Step 4 Click **Save** to complete removing users.

If you want to undo the changes that you made since you last clicked **Save**, click **Revert**.

Viewing and Editing User Details

You can view and edit information for any user. You do so in the Edit User Details area.

To view or edit user details, perform the following steps.

For information about accessing the Manage Users window, see the "Manage Users Window" section on page 3-1.

Procedure

Step 1 In the Manage Users window Users area, take either of these actions:

- Click the user for which you want to change or view information and then click **Details**
- Double-click the user for which you want to change or view information

The Edit User Details area for the selected user displays. If Operational Views is enabled, additional ops views fields appear in this area. For more information, see Chapter 6, "Operational Views."

Note If you choose another user when the Edit User Details area is displayed, the information in this area does not change for the new user until you click **Details** again or double-click the new user.

Step 2 View or update the information that is described in Table 3-3.

Table 3-3 Edit User Details Area Fields

Field	Description
User ID	ID that the user enters when logging into Cisco IPICS and the PMC. Each Cisco IPICS user must have a unique user ID. Valid characters: alphanumeric characters, underscore (_), and period (.). **Note** This field also supports the use of non-ASCII characters, but PMC activity logs that include these characters cannot be viewed or downloaded from the Administration Console. If you need to check the activity for a User ID that contain non-ASCII characters, you must check the logs in the /tomcat/webapps/ipics_server/pmclogs/*user_name*/*pmc_id*/Channel Activity/ directory on the Cisco IPICS server. You can identify these logs by the .err extension. If you want to download these files, you must do so manually.
First Name	First name of the user. Valid characters: alphanumeric characters, space, hyphen (-), and apostrophe (’).
Last Name	Last name of the user. Valid characters: alphanumeric characters, space, hyphen (-), and apostrophe (’).

Table 3-3 Edit User Details Area Fields (continued)

Field	Description
Password	Password that the user enters when logging into Cisco IPICS and the PMC. A user can change this password later. By default, a password must contain at least 8 characters. You can change this default value by entering a new value in the Minimum Password Length field in the System Administrator Options window. For more information, refer to *Cisco IPICS Troubleshooting Guide*. Valid characters: alphanumeric characters, other characters except space.
Confirm Password	Confirmation of entry in the password field.
Digit ID	Numeric ID that the user enters when accessing Cisco IPICS from a Cisco IP Phone. Valid characters: numeric characters.
Digit Password	Password that the user enters when accessing Cisco IPICS from a Cisco IP Phone. By default, a digit password must contain at least 4 characters. You can change this default value by entering a new value in the Minimum Digit Password Length field in the System Administrator Options window. For more information, refer to *Cisco IPICS Troubleshooting Guide*. Valid characters: numeric characters.
Confirm Digit Password	Confirmation of entry in the Digit Password field.
Address	Street address of the user. Valid characters: alphanumeric characters, spaces, and these characters: . , – ‘ # ( ) / :.
Address (cont)	Additional street address information. Valid characters: alphanumeric characters, spaces, and these characters: . , – ‘ # ( ) / :

Table 3-3 Edit User Details Area Fields (continued)

Field	Description
City	City of the user. Valid characters: alphanumeric characters, space, hyphen (-), and apostrophe (’).
State/Province	State or province of the user. Valid characters: alphanumeric characters, space, hyphen (-), and apostrophe (’).
Country	Country of the user. Valid characters: alphanumeric characters, space, and period (.).
Zip/Postal Code	Zip or postal code of the user. Valid characters: alphanumeric characters, space, and period (.).
E-mail	E-mail address of the user. Valid characters: alphanumeric characters, underscore (_), period (.), and ampersand (@).
Default Location	Location that displays by default on the PMC of the user.
Roles	Each Cisco IPICS user is assigned the user role by default, and this role displays in the Role field. You can assign any or all of these additional roles to the user: System Administrator, Operator, or Dispatcher. To assign one of these roles, choose it from the drop-down list in the Role field. When you do so, a new Role field displays, which allows you to assign a second role. Repeat this process as needed to assign additional roles. To assign the user the privileges of all Cisco IPICS roles, choose the All from the first drop-down list. You must temporarily disable a user before you can remove any role from that user. For more information, see the “Removing a Role from a User” section on page 3-24.

Table 3-3 Edit User Details Area Fields (continued)

Field	Description
IPICS Status	Whether the user can listen to PTT channels and participate in VTGs. • Enabled—User can listen to PTT channels and participate in VTGs. • Disabled—User cannot listen to PTT channels and participate in VTGs.
Associated Default User Channels	Lists the PTT channels that appear on the PMC or Cisco IP Phone for the user. If you click **Edit**, Cisco IPICS displays the Associate Channels to User window, in which you can add or remove PTT channels for this user. For more information, see the "Specifying the PTT Channels that are Associated with a User" section on page 3-20.
User VTGs	VTGs templates in which the user is a member or VTGs in which the user is a participant. Includes one of these designations: • Active—Active VTG • Idle—VTG template

Table 3-3 Edit User Details Area Fields (continued)

Field	Description
Communication Preference	Indicates how a user prefers to participate in a VTG. These fields are informational only. They do not affect how a user participates in a VTG. • IP Phone or PMC—User participates using a Cisco IP Phone or a PMC • Channel—User participates on a channel. This option appears only if channels are associated with this user To specify how a user prefers to participate in IPICS communications in VTGs, choose the desired method from the 1 drop-down list. Each time that you choose a method, a new drop-down list appears so that you can specify multiple methods. If you choose **Channel** in a field, a drop down list opens to the right of that field. This list shows the channels that are available for the you. Choose the channel on which the user would like a dispatcher to communicate with the user.
PMC Attributes	
PMC Status	Determines how a user communicates in VTGs and channels: • Default—User can listen and talk • Mic Off—User can listen but not talk • Mic + Speaker Off—User cannot listen or talk

Table 3-3 Edit User Details Area Fields (continued)

Field	Description
Get Logs From PMC	If the user is logged into the PMC, copies the specified log files from the PMC of the user to the following location on the Cisco IPICS server. If the user is not logged into the PMC, this request is ignored. /webapps/ipics_server/pmclogs/*userID*/*pmcID*/*folder* where: • *userID* is the PMC login ID for the user • *pmcID* is the ID that the system generates for the PMC installation • *folder* is Debug for the Debug log file, or Channel Activity for the Authentication, Channel Statistics, or User Interface log files When you request a file, the PMC client closes the file, renames it, and starts a new file. After the renamed file uploads to the Cisco IPICS server, it is deleted from the PMC client. **Note** A log may be empty if logging is not turned on.

Table 3-3 Edit User Details Area Fields (continued)

Field	Description
Set Log Level	Specifies whether these PMC log files are on or off: • Authentication • User Interface • Channel Statistics Specifies the debug level (1 is lowest, and 3 is highest) for the following PMC log files. A value of 0 turns off the log file. • Debug Signaling • Debug User Interface • Debug Media For a description of the PMC log files, refer to the "Using the PMC Application Logs" chapter in *Cisco IPICS PMC Installation and User Guide*. **Note** Do not turn on a PMC log file unless you need it. If you do turn on a log file, set it to the lowest debug level that provides the information that you need. Log files can consume significant disk space, and the higher the debug level, the more disk space used.

Step 3 Click **Save** to exit the Edit User Details area and save any changes that you have made.

To exit without saving changes, click **Cancel**.

Adding a User

Users that you add in Cisco IPICS can perform the following activities:

- Access the User window in the Cisco IPICS Administration Console and perform the tasks that are available in that window
- Access channels with which they are associated
- Participate in VTGs to which they are assigned

If you add a user that has the same channel assignments, user roles, and address as an existing user, you might find it convenient to start by copying the information of the existing user. When you copy such information, Cisco IPICS opens an Edit User Details window, and enters all information that is stored for the for the existing user, except the user ID, password, digit ID, and digit password.

Before you add a user, configure locations as described in the "Managing Locations" section on page 2-38.

To add a new user, perform the following steps.

For information about accessing the Manage Users window, see the "Manage Users Window" section on page 3-1.

Procedure

Step 1 In the Manage Users window Users area, take one of these action:

- To add a user, starting with a blank Edit User Details area, click **Add**.
- To add a user starting with an Edit User Details Area that includes information based an existing user, click the existing user and then click **Copy**.

The Edit User Details area for a new user displays. If you clicked **Copy**, this area includes information for the existing user, except for the user ID and password. If Operational Views is enabled, additional ops views fields appear in this area. For more information, see Chapter 6, "Operational Views."

Step 2 In the Edit User Details area for a new user:

a. In the User ID field, enter a unique identification name for this user.

The User ID can include alphanumeric characters, underscores (_), and periods (.).

b. In the First Name field, enter the first name of the user.

The name can include characters, spaces, hyphens (-), and apostrophes (').

c. In the Last Name field, enter the last name of the user.

The name can include characters, spaces, hyphens (-), and apostrophes (').

d. In the Password and Confirm Password field, enter a password for the user.

By default, the password must contain at least 8 characters. It can include alphanumeric characters and other characters except spaces. (You can change the default password length in the Minimum Password Length field in the System Administrator Options window. For more information, refer to *Cisco IPICS Troubleshooting Guide*.)

e. (Optional) In the Digit ID field, enter the identifier that the user enters when accessing Cisco IPICS from a Cisco IP Phone.

By default, the password must contain at least 4 characters. It can include numeric characters only. (You can change the default digit password length in the Minimum Digit Password Length field in the System Administrator Options window. For more information, refer to *Cisco IPICS Troubleshooting Guide*.)

f. (Optional) In the Digit Password and the Confirm Digit Password fields, enter the password that the user enters when accessing Cisco IPICS from a Cisco IP Phone.

The digit password can contain numeric characters.

g. (Optional) In the Address, Address (cont), City, State/Province, Country, Zip/Postal Code, and E-mail fields, enter information for the user.

This information is not required and can be entered later by the user.

Valid characters for these fields are:

- Address and Address (cont) field—alphanumeric characters, spaces, and these characters: . , – ‘ # ( ) / :
- City and State/Province fields—alphanumeric characters, space, hyphen (-), and apostrophe (')
- Country field—alphanumeric characters, space, and period (.)

- Zip/Postal Code field—alphanumeric characters, space, and period (.)
- E-mail field—alphanumeric characters, underscore (_), period (.), and ampersand (@)

This information can be entered or updated by the user later.

Step 3 From the Default Locations drop-down list, choose that location from which a Cisco IP Phone connects to Cisco IPICS.

Step 4 (Optional) To assign the user any role other than User (which is assigned to all Cisco IPICS users by default), choose the role from the drop-down list in the 2 field.

When you do so, a new Role field displays, which allows you to assign another role. Repeat this process to assign additional roles.

You can assign any or all of these roles to a users: System Administrator, Operator, or Dispatcher. To assign all roles to a user, choose **All** from the drop-down list in the 2 field.

Step 5 Specify the PTT channels to associate with this user, as described in the "Specifying the PTT Channels that are Associated with a User" section on page 3-20.

The PTT channels that you choose appear as options for a PMC or IP Phone user.

If you assign more channels to a PMC user than can display on the PMC, the PMC will display an error message to the user.

Step 6 (Optional) From the Communications Preference drop-down lists, indicate the preferred method in which the user participates in VTGs.

These fields are informational only. They do not affect how a user participates in a VTG.

- IP Phone or PMC—User participates using a Cisco IP Phone or a PMC.
- Channel—User participates on a channel. This option appears only if channels are associated with this user.

Each time that you choose a method, a new drop-down list appears so that you can specify multiple methods.

If you choose **Channel** in a field, a drop down list opens to the right of that field. This list shows the channels that are available for the you. Choose the channel on which the user would like a dispatcher to communicate with the user.

Step 7 (Optional) If the Operational Views is enabled, enter appropriate information in the Ops View Attributes fields.

For more information, see Chapter 6, "Operational Views."

Step 8 From the PMC Status, choose how the user communicates in VTGs:

- Default—User can listen and talk
- Mic Off—User listen but not talk
- Mic + Speaker Off—User cannot listen or talk

Step 9 (Optional) In the Set PMC Log Levels drop down lists, take these actions:

a. Choose whether these PMC log files are on or off:

- Authentication
- User Interface
- Channel Statistics

b. Choose the debug level (1 is lowest, and 3 is highest) for these PMC log files:

- Debug Signaling
- Debug User Interface
- Debug Media

Choose 0 to turn any of these log files off.

Note Do not turn on a PMC log file unless you need it. If you do turn on a log file, set it to the lowest debug level that provides the information that you need. Log files can consume significant disk space, and the higher the debug level, the more disk space used.

For a description of the PMC log files, refer to the "Using the PMC Application Logs" chapter in *Cisco IPICS PMC Installation and User Guide*.

Step 10 Click **Save** to add the user.

If you decide not to add this user, click **Cancel**.

When you create the user, it displays in the All Users list.

Specifying the PTT Channels that are Associated with a User

When you associate PTT channels with a user, the PTT channels that you choose appear as options on a PMC or a properly-configured Cisco IP Phone. You must perform this procedure after you add a user, as described in the "Adding a User" section on page 3-16.

You can change the PTT channels associated with a user by editing user details as described in the "Viewing and Editing User Details" section on page 3-8.

To associate PTT channels with a user, perform the following procedure.

For information about accessing the Manage Users Window, see the "Manage Users Window" section on page 3-1.

Procedure

Step 1 In the Manage Users window Users area, take either of these actions:

- Click the user for which you want to associate channels and then click **Details** in the Users area
- Double-click the user for which you want to associate channels

The Edit User Details area for the selected user displays. If Operational Views is enabled, additional ops views fields appear in this area. For more information, see Chapter 6, "Operational Views."

Step 2 Click **Edit** next to the Associated Default User Channels list.

The Associate Channel to User window displays.

The Associate Channels to User window displays information in these areas:

- Channels Assigned to User—Displays the channels that have been assigned to this user.
- Available Channels—Displays the channels group and channels that have been configured in Cisco IPICS. (If Operational Views is enabled, the channels you see depend on the ops views configuration. For more information, see Chapter 6, "Operational Views.")

  To see the members of a channel group in this list, expand the group by clicking the right arrow next to the user group name. Click the down arrow next to a channel group name to collapse an expanded group.

