CHAPTER 2

Performing Cisco IPICS System Administrator Tasks

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

In addition, the system administrator is responsible for performing backup and restore operations. For more information, see Chapter 9, "Performing Cisco IPICS Database Backup and Restore Operations."

Most of the system administrator activities that you perform are accessible from the Administration Console Configuration and Administration drawers. To access these drawers, log in to the Administration Console as described in the "Accessing the Administration Console" section on page 1-12, then choose the **Configuration** or the **Administration** drawer.

Note You must be assigned the system administrator role to access the Configuration and Administration drawers.

The following sections describe many of the system administrator activities that you can perform from the Cisco IPICS Administration Console:

- Managing PTT Channels and Channel Groups, page 2-2
- Managing Radios, page 2-41

- Managing Radio Descriptors, page 2-69
- Managing the Multicast Pool, page 2-95
- Managing the RMS, page 2-103
- Managing Licenses, page 2-120
- Viewing Active Users, page 2-127
- Managing Activity Logs, page 2-132
- Managing Activity Log Options Per Ops View, page 2-138
- Managing Cisco IPICS Options, page 2-140
- Managing PMC Versions, page 2-155
- Managing PMC Alert Tones, page 2-164
- Managing PMC Skins, page 2-170
- Managing the PMC Installer, page 2-174
- Managing PMC Regions, page 2-176

For information about managing operational views in the Ops Views window, see Chapter 6, "Configuring and Managing Cisco IPICS Operational Views."

For information about managing database backup and restore operations in the Database Management window, see Chapter 9, "Performing Cisco IPICS Database Backup and Restore Operations."

Managing PTT Channels and Channel Groups

A PTT channel, also referred to as a channel, is a communications path that allows users to communicate with each other. A Cisco IPICS channel defines and describes the specific content stream of the channel regardless of the source of that content. Channel connections distinguish one content stream from another, and are determined by location.

A channel carries traffic to and from a VTG, a land mobile radio (LMR) gateway, a PMC, and an IP phone. Remote PMC users can connect to a channel using a unicast SIP connection to an RMS component.

A channel can also refer to a radio control interface (radio or radio channel), which also has an audio stream. For information about managing radios in Cisco IPICS, see the "Managing Radios" section on page 2-41.

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

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

Channel Management Tasks

- Adding a PTT Channel, page 2-7
- Viewing and Editing Channel Details, page 2-8
- Changing the Status of a PTT Channel, page 2-21
- Understanding Association Attribute Behaviors, page 2-22
- Associating PTT Channels to Ops Views, page 2-25
- Associating Users to PTT Channels, page 2-26
- Associating Radio Control Signals to PTT Channels, page 2-28
- Viewing Channel Associations, page 2-30
- Deleting a PTT Channel, page 2-31

Channel Group Management Tasks

- Adding a Channel Group, page 2-33
- Viewing and Editing Channel Group Details, page 2-34
- Viewing Channel Group Associations, page 2-37
- Removing a PTT Channel from a Channel Group, page 2-38
- Associating Ops Views to Channel Groups, page 2-39
- Deleting a Channel Group, page 2-40

You perform the PTT channel management tasks in the Channels and Channel Groups windows, located in the Configuration drawer of the Administration Console. For more information about these windows, including how to access them, see the "Understanding the Channels Window" section on page 2-4 and the "Understanding the Channel Groups Window" section on page 2-31.

Understanding the Channels Window

The Channels window lists information about each of the channels that you have added in Cisco IPICS.

The bottom area of this window displays a list of Cisco IPICS channels and general information for each channel. By default, this area displays all channels, but you can choose to display only channels that match search criteria that you specify in the top area of the window.

Note You can specify the number of rows of channels that display per results page by choosing from the Rows per page drop-down list box at the top right of the window. To navigate between the results pages, click the arrows at the bottom of the window; then click **Go**.

This window also enables you to perform several channel management functions. To display the Channels window, access the Configuration drawer; then click **Channels**.

Table 2-1 describes the items in the Channels window.

Table 2-1 Items in the Channels Window

Item	Description	Reference
Filter		
Channel Name field	This field allows you to display only channel names that include the character string that you enter (characters are not case-sensitive).	To limit the display of channels or to display a certain channel, enter the desired search criteria in the filter field; then, click **Go**.
Ops View drop-down list box	This field allows you to display only channels for which the associated ops view matches the information that you choose.	
Go button	Click this button to display channels by the filters that you choose.	
Clear Filter button	Click this button to remove filter selections and display an empty list of channels. Click the **Channels** link again to display the full list of entries.	
Channel Information		
Channel Name field	This field indicates the unique identifier that is assigned to the channel.	See the "Viewing and Editing Channel Details" section on page 2-8 and the "Adding a PTT Channel" section on page 2-7
Ops View field	This field indicates the ops view to which the channel belongs.	See the "Associating PTT Channels to Ops Views" section on page 2-25
Secure field	This field indicates whether the channel is secure.	See the "Viewing and Editing Channel Details" section on page 2-8

Table 2-1 Items in the Channels Window (continued)

