Cisco IPICS Server Quick Start Guide

Release 2.1(1)

Americas 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: 408 527-0883

Customer Order Number:
Text Part Number: OL-12998-01

Cisco IPICS Server Quick Start Guide, Release 2.1(1)

CONTENTS

CHAPTER 1

Overview of Cisco IPICS

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

This chapter provides an overview of the tasks that you need to perform to set up Cisco IPICS. It also introduces components to help familiarize you with Cisco IPICS.

This chapter includes the following sections:

Related Documentation

For additional information about the Cisco IPICS server and the PMC application, refer to the following documents:

- *Cisco IPICS Server Administration Guide, Release 2.1(1)*
- *Cisco IPICS Server Quick Start Reference Card, Release 2.1(1)*

- *Using Cisco IPICS on Your IP Phone Quick Start Reference Card, Release 2.1(1)*
- *Using the Cisco IPICS TUI Quick Start Reference Card, Release 2.1(1)*
- *Cisco IPICS Radio and Tone Descriptor File Examples Reference Card, Release 2.1(1)*
- *Cisco IPICS Server Installation and Upgrade Guide, Release 2.1(1)*
- *Cisco IPICS Server Quick Start Installation Reference Card, Release 2.1(1)*
- *Cisco IPICS PMC Installation and User Guide, Release 2.1(1)*
- *Cisco IPICS PMC Quick Start Reference Card, Release 2.1(1)*
- *Cisco IPICS PMC Debug Reference Quick Start Guide, Release 2.1(1)*
- *Cisco IPICS PMC Command Line Interface, Release 2.1(1)*
- *Cisco IPICS Troubleshooting Guide, Release 2.1(1)*
- *Release Notes for Cisco IPICS Release 2.1(1)*
- *Cisco IPICS 2.1(1) Resources Card (Documentation Locator)*
- *Solution Reference Network Design (SRND) for Cisco IPICS Release 2.1(1)*
- *Cisco IPICS Compatibility Matrix*

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

http://www.cisco.com/en/US/products/ps7026/tsd_products_support_series_home.html

Getting Started

After installing the Cisco IPICS operating system and server software, you perform a series of procedures in sequence to set up and configure Cisco IPICS.

For more detailed information about installing the Cisco IPICS operating system and Cisco IPICS server software, refer to the *Cisco IPICS Server Installation and Upgrade Guide, Release 2.1(1).*

Table 1-1 provides an overview of the sequential procedures that you need to perform to set up and configure Cisco IPICS, with references to sections in this document that provide additional information. You can use this information as a guide when setting up Cisco IPICS for the first time.

For information about logging in to Cisco IPICS, see the "Logging In to and Out of Cisco IPICS" section on page 2-3.

Table 1-1 Set Up and Configure Cisco IPICS

Procedure	References
Become Familiar with Cisco IPICS	
1. Learn about the hardware and software components that are part of Cisco IPICS	Cisco IPICS Components, page 1-5 Refer to "Introducing Cisco IPICS" in the *Cisco IPICS Server Administration Guide, Release 2.1(1)* for detailed configuration and management information.
2. Learn about the roles that Cisco IPICS users can have	See the "Operator Tasks" section on page 2-17. Refer to "Performing Cisco IPICS Operator Tasks" in the *Cisco IPICS Server Administration Guide, Release 2.1(1)* for detailed information.
3. Learn about the Cisco IPICS Administration Console, including how to access this application	Cisco IPICS Administration Console, page 1-7 See the "Logging In to and Out of Cisco IPICS" section on page 2-3
Set Up and Configure Cisco IPICS	
1. Configure the router media service (RMS) component	See the "System Administrator Tasks" section on page 2-14, the "Managing the RMS" section on page 3-1, and the "Understanding Locations" section on page 2-4. Refer to "Performing Cisco IPICS Server Administration Tasks" and "Performing Cisco IPICS Dispatcher Tasks" in the *Cisco IPICS Server Administration Guide, Release 2.1(1)* for detailed configuration and management information.
2. Configure locations	
3. Configure the multicast pool	
4. Create push-to-talk (PTT) and/or radio channels and VTGs	

Table 1-1 Set Up and Configure Cisco IPICS

Procedure	References
5. Determine user roles and add users and user groups	See the "Operator Tasks" section on page 2-17. Refer to "Performing Cisco IPICS Operator Tasks" in the *Cisco IPICS Server Administration Guide, Release 2.1(1)* for detailed information.
6. Create VTGs	See the "Dispatcher Tasks" section on page 2-18 and the "Understanding VTGs" section on page 2-6. Refer to "Performing Cisco IPICS Dispatcher Tasks" in the *Cisco IPICS Server Administration Guide, Release 2.1(1)* for more detailed information.
7. Install the PMC installer and upload the current PMC version package	See the "System Administrator Tasks" section on page 2-14 and the "Managing the Cisco IPICS PMC" section on page 3-18. Refer to "Performing Cisco IPICS System Administrator Tasks" in the *Cisco IPICS Server Administration Guide, Release 2.1(1)* for more detailed information.
8. Configure the Cisco IPICS policy engine, if needed	See the "Managing and Using the Cisco IPICS Policy Engine" section on page 3-8. Refer to "Using the Cisco IPICS Policy Engine" in the *Cisco IPICS Server Administration Guide, Release 2.1(1)* for detailed information.

Table 1-1 Set Up and Configure Cisco IPICS

Procedure	References
9. Create operational views (ops views), if needed	See the "System Administrator Tasks" section on page 2-14 and the "Understanding Ops Views" section on page 2-7. Refer to "Configuring and Managing Cisco IPICS Operational Views" in the *Cisco IPICS Server Administration Guide, Release 2.1(1)* for detailed information.
10. Set up Cisco Unified IP Phones, if needed	See the "Using Cisco Unified IP Phones with Cisco IPICS" section on page 3-21. Refer to "Setting Up and Using a Cisco Unified IP Phone as a Cisco IPICS Push-To-Talk Device" in the *Cisco IPICS Server Administration Guide, Release 2.1(1)* for detailed information.

Cisco IPICS Components

You can deploy Cisco IPICS in a variety of configurations. Your configuration depends on the types of communications devices that users employ, the media types that are used, and your interoperability requirements. A Cisco IPICS deployment typically includes the following hardware and software components:

- Cisco IPICS server—The Cisco IPICS server software runs on the Cisco IPICS operating system and performs the following functions:
  - Hosts the Administration Console
  - Hosts the Cisco IPICS policy engine, , that provides the ability to create and manage policies
  - Provides Cisco IPICS authentication and security services
  - Stores data that is required for operation
  - Enables integration with various media resources, such as (RMS) components, PMC clients, and Cisco Unified IP Phones

- Push-to-Talk Management Center (PMC)—The PMC is a PC-based audio application that simulates a handheld radio to enable PTT functionality for PC users. It connects Cisco IPICS users via an IP network to enable participation in and monitoring of one or more talk groups or VTGs at the same time. The PMC is supported for use only with the Windows XP operating system.
- LMR gateways—LMR gateways provide voice interoperability between radio and non-radio networks by bridging radio frequencies to IP multicast streams.
- RMS—The RMS provides the following functionality:
  - 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 VTG
  - Support for unicast M1:U12:M2 connection trunks
- Networking components—Networking components may include some or all of the following components:
  - switches
  - routers
  - firewalls
  - mobile access routers
  - wireless points and bridges
- Cisco Unified Communications Manager (previously known as Cisco Unified CallManager) functionality—Cisco Unified Communications Manager , or a Cisco router that is running a supported version of Cisco IOS, enables selected Cisco Unified IP Phone models to participate in channels and VTGs. These applications can also serve as the SIP provider for the Cisco IPICS policy engine.
- Audio clients—Audio clients are devices through which users participate in channels or VTGs. They include PMC clients, and various models of the Cisco Unified IP Phone.

For more detailed information about Cisco IPICS components, refer to the *Cisco IPICS Server Administration Guide, Release 2.1(1)* and the *Cisco IPICS PMC Installation and User Guide, Release 2.1(1)*.

Cisco IPICS Administration Console

The Cisco IPICS server includes the Administration Console, which is a web-based graphical user interface (GUI) that you use to perform various administration, configuration, and management functions in Cisco IPICS. You use the Administration Console to perform and manage Cisco IPICS activities, depending on your Cisco IPICS role. For information about the functionality that is included in the Administration Console, see the "Identifying Items in the Administration Console" section on page 1-7.

Identifying Items in the Administration Console

The Cisco IPICS Administration Console contains several information drawers and tabs. The drawers that display correspond to the Cisco IPICS roles that have been assigned to you. Therefore, depending on your role, you may not see all of the drawers in the Administration Console.

To access the various windows in the Administration Console, click the applicable drawers in the Server and Policy Engine tabs that display along the left side of the Administration Console. When you click the arrow to the left of a drawer, the drawer expands to display the windows that are available in that drawer.

Table 1-2 and Table 1-3 describe the drawers and windows that you can access in the Server and Policy Engine tabs to perform Cisco IPICS functions.

Table 1-2 Server Tab in the Administration Console

Tab	Description
Server	The server tab contains the following drawers that you can access, depending on your user roles: • Home—Users can access the windows in this drawer to manage personal data, view resource associations, and to download the PMC. • VTG Management—Dispatchers can access the window in this drawer to manage VTGs and events, such as notifications and dial-outs. • User Management—Operators can access the windows in this drawer to manage users and user groups. • Configuration—System administrators can access the windows in this drawer to configure various components, such as channels (PTT and radio), channel groups, radio and tone descriptors, locations, multicast pools, ops views, and RMS components. • Administration—System administrators and ops view administrators can access the windows in this drawer to manage functions, such as license, database and activity log management, active users and options. • PMC Management—System administrators can access the windows in this drawer to manage PMC versions, alert tones, skins, regions, and to generate the PMC installer. • Serviceability—System administrators can access the windows in this drawer to monitor system status, get diagnostic information, and to view and download the system logs.

Table 1-3 Policy Engine Tab in the Administration Console

Tab	Description
Policy Engine	The policy engine tab contains the following drawers: • Policy Management—Users can access this drawer to manage Cisco IPICS policies and get information about policy execution status. • Dial Engine—Users access this drawer to manage the dial engine, which enables the telephony user interface (TUI) and its associated features. Tasks that authorized users can perform in the dial engine tab include managing dial-in/dial-out functions, monitoring system status and logs, managing standard and custom script prompts and spoken names, configuring the SIP provider and dial engine parameters, and managing direct dial numbers. **Note** Any Cisco IPICS user can access this tab, but certain activities that are available from this drawer require specific Cisco IPICS user access, such as system administrator. For more information about the various roles in Cisco IPICS and for more detailed information about the functionality of the Administration Console, refer to the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

Cisco IPICS Server Usage Guidelines

Be aware of the following tips and guidelines when you use the Cisco IPICS server:

- Cisco IPICS provides support for various user roles, including system administrator, ops view administrator, operator, dispatcher, and user. The functionality that may be performed is dependent on the specific user role.
- By default, the Administration Console times out after 30 minutes of non use. In this situation, the current Administration Console window remains displayed, but Cisco IPICS prompts you to log back in when you attempt to

perform a function. To log back in, enter your user name and password; then click **Log In**. To exit the Administration Console, click **Logout** in any Administration Console window.

  - You may configure this setting for a different timeout value by accessing the Administration > Options window. For more information, refer to the "Managing Cisco IPICS Options" section in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

- Server login passwords and server host names are case-insensitive; passwords are case-sensitive, so be sure to enter passwords exactly as they are configured in the server.
- Access to the Cisco IPICS server online help system is available from various windows in the Administration Console. To access the server online help, click the **Help** link in any Administration Console window.
- To view information about the version of Cisco IPICS that you are using, click **About** in the Administration Console.
- Many of the Administration Console windows allow you to modify the appearance of the results by specifying search criteria and reformatting the results based on rows per window.
  - Depending on the window, you may be able to search, or filter, your results based on resources, locations, roles, and ops views.
  - You enter your search criteria in the Filter field and click **Go**.
  - When you search on a character string, Cisco IPICS returns all results that begin with the character string that you specify.
  - To clear the search criteria, click **Clear Filter**.
  - To modify the number of rows that display, choose from the Rows per page drop-down list box that displays at the top of the window; then, click **Go**.
  - To navigate between results windows, click the arrows that display at the bottom of the window.
- Many of the resources in Cisco IPICS, such as channels, users, and VTGs, display in lists in the Administration Console. These lists include check boxes that you can check to select the individual resources to perform certain functions. Some of these resource lists provide a check box that appears at the top of the list that enables you to select all resources at one time.

- Many of the Administration Console windows include drop-down list boxes, some of which become available only after you perform certain functions. If you do not perform the required function, the drop-down list box displays as dimmed to indicate that it is not available for use.
- An asterisk (*) that displays next to a field, drop-down list box, or check box, in the Administration Console indicates required information. You must provide this information before you can save changes and exit the window.
- Most windows contain a Save button and a Cancel button. The Save button saves any changes that you make in a window; clicking this button may close the window automatically. The Cancel button cancels any changes that you have made.
- For some resources, separate detailed windows display in which you can take the following actions:
  - To move an item from one list to another list, click the item to highlight it and then click **>** or **<**, or double-click the item.
  - To move several items from one list to another list at one time, Shift-click or Ctrl-click to select the items and then click **>** or **<**.
  - To move all items from one list to another list at one time, click **>>** or **<<**.
- To expand a collapsed list, click the arrow that displays to the left of the list.
- The Cisco IPICS server contains the associated connection configuration, which correlates to its locations, to determine how the PMC users should connect. Cisco IPICS provides connection support for both multicast and unicast communications. Make sure that users are aware of the appropriate location information to use when they log in to Cisco IPICS.
- Cisco IPICS includes the following two predefined locations:
  - ALL—This location signifies no network boundaries; that is, a channel that is designated with the ALL location means that there are no network boundaries within the Cisco IPICS deployment for that associated multicast address.
  - REMOTE—This location is available only to PMC users. When a PMC user chooses the REMOTE location, connectivity is established with the appropriate RMS via a SIP-based unicast connection for each channel or VTG that has been assigned to the user.

    For more information about locations, see the "Understanding Locations" section on page 2-4.

- Users who are in the same multicast domain are also in the same Cisco IPICS location.
- When configuring IP multicast addresses, Cisco strongly recommends that you configure IP multicast addresses that are only in the 239.192.0.0 to 239.251.255.255 range. This address range is part of the Administratively Scoped Block, as specified by RFC 3171, and is intended for use in a local domain. As such, this address range is less likely to cause an addressing conflict in an existing multicast domain. For more detailed information, refer to the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.
- Cisco IPICS does not support the use of multiple Cisco IPICS servers for the same RMS component because each server must have the use of resources on a corresponding RMS for proper functionality.
- Cisco IPICS provides support for more than one RMS component in the same location.
- When you configure your RMS component, make sure that you perform all of the configuration procedures that are documented in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.
- Be aware of the number of participants in a conference and their type of connection to avoid resource contention.
- If you see a VTG become active or inactive unexpectedly, it could be because of a policy that is associated to the VTG. For more information about VTGs and ops views, refer to the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

CHAPTER 2

Cisco IPICS Server Administration

This chapter describes the various administration tasks and concepts that are important to understand when you use Cisco IPICS and includes the following sections:

You install the Cisco IPICS software on supported Cisco Media Convergence Servers (MCS). For information about hardware and software that is compatible for use with Cisco IPICS, refer to the *Cisco IPICS Compatibility Matrix*.

Before you can perform administration tasks in Cisco IPICS, you must first install the Cisco IPICS operating system and the Cisco IPICS server software. For detailed information about installing Cisco IPICS, refer to the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Managing Cisco IPICS Licenses

You must first purchase and upload the applicable Cisco IPICS server license file(s) to use any of the features that are available in Cisco IPICS or to use the Cisco IPICS Administration Console.

After you complete the Cisco IPICS installation, you use the Product Authorization Key (PAK) that was included in your Cisco IPICS product package to obtain the license file.

The license that you purchase is based on the total number of the following licensable features:

- The concurrent number of land mobile radio (LMR) ports
- The concurrent number of multicast ports
- The concurrent number of PMC users
- The concurrent number of Cisco Unified IP phone users
- The concurrent number of dial users (this feature is dependent on the policy engine, which must be specifically licensed and enabled for use)
- The total number of ops views

Tip The total number of licensable features cannot exceed the number that is specified in the license or licenses that you purchased. If you require additional licenses, contact your Cisco representative.

Note You may use valid Cisco IPICS release 2.0(x) license(s) for use with this release.

To purchase your Cisco IPICS license file(s), access the following URL:

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

Tip Be sure to register with Cisco.com before trying to process a license order.

After you have purchased your license file, you can upload the file(s) by accessing the Administration > License Management window in the Administration Console. Refer to the *Cisco IPICS Server Administration Guide, Release 2.1(1)* for information about how to upload and apply your Cisco IPICS licenses.

Cisco IPICS does not overwrite older license files with newer license files. As a best practice, Cisco recommends that you take the following action when license changes occur, such as when you replace a time-bound (demonstration or evaluation) license with a permanent license:

- Make sure that you remove the old license file(s) from the directory where Cisco IPICS stores the license(s).

  For more information about deleting time-bound licenses, refer to the *Cisco IPICS Server Installation and Upgrade Guide, Release 2.1(1)*.

- After you remove the old license(s), restart the server by entering the following command:

  [root] **service ipics restart**

Logging In to and Out of Cisco IPICS

You must log in to the Cisco IPICS Administration Console to perform any administration functions. When you have finished using Cisco IPICS, you should log out of the Administration Console.

You must install the Cisco IPICS operating system and server software, and upload one or more license files before you can log in to Cisco IPICS. For detailed information about obtaining license file(s), refer to the "Managing Licenses" section in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

To log in to and out of Cisco IPICS, complete the following steps:

Step 1 To log in to Cisco IPICS, follow these steps:

a. Launch your browser and enter the IP address or host name of the Cisco IPICS server in the Address field.

b. Enter your user name and password.

Note Be aware that passwords are case-sensitive and must be entered exactly as they were configured by the Cisco IPICS operator.

c. Click **Log In**.

The Cisco IPICS Administration Console displays the My Profile window. You see only the information that relates to your user ID and the user role that has been assigned to you.

Step 2 To log out of Cisco IPICS, click the **Logout** button that displays in the menu at the top of the Administration Console window.

The Cisco IPICS window closes and displays the Cisco IPICS login window.

Accessing Online Help in the Administration Console

You can access the Cisco IPICS online help system from any window in the Administration Console by clicking **Help** link that displays at the top of the window. The help system provides online access to the information that is contained in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

Important Cisco IPICS Concepts

The following sections include information about important concepts that you need to know when you use Cisco IPICS:

Understanding Locations

In Cisco IPICS, locations are used to define multicast domains within a Cisco IPICS deployment. A multicast domain comprises a set of multicast addresses that are reachable within a multicast network boundary. This implementation enables the Cisco IPICS server to assign the appropriate multicast address based on a specific user location.