Icons in the Associate Channels to User window provide information about each channel group and channel name, as described in Table 3-4.

Table 3-4 Channel Group and Channel Icons

Icon	Meaning
	PTT channel
	PTT channel group
	Busy PTT channel. A channel is busy when it is use by an active VTG.
	Secure PTT channel. You can designate a PTT channel as secure when you add the channel.
	Unavailable PTT channel. A channel is unavailable when it is disabled.

Step 3 Take the appropriate action:

- To associate a channel with a user, drag the desired channel name from the Available Channels area to the Channels Assigned to User area.

  If you want to associate all channels in a channel group with the user, drag the desired channel group name from the Available Channels area.

  The channel name or names appears in green in the Channels Assigned to User area. A channel in green is associated with the user when you click **Save**.

  Repeat this action as needed to associate additional channels with the user.

- To disassociate a channel from a user, drag the channel out of the Channels Assigned to User area.

  When you release the mouse button, the channel name changes to red. A channel in red is disassociated from the user when you click **Save**.

Note If you drag a green channel name out of the Channels Assigned to User area, it disappears instead of turning red because it was not yet associated with the user.

Repeat this action as needed to disassociate additional channels from the user.

Step 4 Click **Save** to exit the Associate Channels to User window and save your changes.

If you want to undo the changes that you made since you last clicked **Save**, click **Revert**.

To exit without saving changes, click **Cancel**.

Step 5 In the Edit User Details area, click **Save** or **Cancel**.

The channels that you associated with the user are saved in either case.

Muting or Unmuting a User in the Edit User Details Window

Cisco IPICS lets you as an operator mute a PMC user as follows:

- Allow the user to listen to a channel but not to speak
- Do not allow the user to speak or listen to a channel
- Allow the user to listen to any channel or VTG, but not to speak
- Do not allow the user to speak or listen to any channel or VTG

You can also unmute a muted user

The Mute feature affects PMC users only. It does not mute the microphone or the speaker of a Cisco IP Phone, and it does not mute the microphone of the user in a PTT channel.

A Cisco IPICS dispatcher can mute a VTG. For instructions, see the "Muting or Unmuting a PMC User in the VTG Workspace Window" section on page 4-18.

To mute or unmute a user, perform the following steps.

For information about accessing the Manage Users Window, see the "Manage Users Window" section on page 3-1.

Procedure

Step 1 In the Manage Users window Users area, take either of these actions:

- Click the user that you want to mute and then click **Details** in the Users area
- Double-click the user that you want to mute

The Edit User Details area for the selected user displays. If Operational Views is enabled, additional ops views fields appear in this area. For more information, see Chapter 6, "Operational Views."

Step 2 In the Associated Default User Channels list, click the channel on which you want to mute the user.

If you want to mute the user on all channels and VTGs, click any channel in this list.

The User Details window displays.

Step 3 Take one of these actions:

- To mute a user, in the User Details window, click one of these mute buttons under:
  - **Mute Mic** (under PMC Settings for Channel)—Allows the user to listen to this channel, but not to speak on it
  - **Mute Mic + Speaker** (under PMC Settings for Channel)—Prevents the user from speaking or listening in this channel
  - **Mute Mic** (under Global PMC Settings)—Allows the user to listen to channels and VTGs on the PMC, but not to speak
  - **Mute Mic + Speaker** (under Global PMC Settings)—Prevents the user from speaking or listening to any channel or VTG

  The button that you click changes to **Unmute Mic** or **Unmute Mic + Speaker**.
- To unmute a user, click the appropriate **Unmute** button.

  Buttons under PMC Settings for Channel affect the current channel only. Buttons under Global PMC Settings affect all channels and VTGs.

  The button that you click changes to **Mute Mic** or **Mute Mic + Speaker**.

Step 4 Click **Close** to exit the User Details window.

Removing a Role from a User

When you remove a Cisco IPICS role that is assigned to a user, you must first temporarily disable that user. If you do not disable the user, the user will continue to access features of the role that you remove until the user logs out and then back in to Cisco IPICS.

To remove a role from a user, perform the following steps.

For information about accessing the Manage Users Window, see the "Manage Users Window" section on page 3-1.

Procedure

Step 1 In the Manage Users window Users area, take either of these actions:

- Click the user from which you want to remove the role and then click **Details** in the Users area
- Double-click the user from which you want to remove the role

The Edit User Details area for the selected user displays.

Step 2 From the IPICS Status drop-down list, choose **Disabled**.

Step 3 Click **Save**.

Step 4 From the Roles drop-down list that displays the role that you want to remove, choose **Select**.

Repeat this step as needed to remove additional roles.

Step 5 Click **Save**.

Step 6 From the IPICS Status drop-down list, choose **Enabled**.

Step 7 Click **Save**.

Deleting a User

If a user is no longer needed, you can delete it from Cisco IPICS.

You cannot delete a user that is a participant in an active VTG or that is a member of a VTG template. You must remove the user from the VTG or the VTG template before you delete it.

To delete a user, perform the following steps.

For information about accessing the Manage Users window, see the "Manage Users Window" section on page 3-1.

Procedure

Step 1 In the Manage Users window Users area, click the user that you want to delete.

The user becomes highlighted.

Step 2 Click **Delete**.

A dialog box prompts you to confirm the deletion.

Step 3 To confirm the deletion, click **OK**.

If you do not want to delete this user, click **Cancel**.

Administration Console: Dispatcher Tasks

A Cisco IPIC dispatcher is responsible for setting up virtual talk group (VTG) templates, activating VTGs to begin conferences, and adding or removing members or participants in VTG templates and active VTGs. A dispatcher also monitors active VTGs and can mute and unmute users as necessary.

In addition, a dispatcher manages policies, each of which activates a VTG template at a particular time and then deactivates it after a designated interval.

You perform the Cisco IPICS dispatcher activities from the Dispatcher window in the Administration Console. To access this window, log in to the Administration Console as described in the "Accessing the Administration Console" section on page 1-10, then choose the **Dispatcher** tab.

Note You must be assigned the dispatcher role to access the Dispatcher window.

This chapter includes these sections:

Note Cisco IPICS allows more than one dispatcher to log into the system at a time. This situation requires coordination between dispatchers, because the users, channels, or groups that are committed to a VTG by one dispatcher may be required by another. The Cisco IPICS operational views feature provides a way to handle this

situation. With this feature, a dispatcher sees only the VTG participants that have been assigned to a particular ops view. For more information about ops views, see Chapter 6, "Operational Views."

Managing VTGs

A VTG enables multiple participants on various channels to communicate using a single multicast address. Participants in a VTG can include users, user groups, channels, channel groups, and other VTGs. An active VTG, also called an *event*, is a VTG in which all the participants have live connections with each other.

You can stage a VTG by creating a VTG template, which is an inactive VTG. You use a VTG template to arrange members that can communicate when you activate the VTG template. You can create as many VTG templates as necessary and activate any of them when needed.

After you activate the VTG, you can easily manage it by adding and removing users, PTT channels, and other VTGs, and by muting an unmuting PMC users.

As a Cisco IPICS dispatcher, you can perform these VTG management tasks:

- Managing VTG Templates, page 4-8
- Managing Active VTGs, page 4-15
- Using the Search Utility, page 4-22

You perform the VTG management tasks in the VTG Workspace Window. For more information about this window, including how to access it, see the "VTG Workspace Window" section on page 4-3.

For related information, see the "Best Practices for Managing VTGs" section on page 4-24.

Note 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. To avoid this issue, see Appendix A, "RMS Configuration" for information about properly configuring an RMS.

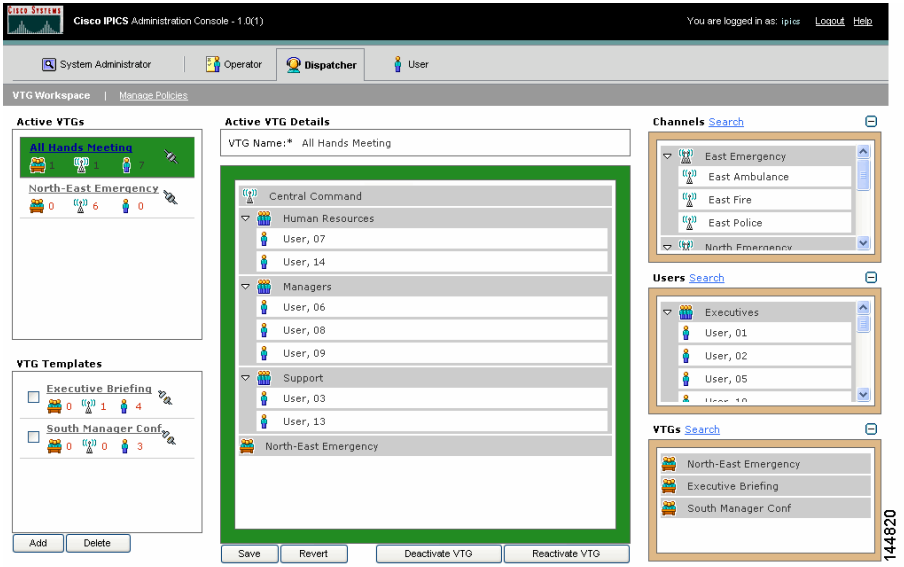
VTG Workspace Window

A Cisco IPICS Dispatcher performs dispatcher tasks in the VTG Workspace window.

To access the VTG Workspace window, log in to the Administration Console as described in the "Accessing the Administration Console" section on page 1-10, then choose the **Dispatcher** tab. Figure 4-1 shows an example of this window.

Note You must be assigned the dispatcher role to access the VTG Workspace window.

Figure 4-1 VTG Workspace Window



For additional information about the VTG Workspace window, see these sections:

- VTG Workspace Window Icons, page 4-4
- VTG Workspace Window Areas and Lists, page 4-5

VTG Workspace Window Icons

Various icons in the VTG Workspace window provide important information. Some icons in the Active VTGs area and in the VTG Templates area display with a number to their right. This number indicates how many of the corresponding item, such as user or PTT channel, are in the VTG or in the VTG template.

Table 4-1 describes the icons that can display in the VTG Workspace window.

Table 4-1 VTG Workspace Window Icons

Icon	Meaning
	Cisco IPICS user.
	User group.
	PTT channel.
	PTT channel group.
	Busy PTT channel. A channel is busy when it is use by an active VTG.
	Secure PTT channel. You can designate a PTT channel as secure when you add the channel.
	Unavailable PTT channel. A channel is unavailable when it is disabled.

Table 4-1 VTG Workspace Window Icons (continued)

Icon	Meaning
	VTG.
	Unavailable VTG channel. For more information, see the "Reactivating a VTG" section on page 4-20.

VTG Workspace Window Areas and Lists

The VTG Workspace Window contains various areas and lists, as described in Table 4-2.

Table 4-2 VTG Workspace Window Areas and Lists

Are or List	Description
Active VTGs area	Displays names of the VTGs that are active and lets you select an active VTG. To see detailed information about a VTG in this area, click the VTG name. Information displays in the Active VTG Details area.
VTG Templates area	Displays names of the VTG templates that have been configured in Cisco IPICS and lets you select a VTG template. To see detailed information about a VTG template in this area, click the VTG name. Information displays in the VTG Template Details area. The check box next to a VTG template name lets you select the template for deletion. For more information, see the "Deleting a VTG Template" section on page 4-14.
Active VTG Details area	Displays when you choose a VTG in the Active VTGs area and shows the participants in the selected active VTG. To see members of a user group or a channel group in this area, expand the group by clicking the right arrow next to the group name. Click the down arrow next to a group name to collapse an expanded group. **Note** To see the participants of a VTG that is a participant if another VTG, look at the Active VTG Details are for the participant VTG.

Table 4-2 VTG Workspace Window Areas and Lists

Are or List	Description
VTG Template Details area	Displays when you choose a VTG template in the VTG Templates area and lists the members in the selected VTG template. To see members of a user group or a channel group in this area, expand the group by clicking the right arrow next to the group name. Click the down arrow next to a group name to collapse an expanded group.
Channels list	Displays the PTT channels and channel groups that can be added to VTGs. To expand this list, click the plus (+) sign to its right. To collapse this list, click the minus sign (-) to its right. To see members of a channel group in this list, expand the group by clicking the right arrow next to the group name. Click the down arrow next to a group name to collapse an expanded group. To search for an item in this list, see the "Using the Search Utility" section on page 4-22.

Table 4-2 VTG Workspace Window Areas and Lists

Are or List	Description
Users list	Displays the users and user groups that can be added to VTGs. This list displays only PMC or Cisco IP Phone users. It does not display users who participate in VTGs using handheld radios or LMRs. To expand this list, click the plus sign (+) to its right. To collapse this list, click the minus (-) sign to its right. To see members of a user group in this list, expand the group by clicking the right arrow next to the group name. Click the down arrow next to a group name to collapse an expanded group. To see additional information about a user, or to mute a user, double-click the user name. The User Details window appears. This window displays information from the user profile, and includes these buttons: • **Mute Mic** or **Unmute Mic** (toggle button)—Clicking **Mute Mic** allows the user to listen to a VTG, but not to speak. Clicking Unmute Mic allows the user to listen and speak in a VTG. Applies to all VTGs and channels in which the user is a participant. • **Mute Mic + Speaker** or **Unmute Mic + Speaker** (toggle button)—Clicking **Mute Mic + Speaker** prevents the user from speaking or listening in a VTG. Clicking **Unmute Mic + Speaker** allows the user to listen and speak in a VTG. Applies to all VTGs and channels in which the user is a participant. • **Close**—Closes the window To search for an item in this list, see the "Using the Search Utility" section on page 4-22.

Table 4-2 VTG Workspace Window Areas and Lists

Are or List	Description
VTGs list	Displays VTG templates that can be added to another VTG. You can add VTG templates from this list to an active VTG or to another VTG template. If you add a VTG template to an active VTG, the VTG that you added and all of its participants become active. To expand this list, click the plus (+) sign to its right. To collapse this list, click the minus (-) sign to its right. To search for an item in this list, see the "Using the Search Utility" section on page 4-22.
Search Results list	Displays the results of a search for channels, users, or VTGs. To expand this list, click the plus sign (+) to its right. To collapse this list, click the minus (-) sign to its right. To see members of a group in this list, expand the group by clicking the right arrow next to the group name. Click the down arrow next to a group name to collapse an expanded group. For more information about searching for a channel, user, or VTG, see the "Using the Search Utility" section on page 4-22.