Item	Description	Reference
VTG field	This field indicates whether the channel is allowed in a Virtual Talk Group (VTG).	See the "Viewing and Editing Channel Details" section on page 2-8 and the "Adding a PTT Channel" section on page 2-7
Users field	This field indicates whether the channel is allowed to be associated to users to affect all endpoints such as the PMC and IP phone.	
Channel Status field	This field indicates whether the channel is enabled, disabled, or active.	See the "Changing the Status of a PTT Channel" section on page 2-21
Prompt field	This field indicates whether a spoken name prompt is recorded for the channel. This prompt plays for a user when the user logs in to the Cisco IPICS telephony user interface. You can record the spoken name prompt for a user by clicking the **Not Recorded** or the **Recorded** link in the Prompt column. When you click a link in the Prompt column, the Spoken Names window displays.	See Chapter 8, "Configuring and Managing the Cisco IPICS Policy Engine"
Add button	Click this button to add a new channel in Cisco IPICS.	See the "Adding a PTT Channel" section on page 2-7
Delete button	Click this button to delete the specified channel(s).	See the "Deleting a PTT Channel" section on page 2-31
Change Status drop-down list box	Choose from the enable or disable option to change the status of a channel.	See the "Changing the Status of a PTT Channel" section on page 2-21

Table 2-1 Items in the Channels Window (continued)

Item	Description	Reference
Associations button	Click this button to view associations for the specified channel.	See the "Associating Users to PTT Channels" section on page 2-26, the "Viewing Channel Associations" section on page 2-30, and the "Associating Radio Control Signals to PTT Channels" section on page 2-28
Display Controls		
Rows per page drop-down list box	Specifies the number of rows of channels that are included in a channels list page.	See the "Navigating Item Lists" section on page 1-16
Page field	Displays channels on a specific page.	
|< (First page) button	Displays the first page of the channels list.	
< (Previous page) button	Displays the previous page of the channels list.	
> (Next page) button	Displays the next page of the channels list.	
>| (Last page) button	Displays the last page of the channels list.	

Adding a PTT Channel

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

Before you add a PTT channel, configure locations as described in the "Adding Descriptors" section on page 2-82.

To add a new channel, perform the following procedure:

Procedure

Step 1 From the Cisco IPICS Administration Console, navigate to the **Configuration > Channels** window.

Step 2 In the Channels window, click **Add**.

The General tab for a new channel displays.

Step 3 Follow the steps in the "Viewing and Editing Channel Details" section on page 2-8.

Step 4 Enter appropriate information in the Ops Views fields as described in the "Configuring and Managing Cisco IPICS Operational Views". This field is optional.

Step 5 Click **Save** to add the channel without exiting the current window.

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

Viewing and Editing Channel Details

You can view and edit information for any channel.

To view or edit channel details, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Channels** window.

Step 2 In the Channel Name column, click the link for the channel for which you want to view or change information.

The General tab for the selected channel displays. This window contains general information for that channel. Table 2-2 provides descriptions of the fields in the General tab.

Note If an endpoint, such as the PMC or dial engine, does not support the attributes that are described in Table 2-2, the attributes do not display in the General tab of the Channels window.

Table 2-2 General Tab Fields in Channels Window

Field	Description
Channel Information	
Name	This field represents the name of the channel. The name can include alphanumeric characters, spaces, and any of these characters: “. , – ‘ # ( ) / :_”. Choose a unique and recognizable name that accurately describes the PTT channel. It is often helpful to name the PTT channel according to the department or organization that use it, or for a particular geographic region (for example *Fire Department* or *North Area*). **Note** The PMC may truncate the channel name if the name includes more characters than the PMC can display.
Short Name	This field represents the condensed name of the channel. The name can include alphanumeric characters, spaces, and any of these characters: “. , _ ‘ # ( ) / :_”.
Description—*Optional*	This field allows you to enter a description for this channel.

Table 2-2 General Tab Fields in Channels Window (continued)

Field	Description
Secure Channel	This drop-down list box allows you to specify whether this channel is a secure channel. This field is for reference only and should be set to reflect the configuration of the channel in your network. Changing this setting does not affect the security configuration of the channel. **Note** This field displays as read-only if the channel is a participant in an active VTG, an active PMC user is associated with this channel, or if a user has activated this channel via an IP phone or PSTN phone. To make the field editable, either disable the channel, or deactivate the VTG of which the channel is a participant.
Allow association to users	This check box allows you to indicate whether this channel is available to all Cisco IPICS users. Use this option to prevent certain channels from being associated to users. If the channel is configured to disallow association to a user (attribute check box is not checked), the channel does not display as available to users in the User window and it is not available on the PMC. In addition, the User tab, in the channel Association window, does not display. **Note** If you change the channel status such that a channel that was previously associated with a user is no longer associated with a user, Cisco IPICS automatically removes the channel associations from the users. This check box is checked by default upon creation of the channel.