In addition to specifically assigning names to locations, Cisco IPICS includes two predefined locations: ALL and REMOTE.

The ALL location signifies no network boundaries; that is, a channel that is designated with the ALL location means that there are no network boundaries within the Cisco IPICS deployment for that associated multicast address.

Note The ALL location defines the scope or reachability or a multicast address. For this reason, the ALL location is applicable to channels and VTGs, which are associated with multicast addresses, but not applicable to IP phones and RMS components, which are not associated with multicast addresses.

- Channels that are designated with the ALL location can be mixed on any RMS, including RMS components that are not configured with the ALL location, because any RMS can send packets to a multicast address that is associated with the ALL location.
- VTGs are always associated with the ALL location because every VTG multicast address is dynamically-assigned and associated with the ALL location.

The REMOTE location is available only to PMC users. When a PMC user chooses the REMOTE location from the drop-down list box, connectivity is established with the appropriate RMS via a SIP-based unicast connection for each channel (should have at least one media connection of multicast type) or VTG that has been assigned to the user.

- For each channel (should have at least one media connection of multicast type) that is associated with the user, the PMC establishes a SIP-based unicast connection with the RMS that is defined in the same location as the channel.
- For each VTG that is associated with the user, the PMC can establish a SIP-based unicast connection with any RMS because VTGs always use a multicast address in the ALL location.

In all cases, the Cisco IPICS server allocates RMS resources upon successful PMC authentication. When additional channels or VTGs are assigned to a logged-in user, the server immediately allocates the necessary RMS resources for each channel or VTG. When the PMC user activates the channel or VTG, the PMC places the SIP call to the appropriate RMS.

Note Each RMS component that you configure for use with Cisco IPICS must be associated with a location. An RMS can host only those channel resources that are assigned to the same location as the RMS or to the ALL location. If the RMS is associated with the ALL location, it can host only those channels that are also assigned to the ALL location. Because of this implementation, Cisco recommends that you do not assign the ALL location to an RMS.

Tip Whenever possible, user access via multicast communications is preferable over SIP to minimize the use of RMS resources.

For more detailed information about configuring locations, refer to the *Cisco IPICS Server Administration Guide, Release 2.1(1)* and the *Cisco IPICS PMC Installation and User Guide, Release 2.1(1).*

Understanding VTGs

A VTG enables multiple participants on various channels to communicate by using a single multicast address. Participants in a VTG can include users, user groups, channels (PTT and radio), channel groups, and other VTGs. An active VTG is a VTG in which all the participants have live connections with each other.

Note To prevent audio loops from occurring, Cisco IPICS allows only one VTG to be active at a given time.

Cisco IPICS dispatchers can stage a VTG by creating an inactive VTG. The dispatcher uses an inactive VTG to arrange participants who can communicate when the VTG gets activated.

An inactive VTG allows the dispatcher to create various arrangements of members without committing network resources or affecting other VTGs that are in progress.

After the VTG is activated, the dispatcher can add and remove users, channels, and other VTGs, notify and dial out to VTG participants, and mute and unmute PMC users at any time; however, when the dispatcher makes changes to an active VTG, the original inactive VTG remains unchanged.

Note Activation or deactivation of a VTG requires that the Cisco IPICS server communicate with the RMS. If a VTG is deactivated during the time when the RMS becomes unavailable, the deactivation occurs in the Cisco IPICS database, but is not reflected in the RMS until the Cisco IPICS server is back in communication, and synchronizes with, the RMS.

For more detailed information about VTGs, refer to the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Understanding Ops Views

Cisco IPICS operational views (ops views) provide the ability to organize or segment different entities, such as agencies, companies, departments, jurisdictions, municipalities, or sites, into separate views that are isolated from each other, providing increased security by limiting operator and dispatcher access. While these views are maintained separately by the 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. In other words, resources in separate ops views are not accessible to users in other ops views unless the users are granted permission to access them.

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 Unified IP Phone.

Ops View Port Allocation

When you purchase Cisco IPICS license(s), the license includes a specified number of ops views that you can configure. By default, Cisco IPICS includes the SYSTEM ops view with every installation. Cisco IPICS users who belong to the SYSTEM ops view can view all ops views, and their resources, that are configured on the system.

Each time the system administrator adds a new ops view, ports are reallocated from the SYSTEM ops view and distributed to the newly created ops view. The system administrator determines the number and types of ports, such as PMC ports, LMR ports, and dial ports that are needed for a particular ops view.

Note If the Cisco IPICS license contains the policy engine, the system administrator can configure dial port information per ops view.

When you add dial numbers (DNs) for ops views in a Cisco IPICS deployment that includes the policy engine, and if the new DNs fall outside of existing route patterns that are assigned to a session initiation protocol (SIP) trunk (in Cisco Unified Communications Manager) or outside of existing destination patterns that are assigned to a dial peer (in Cisco IOS), you must update the SIP provider configuration to include the new DNs. For detailed information, refer to the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

When an ops view gets deleted, the system administrator has the option to reallocate the resources that were in the deleted ops view to other existing ops views in the system.

You must allocate dial ports for users to be able to dial in to Cisco IPICS, dial out to other users, or for the system to notify users. These dial ports are configured in the Dial Information and Dial Port Resources Allocation pane, in the Configuration > Ops Views > <ops view name> window.

Dial port containers (also referred to as *dial pools*) allow you to configure reserve dial ports that are used only for specific dial functions (such as dial-in/invite and notification). Reserved dial ports ensure that you always have ports that are configured specifically for this use and which cannot be used for any other purpose.

The following dial pools are used for reserving ports for dial-in/invite and notification:

- Dial ports reserved for dial-in/invite—This dial pool contains dial ports that can be used only for the dial-in and invite features.
- Dial ports reserved for notification—This dial pool contains dial ports that can be used only for the notification feature.

The Dial ports reserved for dial-in/invite or notifications field is a read-only field that displays ports that Cisco IPICS allocates for both dial-in/invite and notification actions. The ports that display in this field are the ports that remain after you have reserved dial ports for dial-in, invite, and notification. The remaining number are the dial ports that are reallocated from the total number of dial ports in the Dial Ports dial pool.

Note When you create a new ops view, dial port licenses are reallocated from the SYSTEM ops view to the new ops view, but there is no adjustment to the dial port numbers that were configured in the Dial ports reserved for dial-in/invite and Dial ports reserved for notification dial pools for the SYSTEM ops view. For the new ops view, if the dial port numbers that you configure in the reserved dial pools exceed the number of ports in the Dial Ports field, Cisco IPICS displays an error message to alert you. To resolve this issue, reduce the number of reserved ports in the SYSTEM ops view to an appropriate number and try again.

For more detailed information about dial port allocation, refer to the "Allocating Dial Ports for the Dial-In/Invite and Notification Features" section in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

Ops View Attributes

Cisco IPICS ops views support the following attributes:

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.

Note Only an operator or a dispatcher who belongs to a certain ops view should create, edit, or delete policies that are associated with that ops view. For more information, refer to the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

- When a user logs in to a PMC or a Cisco Unified IP Phone, that user uses a PMC or Cisco Unified 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 uses a concurrent multicast 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 is charged the license usage for activation of that VTG.
- Cisco IPICS calculates license usage for a concurrent LMR port against the license limit of the ops view that a channel belongs to. This usage is calculated on a per-connection basis.

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.
- The SYSTEM ops view can always access all resources even if it does not explicitly appear in the list of accessible 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 that 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 the previously-configured ops view from the list of accessible ops views. The resource is accessible to the previous ops view, as well as the newly-configured ops view.

Ops View Considerations

When using ops views, considering the following caveats:

- 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 who 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 windows.
- 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 VTG windows, 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.
- 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.

- As a general rule, VTGs inherit accessibility from the resource that it contains.

For detailed configuration information about Cisco IPICS ops views, refer to the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

Understanding Associations

In Cisco IPICS, you can assign attributes to users that control their behavior. In some cases, attributes may have the same attribute behaviors, so when users are associated to channels or VTGs, the system determines the resulting PMC behaviors based on the attributes that are configured for each associated resource.

For example, a user may be allowed to perform a particular function, such as using the PMC latch feature. However, when the same user is associated to a channel that does not allow the latch feature, the user is not allowed to latch on that channel as long as the user is a part of that particular association. After the user

is no longer associated to that channel, the attributes that were originally configured for the user become applicable; that is, the user is allowed to latch channels again.

Cisco IPICS allows values for attributes to be customized or overridden. When attributes of users or channels that are part of an association get modified, the resulting behavior depends on the attribute settings for those users within the association. When you attempt to override a customized value of an attribute in an association, Cisco IPICS prompts you with a message to inform you that the action will override the custom PMC setting for that specific attribute.

Note When you customize the values for attributes a superscript (1) displays next to the value in the appropriate attribute column in the Associations tab, for both the user and the channel. The superscript indicates a customized value.

For more detailed information about attribute association behaviors, refer to the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

Cisco IPICS Roles and Associated Tasks

Each Cisco IPICS user is assigned one or more roles. Roles define the features that a user can access and the functions that the user can perform.

Cisco IPICS associates specific tasks with every role. Each Cisco IPICS user is assigned a role that determines the scope of user functionality and window accessibility.

The following sections provide brief descriptions of the tasks that Cisco IPICS associates with each role:

- System Administrator Tasks, page 2-14
- Ops View Administrator Tasks, page 2-17
- Operator Tasks, page 2-17
- Dispatcher Tasks, page 2-18
- User Tasks, page 2-19

System Administrator Tasks

The Cisco IPICS system administrator performs the following tasks, as described in Table 2-1.

Table 2-1 System Administrator Tasks

Task	Description and Reference
Install Cisco IPICS	Before you can perform any system administrator tasks, you must first install and configure the Cisco IPICS server. To install and configure Cisco IPICS, refer to the *Cisco IPICS Server Installation and Upgrade Guide, Release 2.1(1)*.
Configure the Cisco IPICS server	
Configure and manage the RMS component	You perform RMS management in the RMS window. Access this window from the Configuration drawer in the Administration Console. See the "Managing the RMS" section on page 3-1 for more information about the RMS. For more detailed information about configuring the RMS component, refer to "Configuring the RMS Component" appendix in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.
Manage locations	You add and delete locations in the Locations window. Access this window from the Configuration drawer. For more information about locations, see the "Understanding Locations" section on page 2-4. For detailed information, refer to the "Managing Locations" section in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.
Set up multicast addresses	You set up multicast IP addresses in the Multicast Pool window. Access this window from the Configuration drawer. For detailed information, refer to the "Managing the Multicast Pool" section in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

Table 2-1 System Administrator Tasks (continued)

Task	Description and Reference
Configure PTT channels, channel groups, and radios, if applicable	You perform channel and channel group management in the Channels and Channel Groups windows. You perform radio management in the Radios windows. Access these windows from the Configuration drawer. For more information about radios, see the "Managing Radios" section on page 3-3. For information about radio and tone descriptors, see the "Managing Radio and Tone Descriptors" section on page 3-5. For detailed information about channel and channel group management, refer to the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.
Manage PMC versions	You upload PMC version packages to the server and configure the PMC installer, as well as manage PMC alert tones, skins, and PMC regions from the PMC Management drawer. For more information about PMC management, see the "Managing the Cisco IPICS PMC" section on page 3-18. For more detailed information, refer to the "Managing PMC Versions" section in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.
Monitor system status	You can monitor system status, and view diagnostic and system log information, to use for troubleshooting and to monitor user activity, from the Serviceability drawer. For more information about monitoring system status, log, and diagnostic information, see the "Cisco IPICS Serviceability" section on page 4-1. For more detailed information, refer to the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.
Review log files	You view log file activities that relate to VTGs, such as operational views (ops views) for each channel, user, and VTG, the creator of log entries, and the time that log activities occurred. You can also download archived log entries for historical reporting. You can perform log activities from the Administration drawer. For more detailed information about log activities, refer to the "Managing Activity Logs" section in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

Table 2-1 System Administrator Tasks (continued)

Task	Description and Reference
Create and manage Cisco IPICS ops views	Ops views enable the use of resource sharing on one Cisco IPICS server. You perform ops view management in the Ops View window from the Configuration drawer. For more information about ops views, see the "Understanding Ops Views" section on page 2-7. For more detailed information about ops views, refer to "Configuring and Managing Cisco IPICS Operational Views" in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.
Back up and restore the Cisco IPICS database	You can back up and restore the Cisco IPICS database, as well as download the backup and restore activity log files, in the Database Management window. Access this window from the Administration drawer. For more information, see the "Cisco IPICS Database Management" section on page 4-8. For detailed information, refer to "Performing Cisco IPICS Backup and Restore Operations" in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.
Set up Cisco Unified IP Phones	You configure Cisco Unified IP Phones for phone service in conjunction with the Cisco Unified Communications Manager or for Cisco Unified Communications Manager Express. For more information, see the "Using Cisco Unified IP Phones with Cisco IPICS" section on page 3-21. For detailed information, refer to the "Setting Up and Using a Cisco Unified IP Phone as a Cisco IPICS Push-To-Talk Device" appendix in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.
Create and manage policies	You create and manage policies by using the policy engine. Policies comprise one or more actions, which are discrete functions that perform when the policy executes, such as starting a VTG and inviting designated users to join the VTG. Some policies can also include one or more triggers , which cause the policy to execute automatically and, optionally, to repeat according to a specified schedule. You perform policy engine tasks by accessing the Policy Management drawer in the Policy Engine tab. For more information, see the "Managing and Using the Cisco IPICS Policy Engine" section on page 3-8. For detailed information about the policy engine, refer to "Using the Cisco IPICS Policy Engine" in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

Table 2-1 System Administrator Tasks (continued)

Task	Description and Reference
Manage the dial engine	The Cisco IPICS dial engine enables the TUI and its associated features. You use the dial engine to manage system and custom script prompts that the TUI uses to handle incoming and outgoing calls, and configure the Cisco Unified Communications Manager or a Cisco router that is running a supported version of Cisco IOS as the SIP provider for use with the policy engine. You perform dial engine tasks by accessing the Dial Engine drawer in the Policy Engine tab. For more information about the dial engine, see the "Managing and Using the Cisco IPICS Policy Engine" section on page 3-8. For detailed information, refer to "Configuring and Managing the Cisco IPICS Policy Engine" in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Ops View Administrator Tasks

The ops view administrator can download and monitor the Cisco IPICS activity logs for the ops view to which the user belongs. This user can also specify which activity types Cisco IPICS should log, per the ops view of the user.

You perform the tasks that relate to activity logs in the Activity Log Management and Activity Log Options windows. You can access these windows from the Administration drawer in the Administration Console.

Refer to the *Cisco IPICS Server Administration Guide, Release 2.1(1)* for more detailed information about the specific tasks that users can perform depending on their Cisco IPICS roles.

Operator Tasks

The operator performs the following tasks:

- Sets up users and user roles—The operator adds users and manages general user information, including user name, login credentials, and the default location of users. Operators can also manage the PMC attributes for users, assign channels, roles, and ops views, associate users with other users, phones, radios, and policies, and perform activities that relate to managing user spoken name prompts.

- Sets up user groups—User groups are logical groupings of users. In addition to creating and deleting user groups, operators can add members to a user group, manage ops views for a user group, and view information about VTGs in which a user group is a participant.

Operators can perform operator activities by navigating to the **User Management > Users** and **User Management > User Groups** windows. Users who are assigned the operator role can also access the dial engine windows.

For detailed information about the Cisco IPICS operator tasks, refer to "Performing Cisco IPICS Operator Tasks" in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Dispatcher Tasks

The dispatcher performs the following tasks:

- Sets up and activates VTGs—The dispatcher creates VTGs and activates them to begin conferences, add participants to inactive and active VTGs, monitor active VTGs, notify participants about active VTGs, and mute and unmute PMC users. VTG management tasks are performed in the VTG Management > Virtual Talk Groups window in the Administration Console. See the "Understanding VTGs" section on page 2-6 for more information about VTGs.
- Manages policies—The dispatcher can view policies of users who belong to the same ops view as the dispatcher. Policy management can be performed by accessing the Policy Management windows in the Policy Engine tab. See the "Managing and Using the Cisco IPICS Policy Engine" section on page 3-8 for more information about policies. For more detailed information, refer to "Performing Cisco IPICS Dispatcher Tasks" in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

User Tasks

A user can perform the following tasks:

- Manage User Profile—Each Cisco IPICS user is assigned the user role. Users can manage personal information by using the My Profile window in Cisco IPICS. The user profile includes information such as user name, password, default location, communication preferences, and other personal information.
- View Associations—Users view the channels, users, phones, VTGs, and policies with which they are associated in the My Associations window.
- Download the PMC—Users download the PMC installer to their client machines and install the most current version of the PMC, as configured in the server, in the Download PMC window.

Users can access the user windows from the Home drawer in the Administration Console. For more information about user tasks, refer to "Performing Cisco IPICS User Tasks" in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

CHAPTER 3

Using the Cisco IPICS System

This chapter provides tips and guidelines for using the Cisco IPICS system and includes the following sections:

Managing the RMS

The RMS enables the Cisco IPICS PMC to remotely attach to a VTG and provides support for remotely combining two or more VTGs through its loopback functionality.

To manage the RMS on Cisco IPICS, you must first configure the RMS for use with the Cisco IPICS server. The Cisco IPICS server accesses the RMS by using Secure Shell Client software and it authenticates the RMS by using the credentials that you configure in the RMS in the Configuration > RMS window in the Administration Console.

Note You must configure the RMS components exactly as described in "Appendix A: Configuring the Cisco IPICS RMS Component" in the *Cisco IPICS Server Administration Guide, Release 2.1(1)* for the Cisco IPICS system to work correctly.

You must configure at least one RMS per Cisco IPICS server. You cannot configure the same RMS in multiple Cisco IPICS servers.

You may implement more stringent security measures and harden your system security by configuring additional security features that Cisco IOS provides. For more information about configuring authentication, password security, and additional layers of security, refer to the *Cisco IOS Security Guide* at the following URL:

http://www.cisco.com/en/US/products/ps6441/products_configuration_guide_book09186a008049e249.html

You must configure at least one T1 or E1 loopback in the RMS to support mixing. The configuration steps that are required to implement the loopback pairs may vary depending on card type, Cisco IOS version, and the type of supported RMS that you use.