Managing VTG Templates

A VTG template lets you create various arrangements of members (users, PTT channels, and VTGs), without committing network resources or affecting VTGs that are in progress. A dispatcher can activate a VTG template at any time, which brings the VTG participants together into a live conference.

You can view information about any VTG template by clicking the template name in the VTG Templates area. Information about the template displays in the VTG Template Details area.

When you modify a VTG template, no changes occur in system resources or in the communication between participants until you activate the VTG template. When you make changes to an active VTG, the original template remains unchanged.

As a Cisco IPICS dispatcher, you can perform these VTG template management tasks:

- Adding a New VTG Template, page 4-9
- Modifying a VTG Template, page 4-11
- Activating a VTG, page 4-13
- Deleting a VTG Template, page 4-14

You perform the VTG template management tasks in the Administration Console VTG Workspace window. For more information about this window, including how to access it, see the "VTG Workspace Window" section on page 4-3.

Adding a New VTG Template

When you add a VTG template, you specify the name of the VTG and, typically, designate the members in it. You can activate the VTG template any time after you save it.

The following guidelines apply to VTGs templates:

- A Cisco IPICS user can appear more than once in a list of VTG members. For example, the user could be added individually and as part of one or more user groups. When the VTG becomes active, Cisco IPICS recognizes such multiple appearances as a single user.
- If you drag a user or a PTT channel into a VTG from the Users or Channels lists and that user or PTT channel already exists in a group within the VTG, the channel or user name does not appear another time as an individual user or PTT channel. If you drag a user or PTT channel into a VTG individually and then add a group that contains the user or PTT channel, Cisco IPICS does display the user or PTT channel in the group and individually.
- Cisco IPICS allows you to create blank VTGs, which are VTGs with no members. You can activate a blank VTG and then add participants to it.
- When adding VTGs to another VTG, each VTG that you add is called a sub-VTG. Activating the top-level VTG activates any sub-VTGs. Activating a sub-VTG does not activate the top-level VTG.

- You cannot make a VTG a participant of itself or create a VTG that would result in a loop of VTGs. For example, if you place VTG-A into VTG-B, you cannot place VTG-B into VTG-A.

  Similarly, if VTG-A contains the sub-VTG-D and VTG-C contains the sub-VTG-D, you cannot add VTG-C to VTG-A.

- Mixing secure and non-secure channels in the same VTG is not recommended because users on secure channels will be able to hear users on non-secure channels.

To add a new VTG template, perform the following steps.

For information about accessing the VTG Workspace window, see the "VTG Workspace Window" section on page 4-3.

Procedure

Step 1 In the VTG Workspace window, click **Add**.

A blank VTG Members area displays with an orange border.

Step 2 In the VTG Name field, type a name for the VTG.

The name can include alphanumeric characters, spaces, and any of these characters: . , – ‘ # ( ) / : ,.

Step 3 Add any number and any combination of these items to the VTG template as follows:

- To add a PTT channel, drag the channel name that you want to add from the Channels list to within the orange border in the VTG Members area.
- To add a PTT channel group, drag the channel group name that you want to add from the Channels list to within the orange border in the VTG Members area.
- To add a user, drag the user name that you want to add from the Users list to within the orange border in the VTG Members area.
- To add a user group, drag the user group name that you want to add from the Users list to within the orange border in the VTG Members area.
- To add another VTG, drag the VTG name that you want to add from the VTGs list to within the orange border in the VTG Members area.
- To add a channel, user, or VTG that you searched for, drag the item from the Search Results list to within the orange border in the VTG Members area.

To expand a collapsed Channels, Users, VTGs, or Search Results list, click the plus sign (+) to the right of it. To expand a PTT channel group or a user group, click the right arrow next to it.

When you release the mouse button, the item that you added to the VTG template displays in green until you click **Save** to commit the change. To remove an item that displays in green, drag it out of the orange border in the VTG Members area.

Step 4 When your finish adding items to the VTG, click **Save**.

If you want to abandon your additions, click **Revert** before you click **Save**.

Modifying a VTG Template

When you modify a VTG template, you can change its name, and add or remove members.

Because a VTG template is not an active event, you can make any changes to the template without affecting any current communication between users.

The following guidelines apply when you modify a VTG template:

- If you remove a PMC user from a VTG and that user monitors a PTT channel that remains in the VTG, that user can still participate in the VTG through the PTT channel.
- If a user or a channel appears in a VTG more than once and you remove a single listing of the user or the channel, Cisco IPICS removes all instances of the user or the channel from the VTG.
- If you drag a user out of a user group in the VTG Members area, you do not change the actual user group.
- Empty PTT groups or user groups are not allowed in a VTG. If a group is included in a VTG and you drag every member out of the group, Cisco IPICS removes the group from the VTG.
- When adding VTGs to another VTG, each VTG that you add is called a sub-VTG. Activating the top-level VTG activates any sub-VTGs. Activating a sub-VTG does not activate the top-level VTG.
- You cannot set up a VTG such that it is a participant of itself. For example, if you place VTG-A into VTG-B, you cannot place VTG-B into VTG-A.

- You cannot make a VTG a participant of itself or create a VTG that would result in a loop of VTGs. For example, if you place VTG-A into VTG-B, you cannot place VTG-B into VTG-A.

  Similarly, if VTG-A contains the sub-VTG-D and VTG-C contains the sub-VTG-D, you cannot add VTG-C to VTG-A.

- Mixing secure and non-secure channels in the same VTG is not recommended because users on secure channels will be able to hear users on non-secure channels.

To modify a VTG template, perform the following steps.

For information about accessing the VTG Workspace window, see the "VTG Workspace Window" section on page 4-3.

Procedure

Step 1 In the VTG Workspace window VTG Templates area, click the VTG template that you want to modify.

The VTG template displays in the VTG Templates Details area.

Step 2 If you want to change the name of the VTG template, enter the new name in the VTG Name field.

The name can include alphanumeric characters, spaces, and any of these characters: . , – ‘ # ( ) / : ,.

Step 3 If you want to add members to the VTG template, take any or all of these actions:

- To add a PTT channel, drag the channel name that you want to add from the Channels list to within the orange border in the VTG Template Details area.
- To add a PTT channel group, drag the channel group name that you want to add from the Channels list to within the orange border in the VTG Template Details area.
- To add a user, drag the user name that you want to add from the Users list to within the orange border in the VTG Template Details area.
- To add a user group, drag the user group name that you want to add from the Users list to within the orange border in the VTG Template Details area.
- To add a VTG, drag the VTG name that you want to add from the VTGs list to within the orange border in the VTG Template Details area. (Adding a VTG to another VTG creates a *conference of conferences*.)

- To add a channel, user, or VTG that you searched for, drag the item from the Search Results list to within the orange border in the VTG Template Details area.

To expand a collapsed Channels, Users, VTGs, or Search Results list, click the plus sign (+) to the right of it. To expand a PTT channel group or a user group, click the right arrow next to it.

When you release the mouse button, the item that you added to the VTG template displays in green until you click **Save** to commit the change. To remove an item that displays in green, drag it out of the orange border in the VTG Members area.

Step 4 If you want to remove members from the VTG template, drag each item from the VTG Template Details area to outside of the orange border.

When you release the mouse button, the item changes to red. It is permanently removed from the VTG template when you click **Save**.

If a user or a channel appears in a VTG more than once and you remove a single listing of the user or the channel, Cisco IPICS removes all instances of the user or the channel from the VTG.

Step 5 To finalize your modifications, click **Save**.

If you want to abandon your modifications, click **Revert** before you click **Save**.

Activating a VTG

Activating a VTG causes Cisco IPICS to commit the network resources required to enable the participants in a VTG template to communicate with each other.

A VTG template can also be activated by a policy. For more information, see the "Managing Policies" section on page 4-26.

When you activate a VTG, it attempts to obtain a multicast address from the multicast pool. If it is successful, it attempts to acquire resources for each of its channels and sub-VTGs. (Channels go into the pending state during this process.) If the VTG successfully obtains a multicast address and some resources, it becomes active. Otherwise, it does not activate.

For information about managing an active VTG, including instructions for deactivating and reactivating a VTG, see the "Managing Active VTGs" section on page 4-15.

Note When you activate a VTG, there may be a delay before users can communicate with each other, especially if the VTG contains many PTT channels, users, and other VTGs. The delay may range from a few seconds to more than one minute, depending on the number of participants in the VTG.

To activate a VTG, perform the following steps.

For information about accessing the VTG Workspace window, see the "VTG Workspace Window" section on page 4-3.

Procedure

Step 1 In the VTG Workspace window VTG Templates area, click the VTG template that you want to activate.

The VTG template displays in the VTG Templates Details area.

Step 2 Click **Activate VTG**, which appears in the VTG Templates area under the list of VTG Members.

The VTG becomes active and it moves from the list in the VTG templates area to the list in the Active VTGs area.

Deleting a VTG Template

If a VTG template is no longer needed, you can delete it from Cisco IPICS. Deleting a VTG template has no effect on the members within it.

You cannot delete a VTG template that is associated with an active VTG. To delete such a VTG template, first deactivate the active VTG.

To delete one or more VTGs, perform the following steps.

For information about accessing the VTG Workspace window, see the "VTG Workspace Window" section on page 4-3.

Procedure

Step 1 In the VTG Workspace window VTG Templates area, check the check box next to each VTG Template you want to delete.

Step 2 Click **Delete**.

A dialog box prompts you to confirm the deletion.

Step 3 To confirm the deletion, click **OK**.

If you do not want to delete the VTG or VTGs, click **Cancel**.

Managing Active VTGs

Managing active VTGs can involve the following activities:

- Adding Participants to and Removing Participants From an Active VTG, page 4-16
- Muting or Unmuting a PMC User in the VTG Workspace Window, page 4-18
- Deactivating a VTG, page 4-20
- Reactivating a VTG, page 4-20

The following guidelines apply to active VTGs:

- You can view information about any active VTG by clicking the name in the Active VTGs area. Information about the VTG displays in the Active VTG Details area.
- You cannot make changes to a user group or to a channel group when the group is in an active VTG.
- You cannot delete a user or a channel that is a participant in an active VTG.
- You cannot delete an active VTG. You must deactivate it first.
- A PTT channel can be a participant in one active VTG at a time. If you try to add a PTT channel that is in an active VTG to a another active VTG, or try to activate another VTG that has the PTT channel it, Cisco IPICS shows the PTT channel as unavailable in the second VTG.

- If the Cisco IPICS server fails, all active VTGs continue without disruption. However, the dispatcher can no longer make changes to the VTG or mute a user.

Adding Participants to and Removing Participants From an Active VTG

You can add participants to or remove participants from an active VTG.

When you add participants to an active VTG, Cisco IPICS does not commit network resources to the VTG until you click **Save**. At that point, Cisco IPICS commits the necessary resources to enable the existing VTG participants to communicate with those that you added.

Changes that you make to an active VTG do not affect the VTG template and are not saved to the VTG template when you deactivate the VTG.

Note There typically is a delay of several seconds for changes to take effect after you save them. Therefore, a user who is added to an active VTG may not be able to hear or communicate immediately, and a user who is removed from an active VTG may be able to continue participating in the VTG for a short time.

A user who is added to an active VTG is affected as follows:

- A PMC user sees a new PTT channel button that represents the VTG
- A handheld radio user on an LMR network hears new voices on the radio channel
- A Cisco IP Phone user sees a new selection in the Services > IPICS menu on the phone that represents the VTG

To add participants to or remove participants from an active VTG, perform the following steps.

For information about accessing the VTG Workspace window, see the "VTG Workspace Window" section on page 4-3.

Procedure

Step 1 In the VTG Workspace window Active VTGs area, click the VTG that you want to modify.

The VTG displays in the Active VTG Details area.

Step 2 If you want to add participants to the VTG template, take any or all of these actions:

- To add a PTT channel, drag the channel name that you want to add from the Channels list to within the orange border in the VTG Template Details area.
- To add a PTT channel group, drag the channel group name that you want to add from the Channels list to within the orange border in the VTG Template Details area.
- To add a user, drag the user name that you want to add from the Users list to within the orange border in the VTG Template Details area.
- To add a user group, drag the user group name that you want to add from the Users list to within the orange border in the VTG Template Details area.
- To add a VTG, drag the VTG name that you want to add from the VTGs list to within the orange border in the VTG Template Details area. (A VTG that is added to another VTG is called a *sub-VTG*.)
- To add a channel, user, or VTG that you searched for, drag the item from the Search Results list to within the orange border in the VTG Template Details area.

To expand a collapsed Channels, Users, VTGs, or Search Results list, click the plus sign (+) to the right of it. To expand a PTT channel group or a user group, click the right arrow next to it.

When you release the mouse button, the item that you added to the VTG template displays in green until you click **Save** to commit the change. To remove an item that displays in green, drag it out of the orange border in the VTG Participants area. The item that you added cannot participate in the VTG until you click **Save**.

Step 3 If you want to remove participants from the VTG template, drag each item from the VTG Template Details area to outside of the orange border.

When you release the mouse button, the item changes to red. It is permanently removed from the VTG template when you click **Save**. The item can continue participating in the VTG until you click **Save**.

If a user or channel appears in a VTG more than once and you remove a single listing of the user or channel, Cisco IPICS removes all instances of the user or the channel from the VTG.

Step 4 To finalize your modifications, click **Save**.

If you want to abandon your modifications, click **Revert** before you click **Save**.

Muting or Unmuting a PMC User in the VTG Workspace Window

Cisco IPICS lets you as a dispatcher mute a PMC user in an active VTG or in all VTGs in which the user is a participant, and to unmute any muted user. This feature can be useful if a user is participating from a noisy location, or if you want to mute a user for any other reason.

You can choose how to mute a PMC user as follows:

- Allow the user to listen to the VTG but not to speak in it
- Do not allow the user to speak or listen to the VTG
- Allow the user to listen to any channel or VTG, but not to speak
- Do not allow the user to speak or listen to any channel or VTG

The Cisco IPICS operator can mute a user from the Edit User Details window. For instructions, see the "Muting or Unmuting a User in the Edit User Details Window" section on page 3-22.

