APPENDIX D

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, see the "Managing Cisco IPICS Options" section on page 2-139.

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 "Backing up the Cisco IPICS Server Database" section on page 9-2.

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 "Restoring Data from a Database Backup" section on page 9-13.

Cisco IPICS Licenses

Q. How are license ports and DS0 loopback port resources counted in Cisco IPICS release 2.2?

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 2.2(x).

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 Appendix A, "Configuring the Cisco IPICS RMS Component." 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, see Appendix A, "Configuring the Cisco IPICS RMS Component."

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, see the Appendix A, "Configuring the Cisco IPICS RMS Component."

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, see Appendix A, "Configuring the Cisco IPICS RMS Component."

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, see Appendix A, "Configuring the Cisco IPICS RMS Component."

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 Appendix A, "Configuring the Cisco IPICS RMS Component."

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 Appendix A, "Configuring the Cisco IPICS RMS Component," 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 "Managing Locations" section on page 2-86.

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 "Managing Locations" section on page 2-86.

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 Chapter 6, "Configuring and Managing Cisco IPICS Operational Views."
- 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, see the “Guidelines for using the TUI” section on page 7-32.

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 the "Configuring SIP" section on page 8-35.

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 "Performing Ops Views Tasks" section on page 6-17.

Q. Which codecs do the dial engine support?

A. The dial engine supports only G.711 u-law. For more information, see Chapter 8, "Configuring and Managing the Cisco IPICS Policy Engine."

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 Actions for a Policy" section on page 7-8.

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, see Chapter 7, "Using the Cisco IPICS Policy Engine."

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, see the "Allocating Dial Ports for the Dial-In/Invite and Notification Features" section on page 6-29.

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, see the "Notifying and Dialing Out to Participants, and Setting PMC Attributes in an Active VTG" section on page 4-28.

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, see Appendix B, "Using Cisco IPICS for External Notifications."

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, see the "Viewing Information about Executing or Executed Policies" section on page 7-26.

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, "Viewing Information about Executing or Executed Policies" section on page 7-26.

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, see Chapter 8, "Configuring and Managing the Cisco IPICS Policy Engine,"and the *Solution Reference Network Design (SRND)* (latest version).

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, see Chapter 8, "Configuring and Managing the Cisco IPICS Policy Engine."

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.*

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 2-41.

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 the Information in the Dashboard Window" section on page 10-2.

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, "Guidelines for Using IP Multicast Addresses with Cisco IPICS" section on page 2-98.

Note Two channels that are in the same location cannot have the same multicast address. For more information, see the "Managing Locations" section on page 2-86.

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 2-41 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 2-41 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 2-41 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 Descriptors” section on page 2-69 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 Chapter 4, “Performing Cisco IPICS Dispatcher Tasks.”

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 Chapter 4, "Performing Cisco IPICS Dispatcher Tasks."

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 Chapter 6, "Configuring and Managing Cisco IPICS Operational Views."

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 viewing ops view ports, see Chapter 6, "Configuring and Managing Cisco IPICS Operational Views."

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 Chapter 6, "Configuring and Managing Cisco IPICS Operational Views."

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 the Information in the Dashboard Window" section on page 10-2.
- 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 Cisco IPICS Server Diagnostic Information" section on page 10-7.
- 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 the Cisco IPICS System Logs" section on page 10-12.

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, "Managing Cisco IPICS Options" section on page 2-139.

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, see Appendix C, "Setting Up and Using a Cisco Unified IP Phone as a Cisco IPICS Push-to-Talk Device."

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, see Appendix C, "Setting Up and Using a Cisco Unified IP Phone as a Cisco IPICS Push-to-Talk Device."

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, see the "Managing Dial Login Information for a User" section on page 3-13.

- 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, see Appendix C, "Setting Up and Using a Cisco Unified IP Phone as a Cisco IPICS Push-to-Talk Device."