Note For a complete list of supported interface cards and RMS routers, refer to the *Cisco IPICS Compatibility Matrix* at the following URL: http://www.cisco.com/en/US/products/ps7026/tsd_products_support_series_home.html

Before adding an RMS, make sure that you meet the following conditions:

- The router must exist on the Cisco IPICS network
- You must define at least one location

For detailed information about how to configure an RMS and locations, refer to the "Managing the RMS" section and the "Configuring the Cisco IPICS RMS Component" appendix in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

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 by pressing the **Activate** or **Deactivate** button.

You can merge, update, and show RMS configuration information by using the Configuration drop-down list box in the RMS window in the Administration Console.

Note By default, Cisco IPICS polls the RMS every ten minutes by using the RMS comparator mechanism. The RMS comparator checks the responsiveness of the RMS. If there have been any changes made to the configuration, and these changes are not reflected in the Cisco IPICS server, the RMS comparator automatically updates the configuration so that the two components are synchronized. You can change the polling period by entering a new value in the **RMS Polling Frequency** field in the Options window in the Administration drawer. This setting specifies how often the Cisco IPICS polling mechanism checks whether the server can reach all RMS components that are listed in the RMS window.

Tip Because the RMS comparator mechanism can interject delays, you can disable it by navigating to **Administration > Options** and checking the **Disable RMS Comparator** check box. You should check this check box if you connect via a high latency, low bandwidth connection, such as a satellite link.

For more detailed information about managing the RMS, refer to "Managing the RMS" in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Managing Radios

This release of Cisco IPICS provides support to define radio channels in the Cisco IPICS server and implements a radio console skin for the PMC that enables the PMC to send RFC 2198 and RFC 2833 packets to control tone sequences on a per-channel basis. At the LMR gateway, the packets gets converted into audible tones via the configured ear and mouth (E&M) interface to the physical radio to provide tone control for radios.

You perform radio management in the Configuration > Radios window.

Tone control (also referred to as *Tone Remote Control* (TRC)) refers to the use of inband tone sequences to control a radio that is connected to an LMR gateway (typically a base station). In Cisco IPICS, you can use tone control to modify or

tune to a different radio frequency (RF) channel, change the transmit power level, and to enable or disable radio built-in encryption, as well as other uses. TRC uses well-defined audio sounds (also referred to as *tones*) to change the behavior of a device. A tone-keyed radio system requires that a specific tone be present on the incoming analog (e-lead) port. If this tone is not present, the radio does not transmit audio.

The PMC includes a radio console skin that provides support for channel selector buttons. The PMC can display up to nine channel selector buttons that PMC users can use for signaling, changing channels, or controlling tone sequences. The PMC generates the necessary radio control tone sequences when users press the associated button.

For more detailed information about channel selectors, refer to "Manging Radios" in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Note For information about various Requests for Comment (RFCs), access the RFC repository that is maintained by the Internet Engineering Task Force (IETF) at the following URL: http://www.ietf.org/rfc.html.

Tip When you configure channel selectors, you should consider the different actions that users may want to perform on the channel and what commands need to be sent to the radio when those actions are being performed.

Tone control sequences, which are defined in either a tone descriptor file or in the radio descriptor file, contain information about how to tune the radio to another frequency within that radio. For more information about tone and radio descriptor files, see the "Managing Radio and Tone Descriptors" section on page 3-5.

A tone control can be either a stateful operation or a momentary operation. If a control is stateful, the PMC displays the button.

For example, Encryption is a stateful operation and the PMC monitors its setting. Another example of a stateful operation is a Transmit Power setting that can be toggled between High, Medium, and Low.

A momentary control is one in which the functional state is not monitored or remembered. Most signals are momentary, meaning that they are sent without being monitored by the system.

For information about tone and radio descriptors, see the "Managing Radio and Tone Descriptors" section on page 3-5. For detailed information, refer to "Managing Radio and Tone Descriptors" in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Managing Radio and Tone Descriptors

Cisco IPICS allows you to create and/or update radio and tone descriptor files. Radio and tone descriptors are .xml files that define the capabilities for specific radio types, and over-the-air signals that can be associated to one or more Cisco IPICS channels.

You can add and update radio and tone descriptors in the Administration Console by navigating to **Configuration > Descriptors.**

This section contains the following topics:

Radio Descriptors

Radio descriptors are .xml files that contain commands that are used to control functions on a radio. These files contain the following elements:

- Channel selectors—Used to change the frequency on a radio
- Control functions—Stateful controls, such as power settings and encryption on/off, and simple (momentary) controls, such as monitor and scan

For each radio capability, the radio descriptor defines the tones (events) that need to be sent to the radio to enable/disable that capability.

Note For channel selectors and control functions, Cisco IPICS supports only RFC 2833 tones. Refer to "Managing Radios" in the *Cisco IPICS Server Administration Guide, Release 2.1(1)* for more detailed information.

The tone control sequences, that define the control functions, can be included directly in the radio descriptor or can be referenced by name in a tone descriptor file. For more information about tone descriptors, see the "Tone Descriptors" section on page 3-6.

You can add and/or update radio descriptors in Cisco IPICS in the Descriptors window by navigating to the **Configuration > Descriptors** window in the Administration Console.

Note If you must modify or create radio descriptors, refer to the documentation that came with your radio, or other device that is being controlled, for the specific tone sequences that it supports.

Caution Because improperly constructing an .xml file, removing a radio descriptor file, or removing elements from a radio descriptor file may have unpredictable results, Cisco recommends that you only modify the radio descriptor file when absolutely necessary.

For detailed information about adding or updating descriptor files, refer to "Managing Radio and Tone Descriptors" in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*. To see examples of valid and invalid descriptor file .xml entries, refer to the *Cisco IPICS Radio and Tone Descriptor File Examples Reference Card, Release 2.1(1).*

Tone Descriptors

A tone descriptor is an .xml file that defines a sequence of momentary controls and over-the-air signals that can be associated to one or more Cisco IPICS channels. Commands can be referenced by any radio descriptor and signals can be associated to any channel.

The maximum number of consecutive control and signaling tones is six.

Note Simple control functions can reference only RFC 2833 tone events. However, momentary signals can reference both RFC 2833 tone and RFC 2833 event (DTMF) commands. For more information, refer to "Managing Radio and Tone Descriptors" in the *Cisco IPICS Server Administration Guide, Release 2.1(1).* For some examples of valid and invalid descriptor file entries, refer to the *Cisco IPICS Radio and Tone Descriptor File Examples Reference Card, Release 2.1(1).*

Unlike momentary controls, signals do not cause the radio to change configuration; rather, signals are treated like voice and are transmitted over the currently-tuned radio channel frequency.

Each tone in a sequence is specified by the frequency (from zero to 3999 Hz), a decibel (db) level (0 to -63), and a duration in milliseconds (ms).

Note An RFC 2833 tone or event has a maximum duration of eight seconds. Refer to the *Cisco IPICS Server Administration Guide, Release 2.1(1)* for more information.

You can add and/or update tone descriptors in Cisco IPICS in the Descriptors window by navigating to the **Configuration > Descriptors** window in the Administration Console.

Note If you must modify or create tone descriptor files, refer to the documentation that came with your radio, for the specific control and signaling sequences that it supports.

Caution Improperly constructing a .xml file, removing a tone descriptor file, or removing elements from a tone descriptor file, that is reference by a radio descriptor file, may have unpredictable results. Cisco recommends that you only modify the tone descriptor file when absolutely necessary.

For detailed information about descriptor management in Cisco IPICS, refer to "Managing Radio and Tone Descriptors" in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Managing and Using the Cisco IPICS Policy Engine

The Cisco IPICS policy engine lets you create and manage policies. Policies are comprised of one or more actions that perform when the policy executes. The policy engine includes the dial engine. Using the dial engine, you can manage standard and custom scripts and prompts that enable telephony user interface (TUI) interaction and incoming and outgoing calls.

Note Only the system administrator, dispatcher, or operator can administer the Cisco IPICS dial engine functionality. A system administrator can perform any activity in the Dial Engine drawer. A dispatcher or operator can perform only those activities that relate to managing spoken name prompts for the users who belong to the same ops view as the dispatcher.

To perform policy engine and dial engine functions, navigate to the Policy Engine tab and choose either the **Policy Management** drawer or the **Dial Engine** drawer.

Note To enable the policy engine, you must install a Cisco IPICS license that includes the policy engine feature.

This section contains the following topics:

Dial Engine Considerations

As part of the dial engine functionality, Cisco IPICS provides default configuration settings for tracing. These settings are designed for optimal system performance but you can change them if needed. Tracing consumes system resources; therefore, if you require additional trace information for the dial engine, follow these guidelines to conserve system resources:

- Increase the number or the size of trace files only if necessary.

- Keep the number and the size of trace files to the minimum values that provide the information that you need.
- Enable only the trace settings that you need or that you are instructed to enable by the Cisco TAC.
- If you enable trace settings, disable them when you no longer need them.

  The system begins to log information in a new trace file each time that the current file reaches the designated maximum file size. When the number of trace files that are stored on the system reaches a designated value, each subsequent trace file overwrites the oldest existing trace file.

Note The total size of all dial engine trace files that are stored on the system cannot exceed 3 GB.

- When you delete a language, in the Dial Engine > Prompt Management > Languages window, the logical folder for that language and all contents of the folder are removed from the repository. You can delete a single language or several languages at one time.

Note If you delete a language while the policy engine is executing a dial engine script that uses that language, script execution may not be successful because the script may not be able to access a prompt that it requires.

- To display the Standard Script Prompts window, navigate to **Dial Engine > Prompt Management > Standard Script Prompts**. By default, the Standard Script Prompts window lists all standard script prompts. To see a list of only standard script prompts that are stored in a particular logical language folder, choose that language from the Language drop-down list and then click **Query**.
- When you delete a standard script prompt or a customized script prompt, it is removed from the repository. You can delete a single prompt or several prompts at one time.

Note Before you delete a prompt, make sure that it is not used by a script. The system does not warn you if the prompt is being used by a script.

- The dial engine includes the following system scripts, which cannot be modified or deleted. You can add additional scripts.
  - BulkNotifyDialer—Used to notify recipients when Cisco IPICS receives an external notification request
  - IppeDialin—TUI main menu
  - IppeDialout—Used to place outbound calls
  - IppeRecording—Used to record spoken names
- The policy engine functionality requires that a SIP provider be configured in your network. A SIP provider handles calls to and from the policy engine.

Note You must use Cisco Unified Communications Manager or a Cisco router that is running a supported version of Cisco IOS as the SIP provider. You configure Cisco Unified Communications Manager for the policy engine in Cisco Unified Communications Manager Administration. Refer to "Configuring and Managing the Cisco IPICS Policy Engine" in the *Cisco IPICS Server Administration Guide, Release 2.1(1)* for detailed information about configuring Cisco Unified Communications Manager as the SIP provider.

- You perform the SIP configuration in the Dial Engine > SIP Configuration window.

  Table 3-1 shows the panes and fields in the SIP Configuration window, and the appropriate actions that you can take to enter required information.

Table 3-1 Fields in the SIP Configuration Window

Pane	Field and Action
SIP Subsystems Configuration	• Port—Enter the SIP port that the policy engine uses. • User Agent—Enter the user agent that the policy engine uses. • Maximum Retransmissions—Enter the maximum number of times that SIP requests and responses are transmitted. • First Retransmission (in msec)—Enter the number of milliseconds to wait before performing the first retransmission. **Note** The default maximum transmissions and first retransmission values are appropriate in most cases. You should not change these values unless you fully understand the characteristics of the network on which Cisco IPICS and the SIP provider are deployed and understand the SIP retransmission algorithms that are described in the RFC 3261 specification.
SIP Provider Configuration	• Host—Enter the IP address or the host name of the SIP provider. • Port—Enter the port number that the SIP provider uses for SIP. • Transport drop-down list—Choose the transport protocol (TCP or UDP) that matches the transport protocol of the SIP provider. **Note** If both protocols are configured on the SIP provider, choose either protocol. • Username—Enter the appropriate information. – If Cisco Unified Communications Manager is the SIP provider, enter the Cisco Unified Communications Manager user name for the SIP trunk. – If a Cisco router that is running a supported version of Cisco IOS is the SIP provider, enter any value in this field. • Password—Enter the appropriate information. – If Cisco Unified Communications Manager is the SIP provider, enter the Cisco Unified Communications Manager password for the SIP trunk. – If a Cisco router that is running a supported version of Cisco IOS is the SIP provider, enter any value in this field.

Table 3-1 Fields in the SIP Configuration Window (continued)

Pane	Field and Action
Cisco Unified Communications Manager Configuration for IP Phone Notifications	**Note** The fields in this pane are optional and are required only to execute policies that use the IP Phone Text Notification action, or that use the dial notification action to send a message to a Cisco Unified IP Phone. • Host Name or IP Address—Enter the host name or the IP address of the Cisco Unified Communications Manager server. • Administrator User Name—Enter the name of the Application User in Cisco Unified Communications Manager who has administrator privileges. • Administrator Password—Enter the password of the Application User in Cisco Unified Communications Manager who has administrator privileges. • End User Name—Enter the name of the end user in Cisco Unified Communications Manager to which Cisco Unified IP Phones are associated. • End User Password—Enter the password of the end user in Cisco Unified Communications Manager to which Cisco Unified IP Phones are associated. **Note** For information about Cisco Unified Communications Manager Application Users and end users, refer to your Cisco Unified Communications Manager documentation. The changes take effect only after you restart the dial engine. To restart the dial engine, follow these steps: 1. Log in to the Cisco IPICS server as the root user. 2. Enter the following command at the command prompt: [root]# **service ipics restart**

Policy Considerations

A policy defines a set of actions that the system executes according to instructions that you provide in the policy. A policy can be either of these types:

- Invitation—Policy activated only through the TUI that causes the TUI to call designated users and invite them to join a VTG or channel. You can invoke an invitation policy from the TUI breakout menu after you have joined a VTG or a channel. Users that the TUI calls are invited to join that VTG.

Note This policy type is activated only through the TUI.

- Multi-Purpose—Policy that includes any one of the following action types:
  - Activate VTG—Activates the designated, preconfigured VTGs.
  - Notification—Contacts designated recipients according to notification instructions that you specify. Notification action types include e-mail, IP Phone Text, Dial, Talk Group, and Dial Engine Script.

    For information about using notification for recipients outside of the Cisco IPICS system, see the "Using External Notifications in Cisco IPICS" section on page 3-14.
  - VTG Add Participants—Adds the designated participants to the designated VTG.
  - Dial Out—Calls the designated users according to their configured dial preferences to invite them to join the designated VTG.

Note A Multi-Purpose type policy can be activated by a trigger, by reactivating it in the Policy Management > Execution Status window, or through the TUI. An Invitation Type policy can be activated only through the TUI.

Tip When you create a policy, make sure that your system has sufficient resources (multicast addresses and dial ports) to accommodate the associated VTGs when they execute. Cisco IPICS does not warn you that the execution of a policy may over-commit system resources when it activates VTGs.

Using External Notifications in Cisco IPICS

You can also use Cisco IPICS to send notifications to recipients who are not configured in Cisco IPICS. This type of notification is called an *external notification* and performs the following functionality:

1. Simultaneously calls many external users at telephone numbers that Cisco IPICS obtains from a file that you specify.
2. Plays a designated message to each user who answers the call.
3. Captures results of each call in a log file that you can review at any time.

You invoke an external notification by sending an HTTP request or by posting a Common Alerting Protocol (CAP) .xml file to the appropriate server.

For more detailed information about external notifications, refer to "Using Cisco IPICS for External Notifications" in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Guidelines for Using the TUI

When you use the TUI, be aware of the guidelines that are listed in the following sections:

- General Guidelines, page 3-14
- Menu Guidelines, page 3-16

General Guidelines

The following general guidelines apply when you use the TUI:

- After you dial in to the TUI, the system prompts you to enter your user ID and PIN (password). You must authenticate before you can continue to use the system.
- When you call the system, the language in which you hear prompts is the default language that is configured for the ops view with which you are associated.
- The system spells out your user name if you do not have a recorded spoken name.

- After you authenticate, the system announces the available menu options, such as joining a channel or VTG, invoking a policy, or accessing the system menu.
- The TUI allows you to interrupt a prompt and dial ahead by entering your next option before the prompt has finished.
- A menu times out if you do not respond within the predefined allowable period of time. In most instances, this period of time is 3 seconds and includes a maximum retry limit of 3. When the allowable period of time has expired, the TUI responds with “Are you still there?” and the menu repeats. When the maximum retry limit has been exceeded, the TUI responds with a warning prompt to inform you that the call will be disconnected and then it terminates the call.
- If the system does not detect a response to the prompts after a predefined number of consecutive attempts, the system returns you to the previous menu or terminates the call, if you are using the main menu.
- When you enter an incorrect key option, the TUI responds with “Please try again” and the menu repeats.
- When you dial out to invite a party in to a call, the called user must press any key to authenticate before the call is connected to the channel or VTG. (As the call is being dialed out, the system does not play any audible sounds.)
- To terminate your input, press #.
- To return to the previous menu, except when you are using the main menu, press *.
- To select resources, such as groups or policies, from a menu, press the number that corresponds to your selection when the number of entries is 9 or less. When 10 or more entries exist, you must press the number that corresponds to your selection followed by #.
- The option to select a resource by spelling its name depends on your locale:
  - The TUI supports the following locales: Afrikaans (af), Albanian (sq), Basque (eu), Catalan (ca), Danish (da), Dutch (nl), English (en), Faroese (fo), Finnish (fi), French (fr), German (de), Icelandic (is), Irish (ga), Italian (it), Norwegian (no), Portuguese (pt), Rhaeto-Romanic (rm), Scottish (gd), Spanish (es), Swedish (sv)

  - If you use a locale that does not support dial by name, such as locales that do not have equivalent characters available on the phone keypad to enable dial by name, you must make your selection from the list of available resources.

Menu Guidelines

The following guidelines apply when you use the TUI menus:

- Transfer and conference features are not supported on a phone when the phone is connected to the TUI.
- From the TUI main menu, you can take the following actions:
  - To join a group, press 1. Then, you can press 1 to select an assigned group to join by spelling out the group name, or press 2 to listen to the list of assigned groups and then selecting from that list. (If you know the name of the group that you want to join, it is quicker to enter the name than to wait for the TUI to announce the list of available groups.) To confirm your selection, press 1. To cancel your section, press 2. To return to the previous menu, press *.
  - To invoke a general purpose policy, press 2. Then, you can press 1 to select a policy by spelling its name, or press 2 to listen to the list of available policies. (If you know the name of the policy that you want to join, it is quicker to enter the name than to wait for the TUI to announce the list of available policies.) To confirm your selection, press 1. To cancel your section, press 2. To return to the previous menu, press *.
  - To invoke the system menu, press 0. From this menu, you can take the following actions:

    - To access system help, press 1. This option provides an overview of the system menu.

    - To manage your user profile, press 2. To change your PIN, or password, press 1. To change your recorded name, press 2.