The Mute feature affects PMC users only. It does not mute the microphone or the speaker of a Cisco IP Phone, and it does not mute the microphone of a particular user in a PTT channel. In addition, because all the user transmissions in a PTT channel are mixed into a single signal, it is not possible to mute the microphone of a LMR user in a PTT channel.

To mute or unmute a user in an active VTG, perform the following steps.

For information about accessing the VTG Workspace window, see the "VTG Workspace Window" section on page 4-3.

Procedure

Step 1 Take either of these actions:

- In the VTG Workspace window Active VTGs area, click the VTG that contains the user that you want to mute, and then in the Active VTG Details area double-click the user that you want to mute.

  If necessary, click the right arrow next to a user group in the Active VTG Details area to expand the group so that you can see a user.

- Double-the user name in the Users list.

  If necessary, click the right arrow next to a user group in the Active VTG Details area or in the Users list to expand the group so that you can locate a user.

The User Details window displays. If you double-clicked the user in the Users list, the PMC Settings for VTG mute buttons are not available

Step 2 Take one of these actions:

- To mute a user, in the User Details window, click one of these mute buttons under:
  - **Mute Mic** (under PMC Settings for VTG)—Allows the user to listen to the active VTG, but not to speak in the active VTG. (This button does not display if you choose the user from the Users list.)
  - **Mute Mic + Speaker** (under PMC Settings for VTG)—Prevents the user from speaking or listening in the active VTG. (This button does not display if you choose the user from the Users list.)
  - **Mute Mic** (under Global PMC Settings)—Allows the user to listen to channels on the PMC, but not to speak. Affects all channels, not just those in the active VTG.
  - **Mute Mic + Speaker** (under Global PMC Settings)—Prevents the user from speaking or listening to any other users in Cisco IPICS. Affects all channels, not just those in the active VTG.

  The button that you click changes to **Unmute Mic** or **Unmute Mic + Speaker**.

- To unmute a user, click the appropriate **Unmute** button.

  Buttons under PMC Settings for VTG affect the active VTG only. Buttons under Global PMC Settings affect all channels.

  The button that you click changes to **Mute Mic** or **Mute Mic + Speaker**.

Step 3 Click **Close** to exit the User Details window.

Deactivating a VTG

When you deactivate a VTG, the channels in the VTG are no longer connected to each other. You can deactivate a VTG at any time.

To deactivate a VTG, perform the following steps.

For information about accessing the VTG Workspace window, see the "VTG Workspace Window" section on page 4-3.

Procedure

Step 1 In the VTG Workspace window Active VTGs area, click the VTG that you want to deactivate.

The VTG displays in the Active VTG Details area.

Step 2 Click **Deactivate VTG**, which appears in the Active VTGs area under the list of VTG participants.

The VTG becomes inactive and it moves from the list in the Active VTGs area to the list in the VTG templates.

Reactivating a VTG

If all channels are not available for a VTG when you activate it, Cisco IPICS activates the channels that are available. A channel may be unavailable because there are insufficient router resources available for it or because it is in use by another active VTG.

An blue X displays to the right of an unavailable VTG channel in the Active VTG Details area. To see why the channel is unavailable, hold the mouse over the X and look at the tooltip that pops up.

When a VTG channel is unavailable, Cisco IPICS allows the VTG to continue operating without the channel, and lets you take the necessary action to obtain the unavailable channel and reactivate the VTG. When you reactivate a VTG, Cisco IPICS determines whether previously unavailable channels are available and adds them to the active VTG if they are. In this way, Cisco IPICS ensures that you do not have to disrupt a VTG if some channels are not available when you activate it.

To reactivate a VTG, perform the following steps.

For information about accessing the VTG Workspace window, see the "VTG Workspace Window" section on page 4-3.

Procedure

Step 1 Make a note of which channels in the active VTG are unavailable and why.

Cisco IPICS displays a blue X next to each unavailable channel in the VTG Workspace window Active VTG Details area. Hold the mouse cursor over the blue X to see why the channel is unavailable.

Step 2 If the channel is unavailable because of insufficient router resources, take these actions to free additional router resources:

- Remove channels from any VTG
- Disable users that have active SIP unicast connections

Note You can see how router resources are being used by looking at information about its loopbacks in the Manage RMS window. For more information, see the "Viewing Detailed Information about a Loopback" section on page 2-11.

Step 3 If the channel is unavailable because it is in use by another VTG, take either of these actions:

- In the System Administrator tab, click Channels, click the channel name in the Channels list, click **Details**, and look at the active VTG that is listed in the Associated VTGs field. Then choose that VTG in the Active VTGs area in the Dispatcher tab.
- Click the name of another active VTG in the Active VTGs area and see if the channel is a participant in that VTG. Repeat as necessary until you locate the VTG in which the channel is a participant.

Step 4 Remove the channel from the VTG that is displayed in the Active VTG Details area by dragging the resources out of the Active VTG Details area and then clicking **Save**.

Make sure that the channel is not needed in this active VTG before you perform this step.

Step 5 Click the name of the original VTG in which the channel is shown as unavailable.

The contents of the original VTG display in the Active VTG Details area. If the VTG contains other unavailable resources, repeat Step 2 through Step 4.

Step 6 Click **Reactivate VTG**.

Using the Search Utility

You can use the scroll bars next to the Channels, Users, and VTGs lists in the VTG Workspace window to locate an item in a list. However, if a list is long, you may find it easier to use the Search utility to quickly find a PTT channel, user, or VTG.

When you complete a search, the results display in the Search Results list in the lower-right corner of the VTG Workspace window. To expand this list, click the plus sign (+) to its right. To collapse this list, click the minus sign (-) to its right.

To use the search utility to find a PTT channel, user, or VTG, perform the following steps.

For information about accessing the VTG Workspace window, see the "VTG Workspace Window" section on page 4-3.

Procedure

Step 1 In the VTG Workspace window, click any one of the **Search** links.

The Search window appears.

Step 2 In the drop-down list in the top right corner of this window, choose one of these options:

- **By Channel**—Lets you search for channels
- **By User**—Lets you search for users
- **By VTG**—Lets you search for VTGs

The Search window adjusts to display fields that apply to the item that you want to search for.

Step 3 Take one of these actions:

- If you are searching for a PTT channel or a VTG, enter a text string for the channel in the Channel Name field, or enter a text string for the VTG in the VTG Name field.

  A text string can be an entire channel name or VTG name, or it can be any consecutive characters in the name. For example, if you are searching for a VTG called Fire West, you could enter the text string "fire," and Cisco IPICS would return all VTGs that include fire in their name.

  Text strings are not case sensitive.

- If you are searching for a user, enter information in any or all of these fields:
  - User Name, First Name, Last Name, and E-mail fields—Enter text strings for the user that you are searching for.

    A text string can be an entire name or e-mail address, or it can be any consecutive characters in the name or address. For example, if you are searching for a search for the user with the last name Williamson, you could enter the text string, "illi" in the Last Name field, and Cisco IPICS would return users whose last names include this string, such as Willis, Williams, and Williamson.

    Text strings are not case sensitive.

  - Location drop-down list—Location of the user

- Role Name drop-down list—Cisco IPICS role of the user
- Associated Channel Name—Name of the PTT channel that is associated with the user

For example, if you know only a portion of the user name, but you also know that the user a dispatcher in the West Side location, you can enter a character string in the User Name field and then choose Dispatcher and West Side from the Role and Location drop-down lists.

Step 4 Click **Find**.

The items that meet your search criteria display in the Search Results area.

Each item displays on its own row under columns that vary depending on the type of item (channel, user, or VTG) that you searched for.

You can resize any column by dragging the border to the right of its name.

You can toggle the display so that items display in ascending or descending order by any column heading. To do so, click the name in a column heading. An up arrow in a column indicates that items are in ascending order by that column, and a down arrow indicates that items are in descending order by that column.

If the search returns a long list or does not display the item that you want, go back to Step 3 and refine your search criteria.

Step 5 When you have the search results you want, click **OK**.

The Search window closes and the search results display in the Search Results list in the VTG Workspace window.

If you want to abandon the search, click **Cancel**.

Best Practices for Managing VTGs

Cisco IPICS presents new opportunities for members of your organization to participate in conferences. Some of these members may be unfamiliar with the technology, conventions, and practices of PTT communication. For example, these users may have never used a PTT device or participated in a large conference with radio users.

Other PTT users may be surprised by the experience of participating in a Cisco IPICS-managed conference. For example, a handheld radio user may be familiar with the experience of conferring only with a small number of other handheld users on a certain LMR channel. When the LMR channel for that user is placed in a VTG, that user becomes part of a potentially much larger and more diverse conference.

Changes in a conference can occur suddenly for a conference participants, especially those participating with handheld radios. For example, at one moment, a user may be speaking with one or more radio users from the same department. Then, when the dispatcher adds the LMR channel to a VTG, the user hears completely different voices.

The following guidelines can be helpful in assisting your new and experienced users with Cisco IPICS:

- Establish a dispatcher-only PTT channel and add this channel to every PMC and VTG. This channel allows the Cisco IPICS dispatcher to announce VTG changes to the participants, so that they can be made aware when users are added or removed from a VTG.
- Instruct new PMC users on the etiquette of PTT communication. For example:
  - In some network configurations one or more users may not hear when another user breaks into a conversation
  - Keep messages brief and to the point
  - If extensive conversation is required, consider an alternate method of communication
  - Wait until an exiting exchange completes before starting a new one

Managing Policies

A policy activates a VTG or VTG. You can create these types of policies:

- Manually triggered—Policy starts when you manually initiate it and immediately activates its associated VTGs.
- Scheduled—Policy activates its associated VTGs at a predefined date and time, deactivates the VTGs at a predefined date and time or after a specified interval, and optionally repeats this process at designated intervals.

  For example, you might have a VTG that you want to activate for two hours at 9:00 a.m. (0900) on the first Friday of every month, for Fire and EMT teams of a city to discuss emergency readiness.

  You could create a policy that would cause Cisco IPICS to automatically activate this VTG, which might include the City Fire PTT channel, the City EMT PTT channel, the mayor (participating on a PMC), and the Police Department Fire/EMT liaison calling from home.

When you create a policy, ensure that your system has sufficient resources to accommodate the associated VTGs. Cisco IPICS does not warn you that a policy would over-commit system resources when it activates VTGs.

As a Cisco IPICS dispatcher, you can perform these policy management tasks:

- Viewing and Editing Policy Details, page 4-27
- Creating a Policy, page 4-30
- Specifying the VTGs that are Associated with a Policy, page 4-32
- Enabling and Disabling a Policy, page 4-34
- Deleting a Policy, page 4-35

You perform the policy management tasks in the Administration Console Manage Policies window. For more information about this window, including how to access it, see the "Manage Policies Window" section on page 4-27.

Manage Policies Window

The Manage Policies window lists the policies that are configured in Cisco IPICS. It also lets you perform the policy management functions.

To open the Manage Policies window, click the **Manage Policies** link in the Administration Console Dispatcher tab.

Icons in the Manage Policies window provide information about each policy, as described in Table 4-3.

Table 4-3 Policy Icons

Icon	Meaning
	Policy is enabled. An enabled policy will activate its associated VTG templates.
	Policy is disabled. A disabled policy will not activate its associated VTG templates.

In addition, a policy has these designations:

- Active—At least one VTG or VTGs that is associated with this policy is active
- Inactive—VTG or VTGs that are associated with this policy are not active

Viewing and Editing Policy Details

You can view and edit information for any policy. You do so in the Edit Policy Details area.

This area also lets you enable or disable a policy.

To edit or view policy details, perform the following steps.

For information about accessing the Manage Policies window, see the "Manage Policies Window" section on page 4-27.

Procedure

Step 1 In the Manage Policies window, take either of these actions:

- Click the policy for which you want to view or change information and then click **Details**
- Double-click the policy for which you want to view or change information

The Edit Policy Details area for the selected policy displays.

Note If you choose another policy when the Edit Policy Details area is displayed, the information in this area does not change for the new policy until you click **Details** again or double-click the new policy.

Step 2 View or update the information that is described in Table 4-4.

Note You cannot change Activation Properties fields when any VTGs that are associated with this policy have been activated by this policy.

Table 4-4 Edit Policy Details Area Fields

Field	Description
Policy Name	Name of the policy, for example, *Executive Conference* or *Weekly Status Meeting*.
Manually Triggered Only	Designates whether the VTGs that are associated with this policy are activated immediately when you enable the policy. If you check this check box, Cisco IPICS makes the Activation Properties fields unavailable, and it ignores any scheduling information that is in these fields.
Associated VTGs	VTGs that this policy activates. If you click **Edit**, Cisco IPICS displays the Associate VTGs to Policy window, in which you can add or remove VTGs for this policy. For more information, see the "Specifying the VTGs that are Associated with a Policy" section on page 4-32.

Table 4-4 Edit Policy Details Area Fields (continued)

Field	Description
Activation Properties	
Start Time: Date	Month, day, and year that the VTGs that are associated with this policy should activate. For example, December 3 2005.
Start Time: Time	Hour, minute, and time designation (AM or PM) that the VTGs that are associated with this policy should activate. For example, 11:45 AM.
Duration	If the VTGs that are associated with this policy should remain active for a designated time, click this radio button, and enter the duration in any combination of the days, hours, and minutes fields. For example, 3 days 12 hours 0 minutes.
End Time: Date	If the VTGs that are associated with this policy should deactivate a designated date and time, click the **End Time** radio button, and choose the month, day, and year that the VTGs should deactivate.
End Time: Time	If the VTGs that are associated with this policy should deactivate at a designated date and time, enter the month, and day, and choose the hour, minute, and time designation (AM or PM) that the VTGs should deactivate.
Repeat: Every	If the VTGs that are associated with this policy should automatically activate more than once, check the **Repeat** check box and enter any combination of days, hours, and minutes to designate the interval between activation times.

Table 4-4 Edit Policy Details Area Fields (continued)

Field	Description
Repeat: indefinitely	If the VTGs that are associated with this policy should continue to activate and deactivate until you disable or delete the policy, click the **indefinitely** radio button.
Repeat: until	If the VTGs that are associated with this policy should activate and deactivate until a designated date and time, click the **until** radio button enter the month, day, year, hour, minute, and time designation (AM or PM) at which the VTGs should stop activating and deactivating.