    - To obtain policy status, press 3. To replay the information, press 1.

    - To return to the previous menu from these menus, press *.
- The TUI provides a dial-in floor control feature to support dial-in users:
  - From the TUI call menu, you can take the following actions:

- To request the floor, press 1. You hear a single beep if you obtain the floor. You hear a busy tone if the floor is not available to you.

- To release the floor, press 2. You hear a double-beep to confirm that the floor is released.

  - The dial-in floor allows one dial-in user at a time to speak in a group. It does not control whether other PTT users can speak.
  - When you have the dial-in floor, you can speak and be heard by other users in a group, but you cannot hear other users talking.
  - When you have the dial-in floor, the TUI prompts every two minutes to confirm that you want to keep the floor. Press 1 to keep the floor or press 2 to release the floor.

- From the TUI breakout menu, you can take the following actions:
  - To access system help, press 1. This option provides an overview of the system menu.
  - To invite a dial user to join the call by using an ad-hoc invitation or by using an invitation policy, press 2.

    - To perform an ad-hoc invitation, press 1. To confirm your selection, press 1 (no audible sounds play during the time that it takes for the remote party to pick up and authenticate). To try your call again, press 2. To cancel, press *.

    - To perform an invitation policy, press 2. To choose an invitation policy by spelling out the name, press 1. To listen to the list of invitation policies, press 2 and then select from that list. To confirm your selection, press 1. To cancel, press 2. To return to the previous menu, press *.
  - To invoke a general purpose policy, press 3. To choose an invitation policy by spelling out the name, press 1. To listen to the list of invitation policies, press 2 and then select from that list. To confirm your selection, press 1. To cancel, press 2. To return to the previous menu, press *.
  - To leave the call and return to the main menu, press 0.
  - To return to the call, press *.

Managing the Cisco IPICS PMC

You can manage PMC functions that include configuring the PMC installer, and uploading PMC version packages, alert tone sets, and PMC skin sets, and configuring PMC regions in the Administration > PMC Management window.

This section contains the following topics:

Managing the PMC Installer

The PMC installer installs new PMC version packages and makes them available to PMC users. When you configure the PMC installer, you can choose the IP address or host name of the server, or you can configure a different IP address or host name that you want the PMC users to use.

Note If you choose another IP address or host name instead of the configured IP address or host name, make sure that you test the IP address in the network domain that will be supported with that server.

Cisco recommends that you use the default HTTP and HTTPS ports that are listed in the PMC installer configuration area. The IP address, HTTP port, and HTTPS port fields affect only the PMC installer and do not have an immediate effect on PMC clients that have already been installed on user PMC client machines.

Note To change the HTTP and HTTPS values, Cisco recommends that you inform all PMC users to connect to the server to download and reinstall an updated version of the PMC.

Managing PMC Versions

The Cisco IPICS server maintains a repository of one or more versions of the PMC. PMC updates can be assembled into upgrade packages that add features and resolve issues. Users can then upgrade their PMC clients at any time by downloading the current version of the PMC executable file.

Note You must configure the PMC installer and upload the PMC upgrade package before users can download and install the PMC on their PMC client machines.

By default, all new PMC versions are saved to a non-operational state after you upload a new PMC version package. The PMC becomes available to users only after you change the state to one of the following states:

- Recommended—This version represents the recommended software version that should run on the PMC. The server notifies the PMC of this recommended version and displays a message to inform the PMC user. The server then sends this version to the PMC and the PMC installs it after the PMC user responds positively to the message prompt or if other installed versions are not supported.
- Staged—This version represents the software version that the PMC downloads according to your discretion. The server sends this version to the PMC for download but the PMC does not download it until you change the state of this version to recommended or operational. At that time, the PMC may install the new version after the PMC user responds positively to the message prompt or if other installed versions are not supported.
- Operational—This version represents a version of PMC software that is operational. This version is supported for use with the server but there may be a later version that is also supported.

Note The server always extends priority to the PMC versions that it marks as recommended.

To force updates immediately, choose the **Not Supported** state from the drop-down list box. This state forces PMC users, who are running this version of the PMC, to restart and download a newer version.

Caution Forcing a PMC automatic update shuts down and then restarts a PMC without warning a user, regardless of the purpose for which the PMC is being used. For this reason, Cisco recommends that you force an update only when it is absolutely necessary.

Managing PMC Alert Tones and Skins

You create PMC alert tone sets and then upload tone sets and skin sets to the server. PMC users can then download the tone and skin sets to their PMC client machines. Alert tone sets and skin sets are associated with ops views, so each PMC user can see only one tone and skin set based on the ops view to which that user belongs.

Note The PMC alert tone feature requires the use of compatible alerting tone files. These files must be .wav files that are encoded in Pulse Code modulation (PCM), which is a sampling technique that digitizes analog signals. These .wav files must be encoded in PCM format with 8 bits monaural samples at 8000 Hz sampling rate for a total of 64 kbps. While higher and lower rates may seem to work, Cisco IPICS does not support the use of any other encoding or bit rates, as they may produce inferior sound quality. Any file that is used with the G.729 codec may sound inferior due to its encoding algorithms. In addition, all alerting tones should be encoded to a nominal value of -20 decibels relative to one milliwatt (dBm) and begin and end with zero deflection to eliminate or minimize “popping” or clicking sounds. For more detailed information, refer to the *Cisco IPICS PMC Installation and User Guide, Release 2.1(1).*

For more information about how to manage PMC alert tones and skins, refer to “Managing PMC Alert Tones” and “Managing PMC Skins” in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Managing PMC Regions

You can configure regions (views) that the PMC displays to the user. A PMC region is a grouping of channels on the PMC. Channels (including radio channels) are divided among regions. Channels, radios, and VTGs are configured to belong to a particular region when they are created.

Note PMC regions display only when you use the 36-channel radio console skin.

When you configure new regions in the Cisco IPICS server, they are represented by tabs that display along the right side of the PMC display. The position of the region determines where the region displays on the PMC.

You can add new PMC regions, view and edit existing regions, and delete regions in the PMC Management > PMC Regions window.

For more information about how to manage PMC regions, refer to "Managing PMC Regions" in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Using Cisco Unified IP Phones with Cisco IPICS

The Cisco IPICS service allows several Cisco Unified IP Phone models to communicate and participate in PTT channels and VTGs. Before a user can access the Cisco IPICS service, Cisco IPICS must be configured as a phone service for Cisco Unified Communications Manager or for Cisco Unified Communications Manager Express. In addition, users in a deployment that includes Cisco Unified Communications Manager must subscribe to the Cisco IPICS service by using the Cisco Unified Communications Manager User Options application.

For detailed information about configuring Cisco Unified IP Phones for use with Cisco IPICS, refer to the "Setting Up and Using a Cisco Unified IP Phone as a Cisco IPICS Push-to-Talk Device" appendix in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

After you configure Cisco IPICS as an available service, and IP phone users have subscribed to the service, the Cisco Unified IP Phone Services menu displays Cisco IPICS as an option.

For additional information about Cisco Unified Communications Manager Administration and about setting up phone services, refer to the Cisco Unified IP Phone Services configuration information in the Cisco Unified Communications Manager Administration Guide for your version of Cisco Unified Communications Manager. You can locate the Cisco Unified Communications Manager documentation at the following URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

Users should be aware of the following guidelines when using Cisco Unified IP Phones with Cisco IPICS:

- To obtain help with using the Cisco IPICS service on a Cisco Unified IP Phone, press the **Help** softkey.
- A phone that is logged in to the Cisco IPICS service logs out automatically after 30 minutes of inactivity. You can configure a different timeout period in the Administration > Options window.
- You can configure whether the Cisco IPICS service requires users to log in before accessing the service from a Cisco Unified IP Phone. If there are users who you do not want to require to log on, you can configure a separate service in Cisco Unified Communications Manager that bypasses the login for each of these users.

  When you configure the Cisco IPICS service so that it does not prompt for user login credentials on the Cisco Unified IP Phone, the service automatically activates a channel or VTG if only one channel or VTG is assigned.

  If you configure the Cisco IPICS service to bypass the user login and if there are more than one channel or VTG that is assigned, Cisco IPICS displays the list of these channels and VTGs on the IP phone.

  For detailed information, refer to the "Setting Up and Using a Cisco Unified IP Phone as a Cisco IPICS Push-To-Talk Device" appendix in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*
- On some model IP phones, you can add a special parameter to the Cisco IPICS Service URL configuration to enable the display of the Logout softkey on the main display while IP phone users are connected to a channel or VTG. For more information, refer to the "Setting Up and Using a Cisco Unified IP Phone as a Cisco IPICS Push-To-Talk Device" appendix in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

- If a phone loses connectivity to the Cisco IPICS server while the phone user is logged in to the Cisco IPICS service, the service retains its current state and the user can continue to use the PTT functionality for the channel or VTG that is currently selected. However, the phone cannot connect to other channels or VTGs until connectivity to the server is re-established.
- A Cisco IPICS user can be logged in to the Cisco IPICS service with the same login credentials on more than one phone simultaneously. In this case, the following information applies:
  - The user can send and receive audio on all of the phones
  - If the user presses a key on any phone that causes the phone to interact with the server (for example, the **Back**, **Latch**, or **Help** softkey), all phones log out except the last one that was logged into.
- When the Cisco Unified Wireless IP Phone 7921 is connected to an active Cisco IPICS channel or VTG, the phone goes into continuous listening mode. In this mode, the phone remains in an active receive state even if Cisco IPICS is not transmitting audio. In this state, the phone continues to draw power from the battery, which limits the battery life to approximately eight hours of talk time. (When the channel or VTG is deactivated, the phone enters standby mode to conserve power.) To ensure that you have an adequate power supply for your Cisco Unified Wireless IP Phone 7921, Cisco recommends that you maintain a backup battery for use with your phone. For more information about the Cisco Unified Wireless IP Phone 7921, refer to the Cisco Unified IP Phone documentation that is available at the following URL:

  http://www.cisco.com/en/US/products/hw/phones/ps379/tsd_products_support_series_home.html

  For information about how to customize the softkeys on the Cisco Unified Wireless IP Phone 7920/7921 to enable direct access to the Services menu, refer to the following URL:

  http://www.cisco.com/en/US/products/hw/phones/ps379/tsd_products_support_series_home.html

Maintaining User Passwords

Cisco IPICS provides password security features that enforce password complexity (strong passwords) that must adhere to certain rules for user password creation. Cisco IPICS checks for user password length and character requirements, keeps track of password expiration settings, maintains historic passwords in the database, and locks out user accounts after a maximum number of invalid login attempts.

As a system administrator, you can manage user password settings in the Administration > Options > Passwords tab, in the Administration Console.

You can specify the following password settings in the Options window:

- Minimum password length—Specifies the minimum number of characters that a user can enter (to ensure a strong login password, configure the minimum password length to contain at least 8 characters total)
- Minimum digit password length—Specifies the minimum number of numeric characters that a user can enter when creating or changing the digit password (or PIN) in the My Profile window
- Minimum lower case letter count—Specifies the minimum number of lower case letters that a user can enter when creating or changing the login password (the total number cannot exceed the number that is set for the minimum password length)
- Minimum upper case letter count—Specifies the minimum number of upper case letters that a user can enter when creating or changing the login password (the total number cannot exceed the number that is specified for the minimum password length)
- Minimum numeric character count—Specifies the minimum numeric characters that a user can enter when creating or changing the login password (the total number cannot exceed the number that is specified for the minimum digit password)
- Minimum special character count—Specifies the minimum special characters that a user can enter when creating or changing the login password (check that the password contains at least one of the following characters: lower case letter, upper case letter, number, and special characters such as pronunciation mark, exclamation point, asterisk, etc.)
- Password history count—Specifies the number of passwords of which Cisco IPICS keeps track and that the user will not be able to use again.

- Password expiration notification—Specifies the number of days, prior to a password expiring, in which the user will be notified with a warning (if you set the number to 0, then the current password will expire on the actual password expiration date and the user will be forced to create a new password at the next Cisco IPICS login)
- Password expiration—Specifies the number of days in which the Cisco IPICS login password will expire (if you set the value to 0, then the password will never expire)

  At each login, Cisco IPICS checks if the user password is about to expire in the number of days that are configured in the password expiration field. If the date has passed, the user gets notified that the password is about to expire.

Note The notification that the user receives does not apply to digit password.

When the digit password expires, the user receives a warning message when logging in to the server. The user can either dismiss the warning or change the digit password. The message lasts only for the duration of the session.

After the user password expires, the user may still log in by using the old password but is restricted to accessing only the user profile window. Cisco IPICS forces the user to change the password before being able to access other windows.

Note After password expiration, PMC and IP phone clients receive an error message prompting the user to change the password when logging in to the server. Users must change their password before they can resume using the Cisco IPICS service.

- Apply password expiration check box—You can apply the password rules, for both the user and digit passwords, by checking this check box. If you leave the check box unchecked, no password expiration rules apply.
- Maximum invalid login attempts allowed—Specifies the maximum consecutive number of times that a user can attempt to log in to Cisco IPICS with invalid login information (user name/password) before the user account gets locked out.

  A user whose account is locked cannot log in to the Cisco IPICS system. Existing logins continue to work until the user logs out of the system.

When users get locked out of Cisco IPICS, either the system administrator or the operator can unlock the user account from the User Management > Users window.

The invalid login attempt counter resets to 0 after the configured number of expiration hours has been exceeded.

- Failed password attempt expiration—Specifies the number of hours in which Cisco IPICS resets the number of invalid login attempts back to 0 (if you set this value to 3 hours, for example, the value is set back to 0 three hours after a failed login attempt)
- Apply user account lockout check box—You can apply the account lockout rules by checking this check box. If you leave the check box unchecked, no account lockout applies.

CHAPTER 4

Maintaining the Cisco IPICS System

Cisco IPICS provides a centralized location for diagnostic and status information, in the Serviceability drawer in the Administration Console. System administrators can use this information for troubleshooting Cisco IPICS issues. The Serviceability drawer allows access to windows that contain system status, diagnostics, and system log information for Cisco IPICS.

This section includes information about using the windows in the Serviceability drawer in the "Cisco IPICS Serviceability" section on page 4-1.

Cisco IPICS Serviceability

From the Serviceability drawer in the Administration Console, you can monitor system status in the various windows.

The following sections provide an overview of some of the system status monitoring tasks that can be performed in the Serviceability drawer:

Viewing Real-Time System Status in the Dashboard Window

Cisco IPICS provides you with current, real-time information regarding the overall status of the system. You can access this information in the Serviceability > Dashboard window. This window lists the resources that Cisco IPICS uses, and includes the following dashboards:

- System Dashboard—Displays information about the Cisco IPICS policy engine, server memory and hard disk usage, and multicast address information.
- Channel Dashboard—Displays information about the total number of channels, the number of enabled, disabled, active, and connected channels in your system, and the current status of those channels.
- Virtual Talk Group Dashboard—Displays information about the number of VTGs and inactive VTGs in your system.
- User Dashboard—Displays information about the number of users who are logged in to the Administration Console, the number of users who are logged in to Cisco IPICS by using a Cisco Unified IP Phone, and the number of users who are logged in to Cisco IPICS by using the PMC.
- License Dashboard—Displays information about the total and available number of ports that are licensed for use with Cisco IPICS.
- RMS Dashboard—Displays information about the available number of voice ports that you system is licensed to use.

Note To refresh the real-time information that displays in this window and obtain the latest data, click **Refresh** at the top of the window.

Viewing and Downloading Diagnostic Information

You can view diagnostic information for various Cisco IPICS components by navigating to the **Serviceability > Diagnostics** window. When you access this window, Cisco IPICS displays a summary of diagnostic information that includes the following elements:

- Cisco IPICS Server Hostname—Displays the host name of the Cisco IPICS server. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session:

  [root]# **hostname**

- Cisco IPICS Server Current Date and Time—Displays the current date and time of the Cisco IPICS server. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session:

  [root]# **date**

- Cisco IPICS Server OS Version—Displays the version of the Cisco IPICS operating system that is currently installed on the server. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session:

  [root]# **cat /etc/redhat-release**

- Cisco IPICS Server Software Version—Displays the current version of the Cisco IPICS server software. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session:

  [root]# **grep -i "ipics.server.version=" ${TOMCAT_HOME}/webapps/ipics_server/WEB-INF/classes/resources/common.properties**

Note Be sure to include the quotation marks when you enter this command. The grep command searches for the text string that is inside the quotation marks.

- Cisco IPICS Server Software Version upgrade history—Displays the date and time that the current version of Cisco IPICS was installed and provides a history, with release versions, of the times that the software has been installed or upgraded. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session:

  [root]# **cat /etc/ipics-release.history**

- Hardware Platform Details—Displays detailed information for the hardware platform. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session:

  [root]# **cat /etc.hwprofile**

- CPU Details—Displays detailed information for the CPU. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session:

  [root]# **cat /proc/cpuinfo**

- Cisco IPICS Server Network Interface Card Information—Displays the configuration of the Network Interface Cards (NICs), and the packets that have been transmitted and received on the NICs, that are installed on the Cisco IPICS server. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session:

  [root]# **ifconfig**

- Uploaded License File Name(s)—Displays the name of the license file(s) that have been uploaded onto the Cisco IPICS server. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session:

  [root]# **ls -l ${TOMCAT_HOME}/webapps/license/***

- Uploaded License File Contents—Displays the contents of the license files that have been uploaded onto the Cisco IPICS server. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session:

  [root]# **cat ${TOMCAT_HOME}/webapps/license/***

- Cisco IPICS Database Status—Displays the current status of the database. The database can be either online or offline. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session:

  [root]# **onstat -**

- Cisco IPICS Tomcat Web Server Status—Displays the current status of the Tomcat service. The Tomcat service functions as the Web server. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session:

  [root]# **ps -ef | grep tomcat**

Note If the Tomcat service is inactive (down), you may not be able to access the Administration Console. In specific situations, your Cisco technical support representative may direct you to manually run the **ps -ef | grep tomcat** script to gather details about the overall state of the system.

- Cisco IPICS Server Hard Disk Utilization Information—Displays usage information for the hard disks in the server. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session:

  [root]# **df -a**

- Cisco IPICS Configuration File Contents—Displays the contents of the pmc.ini file. You can also obtain this information by entering the following command in a Cisco IPICS terminal window session:

  [root]# **cat $ {TOMCAT_HOME}/webapps/ipics_server/pmcdownloads/pmc.ini**

  Cisco IPICS uses the pmc.ini file to determine how to communicate with the Cisco IPICS server. The pmc.ini file is present only if you have generated a PMC installer. If you have not yet generated the PMC installer file, Cisco IPICS displays the following message:

  Cannot find any pmc.ini files under the /opt/cisco/ipics/tomcat/current/webapps/ipics_files/store/installer folder.