Step 3 Click **Save** to save any changes that you have made.

If you want to undo the changes that you made since you last clicked **Save**, click **Revert**.

Creating a Policy

Creating a policy makes it available for use by Cisco IPICS.

To create a policy, perform the following steps.

For information about accessing the Manage Policies window, see the "Manage Policies Window" section on page 4-27.

Procedure

Step 1 In the Manage Policies window, click **Add**.

The Edit Policy Details area for a new policy displays.

Step 2 In the Policy Name field, enter a name for the new policy.

Step 3 If the VTGs that are associated with this policy should activate immediately when you click Enable Policy, check the **Manually Triggered Only** check box and go to Step 7

Otherwise, continue to Step 4.

Step 4 In the Start Time fields, take these actions:

a. In the Date fields, designate a month, day, and year that the VTGs that are associated with this policy should activate.

b. In the Time fields, designate the hour, minute, and time designation (AM or PM) that the VTGs that are associated with this policy should activate.

Step 5 Specify the duration or end time of the VTGs that are associated with this policy as follows:

- If the VTGs should remain active for a designated time, click the **Duration** radio button, and enter the duration in any combination of the days, hours, and minutes fields.
- If the VTGs should deactivate at a designated date and time, click the **End Time** radio button, and choose the month, day, year, hour, minute, and time designation (AM or PM) that the VTGs should deactivate.

Step 6 If the VTGs that are associated with this policy should activate and deactivate repeatedly, take these actions:

a. Check the **Repeat** check box and enter any combination of days, hours, and minutes to designate the interval between activation times of the VTGs.

b. Take either of these actions:

- If the VTGs should continue to activate and deactivate until you disable or delete the policy, click the **indefinitely** radio button.
- If the VTGs should continue to activate and deactivate until a designated date and time, click the **Until** radio button and enter the month, day, year, hour, minute, and time designation (AM or PM) at which the VTGs stop activating and deactivating.

Step 7 Click **Save** to create the policy.

If you decide not to create this policy, click **Cancel**.

Step 8 If you entered a duration or end time for the policy, specify the VTGs to associate with this policy as described in the "Specifying the VTGs that are Associated with a Policy" section on page 4-32.

Step 9 If you want to enable the policy so that its associated VTGs activate and deactivate as scheduled in the Activation Properties fields, click **Enable Policy**.

If you do not want to enable the policy now, you can enable it later as described in the "Enabling and Disabling a Policy" section on page 4-34.

If you checked the **Manually Triggered Only** check box, any VTGs that are associated with the policy will activate immediately when you click **Enable Policy**.

Specifying the VTGs that are Associated with a Policy

When you associate VTGs with a policy, you designate the VTGs that activate when the scheduled policy is enabled.

To associate VTGs with a policy, perform the following procedure.

For information about accessing the Manage Policy Window, see the "Manage Policies Window" section on page 4-27.

Procedure

Step 1 In the Manage Policies window, take either of these actions:

- Click the policy for which you want to view or change information and then click **Details**
- Double-click the policy for which you want to view or change information

The Edit Policy Details area for the selected policy displays.

Step 2 In the Edit Policy Details area, click **Edit**.

Note The **Edit** button does not appear unless you have created and saved a policy. In addition, this button does not appear if any VTGs that are associated with the policy are active.

The Associate VTGs to Policy window displays. This window displays information in these areas:

- VTGs Assigned to Policy—VTGS that the policy triggers when it is activated
- Available VTGs—VTGs that have been configured in Cisco IPICS

Step 3 Take the appropriate action:

- To associate a VTG with a policy, drag the desired VTG from the Available VTGs area to VTGs Assigned to Policy area.

  The VTG name appears in green in the VTGs Assigned to Policy area. A VTG in green is associated with the user when you click **Save**.

  Repeat this procedure as needed to associate additional VTGs with the policy.

- To disassociate a VTG from a policy, drag the VTG out of the VTGs Assigned to Policy area.

  When you release the mouse button, the VTG name changes to red. A VTG in red is disassociated from the policy when you click **Save**.

  Note If you drag a green VTG name out of the VTGs Assigned to Policy area, it disappears instead of turning red because it was not yet associated with the policy.

  Repeat this procedure as needed to disassociate additional VTGs from the policy.

Step 4 Click **Save** to exit the Associate VTGs to Policy window and save your changes.

If you want to undo the changes that you made since you last clicked **Save**, click **Revert**.

To exit without saving changes, click **Cancel**.

Step 5 In the Edit Policy Details area, click **Save** or **Cancel**.

The VTGs that you associated with the policy are saved in either case.

Enabling and Disabling a Policy

Enabling or disabling a policy specifies how the policy controls its associated VTGs. Table 4-5 Describes the results of these actions.

Table 4-5 Results of Enabling and Disabling a Policy

Action	Result
Enable Policy	• If a schedule is specified in the Activation Properties fields for the policy, the policy activates and deactivate its associated VTGs as scheduled • If the **Manually Triggered** check box is checked for the policy, the policy activates its associated VTGs immediately
Disable Policy	• If a schedule is specified in the Activation Properties fields for the policy, the policy will not activate and deactivate its associated VTG as scheduled • If there are any VTGs associated with this policy that have been activated by the policy, immediately deactivates these VTGs

To enable or disable a policy, perform the following procedure.

For information about accessing the Manage Policy Window, see the "Manage Policies Window" section on page 4-27.

Procedure

Step 1 In the Manage Policies window, take either of these actions:

- Click the policy for which you want to view or change information and then click **Details**
- Double-click the policy for which you want to view or change information

The Edit Policy Details area for the selected policy displays.

Step 2 Take one of these actions:

- To enable a policy, click **Enable Policy**.

  The Enabled icon appears next to the policy in the Policies list, and the **Enable Policy** button changes to **Disable Policy**.

- To disable a policy, click **Disable Policy**.

  The Disabled icon appears next to the policy in the Policies list, and the **Disable Policy** button changes to **Enable Policy**.

Deleting a Policy

When you delete a policy, it is permanently removed from Cisco IPICS. The process also deactivates any active VTGs that are associated with the policy. Deleting a policy does not affect any VTGs that are associated with that policy.

You cannot delete a policy when any VTGs that are associated with the policy have been activated by the policy.

To delete a policy, perform the following procedure.

For information about accessing the Manage Policy Window, see the "Manage Policies Window" section on page 4-27.

Procedure

Step 1 In the Manage Policies window, click the policy that you want to delete.

The policy becomes highlighted in blue.

Step 2 Click **Delete**.

A dialog box prompts you to confirm the deletion.

Step 3 To confirm the deletion, click **OK**.

If you do not want to delete this policy, click **Cancel**.

Administration Console: User Tasks

Everyone who uses Cisco IPICS is assigned a user role. This role allows you to log into the Administration Console, view and update your user information, update your communication preferences so that you can use Cisco IPICS to communicate with other Cisco IPICS users, and download the Cisco PMC client application to your PC.

The user role may be your only role, or you may have one or more other roles (system administrator, dispatcher, or operator).

This chapter contains the following sections:

Logging in to Cisco IPICS

When you start Cisco IPICS, the Cisco IPICS Login window displays.

To log into Cisco IPICS, enter your user name in the User Name field, enter your password in the Password field, and then click **Log In**.

User names and passwords are case-sensitive, so make sure to enter them exactly as they are configured.

After you log in, Cisco IPICS Administration Console displays your user profile. If you have been assigned more than one user role, tabs for those roles display beside the User tab. For more information about how an operator assigns user roles, see the "Managing Users and User Groups" section on page 3-3.

Managing Your User Profile

Your user profile includes your name, password, default location, communication preference, and other optional personal information. Your user profile was initially set up by a Cisco IPICS operator, but you can change information as needed.

Your user profile information is shown in the Edit User Details window, which displays after you log in to Cisco IPICS.

Managing your user profile involves reviewing and updating this information. To manage your user profile, perform this procedure:

Step 1 If the Edit User Details window is not displayed, click the **Maintain Profile** link in the Administration Console User tab.

Step 2 Review the information that is described in Table 5-1 and update this information as needed.

Fields that are designated as display only can be changed by a Cisco IPICS operator as described in the "Managing Users and User Groups" section on page 3-3.

Table 5-1 Edit User Details Area Fields

Field	Description
User ID—*Display only*	The ID that you enter when you log into Cisco IPICS.
First Name	Your first name. Valid characters: alphanumeric characters, space, hyphen (-), and apostrophe (’).

Table 5-1 Edit User Details Area Fields (continued)

Field	Description
Last Name	Your last name. Valid characters: alphanumeric characters, space, hyphen (-), and apostrophe (’).
Password	The password that you enter when you log into Cisco IPICS. For security, you should change your password periodically. A password must contain at least 8 characters. Valid characters: alphanumeric characters, special characters except space.
Confirm Password	Confirmation of the entry in the password field.
Digit ID	Identifier that you enter when you access Cisco IPICS from a Cisco IP Phone that has been configured for use with Cisco IPICS. Valid characters: numeric characters.
Digit Password	Password that you enter when you access Cisco IPICS from a Cisco IP Phone that has been configured for use with Cisco IPICS. Valid characters: numeric characters.
Confirm Digit Password	Confirmation of entry in the Digit Password field.
Address	Your street address. Valid characters: alphanumeric characters, spaces, and these special characters: . , – ‘ # ( ) / :.
Address (cont)	Additional street address information. Valid characters: alphanumeric characters, spaces, and these special characters: . , – ‘ # ( ) / :.
City	Your city. Valid characters: alphanumeric characters, space, hyphen (-), and apostrophe (’).

Table 5-1 Edit User Details Area Fields (continued)

Field	Description
State/Province	Your state or province. Valid characters: alphanumeric characters, space, hyphen (-), and apostrophe (’).
Country	Your country. Valid characters: alphanumeric characters, space, and period (.).
Zip/Postal Code	Your zip or postal code. Valid characters: alphanumeric characters, space, and period (.).
E-mail	Your e-mail address. Valid characters: alphanumeric characters, underscore (_), period (.), and ampersand (@).
Default Location	Location used by your Cisco IP Phone.
Roles—*Display only*	Cisco IPICS roles that have been assigned to you. “All” indicates that you have been assigned the privileges of all roles.
IPICS Status—*Display only*	Whether you can listen to PTT channels and participate in VTGs: • Enabled—You can listen to PTT channels and participate in VTGs. • Disabled— You cannot listen to PTT channels and participate in VTGs.
Associated Default User Channels—*Display only*	PTT channels that appear on your PMC or Cisco IP Phone.
User VTGs—*Display only*	VTGs templates in which you are a member or VTGs in which your are participant. Includes one of these designations: • Active—Active VTG • Idle—VTG template

Table 5-1 Edit User Details Area Fields (continued)

Field	Description
Communication Preference	Indicates how you prefer to participate in VTGs. These fields are informational only. They do not affect how you participates in a VTG. • IP Phone or PMC—You participate using a Cisco IP Phone or a PMC. • Channel—You participate on a channel. This option appears only if channels have been associated with you by the Cisco IPICS operator. To specify how you prefer to participate in IPICS communications in VTGs, choose the desired method from the 1 drop-down list. Each time that you choose a method, a new drop-down list appears so that you can specify multiple methods. If you choose **Channel** in a field, a drop down list opens to the right of that field. This list shows the channels that are available for the you. Choose the channel on which you would like a dispatcher to communicate with you.
Belongs To	Appears if Operation View is enabled and indicates the ops view to which you belong. For more information, see For more information, see Chapter 6, "Operational Views."
PMC Attributes	
PMC Status—*Display only*	Indicates how you can communicate in VTGs or channels: • Default—You can listen and talk • Mic Off—You listen but not talk • Mic + Speaker Off—You cannot listen or talk

Step 3 Click **Save** to save any changes that you have made.

To discard your changes, click **Cancel**.

Downloading the PMC

As a Cisco IPICS user, you can download the current version of the PMC to your PC. To do so, perform the following steps from the PC to which you want to download the PMC.

For more information about the PMC, refer to *Cisco IPICS PMC Installation and User Guide*.

Procedure

Step 1 Click the **PMC Download** link in the Administration Console User tab.

Cisco IPICS initiates the PMC download utility, which installs the PMC on your PC and creates a shortcut on your desktop.

Step 2 Follow the on-screen prompts to download and install the PMC.

Operational Views

This chapter describes the Cisco IPICS operational view functionality and it includes information about relevant terminology, caveats, and administration tasks.

This chapter includes the following sections:

Overview of Cisco IPICS Operational Views

This section provides an overview of Cisco IPICS operational views; it includes the following topics:

Introducing Cisco IPICS Ops Views

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

Note The use of ops views allows segmentation of resources that authorized Cisco IPICS users may see on the Administration Console. Ops views does not affect the way in which channels and VTGs display on the PMC or Cisco IP Phone.

This section provides an overview of the Cisco IPICS ops view functionality. It includes the following topics:

Enabling Ops Views

By default, Cisco IPICS disables the ops views functionality on the server. To enable this feature, you must purchase and install a Cisco IPICS license that includes a license for the ops views functionality; then, restart the server. You install this ops view license by uploading it to the server. Navigate to the **System Administrator > License** window in the Administration Console to view the license information.

Note Although the Ops Views check box is checked in the **System Administrator > Options** window by default, the feature is not actually enabled until you upload the license and restart the server. For more information about enabling ops views, see the "Activating the Ops View Feature" section on page 6-18.

When the ops view feature has been enabled on the server, the system displays a Cisco Ops View entry under the Configured License area in the License window, along with the word "Licensed" to indicate that the ops view functionality has been enabled. (When ops views is not enabled, this entry displays "Not Licensed.") Cisco IPICS also displays the number of available licenses and current usage in this window. For more detailed information about license limits and current usage, navigate to the **System Administrator > Ops Views** window. (For more information, see the "Viewing Ops Views Details" section on page 6-10.)

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

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

Note Cisco IPICS displays the number of available licenses and concurrent usage information in the License browser window. As a best practice, make sure that you update your browser window often and before you perform any server administrative functions to ensure that you are working with the most current information. If you attempt to perform an administrative update in a window that does not display the most current data, the update will not succeed and Cisco IPICS will display an error. If this situation occurs, update your browser window and retry the operation.