  For more information about generating the PMC installer, refer to "Managing PMC Versions" in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

You have the ability to execute the diagnostic script or download diagnostic results by clicking the buttons that display under the Diagnostic Summary pane.

Note The PC from which you access the Cisco IPICS Administration Console must have an application installed, such as Win Zip, that can open, and extract files from, a tar file archive.

You must also use a text file viewer that can understand UNIX new-line characters, such as WordPad. If you use Notepad, the file does not display properly.

Viewing and Downloading the Cisco IPICS System Logs

The system logs that you view in the **Serviceability > System Logs** window contain messages of different severities, ranging from informational-level messages to messages that indicate a fatal error has occurred in Cisco IPICS.

Table 4-1 describes the types of system log entries that can display in the Recent System Log Entries pane.

Table 4-1 System Log Entry Types

Log Entry Type	Purpose
TRACE	Detailed debug information about the programmatic steps that Cisco IPICS performs to fulfill a request.
DEBUG	Debug information that is less detailed than TRACE information.
INFO	Informational messages about noteworthy events, such as the start of a scheduled policy.
WARN	Warning messages about occurrences such as incorrect user input or requests that Cisco IPICS cannot fulfill.

Table 4-1 System Log Entry Types (continued)

Log Entry Type	Purpose
ERROR	Messages that are similar to a WARN message, but with higher severity, such as in the case of insufficient licenses. ERROR messages display in red in the Recent System Log Entries pane.
FATAL	An unrecoverable error that requires your attention, such as a failed database connection or a router initialization failure. Often a FATAL error requires you to take immediate action to fix the specified error. When a FATAL error occurs, Cisco IPICS generates an error notification message and displays the message prominently in the current window of any user with system administrator or All privileges. Also, FATAL messages display in red in the Recent System Log Entries pane. If you continue to encounter FATAL errors, or if you experience unexpected system failures, contact your Cisco technical support representative for further analysis.

To visually identify the type of status message that appears in this window, Cisco IPICS displays log entries of different severities in the following text colors:

- Red—Red messages indicate that an ERROR-level error has occurred.
- Blue—Blue messages indicate that a WARNING-level error has occurred.
- Black—Black messages indicate that an INFO-level error has occurred.

You can view the total number of ERROR, WARNING, and INFO messages in the Status Summary area, which is directly below the Recent System Logs pane.

Note By default, the TRACE and DEBUG messages are not captured in the system logs. You should not activate these logging levels unless you are specifically instructed to do so by your Cisco technical support representative.

Cisco IPICS displays the most current system log information in the System Logs window and allows you to download all the system logs.

Cisco IPICS records system log information in the ipics.log file and continues to add data to it until the file reaches approximately 5.2 MB. When that file size limit has been reached, Cisco IPICS renames the file with an incremental number (starting at 1) and creates a new ipics.log file to capture the most current log data. This process continues until there are 10 system log files that range from ipics.log.1 to ipics.log.10. Cisco IPICS automatically purges the oldest file when you have accumulated 10 files.

When you download the system logs in the Serviceability > System Logs window, Cisco IPICS creates a zip file of all the ipics.log files. The system logs are located in the following directory:

/opt/cisco/ipics/tomcat/current/logs

Cisco IPICS Database Management

As a best practice, Cisco recommends that you back up your Cisco IPICS database on a regular basis and maintain your backups in a secure location. This practice ensures that you do not lose all system configuration if your Cisco IPICS server experiences a software or hardware failure.

Cisco IPICS performs regularly scheduled database backups to preserve your data. If you need to configure specific database parameters, you can do so in the Administration > Database Management window.

You can back up and restore data from a backed-up database, and then download and view the logs in the Database Management window in the Administration Console. You can also export and import the database using command line interface commands.

Note For optimum performance, Cisco recommends that you back up your database during periods of low activity or other off-peak hours. If you perform a backup during periods of high activity, the length of time that it takes to complete this operation can be significantly increased.

This section includes the following database management topics:

Backing Up the System

Cisco IPICS provides you with the following options for database backups:

- Manual backups—You can perform a manual database backup to capture the current state of the Cisco IPICS database.

Note Use the Remote Host option only if the remote host supports the Linux Secure Copy (scp) command. If you are using a remote host that does not support scp (for example, a Windows PC or server), click the **Local Directory** radio button. You must back up your data to the Cisco IPICS server, then use a secure file transfer protocol (SFTP) client software program, such as SSH Secure Shell Client software (or similar software), to copy the backup files to a remote host. Refer to "Performing Cisco IPICS Database Backup and Restore Operations" in the *Cisco IPICS Server Administration Guide, Release 2.1(1)* for detailed information about how to back up your files to a remote host that does not support scp.

- Scheduled backups—By default, Cisco IPICS backs up the database every day at a predefined time and stores the backup in a predefined location. You can define the time, frequency, and the location of the backed-up database. After you modify the default settings for a scheduled backup, you click **Save** and the new settings become the default settings, and remain in effect until you change them.

Caution Be sure to click **Save** after you make any changes. If you do not click **Save**, the server reverts to the current default settings.

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

- To ensure data integrity in the event of a system failure, Cisco recommends that you back up your files to a remote host location.
- Cisco recommends that you regularly check the database logs for status messages and/or error information that may be pertinent to recent backup and recovery activity.
  - To view the backup log, navigate to the **Administration > Database Management > Database Backup** window. Log entries display in the Backup Log pane.
  - To view and/or download the database logs, navigate to the **Administration > Database Management > Log** window.
- To help ensure the security of your data, Cisco IPICS does not support the use of different user IDs for remote backup and restore operations that you perform on the same data set. Therefore, when you restore your data, make sure that you specify the same user ID as the one that you used to back up your data. If you specify a different user ID, the restore procedure does not succeed because of file accessibility issues; in this situation, Cisco IPICS displays "permission denied" error messages in the db-maintenance.log. As a best practice, Cisco recommends that you designate a specific user ID that you can use for all of your remote backup and restore activities.

Choosing the Destination for a Backup

When you specify the options for a scheduled backup, or when you perform a manual backup, you should determine the best location to store the backup. The location for the database backup can be to the default directory of the local Cisco IPICS server, to another directory of the local server, or to a remote host.

You can choose from the following types of locations for your database backup:

- **Default**—This directory is the default location that Cisco IPICS uses. When you choose this location, the backups are stored in the **/idspri/backup** directory.

- **Local Directory**—Use this option to specify a directory for the backup. Cisco prepopulates the Local Directory field with the **idspri/backup/cron** directory. You can remove the /cron subdirectory in the field to place your files in the **/idspri/backup** directory. However, if you back up your files to a local directory in the server, that directory must be a subdirectory of the **/idspri/backup** directory. Any directory within the **/idspri/backup** directory, (for example, **/idspri/backup/mybackups**) is valid as a location for a database backup. If the directory that you specify does not exist, Cisco IPICS creates the directory for you.

Note Make sure that you enter the path within **/idspri/backup** directory in the Cisco IPICS server, and that you precede the destination path with a forward slash (/). If you do not specify a forward slash, Cisco IPICS displays a pop-up window with an error and does not perform the backup.

- **Remote Host**—Choose this option to back up your database to a remote location.

Note Use the Remote Host option only if the remote host supports the Linux Secure Copy (scp) command. If you are using a remote host that does not support scp (for example, a Windows PC or server), click the **Local Directory** radio button. You must back up your data to the Cisco IPICS server, then use a secure file transfer protocol (SFTP) client software program, such as SSH Secure Shell Client software (or similar software), to copy the backup files to a remote host. For more information, refer to "Backing Up Data to a Remote Host Without scp Support" in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

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

Cisco recommends that you use the following guidelines when choosing a destination for your Cisco IPICS database backups:

- Choose a remote host location when you back up your database. Using the remote host option ensures that you have a location for your backups that cannot be affected by any hardware or software failures that might occur with the Cisco IPICS server.
- For an extra safeguard, you can also copy or move a database backup from one remote host to another for redundancy purposes.
- Manually perform a database backup to a remote host before you uninstall, reinstall, or upgrade the Cisco IPICS server software to ensure that you have a copy of the most recent data.
- The Cisco IPICS software requires the Cisco IPICS operating system to operate. If you reinstall the Cisco IPICS operating system software on your server, the installation process formats the hard drive and removes all data from your server. To prevent the loss of all of your backups, you should back up your database to a remote location prior to installing the Cisco IPICS operating system.
  - For this backup, choose the remote host option only if the remote host supports the scp command, such as a Linux server. To back up your data to a remote host that does not support scp, such as a Windows-based PC or server, choose the local directory option.

    To back up your files to a Linux-based server, use the remote host option before you install the new Cisco IPICS operating system.

    To back up your files to a Windows-based machine, use the local directory option; then, use the SSH Secure Shell Client software, or similar software, to perform a secure copy (scp) to the Windows-based machine.

Restoring the System

You may need to restore your database if you encounter any of the following situations:

- You have to reinstall the server software, and you need to restore the database to the state that it was in before you reinstalled the software.

- Server data, such as channels, channel groups, or VTG templates, were deleted from the database mistakenly and you need to retrieve them.
- You need to copy a database from one Cisco IPICS server to another. You copy the database by performing a database backup from one server, and restoring the database from that backup to another server.

Note You can restore data from one server to another only if both servers are running the same version of Cisco IPICS software. If the software versions of the two servers differ, the database schema might not be the same. In this case, the restore operation may not succeed or you could encounter unpredictable errors when you perform tasks in the Administration Console.

Caution Be aware that a restore operation logs all users out of the Cisco IPICS database, and users cannot log in to Cisco IPICS until the restore operation completes. To minimize any disruption that the restore operation may cause to users, Cisco recommends that you perform a restore procedure during maintenance operations or other off-peak hours.

You can choose from the following options to restore your data:

- **Default**—Choose this option to restore your data from the default location, which is **/idspri/backup**. If you backed up your database in the default location, choose this option. If there is more than one database backup in the default directory (for example, if you perform regularly scheduled database backups), Cisco IPICS uses the most recent backup for the restore operation.
- **Local Directory** (requires full path)—Choose this option to restore your data from the local directory that you specify.

  When you specify a local directory or remote host for your restore operation, make sure that you specify the entire directory path and that you include the following directories in the directory path:

  - The **/idspri/backup** directory—Cisco IPICS stores every backup to a local directory in the **/idspri/backup** directory.
  - The **IDSB**_yyyy-mm-dd_hh-*mm-ss* directory that Cisco IPICS created when it performed the database backup.

- **Remote Host**—Choose this option to restore your data from a remote host, in the directory location that you specify.

  When you choose to restore your data from a remote host, you must specify the following information:

  - Remote Host IP Address—Enter the IP address of the remote host.
  - User Name—Enter a valid user name for access to the remote host.

    The user name to restore the database must be the same user name that you used to back up the database. If you specify a different user name, the restore procedure does not succeed because the user does not have the correct permissions to access the database backup.
  - User Password—Enter a valid password for this user.
  - Remote Directory—Enter the directory path for the remote host from which you want the database to be restored. Enter the full directory path, including the directory that was generated by Cisco IPICS for the database backup, for example **/mybackups/IDSB_2006-08-25_17-13-55**.

Note Be sure to enter the correct user name, password, and remote directory; otherwise, the scp process fails. If the scp process fails, you can determine the cause of the failure by checking the logs in the **Administration > Database Management > Log** window.

A restore operation does not allow you to view the log details of the operation while it is in progress. The Tomcat service restarts during the restore operation and automatically logs all users out of Cisco IPICS. You must wait for the restore process to complete before you can log in again.

Tip You can check the status of the restore process in the **/opt/cisco/ipics/database/logs/db-maintenance.log** file on the Cisco IPICS server. For more information, refer to "Checking the Restore Status in the Database Log" in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

CHAPTER 5

Frequently Asked Questions

This appendix contains frequently asked questions and answers relating to the Cisco IPICS server and its various components and includes the following sections:

Cisco IPICS Server and Administration Console

Q. Can I specify a timeout period for my Cisco IPICS Administration Console browser session?

A. Yes, you can specify a browser session timeout period by changing the value in the Cisco IPICS Session Timeout Period setting in the **Administration > Options** window. The default specifies 30 minutes. The range of values that you can use includes zero to 99999. (A value of zero specifies that the browser never times out.)

For more information about Cisco IPICS options, refer to the "Managing Cisco IPICS Options" section in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Q. Can I use pop-up blocker software with Cisco IPICS?

A. The Cisco IPICS Administration Console uses browser pop-up windows for certain functionality. If you have 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 administrative tasks in Cisco IPICS, disable any pop-up blocker software that is installed on your machine before you use the Administration Console.

Q. Do windows in the Cisco IPICS Administration Console update automatically?

A. No. As a best practice, 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, you can update your browser window and retry the operation.

Q. How do I update my browser window?

A. 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. Some windows in the Administration Console provide a Refresh button, which you can use to refresh or update the window.

Note Cisco IPICS does not support the use of the browser Refresh button to refresh a window in the Administration Console.

Q. What does an asterisk (*) denote in the Administration Console graphical user interface (GUI)?

A. An asterisk in the GUI indicates a required field.

Q. What do the Cisco IPICS roles define and to whom are they assigned?

A. Each Cisco IPICS user is assigned one or more roles. Roles define the Cisco IPICS features that a user can access and the functions that a user can perform. The following list describes the roles that are available in Cisco IPICS:

- User—Provides the ability to maintain personal information, download the PMC client application, specify communication preferences that are used to configure audio devices, activate a policy, and view associated policies.

Note Every Cisco user is assigned the User role, although the users may also have additional roles assigned to them.

- System administrator—Responsible for installing and setting up Cisco IPICS resources, such as servers, routers, multicast addresses, locations, and PTT channels. Also creates, edits, or deletes ops views, manages Cisco IPICS licenses and PMC versions, performs activities relating to the dial engine, activates policies, views certain policies, and monitors the status of the system and its users via the activity log files and the Dashboard.
- Ops view administrator—Provides the ability to manage and monitor the activity logs that are filtered by ops views and accessible in the Administration Console (Administration > Activity Log Management) window.
- Operator—Responsible for setting up and managing users and user groups, granting access to Cisco IPICS and the PMC, assigning user channels, roles and ops views, and creating and managing policies.

- Dispatcher—Responsible for setting up inactive VTGs, activating VTGs to begin conferences, and adding or removing participants in inactive and active VTGs. Creates and manages policies. Also monitors active VTGs and events and can mute and unmute PMC users, as necessary.
- All—Equivalent to being assigned each of the other Cisco IPICS roles.

Q. When should I back up my database?

A. For optimum performance, Cisco recommends that you back up your database during periods of low activity or other off-peak hours. If you perform a back up during periods of high activity, the length of time that it takes to complete this operation can be significantly increased. For more information, see the "Cisco IPICS Database Management" section on page 4-8 or refer to "Backing up the Cisco IPICS Server Database" in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

Q. Can I restore data from one server to another?

A. You can restore data from one server to another only if both servers are running the same version of Cisco IPICS software. If the software versions of the two servers differ, the database schema might not be the same; therefore, the restore operation could fail, or you could encounter unpredictable errors when you perform tasks in the Administration Console. For more information, see the "Cisco IPICS Database Management" section on page 4-8 or refer to "Restoring Data from a Database Backup" in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*.

Cisco IPICS Licenses

Q. How are license ports and DS0 loopback port resources counted in Cisco IPICS release 2.1(1)?

A. To use the Cisco IPICS solution, you must first upload and install one or more licenses. Cisco IPICS supports the following licenses:

- LMR port license—Cisco IPICS uses this license when PTT channels are enabled.

Cisco IPICS also uses a single LMR license when a radio channel is enabled. However, when subsequent radio channels are configured within the radio, those channels do not use separate licenses. Cisco IPICS uses only one LMR license per enabled radio channel.

- Multicast port license—Cisco IPICS uses a single multicast port license when a VTG is activated.
- PMC users license—Cisco IPICS uses a single PMC license each time that a PMC user logs in to the system. If a PMC user logs in multiple times, Cisco IPICS uses a license when a channel is enabled.
- Cisco Unified IP Phone users license—Cisco IPICS uses a single Cisco Unified IP Phone license each time that a Cisco Unified IP Phone user (PMC xml client) logs in to the system.
- Dial user license—Cisco IPICS uses a single PSTN (dial user) license in each of the following scenarios:

  - Cisco IPICS uses one license for an active inbound call

  - Cisco IPICS uses one license for an active outbound call

  Cisco IPICS uses a single DS0 loopback pair in the following scenarios:

  - For each remote channel on a PMC

  - For each channel in an active VTG

  - For each instance of an active VTG that is accessed by a dial-in or dial-out user, regardless of the number of users who are connected to the VTG

- Ops view license—Cisco IPICS uses a single ops view license for each configured ops view.
- Cisco IPICS base server license—A Cisco IPICS base server license displays as enabled or disabled in the **Administration > License Management** window to indicate whether the license is activated.
- Policy engine base license—A policy engine base license displays as enabled or disabled in the **Administration > License Management** window to indicate whether the policy engine is activated.

Note Cisco IPICS supports the use of release 2.0(x) licenses with release 2.1(1).

Q. Why would a VTG suddenly become active or inactive?

A. If a VTG unexpectedly becomes active or inactive, the change in status could be caused by a policy that has executed and forced a change to the VTG state. Make sure that you have sufficient licenses in Cisco IPICS to avoid a sudden change in status.

RMS Components

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, Cisco IPICS allows you to configure more than one RMS in the same location.

Q. If I have more than one RMS component configured in the server, do all RMS components need to be configured alike?

A. If you have more than one RMS component configured in the server, make sure that you configure each RMS according to the instructions that are documented in the "Configuring the Cisco IPICS RMS Component" appendix in the *Cisco IPICS Server Administration Guide, Release 2.1(1).* Be aware that Cisco IPICS provides support only for RMS components that are configured as described in that document.

Q. How do I configure an RMS router for T1 or E1 connectivity?

A. When you configure an RMS router for T1 or E1 connectivity, there are specific guidelines that you must follow to ensure successful operation of your RMS. For these details, refer to "Configuring the Cisco IPICS RMS Component" appendix in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Q. Must timeslot 24 (for a T1 controller) and timeslot 31 (for an E1 controller) always be configured?

A. Yes, timeslot 24 (for a T1 controller) and timeslot 31 (for an E1 controller) must always be configured even if you a fractional T1 or E1 controller. Typically, a T1 controller supports 24 ds0s and an E1 controller supports 30 ds0s, but your controller may support fewer ds0s, depending on the number of digital signal processors (DSPs). For more detailed information, refer to "DS0 Group-to-Timeslot Mapping Guidelines" in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Q. How do I select RMS IP addresses?

A. When you select the IP addresses for the RMS, there are specific guidelines that you must follow and interfaces that you must configure to ensure successful interoperability with Cisco IPICS components. For the details about RMS configuration, refer to "Configuring the Cisco IPICS RMS Component" appendix in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Q. Must the IP addresses that I configure for my interfaces be routable?

A. Yes, the IP addresses that you configure for both the Loopback0 and the Vif interfaces must be routable; this requirement is mandatory for both of these interfaces to ensure proper operation with Cisco IPICS.

If the IP addresses for either of these interfaces are not routable, you may experience intermittent delays, of varying duration, from the time that you press the PMC PTT button to the time that the media is established between the remote PMC and multicast channels. This delay results from the inability of the RMS to perform Reverse Path Forwarding (RPF) checks on multicast Real-time Transport Protocol (RTP) packet source addresses. Therefore, to avoid this issue, make sure that the IP addresses for both the Loopback0 and the Vif interfaces are routable. For detailed information, refer to "Configuring the Cisco IPICS RMS Component"appendix in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Q. How do I configure an inbound dial peer in the RMS?

A. When you configure an inbound dial peer in the RMS, there are specific values that you should enter. Although Cisco IOS supports other values for some of the fields in the configuration, Cisco recommends that you configure the values exactly as they are documented in the "Configuring the Cisco IPICS RMS Component" appendix in the *Cisco IPICS Server Administration Guide, Release 2.1(1)* to ensure consistency.

Q. How do I set up a SIP connection for the direct dial functionality if I have more than one RMS component in the server?

A. If you have more than one RMS component in the server, make sure that you perform the direct dial configuration, as documented in Step 19 and Step 20 in the "Configuring the Cisco IPICS RMS Component" appendix in the *Cisco IPICS Server Administration Guide, Release 2.1(1)*, for each RMS. When more than one RMS component is configured in the server, Cisco IPICS may use any one of these configured components, depending on load conditions, to set up the SIP connection for the direct dial functionality.

Locations

Q. Why are some channels designated as remote?

A. A channel is designated as remote when it is in a different multicast domain than the user who is accessing it. In this case, the channel uses the resources of the RMS to create a SIP-based connection to the Cisco IPICS server.

Q. What does the remote designation mean for a PMC location?

A. The remote location is available only to PMC users. When a PMC user chooses **REMOTE** from the Location drop-down list box, connectivity is established with the appropriate RMS via a SIP-based unicast connection for each channel or VTG that has been assigned to the user. For more detailed information about locations, see the "Understanding Locations" section on page 2-4 or refer to the "Managing Locations" section in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Q. If I have only one router in a location and my channel is defined as ALL, will the channel be accessible to a user?

A. Yes. However, if a router location is defined as ALL, a channel that is not also configured as ALL is not accessible to users or VTGs that the router supports.

The ALL location defines the scope or reachability of a multicast address. For this reason, the ALL location is applicable to channels and VTGs, which are associated with multicast addresses, but no applicable to IP phones or RMS components, which are not associated with multicast addresses. For more detailed information about locations, see the "Understanding Locations" section on page 2-4 or refer to the "Managing Locations" section in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Resources

Q. How many resources (voice ports, multicast addresses) do I need in Cisco IPICS?

A. The following guidelines apply to the use of resources:

- Every channel that is active in a VTG uses one DS0 pair (also called a loopback)
- Every sub-VTG in a VTG uses one DS0 pair
- Every SIP connection uses one DS0 pair per channel or VTG per user, per location
- Local channels do not use any DS0 pairs
- G.729, which is used for a SIP connection, requires DSP resources
- A dial connection uses two DS0 pairs (for two multicast addresses) for the first dial user, and then one DS0 per subsequent dial user

The following resources do not use voice resources:

- A user with an associated channel (the system only uses resources when the user logs in from a remote location)
- A VTG that includes only users
- User groups
- Channel groups

Cisco IPICS Policy Engine

Q. How do I access the telephony user interface (TUI)?

A. You can access the TUI from a touch-tone telephone. From the phone, you can access the TUI in the following ways:

- By calling the policy engine—Call the number that is configured in the Dial Number field for your ops view. For related information, see the "Understanding Ops Views" section on page 2-7 or refer to "Configuring and Managing Cisco IPICS Operational Views" in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*
- By receiving a call from the policy engine—You receive a call when another user invites you to join a group, when a Cisco IPICS dispatcher initiates a dial out from the VTG Management window, when a policy that includes one or more actions to call you executes, or when you record a prompt.

Q. Are there any guidelines that I should follow when using the TUI?

A. There are some usage guidelines that you should be aware of when using the TUI. A few of these guidelines are described in the following list:

- After you dial in to the TUI, the system prompts you to enter your user ID and PIN (password). You must authenticate before you can continue to use the system.
- After you authenticate, the system announces the available menu options, such as joining a group, invoking a policy, or accessing the system menu.
- A menu times out if you do not respond within the predefined allowable period of time. In most instances, this period of time is three seconds and includes a maximum retry limit of three. When the allowable period of time has expired, the TUI responds with "Are you still there?" and the menu repeats. When the maximum retry limit has been exceeded, the TUI responds with a warning prompt to inform you that the call will be disconnected and then it terminates the call.
- When you dial out to invite a party in to a call, the called user must press any key to authenticate before the call is connected to the group. (As the call is being dialed out, the system does not play any sounds.)
- Transfer and conference features are not supported on a phone when the phone is connected to the TUI.

- From the TUI main menu, you can take the following actions:

  - To join a group, press 1. Then, you can press 1 to select an assigned group to join by spelling out the group name, or press 2 to listen to the list of assigned groups and then selecting from that list. (If you know the name of the group that you want to join, it is quicker to enter the name than to wait for the TUI to announce the list of available groups.) To confirm your selection, press 1. To cancel your selection, press 2. To return to the previous menu, press *.

  - To invoke a general purpose policy, press 2. Then, you can press 1 to select a policy by spelling its name, or press 2 to listen to the list of available policies. (If you know the name of the policy that you want to invoke, it is quicker to enter the name than to wait for the TUI to announce the list of available policies.) To confirm your selection, press 1. To cancel your selection, press 2. To return to the previous menu, press *.

For more information and for a complete list of TUI guidelines, refer to "Using the Cisco IPICS Policy Engine" in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Q. Can an internal party dial the Cisco IPICS dial engine telephony user interface (TUI)?

A. Yes, an internal party can dial the dial engine TUI as long as you have configured a SIP provider in your network.

The Cisco IPICS policy engine requires that a SIP provider be configured in your network to use the dial-in, dial-out, or PMC direct dial features. A SIP provider handles calls to and from the policy engine.

You must use Cisco Unified Communications Manager or a Cisco router that is running a supported version of Cisco IOS as the SIP provider and enter the required configuration information, as described in "Configuring the SIP Provider" in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

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

If the SIP provider is a Cisco Unified Communications Manager, then you must configure a route pattern for the SIP trunk.

If the SIP provider is a supported Cisco IOS gateway, you must make sure that you configure a dial peer that routes the call to Cisco IPICS.

Note The dial number (DN) that you want to use to allow dial-in access must be assigned to an ops view (typically the System ops view). For more information, see the "Understanding Ops Views" section on page 2-7 or refer to "Performing Ops View Tasks" in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Q. Which codecs do the dial engine support?

A. The dial engine supports only G.711 u-law. For more information, see the "Managing and Using the Cisco IPICS Policy Engine" section on page 3-8 or refer to "Configuring and Managing the Cisco IPICS Policy Engine" in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Q. What is an action as it relates to a policy?

A. An action specifies the activity that a policy performs when it executes. The actions available for a policy depend on the policy type. Actions include the activities that are described in the following list:

- Invite to VTG—This action is an invitation policy type that calls designated users and invites them to join a VTG by responding to TUI prompts. This action can be activated only through the TUI when you break out of an existing VTG.
- Activate VTG—This action is a multi-purpose policy type that activates designated, preconfigured VTGs.
- Notification—This action is a multi-purpose policy type that contacts designated recipients according to notification instructions that you specify.
- VTG Add Participants—This action is a multi-purpose policy type that adds the designated participants to the designated VTG.
- Dial Out—This action is a multi-purpose policy type that calls designated users according to their configured dial preferences to invite them to join the designated VTG.

For more information about policy actions, see the "Managing and Using the Cisco IPICS Policy Engine" section on page 3-8 or refer to "Managing Actions for a Policy" in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Q. Which types of notification actions can I use with the Cisco IPICS policy notification feature?

A. The Cisco IPICS policy notification features includes the following notification action types:

- Email Notification—This type of notification sends a message that you enter to the e-mail, short message service (SMS), and pager addresses that are configured as communication preferences for each user that you designate as a recipient.
- IP Phone Notification—This type of notification displays a designated message on supported Cisco Unified IP Phones.
- Dial Notification—This type of notification calls out to designated users and plays the selected prompt or sends a message to the Cisco Unified IP Phones of the designated users and plays automatically on the speaker of the phone.
- Talk Group Notification—This type of notification plays out the selected prompt to all users in the VTG.

Q. What types of messages can I send when I configure a new policy notification action?

A. The policy notification action includes the following message options:

- Email—This notification option sends a message that you enter to the e-mail, SMS, and pager addresses that are configured as communication preferences for each user that you designate as a recipient.
- IP Phone Text—This notification option displays a designated message on supported Cisco Unified IP Phone models. The telephone numbers of each phone must be configured as a dial preference for the associated user.
- Dial—The policy engine executes a Dial notification action as follows:

  - If the Cisco Unified Communications Manager Configuration for IP Phone Notifications parameters are configured in the SIP Configuration menu, the system checks whether each designated user has

an associated Cisco Unified IP Phone that is configured in Cisco Unified Communications Manager. If a user does have an associated phone, the system plays the designated message on the speaker of the phone.

- If Cisco Unified Communications Manager Configuration for IP Phone Notifications parameters are configured but a user does not have an associated Cisco Unified IP Phone, or if the phone of a user is busy, the system calls the user as specified in the communication preferences for the user and plays the designated message.

- If Cisco Unified Communications Manager Configuration for IP Phone Notifications parameters are not configured, the system calls the user as specified in the dial preferences for the user and plays the designated message.

- Talk Group—This notification option plays the selected prompt to all participants in the selected VTG.
- Dial Engine Script—This notification option executes the designated dial engine script once for each designated recipient.

For more detailed information about notification actions, refer to "Using the Cisco IPICS Policy Engine" in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Q. In the case of a notification action that is in the form of an e-mail, SMS, or page, and a dial notification to a large number of users, what is the sequence of notification events?

A. The dial engine uses a scalable, multi-threaded dial-pool implementation for dialing out to users. Ports from the available dial pools are used by the currently executing policy notification/invite actions. If there are fewer dial ports available than what is needed, the other policy actions are put in a waiting state until more ports become available.

A call is considered successful when the call recipient authenticates. If there is no authentication, the system moves to the next dial preference that is listed in the Communications Preferences tab for the user in the user profile until either the call is successful or every number has been tried by the system. For detailed information, refer to the "Allocating Dial Ports for the Dial-In/Invite and Notification Features" section and the "Managing Communications Preferences for a User" section in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Q. Can a dispatcher enter specific notification information when sending a notification to VTG participants?

A. Yes, Cisco IPICS includes the capability for the dispatcher to enter specific subject and body text when sending notifications to participants in a VTG from the **VTG Management > Virtual Talk Groups** window. For more information, refer to the "Notifying and Dialing Out to Participants, and Setting PMC Attributes in an Active VTG" section in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Q. Can a notification action be sent to recipients who are not configured as users in Cisco IPICS?

A. Yes, the Cisco IPICS policy engine includes an external notification action which sends notification actions to designated recipients who are not configured as Cisco IPICS users and provides them with information that you specify.

The external notification feature is not configurable via the Cisco IPICS Administration Console. Instead, you must configure one or more dedicated dial engines, designate a list of recipients, and designate a message file to play to the recipients.

To configure a a Cisco IPICS server as a primary dial engine, you edit a .xml configuration file on that server and set the dialEngine sub-element attributes for each dedicated dial engine, including the primary dial engine.

A recipient list is a .xml file that contains a list of each person who should receive the external notification message.

Note To invoke an external notification that contacts these recipients, you must know the URL of the server on which the recipient list resides.

A message file is a .wav file in pulse code modulation (PCM) or CCITT u-Law format that contains the recorded message to play to recipients. Cisco recommends that the message be no longer than 90 seconds.

Note To invoke an external notification that plays this message, you must know the URL of the server on which the message file resides.

The external notification action performs the following actions:

- Simultaneously calls many external users at telephone numbers that Cisco IPICS obtains from a file that you specify.

  To designate a recipient list, you create an .xml file that contains the telephone numbers of all users who you want to contact.

- Plays a designated message to each user who answers the call.

  To designate a message file, you create a .wav file that contains the message that you want to play to the recipients.

  To invoke the external notifications, you send an HTTP request or a Common Alerting Protocol (CAP) .xml file to the appropriate dedicated dial server.

- Captures results of each call in a log file that you can review at any time.

  For more information, refer to the "Using Cisco IPICS for External Notifications" appendix in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Q. When Cisco IPICS dials out to users, does the dispatcher get notified about numbers that have not yet been reached and is there any way to determine how long it should take to reach all the participants in a VTG?

A. Dialed numbers display in the **Policy Execution Status > Executed/Executing Policy** window, showing which numbers have been reached and which are still in progress.

For each available port, the user must authenticate by entering a digit ID/PIN and then the notification message is played. Whenever errors occur, such as the entry of an incorrect digit ID or PIN and/or the occurrence of a timeout because the user is not reached, the dial-out notification takes longer to complete. The total time for dial-out notification depends on these factors. For more information, refer to the "Viewing Information about Executing or Executed Policies" section in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Q. Is there a way to export and track the history of executing and executed policies in Cisco IPICS?

A. Yes, Cisco IPICS includes the ability to export executing and executed policy history to a Microsoft Excel format that you can download. To download the execution status history, navigate to the **Policy Management > Execution**

Status window and click the **Download Execution Status** button. You can either open the file or save the file to a location of your choice and then open it by using Microsoft Excel. For more information, refer to the "Viewing Information about Executing or Executed Policies" section in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Q. How do you integrate the dial engine into an existing network that runs an earlier version of Cisco Unified Communications Manager and does not have native SIP trunk support?

A. This integration can be accomplished by using a Cisco IOS router that runs Cisco Unified Communications Manager Express as the SIP provider and configuring an H.323 Intercluster Trunk (ICT) between the Cisco Unified Communications Manager and the SIP provider. For detailed information, refer to "Configuring and Managing the Cisco IPICS Policy Engine" in the *Cisco IPICS Server Administration Guide, Release 2.1(1)* and the *Solution Reference Network Design (SRND) Guide for Cisco IPICS , Release 2.1(1).*

Q. Is there any special SIP configuration required when executing policies that use the IP Phone Text Notification action or the Dial Notification action to send a message to a Cisco Unified IP Phone?

A. Yes, you must enter configuration information for the Cisco Unified Communications Manager in the **Dial Engine > SIP Configuration** window. For detailed information, refer to the "Configuring and Managing the Cisco IPICS Policy Engine" section in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Push-to-talk Channels

Q. What is a push-to-talk (PTT) channel?

A. A PTT channel, also referred to as a *channel*, is a communications path that allows users to communicate with each other. In Cisco IPICS, a channel defines and describes the specific content stream of the channel regardless of the source of that content.

PTT channels appear on the PMC and on Cisco Unified IP Phones. For more information about the PMC, refer to the *Cisco IPICS PMC Installation and User Guide, Release 2.1(1).*

Note In Cisco IPICS, a channel can also refer to a radio control interface (radio or radio channel), which also has an audio stream. For more information, see the "Managing Radios" section on page 3-3 or refer to "Managing Radios" in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Q. Can a channel be assigned to multiple locations in Cisco IPICS?

A. Yes. Channels achieve media connectivity by being mapped to a multicast address and port in a location. When a channel is assigned to multiple locations, it can have more than one media connection. The media connection count in the **Serviceability > Dashboard** window reflects the total number of media connections. For more information, see the "Viewing Real-Time System Status in the Dashboard Window" section on page 4-2 or refer to "Viewing Information in the Dashboard Window" in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Q. Are there any guidelines that I should follow when selecting multicast IP addresses that are to be used for channels?

A. Yes. Cisco strongly recommends that you configure only multicast IP addresses that are in the 239.192.0.0 to 239.251.255.255 range. For more detailed information, refer to "Guidelines for Using IP Multicast Addresses with Cisco IPICS" in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Note Two channels that are in the same location cannot have the same multicast address. For more information, see the "Understanding Locations" section on page 2-4 or refer to "Managing Locations" in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Radio Communications

Q. What is tone control?

A. Tone control (also referred to as *Tone Remote Control* (TRC)) refers to the use of inband tone sequences to control a radio that is connected to an LMR gateway (typically a base station). In Cisco IPICS, you can use tone control to perform various functions, such as modifying or tuning a channel to a different radio frequency (RF), changing the transmit power level, and

enabling or disabling radio built-in encryption. TRC uses well-defined audio sounds (also referred to as *tones*) to change the behavior of a device. A tone-keyed radio system requires that a specific tone be present on the incoming analog (e-lead) port. If this tone is not present, the radio does not transmit audio.

See the "Managing Radios" section on page 3-3 or refer to the "Managing Radios" section in the *Cisco IPICS Server Administration Guide, Release 2.1(1)* for more information.

Q. What are tone sequences?

A. Each radio channel that you configure in the Cisco IPICS Administration Console represents a physical radio that you can configure with one or more tone sequences. Tone sequences control various tones and functionality on the radio. Each tone sequence includes the frequency or frequencies, volume (power), duration, and other parameters that are necessary to generate a specific tone and invoke a specific action on the radio.

See the "Managing Radios" section on page 3-3 or refer to the "Managing Radios" section in the *Cisco IPICS Server Administration Guide, Release 2.1(1)* for more information.

Q. How can tone-controlled radios be used with Cisco IPICS?

A. Cisco IPICS provides support for tone-controlled radios by enabling the definition of radio channels in the Cisco IPICS server configuration and implementing a 36-channel radio console skin in the PMC. The PMC sends RFC 2198 and RFC 2833 packets to control tone sequences on a per-channel basis. At the LMR gateway, these packets get converted into audible tones via the configured ear and mouth (E&M) interface to the physical radio to provide tone control for radios.

See the "Managing Radios" section on page 3-3 or refer to the "Managing Radios" section in the *Cisco IPICS Server Administration Guide, Release 2.1(1)* for more information.