For more information about managing licenses in Cisco IPICS, see the "Managing Licenses" section on page 2-45. For detailed information about licenses and how to obtain them, refer to *Cisco IPICS PMC Installation and User Guide*.

Creating New Ops Views

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

After a new ops view has been created, the system administrator can associate resources, such as channels, to the ops view, while the operator creates an operator user who belongs to that ops view and who can manage the ops view resources that are visible within the specific ops view.

Note Although operators and dispatchers cannot create ops views, these users may assign resources, and define the resources that are accessible to, different ops views if they have the necessary permissions. Cisco recommends that each ops view contain at least one dispatcher and one operator to manage the resources that are visible to these roles.

For information about assigning the relevant Cisco IPICS resources to ops views, see the "Performing Ops Views Tasks" section on page 6-18.

Assigning Ops Views Resources

Table 6-1 shows the Cisco IPICS resources that you can associate or assign to different ops views.

Table 6-1 Cisco IPICS Ops View Resources

Resource	Where to Find More Information
Users	Creating a User Who Belongs to an Ops View, page 6-21
User groups	Configuring Ops Views for Existing Users or User Groups, page 6-23
Channels/ Channel groups	Associating a Channel or Channel Group to an Ops View, page 6-25
VTGs	How Ops Views Affect VTGs, page 6-27
Policies	How Ops Views Affect Policies, page 6-28

The Benefits of Using Ops Views

By allowing you to segment your resources, the use of ops views enables greater flexibility and enhanced manageability of Cisco IPICS resources. The ops views feature may provide the following organizational benefits:

- Enhanced management of Cisco IPICS resources, such as users, channels, and VTGs for dispatchers by allowing the creation of customized ops views that enable interoperability.
- Increased security by limiting operator and dispatcher access to certain Cisco IPICS resources and isolating certain Cisco IPICS resources from the view of other users.
- Extended functionality by allowing multiple virtual instances of Cisco IPICS on the server.
- Simplified dispatcher and operator responsibilities by limiting access to only those resources that they need to manage.
- Expanded levels of responsibility by authorizing specific operators or dispatchers for the SYSTEM ops view so that these users can manage resources for the entire system.

Specific Cisco IPICS users are authorized to set up and use ops views. The "Ops Views User Roles" section on page 6-7 explains the ops view user roles.

Ops Views Terminology

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

To access this information for users, navigate to **Operator > Manage Users**. Click to highlight a specific user name; then, click **Details** to display the user information.

To access this information for channels, navigate to **System Administrator > Channels**. Click to highlight a specific channel; then click **Details** to display the channel information.

For information about the Belongs To and Accessible To attributes that Cisco IPICS supports for use with ops views, see the "Ops Views Attributes" section on page 6-6.

Ops Views Attributes

This section describes the ops views attributes that Cisco IPICS supports:

Belongs To

- This attribute determines the ops view that the resource belongs to. In other words, the ops view that you specify for this attribute is the ops view that owns this resource.
- A resource belongs to only one ops view.
- For users, the Belongs To attribute determines the resources that users see when they log in to the Cisco IPICS system. A user can view only those resources that are accessible to the ops view to which they belong.
- A VTG belongs to the same ops view as the dispatcher who created the VTG. A dispatcher who belongs to a specific ops view will always have visibility to the VTGs that belong to that same ops view.
- A policy belongs to the same ops view as the dispatcher who created the policy. A dispatcher who belongs to a specific ops view will always have visibility to the policies that belong to that same ops view.
- When a user logs in to a PMC or a Cisco IP Phone, that user consumes a PMC or Cisco IP Phone usage license. Cisco IPICS calculates this license usage against the license limit of the ops view that the user currently belongs to.
- When a dispatcher activates a VTG, or when an enabled policy activates a VTG, that VTG consumes a Cisco IPICS port license. Cisco IPICS calculates this license usage against the license limit of the ops view that the dispatcher belongs to. When an enabled policy activates a VTG, the ops view that the policy belongs to will be charged the license usage for activation of that VTG.
- Cisco IPICS calculates license usage for a Cisco IPICS port against the license limit of the ops view that a channel belongs to. This usage is calculated on a per-connection basis. For more information about license usage, see the "Ops Views License Usage and Limits" section on page 6-10.

- With the exception of VTGs and policies, the Belongs To attribute does not imply that the specified resource can be accessed by this ops view. However, Cisco IPICS automatically adds the Belongs To attribute to the list of ops views that can access this list for users, user groups, channels, and channel groups.

Note By default, all resources that were added to Cisco IPICS before the ops view feature was enabled belong to the SYSTEM ops view.

Accessible To

- This attribute specifies that the resource is accessible to, or visible to, the ops view(s) that Cisco IPICS displays in this field.
- Users have access only to the resources that are accessible to the ops view to which they belong.
- A resource can be accessible to an unlimited number of ops views or no ops views at all.
- The SYSTEM ops view can always access a resource whether or not the SYSTEM ops view is explicitly added to the list of accessible to ops views.

Note

- When you configure a resource to belong to a specific ops view, Cisco IPICS automatically adds that resource as being accessible to the same ops view.
- When you reconfigure the belongs to field for a resource to a different ops view, Cisco IPICS adds the newly-configured ops view to the accessible to list for that resource. However, Cisco IPICS does not remove, from the list of accessible ops views, the ops view that was previously configured.

Ops Views User Roles

When the ops views functionality is enabled, some Cisco IPICS user roles expand to assume additional responsibilities. Table 6-2 describes the various Cisco IPICS ops view user roles and their associated responsibilities.

Note Operators and dispatchers who belong to an ops view can view the VTGs that also belong to that ops view. In addition, they can also view all resources that are accessible to that ops view. These users may not view any resources that do not belong to, or are not accessible to, that ops view.

Note An operator or a dispatcher who belongs to the SYSTEM ops view can view all resources in all ops views.

Table 6-2 Cisco IPICS Ops View User Roles

Cisco IPICS User Role	Responsibilities
System administrator	• The system administrator can add and delete ops views and can also modify the attributes of ops views. • This system administrator can associate an ops view to a channel and a channel group. • As part of the SYSTEM ops view, the system enables full access to the system administrator (and all users who belong to the SYSTEM ops view); that is, these users can see all of the resources in all of the ops views that are configured on the system. • Only those users who belong to the SYSTEM ops view can be assigned the system administrator or all roles.

Table 6-2 Cisco IPICS Ops View User Roles (continued)

Cisco IPICS User Role	Responsibilities
Operator	• Operators who belong to the SYSTEM ops view must create at least one operator per ops view (for all ops views except the SYSTEM ops view) and define each operator as belonging to a specific ops view. These definitions allow the operators who belong to specific ops view(s) to manage the resources for their individual ops view(s). • The operator can add, edit, and delete users and user groups and assign ops views to users and user groups. • The operator can assign each user or user group to any ops view as long as the operator belongs to the SYSTEM ops view. • The operator can only belong to one ops view. Unless the operator belongs to the SYSTEM ops view, this user is limited to only viewing and managing the resources that belong to the ops views that the operator belongs to or other ops views that are accessible to the operator.
Dispatcher	• The dispatcher can belong to only one ops view. Unless the dispatcher belongs to the SYSTEM ops view, this user is limited to only viewing and managing the resources that are accessible to the ops views that the dispatcher belongs to. • The dispatcher manages VTGs but otherwise cannot make changes that affect ops views. • The dispatcher can share management of a VTG with another dispatcher, even if the dispatchers are in different ops views, if the VTG contains resources that are accessible to each of the ops views. • The dispatcher manages policies that belong to the same ops view as the dispatcher or are associated to VTGs that are accessible to the ops view that the dispatcher can access.

Viewing Ops Views Details

This section includes information about how to view the details about each ops view and how to configure the licenses. It includes the following topics:

- Ops Views License Usage and Limits, page 6-10
- Configuring Licenses for Ops Views Usage, page 6-12

From the **System Administrator > Ops Views** link, you can access the detailed information for each ops view. In the Manage Ops Views pane, click the name of an ops view to highlight it; then, click **Details**. The system displays the details for the specific ops view in the Edit Ops View Details pane.

The Manage Ops Views pane includes information about the number of available license limits for licensable features, which includes Cisco IPICS ports, PMC users, and Cisco IP Phone users. The number in each column represents the number of users or ports that can use Cisco IPICS per the license configuration. For example, the number 50 indicates that 50 ports or users are licensed to use the system; the number 0 indicates that no ports or users are licensed to use the system. In this window, the system also displays, via collapsible lists, the resources that belong to, and the resources that are accessible to, the ops view that you are viewing.

Ops Views License Usage and Limits

Cisco IPICS displays detailed license information for current usage and license limits for licensable features in the Edit Ops Views Details pane. To see this information, click the name of an ops view in the Manage Ops Views pane; then, click **Details**.

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

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

- Cisco IPICS Ports Usage—Cisco IPICS ports determine the number of enabled channels and active VTGs that the system can use. An enabled channel or activated VTG consumes a port license. After the channel is deleted or disabled or the VTG is deactivated, the server releases the license and makes it available for use.
  - Cisco IPICS bases license usage for ports on the unique combination of a multicast address and a location; that is, if a channel has two multicast addresses that are assigned to the channel, two licenses are used. If one of the multicast addresses is removed, the system releases one of the licenses so that the port now consumes one license.

Note Be aware that VTGs can be automatically activated by an enabled policy and, therefore, consume a license. The ops view that a policy belongs to will be charged the license usage for activation of that VTG. If the number of licenses has been exceeded, the policy will not be able to activate the VTG. Make sure that the server has a sufficient number of licenses available for the configuration of policies.

- Cisco IPICS PMC Usage—A PMC user consumes a license each time that the user logs in to a PMC session. This license is consumed against the ops view that the user belongs to.

  If the same PMC user logs in to multiple PMC sessions from different PMC client machines, that user will consume multiple licenses (one for each PMC session).

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

Configuring Licenses for Ops Views Usage

In the Edit Ops Views Details pane, the system administrator can configure the number of licenses that should be allocated to ports, PMC users, and Cisco IP Phone users on a per ops view basis by entering the values under the License Limits area.

Note The allocation of licenses per ops view is dependent on the installation of a valid ops view license and ennoblement of the ops view functionality on the server. For more information, see the "Enabling Ops Views" section on page 6-2.

The ability to configure these license limits allows the administrator to distribute and balance the licenses amongst the ops views. This distribution ensures that no one ops view can use more licenses than it has configured. The total number of licenses that can be allocated for each licensable feature cannot exceed the total number of licenses that are available for the entire system.

Note Cisco IPICS automatically computes any available licenses that are not being used in other ops views and allocates them to the SYSTEM ops view.

At any time, the administrator can add and/or remove ops views. When this activity occurs, the available licenses may be taken from the SYSTEM ops view (if available) or added to the SYSTEM ops view. The system administrator can also modify the allocation of ops views licenses to allow redistribution among features or ops views. When the license limits are modified, Cisco IPICS assigns to the SYSTEM ops view any licensable features that are not assigned to a specific ops view.

Additional licenses may be purchased for some or all of the licensable features. If the new license includes a greater number of licenses, Cisco IPICS allocates the additional licenses to the SYSTEM ops view.

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

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

Ops Views Caveats

This section includes information about ops views caveats that apply to this release of Cisco IPICS. For specific information about the caveats that apply to VTGs and sub-VTGs, see the "VTG and Sub-VTG Caveats" section on page 6-14.

The following caveats pertain to the use of Cisco IPICS ops views:

- When you are logged in to Cisco IPICS as a user who belongs to the SYSTEM ops view, or when there are no ops views currently in use, the system does not perform any ops view filtering.
- Users who do not belong to a specific ops view default to the SYSTEM ops view.
- As a Cisco IPICS operator, the system allows you to view and modify only those users that either belong to or are accessible to your ops view. As a Cisco IPICS dispatcher, the system allows you to view and modify only those VTGs that contain resources that either belong to or are accessible to your ops view. You can view only those users and channels that either belong to or are accessible to your ops view.
- VTGs and policies always belong to the ops view of the user who created the VTG or the policy.
- The dispatcher can see all of the resources in a VTG as long as one of the VTG resources is in the same ops view as the dispatcher or if the VTG belongs to the same ops view as the dispatcher. If the remaining resources are not in the same ops view, the system does not display these resources in the Users or Channels panes.
- The system displays only resources that either belong to or are accessible to your specific ops view.
- Members of channel and user groups do not inherit accessibility from the groups; therefore, the system displays all of these resources whether or not they are individually accessible to the specific ops view.

- When you search for a resource by using the search functionality in the Channels, Users, and VTGs panes, the system displays only the resources that are accessible to the specific ops view.
- The policies information that the system displays in the Ops Views window reflects the policies that belong to or are accessible to the specific ops view; that is, the policies that the system shows in this area are those policies that were created by someone who belongs to this ops view.
  - Cisco IPICS enables users who belong to the SYSTEM ops view to view all of the policies that are configured on the server.
  - You can view a policy if the policy contains a VTG and that VTG contains a resource that belongs to or is accessible to your ops view.
  - You cannot view a policy that controls a VTG if that VTG does not contain resources that belongs to or is accessible to your ops view.

VTG and Sub-VTG Caveats

The Cisco IPICS implementation of ops view access for VTGs enables resource sharing among multiple ops views. The ops view functionality allows any dispatcher, who has access to shared resources within a VTG that belongs to a different ops view, to fully access that VTG.

Note When a dispatcher has access to shared resources within a VTG, Cisco IPICS also provides that dispatcher with full control over any of the shared resources in that VTG, such that resources that do not belong to the dispatcher can be modified or deleted.

For example, if a resource (user, channel, or VTG) from ops view 1 is shared within a VTG and the VTG was activated by dispatcher 2 who belongs to a ops view 2, then the VTG belongs to ops view 2. However, dispatcher 1 who belongs to ops view 1 will also be able to access that VTG because at least one of the VTG resources is in the same ops view as the dispatcher who belongs to ops view 1.

The following caveats pertain to VTGs and sub-VTGs when you use ops views:

- As a general rule, VTGs inherit accessibility from the resources that it contains. That is, VTGs belong to the same ops view as the dispatcher who created them.