Q. What are stateful and momentary control sequences on a tone-controlled radio?

A. Cisco IPICS enables the following controls on a tone-controlled radio:

- Stateful controls—Control functions can display on the PMC as single channel selector buttons or as stateful control sequences. Stateful control sequences are comprised of multiple states, where each state displays as a separate channel selector (tone control) button on the PMC. An example of a stateful control sequence is the power level of a radio.
- Momentary controls—Momentary tones begin to play when the PMC user presses the associated button. After the user presses a momentary control button, the button appears to be pressed momentarily before it appears raised again.

Q. What are descriptor files and how are they used in Cisco IPICS?

A. There are two types of descriptor files in Cisco IPICS:

- Radio descriptor files—Radio descriptors are .xml files that contain commands that are used to control functions on a radio. These files contain channel selectors that are used to change the frequency on a radio and control functions that allow for stateful and momentary controls of the radio.
- Tone descriptor files—Tone descriptors are .xml files that define commands and over-the-air signals that can be associated to one or more Cisco IPICS channels. Commands can be referenced by any radio descriptor and signals can be associated to any channel.

See the "Managing Radio and Tone Descriptors" section on page 3-5 or refer to the "Managing Radio and Tone Descriptors" section in the *Cisco IPICS Server Administration Guide, Release 2.1(1)* for more information.

VTGs

Q. What is a VTG?

A. A VTG, or virtual talk group, enables multiple participants on various channels to communicate by using a single multicast address. Participants in a VTG can include users, user groups, channels (PTT and radio), channel groups, and other VTGs. An active VTG is a VTG in which all the participants have live connections with each other. For more information

about VTGs, see the "Understanding VTGs" section on page 2-6 or refer to "Performing Cisco IPICS Dispatcher Tasks" in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Q. Can more than one dispatcher log in to Cisco IPICS at the same time?

A. Yes, Cisco IPICS allows more than one dispatcher to log in to the system at a time. This scenario 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 ops views feature provides a mechanism to support this scenario by segmenting views. With ops views, a dispatcher sees and can control only the VTG participants that have been assigned to the particular ops view to which the dispatcher also belongs.

Q. What is the difference between an inactive VTG and an active VTG?

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

When you modify an inactive VTG, no changes occur in system resources or in the communication between participants until you activate that VTG. When you make changes to an active VTG, the original attributes of the VTG (inactive VTG) remain unchanged.

You can view information about any VTG by clicking the VTG name that displays in the **VTG Management > Virtual Talk Groups** window. Information about the VTG displays in a separate window.

For more information about inactive and active VTGs, see the "Understanding VTGs" section on page 2-6 or refer to "Performing Cisco IPICS Dispatcher Tasks" in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Ops Views

Q. What is an ops view?

A. An ops view, or operational view, allows segmentation of resources that authorized Cisco IPICS users may see on the Cisco IPICS Administration Console. With ops views, you can organize or segment different entities, such as agencies, companies, departments, jurisdictions, municipalities, or sites, into separate views that are isolated from each other.

Note Ops views does not affect the way in which channels and VTGs display on the PMC or Cisco Unified IP Phones.

Q. What is the difference between the *Belongs To* attribute and the *Accessible To* attribute for an ops view?

A. The Belongs To attribute determines the ops view to which the resource belongs or that the ops view owns. After a new ops view is created, the system administrator can associate resources, such as channels or users, to the ops view. The operator creates another operator user ID who belongs to that ops view and who can manage the ops view resources that are visible within the specific ops view.

The Accessible To attribute specifies that the resource is accessible to, or visible to, the ops view(s). Users only have access to the resources that are accessible to the ops view to which they belong. For more detailed information about ops views, see the "Understanding Ops Views" section on page 2-7 or refer to "Configuring and Managing Cisco IPICS Operational Views" in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Q. What is a SYSTEM ops view?

A. The SYSTEM ops view is an ops view that the Cisco IPICS server displays by default. The SYSTEM ops view is the home base or system-wide view to which the Cisco IPICS administrators belong. When new ops views are created, ports are reallocated from the SYSTEM ops view to the new ops view, and any additional ops views that you create.

Q. Which Cisco IPICS roles are allowed to create new ops views?

A. Only a system administrator can create new ops views on the server. The number of ops views that can be created depends on the number of ops view ports that the Cisco IPICS license provides. You can view the number of ops view ports that are in the system by accessing the **Administration > License Management** window in the Administration Console. For more information about ops view ports, refer to "Understanding the License Management Window" in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

After a new ops view has been created, you can associate resources, such as channels, to the ops view. 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.

When a resource contains or is associated to another resource that belongs to the ops view of a user, the user has the ability to remove the associated resource but cannot modify it in any other way. For more information about ops views, see the "Understanding Ops Views" section on page 2-7 or refer to "Configuring and Managing Cisco IPICS Operational Views" in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Serviceability

Q. How can I view serviceability and diagnostic information in Cisco IPICS?

A. To view real-time serviceability and diagnostic system information in Cisco IPICS, you can navigate to the Serviceability drawer and the following windows:

- Dashboard—This window provides you with Cisco IPICS system and resource information. For more information, see the "Viewing Real-Time System Status in the Dashboard Window" section on page 4-2.
- Diagnostics—This window contains summary information about the Cisco IPICS server and the components of the Cisco IPICS system that interact with the server. From this window, you can also execute a diagnostic script and additional diagnostic information. For more information, see the "Viewing and Downloading Diagnostic Information" section on page 4-2.

- System Logs—This window displays logging information for Cisco IPICS. This information can be useful for troubleshooting or debugging your system. For more information, see the "Viewing and Downloading the Cisco IPICS System Logs" section on page 4-6.

Cisco Unified IP Phones

Q. Can I specify a timeout period for a Cisco Unified IP Phone, so that the phone times out after a period of inactivity?

A. Yes, you can specify whether an IP phone times out after a configured period of inactivity, forcing the user to log in again, by changing the value in the Cisco Unified IP Phone Timeout Period setting in the **Administration > Options** window. For more detailed information about Cisco IPICS options, refer to "Managing Cisco IPICS Options" in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Q. Can I bypass the login for an IP phone user so that the user can more quickly access the Cisco IPICS service?

A. Yes. If there are users who you do not want to require to log in, you can configure a separate service, in Cisco Unified Communications Manager, that bypasses the log in for each of these IP phone users.

When you configure the Cisco IPICS service so that it does not prompt for user login credentials on the Cisco Unified IP Phone, the service automatically activates a channel or VTG if only one channel or VTG is assigned.

If you configure the Cisco IPICS service to bypass the user login and if there are more than one channel or VTG that is assigned, Cisco IPICS displays the list of these channels and VTGs on the IP phone.

For detailed information, refer to the "Setting Up and Using a Cisco Unified IP Phone as a Cisco IPICS Push-To-Talk Device" appendix in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Q. Is there a way to configure an IP phone to display the Logout softkey on the main display screen while users are connected to a channel or VTG?

A. Yes. On some model IP phones, you can add a special parameter to the Cisco IPICS Service URL configuration to enable the display of the Logout softkey while IP phone users are connected to a channel or VTG.

This setting allows the Logout softkey to display such that users do not need to press the **Back** softkey, after exiting a channel or VTG, to access it.

Note If you configure this parameter, a user may need to press the **More** softkey on some phone models to see **Logout**.

For more information, refer to the "Setting Up and Using a Cisco Unified IP Phone as a Cisco IPICS Push-To-Talk Device" appendix in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

Q. Will an IP phone keep working if it loses connectivity to the Cisco IPICS server while the phone user is logged in to the Cisco IPICS service?

A. If a phone loses connectivity to the Cisco IPICS server while the phone user is logged in to the Cisco IPICS service, the service retains its current state and the user can continue to use the PTT functionality for the channel or VTG that is currently selected. However, the phone cannot connect to other channels or VTGs until connectivity to the server is re-established.

Q. Are there any guidelines that I should follow when using the Cisco IPICS service on a Cisco Unified IP Phone?

A. There are some usage guidelines that you should be aware of when using the Cisco IPICS service on a Cisco Unified IP Phones. A few of these guidelines are described in the following list:

- To obtain help with using the Cisco IPICS service on a Cisco Unified IP Phone, press the **Help** softkey.

The Cisco IPICS operator configures the digit ID and digit password (PIN) that are used to log into the Cisco IPICS service, or configures the system so that these login credentials are not required. For more information, refer to "Managing Dial Login Information for a User" in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

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

- Channels that are returned from Cisco IPICS to a Cisco Unified IP Phone must have a multicast connection defined in the Default Location field in the Dial Login tab for the user.

For more information and for a complete list of usage guidelines, refer to "Using the Cisco IPICS Service on a Cisco Unified IP Phone" in the *Cisco IPICS Server Administration Guide, Release 2.1(1).*

GLOSSARY

A

action — A discrete function that is performed through a policy. Discrete functions include activate VTG, notification, VTG add participant, dial-out, and invite to VTG.

activate VTG — An action that activates a preconfigured VTG; can also specify a duration. At the end of the specified duration, the VTG is deactivated. If no duration is specified, the VTG must be manually deactivated by the dispatcher from the VTG Management drawer in the Cisco IPICS administration console.

activated — A state that indicates that the SIP (unicast) or multicast channel is fully operational. When a channel/VTG on the PMC is enabled and activated, all of the PMC buttons are operational.

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

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

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

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

alert tone An audible tone, such as a siren, warble or chirp, that is used to attract the attention of a radio listener.

alert tone buttons Buttons on the PMC that can play out alert tones on one channel or multiple channels.

all talk button Allows you to simultaneously talk on all of the channels that you selected.

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

B

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

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

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

C

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

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

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

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

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

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

channel A communication path that is wide enough to permit a single RF transmission. Multiple channels can be multiplexed over a single cable in certain environments. There are many different types of channels in Cisco IPICS, including direct dial, 2-way, VTGs, and radio channels. Channels can be dynamically or statically allocated. Channels may have one or more channel connections that define the source for the channel. *See* PTT channel.

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

channel connection One or more methods by which a content stream can be obtained. For instance, a particular channel may be found on several different multicast addresses in different locations and also on several different radios at different locations.

channel folder A logical grouping of channels

channel select check box Provides the ability to select or deselect the specified channel on the PMC for audio transmission.

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

Cisco Unified Communications Manager (CallManager) The software-based call-processing component of the Cisco IP telephony solution. Cisco Unified Communications Manager (CallManager) extends enterprise telephony features and functions to packet telephony network devices, such as Cisco Unified IP Phones, media processing devices, VoIP gateways, and multimedia applications.

Cisco IPICS Cisco IP Interoperability and Collaboration System. The Cisco IPICS system provides an IP standards-based solution for voice interoperability by interconnecting voice channels, talk groups, and VTGs to bridge communications amongst disparate systems.

Cisco IPICS policy engine Integrated with the Cisco IPICS server, this component enables telephony dial functionality and is responsible for the management and execution of policies and user notifications.

Cisco IPICS server Provides the core functionality of the Cisco IPICS system. The Cisco IPICS server software runs on the Linux operating system on selected Cisco Media Convergence Server (MCS) platforms. The server software includes an incident management framework administration GUI that enables dynamic resource management for users, channels, and VTGs. The server also includes the Cisco IPICS policy engine, which enables telephony dial functionality and is responsible for the management and execution of policies and user notifications.

Cisco Unified IP Phone A full-featured telephone that provides voice communication over an IP network. A user can participate in a PTT channel or VTG by using a Cisco Unified IP Phone as a PTT device.

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. An electrical signal that is used to signal when a radio is receiving traffic.

coverage In radio communications, the geographical area that is within the range of, or that is covered by, a wireless radio system to enable service for radio communications. Also referred to as service delivery area.

D

delay time The sum of waiting time and service time in a queue.

decrypt Cryptographically restore ciphertext to the plaintext form it had before encryption.

decryption Reverse application of an encryption algorithm to encrypted data, thereby restoring that data to its original, unencrypted state.

dial engine scripts Scripts that the Cisco IPICS dial engine executes to provide the telephony user interface (TUI) for interaction with incoming and outgoing phone calls.

dial-in A phone call that is dialed in to the policy engine.

dial-in floor control A feature that allows one dial-in user, at a time, to talk in a VTG or a channel. The telephony user interface provides this dial-in floor control feature to support dial-in users. It does not provide support for floor control for other PTT users.

dial number The phone number that is used by the policy engine and the SIP provider and configured in the Dial Information pane in the Ops Views window. Dialing this number provides user access to the telephony user interface.

dial out invite An action that invites selected user(s) to the selected VTG.

A phone call that is dialed out by the policy engine to a phone user to invite the user in to a talk group.

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

digit ID A numeric identifier that is chosen by a Cisco IPICS user and stored in the user profile. Cisco IPICS uses this ID and a numeric password to authenticate a Cisco Unified IP Phone user.

digital modulation technique A technique for placing a digital data sequence on a carrier signal for subsequent transmission through a channel.

discrete tone Any tone that is sent without any summed or added tone. For example, adding a function tone with a low level guard tone may impact the recognition of the function tone. Contrast with mixed tones.

dispatcher The Cisco IPICS dispatcher is responsible for setting up the VTGs, activating the VTGs to begin conferences, and adding and/or removing participants in inactive VTG and active VTGs. The dispatcher also monitors the active VTGs and events, can mute and unmute PMC users, as necessary, and manages policies, which activate/deactivate VTGs based on specific criteria and designated intervals. Policy management activities include create/modify/delete policies, view policies, execute policies, and activate privileges.

DS0 digital service zero (0). Single timeslot on a DS1 (also known as T1) digital interface—that is, a 64-kbps, synchronous, full-duplex data channel, typically used for a single voice connection on a PBX.

DTMF dual tone multi-frequency. The signal to the phone company that you generate when you press keys on a telephone keypad. With DTMF, each key that you press on your phone (0 through 9, ‘*’ and ‘#’) generates two tones of specific frequencies; one tone is generated from a high frequency group of tones and the other from a low frequency group. Voice gateways often strip these inband tones and present them out-of-band in SIP, H.323, or other messages.

dynamic radio channel (dynamic control) The controls that are used to preset radio characteristics so that channels are available to clients.

dynamic regrouping A trunking system feature that allows multiple radios to be placed upon a specific talk group without manual manipulation of the programming of the radios. Dynamic regrouping is initiated through a system control console and transmitted to the radio via the trunking systems control channel.

E

E & M recEive and transMit (or ear and mouth). As the analog interface between a radio and the LMR gateway, the E&M interface provides voice signals from radio channels, which are then mapped to IP multicast or unicast. The E&M interface provides the most common form of analog trunking.

1. Trunking arrangement that is generally used for two-way switch-to-switch or switch-to-network connections. 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.

e-lead The ear portion of the E & M interface. The e-lead is the receive path of the LMR gateway.

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 is used in several different contexts. For example, transmission frequency (the band on which the radio sends signals) or the frequency of an audible signal measured in hertz (Hz). All tone control operations require audible tones that fall within a narrow band of a specific frequency and at a specific volume (amplitude).

frequency assignment Assignment that is given to a radio station to use a radio frequency or radio frequency channel under specified conditions.

frequency hopping The repeated switching of frequencies during radio transmission according to a specified algorithm, intended to minimize unauthorized interception or jamming of telecommunications.

frequency modulation Modulation technique in which signals of different frequencies represent different data values.

frequency sharing The assignment to or use of the same radio frequency by two or more stations that are separated geographically or that use the frequency at different times.

function tone A tone that follows the high level guard tone and causes the radio to perform a specific function, such as selecting a new transmit frequency. Function tones are often referred to as F1, F2, F3, and so on. *See* preamble and high level guard tone.

G

gateway Device that performs an application-layer conversion of information from one protocol stack to another. In Cisco IPICS, the gateway component includes LMR gateways, which functionality is usually installed as an additional feature in a supported Cisco router. LMR gateways provide voice interoperability between radio and non-radio networks by bridging radio frequencies to IP multicast streams.

GRE generic routing encapsulation. Tunneling protocol that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP internetwork. By connecting multiprotocol subnetworks in a single-protocol backbone environment, IP tunneling that uses GRE allows network expansion across a single-protocol backbone environment. GRE is generally used to route multicast traffic between routers.

guard tone The most common guard tones are the high level guard tone (HLGT) and the low level guard tone (LLGT). The HLGT is used to alert the radio that a function tone follows. The LLGT is used as a hold tone or keying tone. *See* tone keyed.

H

H.323 Defines a common set of codecs, call setup and negotiating procedures, and basic data transport methods to allow dissimilar communication devices to communicate with each other by using a standardized communication protocol.

high-band frequency Refers to the higher frequency levels in the VHF band, typically 138-222 MHz.

HLGT high level guard done. Also known as awake tone. This tone is set at high volume and is usually the first tone in a preamble. It is used to alert the radio that another tone, usually a function tone, will follow. *See* guard tone.

Hoot ‘n’ Holler (Hootie) A communications system where the loudest and most recent talker or talkers are mixed into one multicast output stream. Also known as hootie, these networks provide “always on” multiuser conferences without requiring that users dial in to a conference.

Cisco enables the Cisco Hoot 'n' Holler feature in specific Cisco IOS versions.

I

idle tone The tone that a radio may deliver on the m-lead to signal the LMR gateway that there is no incoming traffic. When the idle tone is removed, the LMR gateway deems all signals to be valid voice traffic.

inactive VTG A VTG that is stored for use. The Cisco IPICS server stores inactive VTGs with the information that you enter so that they can be automatically activated by a policy or manually activated by a dispatcher.

inband Traffic that is sent inband is included in the same stream as the real-time traffic protocol (RTP). Inband signals can be encoded signals and RFC 2833 signals.

incident management framework A software framework that includes an adaptable GUI to facilitate resources, such as users, radio channels, cameras, and sensor information, for delivery that is based upon policy or incident needs.

informix linux group Members of this group have full permission to Cisco IPICS server folders, files, and scripts that are related to the Informix database application. Members of this group include the informix and ipicsdba users.

informix user ID The Cisco IPICS Linux user that belongs to both the informix linux group, which includes full permission to the Cisco IPICS database server folders, files, and scripts, and the ipics linux group, which includes permission to Cisco IPICS application-related folders, files, and scripts. In addition, this user has full administrative permission to the Informix database instance. Cisco IPICS creates this Linux system user ID and generates the password during the software installation process. The password for this user ID never expires.