The following examples depict this rule:

a. If an operator who belongs to the SYSTEM ops view creates a VTG or policy, that VTG or policy belongs to the SYSTEM ops view. The system displays this information in the ops view details pane only for the SYSTEM ops view (it does not display in other ops views).

b. If VTG 1 contains only a single channel (channel 1) and that channel is accessible to ops view 1 and ops view 2, then VTG 1 is also accessible to ops view 1 and ops view 2.

   Table 6-3 shows an example of VTG ops view accessibility.

Table 6-3 VTG Ops View Accessibility

Resource	Contents	Accessibility
VTG 1	Contains a single channel (channel 1)	
Channel 1		Accessible to ops view 1 and ops view 2
VTG 1		Accessible to ops view 1 and ops view 2

- This same general rule applies to VTGs that contain other VTGs (also known as sub-VTGs), depending on their states (see the next bullet for more information about this dependency).

  For example, if VTG 1 contains only VTG 2 and VTG 2 is accessible to ops view 1, then VTG 1 is also accessible to ops view 1 (because VTG 1 contains VTG 2, which is accessible to ops view 1).

  Table 6-4 shows an example of sub-VTG ops view accessibility.

Table 6-4 Sub-VTG Ops View Accessibility

Resource (state)	Contents	Accessibility
VTG 1 (active)	Contains sub-VTG (VTG 2)	
VTG 2 (active)		Accessible to ops view 1
VTG 1		Accessible to ops view 1

- With sub-VTGs, there is a dependency on the active/inactive state of the sub-VTG for purposes of determining accessibility. That is, an active VTG can only inherit accessibility from an active sub-VTG and an inactive VTG can only inherit accessibility from an inactive sub-VTG.

  By using the previous example, this means that if VTG 1 is active and VTG 2 is inactive, then VTG 1 will not be accessible to ops view 1.

  Table 6-5 shows an example of active/inactive state dependency on sub-VTG ops view accessibility.

Table 6-5 Active/Inactive Sub-VTG Ops View Accessibility

Resource (state)	Contents	Accessibility
VTG 1 (active)	Contains sub-VTG (VTG 2)	
VTG 2 (inactive)		Accessible to ops view 1
VTG 1		Not accessible to ops view 1

- An ops view that can access a sub-VTG can also access the resources in the VTG that contains the sub-VTG.
- However, an ops view that can access a VTG that contains a sub-VTG may not be able to access that sub-VTG unless there is a resource in the sub-VTG that provides access to the ops view.

  Table 6-6 shows an example of how resources in sub-VTGs can affect ops view accessibility.

Table 6-6 Sub-VTG Resources for Ops View Accessibility

VTG 1	VTG 2

Table 6-6 Sub-VTG Resources for Ops View Accessibility (continued)

VTG 1 contains the following resources: • User 1, who is accessible to ops view 1 • VTG 2 (sub-VTG)	VTG 2 contains the following resource: • User 2, who is accessible to ops view 2
VTG 1 becomes accessible to the following ops views: • Ops view 1—VTG 1 inherits accessibility from User 1 • Ops view 2—VTG 1 inherits accessibility from VTG 2, which contains User 2	VTG 2 becomes accessible to the following ops view: • Ops view 2—VTG 2 inherits accessibility from User 2
Ops View 1 Dispatcher	**Ops View 2 Dispatcher**
The ops view 1 dispatcher can see the details for the following resources: • VTG 1—User 1, who is accessible to ops view 1, is in VTG 1 (The ops view 1 dispatcher has no access to the contents in VTG 2 because ops view 1 does not have access to ops view 2)	The ops view 2 dispatcher can see the details for the following resources: • VTG 2—User 2, who is accessible to ops view 2, is in VTG 2 • VTG 1—VTG 2 is a sub-VTG of VTG 1

  - The ops view 1 dispatcher can see the details for VTG 1 and can add or remove resources from VTG 1. Because a sub-VTG shows as a resource in a VTG, the ops view 1 dispatcher can also remove the sub-VTG (VTG 2) even though the ops view 1 dispatcher cannot see the details of VTG 2. (The ops view 1 dispatcher can see that VTG 2 is contained in VTG 1 and this dispatcher can make changes even though the contents of VTG 2 cannot be seen.)

- You can use sub-VTGs as a way to shield the participants in the sub-VTG from other resources who should not be able to see them.
- When you associate VTGs to policies, the system displays only the VTG templates that are accessible to the ops view.

- The VTG Workspace pane displays the VTGs that belong to the specific ops view or the VTGs that contain resources that are accessible to the specific ops view. The system displays all contents of a highlighted VTG in this workspace, but the Channels, Users, and VTGs panes display only the resources that are accessible to this specific ops view.

Performing Ops Views Tasks

There are several tasks that must be performed to activate, create, and configure ops views for use on the server. You can also edit or remove ops views, as needed. This section describes these ops views-related tasks and the affect that ops views has on Cisco IPICS resources, such as VTGs and policies.

This section includes the following topics:

Activating the Ops View Feature

To activate the Cisco IPICS ops views feature, you must upload and install the Cisco Ops View license on the server. For information about uploading the license, see the "Uploading the License to the Server" section on page 6-19.

Uploading the License to the Server

To upload the Cisco Ops View license to the server, perform the following procedure:

Procedure

Step 1 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***>**

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

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

The User menu on the Cisco IPICS server displays.

Step 4 Click the **System Administrator** tab; then click **License**.

The system license information displays.

Step 5 In the Add a License area, click the **Browse** button to locate the license file that you want to upload to the server. Alternatively, you can enter the path for the file in the License File field.

Step 6 Click **Upload** to upload the license file to the server.

Step 7 Click **Apply** to enable the changes to become effective.

If you are uploading a new ops views license, you must restart the server.

Note Step 8 to Step 10 document the procedure for restarting the server. These steps apply only if the ops view license status has changed from "not licensed" to "licensed."

Step 8 To restart the server, connect to the Cisco IPICS server by using SSH Secure Shell client software (or equivalent software).

Step 9 Log in to the server with root user privileges.

Step 10 From root, enter the following command to restart the Tomcat web server:

[root]# service ipics_tomcat restart

The system restarts the Tomcat web server.

With the Cisco Ops View license installed, the ops view functionality is activated and you are ready to use ops views. From this point, you can add new ops views and assign users and resources to the ops views.

Step 11 To create an ops view, continue with the "Creating Ops Views" section on page 6-20.

Note To view the Cisco Ops View license on the server, navigate to **System Administrator > License** and locate the ops view license entry under the Configured License area. For more information about this license, see the "Enabling Ops Views" section on page 6-2.

Creating Ops Views

After you have enabled the ops view feature, you can begin to create ops views.

The system displays the ops views that the system administrator creates and allows Cisco IPICS resources, such as users, user groups, channels, channel groups, VTGs, and policies, to be assigned to these ops views.

Note By default, Cisco IPICS includes a SYSTEM ops view. You cannot delete or edit the SYSTEM ops view.

To create an ops view, perform the following procedure:

Procedure

Step 1 Log in to the server by using the system administrator user name and password.

Step 2 From the System Administrator tab, click the **Ops Views** link.

The Manage Ops Views window displays.

Note When you open the Manage Ops Views window for the first time, the system displays the SYSTEM ops view as the default ops view.

Step 3 To add a new ops view, click **Add**.

The Edit Details pane displays.

Step 4 In the Edit Details pane, enter a name for the ops view.

Tip The name that you enter for the ops view should be descriptive to reflect the nature of its use.

Step 5 Enter the applicable license information, as described in the "Configuring Licenses for Ops Views Usage" section on page 6-12.

Step 6 Click **Save**.

The newly-created ops view displays in the Manage Ops Views window.

Creating a User Who Belongs to an Ops View

After the system administrator creates the ops view, an operator must be defined as belonging to the specific ops view.

Note To add the first operator to an ops view, you must be logged in to the server with operator privileges and belong to the SYSTEM ops view.

To create a user who belongs to an ops view, perform the following procedure:

Procedure

Step 1 From the Operator tab, click the **Manage Users** link.

The Manage Users window displays.

Step 2 To add a new user, click the **Add** button that displays under the Users pane.

The Edit User Details pane displays.

Step 3 Enter the user information in the fields that display along the left side of the pane.

Tip User names, including VTG, channel groups, and user groups, must be unique across all ops views that are configured on the server.

Step 4 Click **Save** to apply your changes and save them to the database.

Step 5 In the Ops View Attributes area, complete the **Belongs To** field by choosing an ops view, from the drop-down list box, that the user will belong to.

Note Operators who do not belong to the SYSTEM ops view cannot set the belongs to field to any ops view other than the one to which they belong.

Step 6 In the Ops View Attributes area, complete the **Accessible To** field by clicking the **Edit** button to associate an ops view to this user.

Note When you create a new user, the **Edit** button does not display until you complete the user profile by clicking **Save**.

The Associate Ops Views window displays to show the ops views that this user is visible to and the available ops views.

Step 7 From the list of Available Ops Views, click to highlight the individual ops view that you want to assign to this user. Then, drag the ops view to the User Visible by Ops Views pane.

The system highlights, in green text, the ops view that you dragged.

Step 8 Repeat Step 6 for each ops view that you want to associate to this user.

Step 9 Click **Save** to associate this ops view to the user.

To discard your changes, click **Revert**.

The Associate Ops Views to User window closes. The system displays the ops views that you associated to the user in the Accessible To field.

Note Users who are in the system administrator or all roles must belong to the SYSTEM ops view.

Note Operators who do not belong to the SYSTEM ops view cannot assign the system administrator or all roles to users.

Operators who do belong to the SYSTEM ops view cannot change a user who is in the system administrator or all role to belong to or be accessible to an ops view.

Configuring Ops Views for Existing Users or User Groups

When you configure ops views to users or user groups, the system displays only those users or user groups who are accessible to the specific ops view.

Note You must perform this procedure as a Cisco IPICS operator.

The Cisco IPICS operator may add only those users or user groups who belong to the specific ops view of which the operator is a member.

To configure ops views to a user or user group, perform the following procedure:

Procedure

Step 1 From the Operator tab, click the **Manage Users** link.

The Manage Users window displays.

Step 2 In the User area, click a user name to highlight it; then click **Details**. (To add a user group, click a user group name to highlight it; then, click **Details**.)

The Edit User (or User Group) Details pane displays.

Step 3 In the Ops View Attributes area, complete the **Belongs To** field by choosing an ops view, from the drop-down list box, that this user (or user group) belongs to.

Note The system automatically adds to the accessible to field the ops view that you choose in the belongs to field.

Step 4 In the Ops View Attributes area, complete the **Accessible To** field by clicking the **Edit** button to associate this user (or user group) to an ops view.

The Associate Ops Views window displays to show the ops views that the user (or user group) is visible by and the available ops views.

Note In this window, you can also change the associated ops views that have access to this user or user group.

Step 5 From the list of Available Ops Views, click to highlight the individual ops view that you want to associate to this user (or user group). Then, drag the ops view to the User (or User Group) Visible by Ops Views pane.

The system highlights, in green text, the ops view that you dragged.

Note From the list of Visible Ops Views, you can also click to highlight the individual ops view that you want to disassociate from this user or user group. Then, drag the ops view to the Available Ops Views pane. The system highlights, in red text, the ops view that you dragged.

Step 6 Repeat Step 5 for each ops view that you want to associate (or disassociate).

Step 7 Click **Save** to associate this user or user group to the ops view (or to remove the association between this ops view and the user or user group).

To discard your changes, click **Revert**.

The Associate Ops Views to User (or User Group) window closes. The system displays the updated list of ops views that are associated to the user or user group in the Accessible To field.

Note Users do not inherit accessibility from user groups and user groups do not inherit accessibility from users.

Associating a Channel or Channel Group to an Ops View

When you associate a channel or channel group to an ops view, you must also specify the belongs to and the accessible to fields in the Ops View Attributes area.

Note You must perform this procedure as a Cisco IPICS system administrator and belong to the SYSTEM ops view.

To associate a channel or channel group to an ops view, perform the following procedure:

Procedure

Step 1 From the System Administrator tab, click the **Channels** link.

The Manage Channels window displays.

Step 2 In the Channels pane, click to highlight a channel (for channel groups, click to highlight a channel group in the Channel Groups pane); then, click **Details**.

The Edit Channel (or Channel Group) Details window displays.

Step 3 In the Ops View Attributes area, complete the **Belongs To** field by choosing an ops view, from the drop-down list box, that this channel (or channel group) belongs to.

Note The system automatically adds to the accessible to field the ops view that you choose in the belongs to field.

Step 4 In the Ops View Attributes area, complete the **Accessible To** field by clicking the **Edit** button to associate the channel (or channel group) to an ops view. Choose the ops views that the channel (or channel group) is accessible to. (This entry defines which ops views can view and manage the channel or channel group.)

The Associate Ops Views window displays to show the associated and available ops views for this channel (or channel group). In this window, you can associate the channel (or channel group) that can has access the ops views.

Note In this window, you can also change the associated ops views that have access to this channel or channel group.

Step 5 From the list of Available Ops Views, click to highlight the individual ops view that you want to associate to this channel. Then, drag the ops view to the Associated Ops Views pane.

The system highlights, in green text, the ops view that you dragged.

Note From the list of Associated Ops Views, you can also click to highlight the individual ops view that you want to disassociate from this channel or channel group. Then, drag the ops view to the Available Ops Views pane. The system highlights, in red text, the ops view that you dragged.

Step 6 Repeat Step 5 for each ops view that you want to associate (or disassociate).

Step 7 Click **Save** to associate this ops view to this channel.

To discard your changes, click **Revert**.

The Associate Ops Views window closes. The system displays the updated list of ops views that are associated to the channel (or channel group) in the Accessible To field.

Note Channels do not inherit ops view associations from channel groups and channel groups do not inherit ops view associations from channels.

How Ops Views Affect VTGs

This section describes the affect that ops views have on VTGs. For the specific caveats that pertain to this section, see the "Caveats" section on page 6-27. For information about additional caveats, see the "VTG and Sub-VTG Caveats" section on page 6-14.

VTGs do not require a dispatcher to associate ops views. The Cisco IPICS implementation automatically determines the ops views that can access each individual VTG based on the VTG contents and the VTG creator.

VTGs belong to the same ops view as the user who created the VTG. Therefore, you do not need to define the belongs to field for VTGs.

For example, if an operator who belongs to the SYSTEM ops view creates a VTG, that VTG belongs to the SYSTEM ops view. The system displays this VTG in the ops view details pane only for the SYSTEM ops view (it does not display this VTG information in any of the other ops views).

Note VTGs always belong to the ops view of the user who created the VTG.

Caveats

Be aware of the following caveats as you use this ops view functionality:

- The VTG Workspace window displays the VTGs that belong to a specific ops view and the VTGs that contain resources that are accessible to specific ops views.
- The system displays all contents of a highlighted VTG in this workspace area, while the inactive VTG resources, such as channels, users, and VTGs, display only the resources that are accessible to the specific ops view.
- The exception pertains to members of a channel or user group, who the system displays whether or not they are individually accessible to the specific ops view.

Tip If a VTG unexpectedly becomes active or inactive, check for any policies that may be associated to the VTG. An operator in another ops view can create a policy that is associated to any VTG that the operator has access to.

How Ops Views Affect Policies

This section describes how ops views affect policies. For specific caveats that pertain to this section, see the "Caveats" section on page 6-28. For information about additional caveats, see the "Ops Views Caveats" section on page 6-13.

You do not need to take explicit action to assign an ops views to a policy. When you create a new policy, or when you have existing policies, the system displays these policies as resources in the ops view of the user who created the policies.

A policy is accessible to any ops view that has access to the VTGs that are associated to the policy.

Note Policies always belong to the ops view of the user who created the policy.

Caveats

Be aware of the following caveats as you use this ops view functionality:

- The policies information that the system displays as resources for a specific ops view reflects the policies that belong to the specific ops view; that is, the policies that the system shows in this area are those policies that were created by someone who belongs to this ops view.
- When the Cisco IPICS operator views the policies in the Manage Policies window, the system displays only those policies that belong to or are accessible to the specific ops view of which the operator is a member.
- When you associate VTGs to policies, the system displays only those VTG templates that are accessible to the specific ops view.
- Like VTGs, policies belong to the same ops view as the user who created them. For example, if an operator who belongs to the SYSTEM ops view creates a policy, that policy belongs to the SYSTEM ops view. The system displays this information in the ops view details pane only for the SYSTEM ops view (it does not display in any of the other ops views).

Tip If a VTG unexpectedly becomes active or inactive, check for any policies that may be associated to the VTG. An operator in another ops view can create a policy that is associated to any VTG that the operator has access to.

Disabling Ops Views

You can disable the ops views functionality on the server after it has been enabled.

Note You must perform this procedure as a Cisco IPICS system administrator.

To disable ops views, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to **System Administrator > Options**.

Step 2 Under Options, check the **Ops Views** check box to disable this feature.

This check box allows you to enable and disable ops views.

Step 3 Click **Save** to save your changes.

You must restart the server to complete this task.

Step 4 To restart the server, connect to the Cisco IPICS server by using SSH Secure Shell client software (or equivalent software).

Step 5 Log in to the server with root user privileges.

Step 6 From root, enter the following command to restart the Tomcat web server:

[root]# service ipics_tomcat restart

The system restarts the Tomcat web server.

Note To reenable ops views, check the **Ops Views** check box in the System Administrator > Options window, upload the license, and restart the server.

Recovering a Deleted System Administrator User

You can recover your system if you delete the system administrator user name in error and there are no users who can log in to the server by using the system administrator or all role, and there are no users in the SYSTEM ops view (when ops views are enabled).

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

Procedure

Step 1 Log in to the server by using the operator user name and password.

Note Cisco IPICS includes a safeguard that prevents all operators from being deleted from the system. Therefore, if you have deleted the system administrator user role in error, the operator maintains the ability to assign another system administrator user role.

Step 2 From the Operator tab, click the **Add** button that displays under the Users pane.

The Edit User Details pane displays.

Step 3 In the required fields, that are indicated by an asterisk, enter the user information.

Step 4 From the Roles drop-down list box, choose **system administrator** or **all** for the user role.

The new user appears in the SYSTEM ops view; this user can access the System Administrator tab to perform administrative tasks.

RMS Configuration

Before you can use an RMS with Cisco IPICS or perform the RMS management tasks that are described in Chapter 2, "Administration Console: System Administrator Tasks," you must configure the RMS. Cisco IPICS will not support an RMS that is not configured as described in this appendix.

When you set up an RMS, follow these guidelines:

- Configure at least two T1 controllers and assign DS0 groups to each controller. In addition, allocate only as many DS0s on a controller as the RMS can support simultaneously. The ports that you allocate must start with port 0 and must be sequential. Typically, a controller will support 24 DS0s, but your controller may support fewer, depending on the number of available DSPs. Allocating more DS0s than a controller has resources to support can cause loss of voice and voice quality issues.
- Configure T1 controllers for individual voice ports by including this command in the router configuration.

  DS0-group *DS0-group-number* **timeslots** *timeslot-list* **type e&m-lmr**

  Where:

  - **DS0-group** *DS0-group number* identifies the DS0 group and must be a a value from 0 to 23. DS0 groups must start with 0 and must be sequential.
  - **timeslots** *timeslot-list* specifies a single time-slot number. For T1, allowable values range from 1 to 24.

For example,

```
DS0-group 0 timeslots 24 type e&m-lmr
DS0-group 1 timeslots 1 type e&m-lmr
...
DS0-group 23 timeslots 23 type e&m-lmr
```

These commands specify the DS0 time slots that define logical voice ports on a T1 controller and specify the signaling type by which the router communicates with the PSTN.

If you want to configure only 12 DS0s, configure DS0 groups 0 through 11 in this example.

To configure an RMS to interact with the Cisco IPICS sever, perform the following steps.

Note The following steps uses sparse-dense-mode. The design of your multicast network may require you to use an ip pim mode other than sparse-dense-mode.

Procedure

Step 1 Configure DS0 groups on controllers by including the following commands in the router configuration.

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

Use these commands for the first controller in a loopback pair:

```
Router(config)#controller T1 1/0
Router(config-controller)#framing esf
Router(config-controller)#clock source internal
Router(config-controller)#linecode b8zs
Router(config-controller)#cablelength short 133
Router(config-controller)#DS0-group 0 timeslots 24 type e&m-lmr
Router(config-controller)#DS0-group 1 timeslots 1 type e&m-lmr
Router(config-controller)#DS0-group 2 timeslots 2 type e&m-lmr
...
Router(config-controller)#no shutdown
```

Use these commands for the second controller in a loopback pair:

```
Router(config)#controller T1 1/1
Router(config-controller)#framing esf
Router(config-controller)#linecode b8zs
Router(config-controller)#cablelength short 133
Router(config-controller)#DS0-group 0 timeslots 24 type e&m-lmr
Router(config-controller)#DS0-group 1 timeslots 1 type e&m-lmr
Router(config-controller)#DS0-group 2 timeslots 2 type e&m-lmr
...
Router(config-controller)#no shutdown
```

Step 2 Enable multicast routing in the router by including the IP multicast-routing command in the router configuration:

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

Step 3 Create a virtual interface for multicast communication by including the following commands in the router configuration.

```
Router(config)#interface Vif1
Router(config-if)#ip address ip_address subnet_mask
Router(config-if)#ip pim sparse-dense-mode
```

Step 4 Create a loopback interface for voice signaling and media by including these command in the router configuration:

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

Step 5 Assign voice signaling and media to the loopback interface by including these command in the router configuration:

```
Router(config)#voice service voip
Router(conf-voi-serv)#sip
Router(conf-serv-sip)#bind control source-interface Loopback0
Router(conf-serv-sip)#bind media source-interface Loopback0
```

Step 6 Enable multicast routing for each interface that will participate in multicast traffic by including this command in the router configuration for each participating interface:

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

Step 7 Create a voice class that will be applied to all voice configurations by including these command in the router configuration:

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

Step 8 Create a cryptographic key to enable SSL (HTTPS) secure access from the Cisco IPICS server by including this command in the router configuration

```
Router(config)#ip http secure-server
```

Step 9 Enable log in through Telnet and SSH by including these command in the router configuration:

```
Router(config)#line vty 0 15
Router(config-line)#transport input telnet ssh
Router(config-line)#exec-timeout 22 0
Router(config-line)#privilege level 15
Router(config-line)#login local
```

Note Optimally, set exec-timeout to 22 (22 minutes). Setting to a shorter time such as 5 or 10 minutes can cause undesirable delays every time that Cisco IPICS accesses the router, such as when you make a change to a VTG. Setting a long time such as 60 minutes can cause authorized logins to accumulate and cause the router to run out of open lines. Do not set exec-timeout to 0.

Step 10 Take these actions:

a. Create a user name and password for the router by including this command in the router configuration:

```
Router(config)#username username privilege 15 password 0 password
```

b. Apply the same *password* to the enable password on the router by including this command in the router configuration:

```
Router(config)#enable password 0 password
```

You will enter this user name and password in the Cisco IPICS Administration Console when you configure the RMS.

Step 11 Configure SIP inactivity timeout by including these commands in the router configuration:

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

Step 12 Configure the list of codecs that Cisco IPICS will support by including these command in the router configuration:

```
Router(config)#voice class codec 1
Router(config-class)#codec preference 1 g729r8
Router(config-class)#codec preference 2 g711ulaw
```

Step 13 Create the following inbound dial peer by including the following commands in the router configuration.

These commands cause the default SIP PMC connection to have vad off.

```
Router(config)#dial-peer voice 555 voip
Router(config-dial-peer)#voice-class codec 1
Router(config-dial-peer)#session protocol sipv2
Router(config-dial-peer)#incoming called-number .
Router(config-dial-peer)#no vad
```

Step 14 Reset the router command prompt by including this command in the router configuration:

```
Router(config)#no prompt
```

Step 15 Execute the following command and verify that the output reflects the modifications that you have made in this procedure:

```
Router#show running-config
```

Step 16 Execute the following command to save the changes that you have made:

```
Router#copy running-config startup-config
```

For detailed configuration information, refer to the Land Mobile Radio over IP documentation at the following URL:

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

Setting Up and Using the Cisco IP Phone with Cisco IPICS

Cisco IPICS allows you to use a Cisco IP Phone model 7960 or 7970 to communicate on PTT channels and participate in channels and VTGs.

Before a user can access the Cisco IPICS service, the system administrator must configure Cisco IPICS as an available phone service in Cisco CallManager Administration. Then, the user must subscribe to the Cisco IPICS service by using the Cisco CallManager User Options web-based application, which provides limited, end-user configuration of Cisco IP Phone applications.

This appendix includes these topics:

Configuring Cisco IPICS as a Phone Service

To configure Cisco IPICS as an available service, choose **Feature > Cisco IP Phone Services** from Cisco CallManager Administration.

For more information about setting up phone services in Cisco CallManager Administration, refer to the Cisco IP Phone Services configuration information in the *Cisco CallManager Administration Guide* for the version of Cisco CallManager that you use. You can find the Cisco CallManager documentation at the following URL:

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

To configure Cisco IPICS as a phone service, enter the following values in the Cisco IP Phone service configuration fields:

- **Service Name**—Cisco IPICS

  This field displays the name of the service as Cisco IPICS in the menu of available services.

- **Service Description**—Access to the Cisco IPICS System.

  This field contains a description of the content that the Cisco IPICS service provides. You can enter any description, as appropriate.

- **Service URL**—
  http://<*ipics_server IP address*>/ipics_server/servlet/IPPhoneManager

  where <*ipics_server IP address*> represents the IP address of the Cisco IPICS server.

  This field specifies the URL of the Cisco IPICS server where the Cisco IP Phone Services application is located.

- **Character Set**—Choose your default language if you use a language other than English.

  This field specifies the correct character set to use for your default language.

After you configure Cisco IPICS as an available service, IP phone users can subscribe to the service by using the Cisco CallManager User Options web site. When users subscribe to the Cisco IPICS service, the Cisco IP Phone Services menu displays Cisco IPICS as an option.

Using Cisco IPICS as a Service on the Cisco IP Phone

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

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

Procedure

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

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

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

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

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

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

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

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

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

Step 7 To access the Cisco IPICS service, press the **Services** button on the Cisco IP Phone.

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

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

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

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

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

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

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

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

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

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

If you want to latch, or lock in, the channel or VTG, press the **Latch** softkey. You can disengage the latch by pressing the **Stop** softkey.

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

Step 14 Press the **Logout** softkey when you are done using the Cisco IPICS service on your Cisco IP Phone.

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

Tip To obtain help with using the Cisco IPICS service on a Cisco IP Phone, press the **Help** softkey.

Frequently Asked Questions

This appendix contains frequently asked questions about Cisco IPICS, and provides answers to these questions.

This section provides information about using an RMS with Cisco IPICS.

Q. Does Cisco IPICS allow multiple Cisco IPICS servers to use the same RMS?

A. No, Cisco IPICS does not support the use of multiple Cisco IPICS? servers for the same RMS. Each server must have the use of resources on a corresponding RMS to ensure proper functionality.

Q. Does Cisco IPICS support more than one RMS in the same location.

A. Yes.

Q. What makes a channel remote?

A. A channel is remote when it is in a different multicast domain than the user who is accessing it.

Q. What does the designation “remote” mean for a location?

A. This designation indicates a special Cisco IPICS location that treats every channel or VTG as if it were in a remote location.

Q. If I only have one router in a location and my channel is defined as All, will the channel be accessible a user?

A. Yes. However, if a router location is All, a channel that is not also configured as All will not be accessible to users or VTGs that the router supports.

Q. How many resources (voice ports, multicast addresses) do I need?

A. The following guidelines apply to the use of resources:

- Every active VTG consumes one multicast address from the global address pool (but it does not consume a DS0 pair)
- Every channel that is active in a VTG consumes one DS0 pair (also called a loopback)
- Every sub-VTG in a VTG consumes one DS0 pair
- Every SIP connection consumes one DS0 pair per channel or VTG per user, per location
- Local channels do not consume any DS0 pairs
- G.729, used for a SIP connection, requires DSP resources

The following items do not consume voice resources:

- A user with an associated channel (the system only consumes resources when the user logs in from a remote location)
- A VTG that includes only users
- User Groups
- Channel Groups

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 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.

Symbols

A

B

C

D

E

G

H

I

L

M

N

O

P

R

S

T

U

V

X