To access the informix user, log in to the Cisco IPICS server by using the root user ID; then, enter **su - informix** (superuser from root).

interference The effect of unwanted energy due to one or a combination of emissions, radiation, or inductions upon reception in a radio communication system, manifested by any performance degradation, misinterpretation, or loss of information, which could be extracted in the absence of such unwanted energy.

interoperability The capability of equipment manufactured by different vendors to communicate with each other successfully over a network.

invitation policy A policy that can be invoked only through the telephony user interface and can include only the invite to VTG action. After joining a talk group, a user can access the breakout menu and invoke invitation policies. The talk group that this user has joined is the talk group that the invited users join.

invite to VTG A version of the dial out invite action where users to be invited are preconfigured but the VTG that they are invited to depends on which VTG the invoker of the policy is dialed into.

ipicsadmin user ID The Cisco IPICS Linux user that, as part of the ipics linux group, has full permission to the Cisco IPICS server folders, files, and scripts that are related to the Cisco IPICS application and database backup and restore operations. In addition, the ipicsadmin user has permission to read and write data from and/or to the Informix database. Cisco IPICS creates this Linux system user ID during the software installation process. The password for this user ID never expires.

ipicsdba user ID The Cisco IPICS Linux user that belongs to both the informix linux group, which includes full permission to the Cisco IPICS database server folders, files, and scripts, and the ipics linux group, which includes permission to Cisco IPICS application-related folders, files, and scripts. In addition, the ipicsdba user has permission to read data, write data, create tables, and create databases in the Informix database instance. Cisco IPICS creates this Linux system user ID and generates the password during the software installation process. The password for this user ID never expires.

To access the ipicsdba user, log in to the Cisco IPICS server by using the root user ID; then, enter **su - ipicsdba** (superuser from root).

ipics linux group Members of this group have full permission to Cisco IPICS server folders, files, and scripts that are related to the Cisco IPICS application and database backup and restore operations. Members of this group include the ipicsadmin, ipicsdba, and informix users.

ipics user ID The Cisco IPICS application-level user ID that can perform all administration-related tasks via the Cisco IPICS Administration Console. Cisco IPICS creates this web-based user ID during the software installation process.

IPSec IP Security. A framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer. IPSec uses IKE to handle the negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPSec. IPSec can protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

K

keepalive A message that is sent by one network device to inform another network device that the virtual circuit between the two devices is still active.

key The parameter that defines an encryption code or method.

Key (a radio) causes the radio to transmit. *See* tone keyed.

kilohertz (kHz) A unit of frequency that denotes one thousand Hz.

L

latch The 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.

LLGT low level guard tone. This tone is used as a hold tone or keying tone. *See* guard tone.

LMR Land Mobile Radio. A Land Mobile Radio (LMR) system is a collection of portable and stationary radio units that are designed to communicate with each other over predefined frequencies. They are deployed wherever organizations need to have instant communication between geographically dispersed and mobile personnel.

This term is often used interchangeably between a handheld or vehicle-mounted device and a stationary transmitter. Stationary devices are typically referred to as base stations.

Cisco IPICS leverages the Cisco Hoot 'n' Holler feature, which is enabled in specific Cisco IOS versions, to provide radio integration into the Cisco IPICS solution. LMR is integrated by providing an ear and mouth (E&M) interface to a radio or other PTT devices, such as Nextel phones. Configured as a voice port, this interface provides the appropriate electrical interface to the radio. You configure this voice port with a connection trunk entry that corresponds to a voip dial peer, which in turn associates the connection to a multicast address. This configuration allows you to configure a corresponding channel in Cisco IPICS, using the same multicast address, which enables Cisco IPICS to provide communication paths between the desired endpoints.

LMR gateway Land Mobile Radio gateway. Refers to the router E&M interface that converts IP traffic from digital to analog for use by radios.

location In Cisco IPICS, location signifies reachability; meaning, channels or users who are associated with the same location can communicate with each other without additional network configuration. Location may refer to a physical or virtual location, as defined in the server.

low-band frequency Lower frequency levels in the VHF band, typically 25–50 MHz.

M

megahertz (MHz) A unit of frequency denoting one million Hz.

mixed tone Two tones that are mixed together. DTMF is an example of a mixed tone. To be transmitted properly, tone signals must be mixed with the LLGT. *See* DTMF.

m-lead The mouth portion of the E&M interface. The m-lead is the transmit path of the LMR gateway.

modulation The process, or result of the process, of varying a characteristic of a carrier in accordance with an information-bearing signal.

multicast Single packets that are copied by the network and sent to a specific subset of network addresses. Multicast refers to communications that are sent between a single sender and multiple recipients on a network.

multicast address A single address that may refer to multiple network devices.

multicast address/port Cisco IPICS uses this type of connection to enable the PMC to directly tune in to the multicast channel. Multicast address/port combinations are also used by gateways and RMS components.

multicast pool Multicast IP addresses that are defined as part of a multicast pool. Cisco IPICS allocates a multicast address from this pool of resources when a dispatcher activates a VTG.

multiplexing The combination of two or more information channels on to a common transmission medium. In electrical communications, the two basic forms of multiplexing are time-division multiplexing (TDM) and frequency-division multiplexing (FDM).

multipurpose policy A policy that can include any of the supported actions; may be invoked through the telephony user interface or the Cisco IPICS administration console.

multiselect buttons Provides the ability to select or deselect all channels on the PMC for audio transmission.

mute The functionality that enables a dispatcher to mute a PMC user from talking or transmitting voice on one or more channels. The dispatcher can mute the microphone of the user or both the microphone and the speaker.

mutual aid channel A national or regional channel that has been set aside for use only in mutual aid interoperability situations. Restrictions and guidelines governing usage usually apply.

N

narrowband channels Channels that occupy less than 20 kHz.

National Public Safety Planning Advisory Committee The committee that was established to conduct nationwide planning and allocation for the 821–824 MHz and 866–869 MHz bands.

National Telecommunication and Information Administration The United States executive branch agency that serves as the principal advisor to the president on telecommunications and information policies and that is responsible for managing the federal government's use of the radio spectrum.

near end The device or devices that are physically connected to the Ethernet or an RS-232 link. Compare with far end, which refers to devices on the other side of the broadcast. A base station that is connected to an LMR gateway is a near end device while a handheld radio that receives over-the-air signals from the base station is a far end device.

network An interconnection of communications entities.

NAT Network Address Translation. Provides a mechanism for translating addresses that are not globally unique into globally routable addresses for connection to the Internet.

not activated A VTG state that becomes effective when the Activate button is clicked a second time (to deactivate the channel) or if the connection terminates. No PMC buttons appear highlighted.

notification An action that notifies selected user(s) via email, SMS, pager, or phone. The necessary IDs and phone numbers are configured in the communication preferences for each user. Notifications that are sent via the phone require user authentication before the notification prompt is heard.

An email, SMS, pager, or phone call that is placed to a user for the purpose of sending a notification message.

O

offline mode When the connection to the server goes offline, the PMC enters offline mode. Offline mode enables continuous communication during periods of server downtime. Using offline mode requires at least one successful login to the server.

operator The Cisco IPICS operator is responsible for setting up and managing users, configuring access privileges, and assigning user roles and ops views.

ops view operational view. A Cisco IPICS feature that provides the ability to organize users, user groups, channels, channel groups, VTGs, and policies into different user-definable views across multiple organizations or agencies that normally would not share resources. While ops views are maintained separately by the Cisco IPICS system administrator and/or ops view administrator, this functionality also allows multiple entities to use one Cisco IPICS server to enable resource sharing across multiple ops views, according to business need.

ops view administrator The ops view administrator capabilities include managing and monitoring the activity logs that are filtered by ops views and accessible in the Administration Console (**Administration > Activity Log Management**) window.

OTAR over-the-air re-keying. Provides the ability to update or modify over radio frequency the encryption keys that are programmed in a mobile or portable radio.

P

packet A logical grouping of information that includes a header that contains control information. Usually also includes user data.

packet switching The process of routing and transferring data by using addressed packets so that a channel is occupied during the transmission of the packet only. Upon completion of the transmission, the channel is made available for the transfer of other traffic.

PIM Protocol Independent Multicast. Multicast routing architecture that allows the addition of IP multicast routing on existing IP networks. PIM is unicast routing protocol independent and can be operated in two modes: PIM dense mode and PIM sparse mode.

PIM dense mode One of the two PIM operational modes. PIM dense mode is data-driven and resembles typical multicast routing protocols. Packets are forwarded on all outgoing interfaces until pruning and truncation occurs. In dense mode, receivers are densely populated, and it is assumed that the downstream networks want to receive and will probably use the datagrams that are forwarded to them. The cost of using dense mode is its default flooding behavior. Sometimes called dense mode PIM or PIM DM.

PIM sparse mode One of the two PIM operational modes. PIM sparse mode tries to constrain data distribution so that a minimal number of routers in the network receive it. Packets are sent only if they are explicitly requested at the RP (rendezvous point). In sparse mode, receivers are widely distributed, and the assumption is that downstream networks will not necessarily use the datagrams that are sent to them. The cost of using sparse mode is its reliance on the periodic refreshing of explicit join messages and its need for RPs. Sometimes called sparse mode PIM or PIM SM.

PMC Push-to-Talk Management Center. A standalone PC-based software application that simulates a handheld radio to enable PTT functionality for PC users. This application enables Cisco IPICS PMC end-users, dispatch personnel, and administrators to participate in one or more channels/VTGs at the same time.

PMC ID The unique ID that the Cisco IPICS server generates for each PMC to track requests between the PMC and the server and to verify and manage concurrent PMC usage for licensing requirements.

policy Policies include one or more actions that execute sequentially and can be manually activated via the Cisco IPICS administration console or the telephony user interface. Cisco IPICS provides support for multiple policy types.

policy channel A channel that can be set up by the dispatcher and configured as a designated channel; that is, a channel that is always open to enable your interaction with the dispatcher.

policy execution status An indicator of policy execution success or failure. The Cisco IPICS administration console provides a status for each action under a policy,

portalization A web programming paradigm for customizing the interface and functionality of a client application.

preamble The sequence of tones that precede a transmission. The preamble generally includes the HLGT and the function tone.

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.

The action that keys a radio or causes the radio to transmit. On the Cisco router, the e-lead, or key tone, is used to signal the radio to transmit.

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 control service The logical element in the Cisco IPICS system that can tune a radio to the desired channel without manual intervention. Refers to a serial control entity.

radio equipment Any equipment or interconnected system or subsystem of equipment (both transmission and reception) that is used to communicate over a distance by modulating and radiating electromagnetic waves in space without artificial guide. This equipment does not include microwave, satellite, or cellular telephone equipment.

receive indicator The indicator on the 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.

RFC 2833 The Internet Engineering Task Force (IETF) specification that describes how to carry DTMF signaling, other tone signals, and telephony events in RTP packets. Using RFC 2833 a packet can be compactly composed to play a series of tones, including DTMF, in a specific sequence that includes specified durations and volume levels.

RF repeater An analog device that amplifies an input signal regardless of its nature (analog or digital). Also, a digital device that amplifies, reshapes, retimes, or performs a combination of any of these functions on a digital input signal for retransmission.

RMS router media service. Component that enables the Cisco IPICS PMC to remotely attach to a VTG. It also provides support for remotely attaching (combining) two or more VTGs through its loopback functionality.

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

root user ID The Cisco IPICS Linux user that has access to all files in the Cisco IPICS server. Strong passwords are enforced and Linux operating system password expiration rules apply to this user ID.

RTP Real-Time Transport Procotol. Commonly used with IP networks to provide end-to-end network transport functions for applications that transmit real-time data, such as audio, video, or simulation data, over multicast or unicast network services.

RTCP Real-time Transport Control Protocol. The standard for notifying senders and receivers of important events or transmission statistics. The most common forms of RTCP are the sender report and the receiver report.

S

scanning A subscriber unit feature that automatically allows a radio to change channels or talk groups to enable a user to listen to conversations that are occurring on different channels or talk groups.

script prompts The audio prompts that the dial engine scripts play out during execution and which callers hear when they are interacting with the telephony user interface.

secure channel A channel that is connected to a radio that provides secure (encrypted or scrambled) communications on the Common Air Interface (CAI) side of the radio. (The level of security that is configured in the data network determines the security of the communications between the LMR gateway and a network attached device, such as a PMC or Cisco Unified IP Phone.)

An attribute that is set in the server to indicate that a channel is secure. A PTT channel that is configured as secure cannot be combined with unsecure channels in a VTG.

serial controlled radio A type of control for a radio that uses out-of-band signaling (usually RS-232). *See* radio control service.

service delivery area *See* coverage.

signal The detectable transmitted energy that carries information from a transmitter to a receiver.

skin Skins form the appearance of the PMC. In Cisco IPICS, skins are customizable and available in various options, including 4-channel and 8-channel mouse and touch screen formats.

speaker arbitration The procedure that is used to determine the active audio stream in a Push-to-Talk system.

spectrum The usable radio frequencies in the electromagnetic distribution. The following frequencies have been allocated to the public safety community:

High HF 25–29.99 MHz
Low VHF 30–50 MHz
High VHF 150–174 MHz
Low UHF 406.1–420/450–470 MHz
UHF TV Sharing 470–512 MHz
700 MHz 764–776/794–806 MHz
800 MHz 806–824/851–869 MHz.

spoken names The recorded names that are used for entities, such as channels, channel groups, VTGs, users, user groups, ops views, and policies. The names can be recorded through the policy engine or externally-recorded .wav files that can be uploaded into the system.

squelch An electric circuit that stops input to a radio receiver when the signal being received is too weak to be anything but noise.

statically configured tone control Every stream of data that flows to the LMR gateway can be applied with a preamble and/or guard tone by using a static configuration in the LMR gateway. When traffic is sent on a multicast address, the radio automatically switches (because of the preamble) to the specific radio channel that is requested by the tone control sequence.

stored VTG Also referred to as inactive VTG.

subchannel A channel that shares the same multicast address as another channel or channels. These multiple source streams (channels) may be present on a single radio channel. On the PMC, you access these channels by pressing the channel selector buttons on the radio channel.

subscriber unit A mobile or portable radio unit that is used in a radio system.

system administrator The Cisco IPICS system administrator is responsible for installing and setting up Cisco IPICS resources, such as servers, routers, multicast addresses, locations, and PTT channels. The system administrator also creates ops views, manages the Cisco IPICS licenses and PMC versions, and monitors the status of the system and its users via the activity log files.

system architecture The design principles, physical structure, and functional organization of a land mobile radio system. Architectures may include single site, multi-site, simulcast, multicast, or voting receiver systems.

T

T1 Digital WAN carrier facility. T1 transmits DS-1-formatted data at 1.544 Mbps through the telephone-switching network, using alternate mark inversion (AMI) or binary 8 zero suppression (B8ZS) coding.

T1 loopback Allows mapping from multicast to unicast so that unicast phone calls can be patched into an LMR or into other multicast audio streams. A loopback is composed of two of the available T1 interfaces.

talk group A VTG or a channel.

A subgroup of radio users who share a common functional responsibility and, under normal circumstances, only coordinate actions among themselves and do not require radio interface with other subgroups.

TCP Transmission Control Protocol. A connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack.

TDMA time division multiple access. Type of multiplexing where two or more channels of information are transmitted over the same link by allocating a different time interval (“slot” or “slice”) for the transmission of each channel; that is, the channels take turns to use the link.

terminal A device capable of sending, receiving, or sending and receiving information over a communications channel.

throughput The number of bits, characters, or blocks passing through a data communications system, or a portion of that system.

TIA/EIA-102 standards A joint effort between government and industry to develop voice and data technical standards for the next generation of public safety radios.

tone control The process of using inband tone sequences to change the behavior of a radio end point. An inband tone can be used to control functions, such as modifying (retuning) the radio frequency (RF channel), changing the transmit power level, and monitoring a channel. The most basic form of tone control (tone keyed) is used to key the radio. With the Cisco IPICS solution, the radio that is being controlled is directly connected to the LMR gateway E&M leads.

tone frequency A specific form of a function tone. The tone that is used to signal the radio to select a frequency. These audible tone frequencies are generated in the router and combined in a specific sequence to perform a tone control function.

tone keyed A tone keyed radio requires the presence of a specific tone on the incoming analog (e-lead) port. Without this tone, the radio cannot transmit. The tone is generally used to prevent spurious transmission that may occur because of injected noise.

tone signaling Any form of over-the-air audible signals that are intended to terminate at the far end. Examples include alerting tones, DTMF tones, and paging tones.

transmit indicator On some of the PMC skins, this indicator blinks red when traffic is being transmitted.

trigger A time-based event that invokes a policy on a scheduled basis, without manual intervention.

trunk A physical and logical connection between two switches across which network traffic travels. In telephony, a trunk is a phone line between two central offices (COs) or between a CO and a PBX.

trunked (system) Systems with full feature sets in which all aspects of radio operation, including RF channel selection and access, are centrally managed.

trunked radio system Integrates multiple channel pairs into a single system. When a user wants to transmit a message, the trunked system automatically selects a currently unused channel pair and assigns it to the user, decreasing the probability of having to wait for a free channel.

TUI telephony user interface. The telephony interface that the dial engine provides to enable callers to perform tasks, such as joining talk groups and invoking policies.

tune (a radio) To change the current send and receive frequencies on a radio. This task is usually accomplished via a preset with some form of radio control.

U

user The Cisco IPICS user may set up personal login information, download the PMC application, customize the PMC skin, and specify communication preferences that are used to configure audio devices. By using a predefined user ID and profile, the user can participate in PTT channels and VTGs by using the PMC, supported models of Cisco Unified IP Phones, and the Public Switched Telephone Network (PSTN) via the telephony dial functionality of the Cisco IPICS IP policy engine. Users may have one or more Cisco IPICS roles, such as system administrator, ops view administrator, operator or dispatcher.

unicast Specifies point-to-point transmission, or a message sent to a single network destination.

V

VAD Voice Activity Detection. When VAD is enabled on a voice port or on a dial peer, only audible speech is transmitted over the network. When VAD is enabled on Cisco IPICS, the PMC only sends voice traffic when it detects your voice.

virtual channel A virtual channel is similar to a channel but a radio system may not be attached. By creating a virtual channel, participants who do not use physical handheld radios to call into a VTG become enabled by using the PMC application or a supported Cisco Unified IP Phone model.

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

voice replay A feature that allows the PMC user to replay buffered audio on a per channel basis.

VoIP Voice over Internet Protocol. By digitalizing and packetizing voice streams, VoIP provides the capability to carry voice calls over an IP network with POTS-like functionality, reliability, and voice quality.

volume indicator The volume indicator on the PMC that shows the current volume level on the channel in a graphical format.

volume up/down buttons The buttons on the PMC that let you control the volume level.

VOX Voice-operated transmit. A keying relay that is actuated by sound or voice energy above a certain threshold and sensed by a connected acousto-electric transducer. VOX uses voice energy to key a transmitter, eliminating the need for push-to-talk operation.

VTG virtual talk group. A VTG can contain any combination of channels, channel groups, users, and user groups. A VTG can also contain other VTGs.

VTG add participant An action that adds selected participant(s) to the selected VTG.

W

wavelength The representation of a signal as a plot of amplitude versus time.

wideband channel Channels that occupy more than 20 kHz.

INDEX

A

B

C

D

F

I

L

M

N

O

P

R

S

T

U

V