Table 2-2 General Tab Fields in Channels Window (continued)

Field	Description
Allow use in VTGs	This check box allows you to indicate whether this channel is an available resource for participation in a VTG. Use this setting to prevent certain channels from being included in a VTG. For example, a PMC user who interacts with a another user may wish to hear all the call progress tones that the other user’s handset generates, to give feedback when a radio channel is available. These types of progress tones can be assigned to this channel. Because the tones can be disruptive, however, you might not want to add this type of channel to a VTG with a large group of users; therefore, when you create this channel, you would disallow its use in VTGs. If the channel is configured to disallow this channel in a VTG (attribute check box is not checked), the channel does not display in the Resources area of the VTGs in the VTG Management window and is not available for participation in VTGs. The channel can, however, display as available for association to users and user groups, in the User and User Groups windows. If you change the channel such that it is no longer allowed in a VTG, the channel remains active in any current VTG to which it is a participant. However, the channel is not allowed to join any other VTG. **Note** This attribute is checked by default upon creation of the channel.

Table 2-2 General Tab Fields in Channels Window (continued)

Field	Description
Status—*Display only*	This field displays one the following channel states: • Active—Channel is connected to a VTG. • Enabled—Channel is available (channel can be connected to a VTG) and PMC clients can use the channel. • Disabled—Channel is not in use and PMC clients cannot use the channel (it is dimmed), and the channel cannot be connected to a VTG. You can still modify connection attributes on the channel.
Media Connection Assignments	
Type	This field specifies the type of connection that Cisco IPICS and devices use to connect to this channel when connecting from the corresponding location. Choose one of the following options from the drop-down list box: • **Multicast**—If you choose a multicast connection type, you must configure a location, address, and a port for the connection type. • **Radio**—If you choose a radio device type, you can choose a specific radio from a drop-down list box and the channel selector for that radio connection. The channel selector that you choose maps the channel short name to the selector on the radio instance. The Radio options appears only if you have configured one or more tone control radios and have enabled one or more channel selectors for a tone control radio.

Table 2-2 General Tab Fields in Channels Window (continued)

Field	Description
Location	This field displays when you choose a multicast connection type from the Type drop-down list box. Channels or users who are associated with the same location are reachable within a multicast network boundary. Therefore, users who are in the same multicast domain are also in the same Cisco IPICS location. Remote, SIP-based users are not in the same location as multicast users. Remote users connect by establishing connectivity with the appropriate RMS via a SIP-based unicast connection for each channel or VTG that has been assigned to the user. **Note** Channels achieve media connectivity by being mapped to a multicast address and port in a location. A channel can be assigned to multiple locations. In this case, a channel can have more than one media connection. The media connection count in the **Serviceability > Dashboard** window reflects the total number of media connections. See the "Viewing the Information in the Dashboard Window" section on page 10-2 for more information about the Dashboard window. If the network is configured so that the channel can be accessed by users in every location, set this value to **All**. See the "Adding Descriptors" section on page 2-82 for more detailed information about how to configure locations.

Table 2-2 General Tab Fields in Channels Window (continued)

Field	Description
Address	This field displays when you choose a multicast connection type from the Type drop-down list box. This field specifies the multicast address, in the corresponding location, that is used to connect to this channel. **Note** 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, see the "Guidelines for Using IP Multicast Addresses with Cisco IPICS" section on page 2-98. Two channels in the same location cannot have the same multicast address. See the "Managing Locations" section on page 2-86 for more detailed information about locations.
Port	This field displays when you choose a multicast connection type from the Type drop-down list box. This field specifies the multicast address port number, in the corresponding location, that is used to connect to this channel. **Note** This value must be an even number in the range of 21000 through 65534. Cisco IPICS does not allow the configuration of ports below 21000 or any odd ports.

Table 2-2 General Tab Fields in Channels Window (continued)

Field	Description
Codec	This drop-down list box allows you to choose the codec (G.711 or G.729) that is used by this connection. Use G.711 if this connection should be available to Cisco Unified IP Phone users or if it is part of a VTG. Use G.711 or G.729 if this connection is available to PMC users. G.729 requires digital signal processor (DSP) resources for transcoding. **Note** You cannot edit the codec and media connection attributes if users who are associated to the channel are logged in to an IP phone or a PMC. For more information about codecs, refer to the *Solution Reference Network Design (SRND)* (latest version).
Radio	This drop-down list box displays when you choose a radio device type from the Type drop-down list box.

Table 2-2 General Tab Fields in Channels Window (continued)

Field	Description
Channel Selector	This field displays when you choose a radio device type from the Type drop-down list box. Choose a channel selector from the drop-down list box. **Note** You cannot configure multiple channels on the same radio with the same channel selector. However, a channel can have more than one radio connection for a given radio. That is, a radio has more than one control sequence to tune to the same content. For more information about radios, see the "Managing Radios" section on page 2-41. Each channel can have a specific set of signaling (over-the-air) tones that need to be broadcast over the radio. When a user is associated with the channel, any signaling tones that are defined for that channel are available for use by the PMC in that channel. The PMC user must use the radio-centric skin to see radio channels signaling tones. By using this skin, the PMC user can transmit tones over the channel. **Tip** When you define channel selectors, consider the different actions that users may want to perform on the channel, such as tuning the radio or beginning a transmission over-the-air. These actions determine the commands that are sent to the radio when the user invokes the action by pressing the button on the channel. For more information about the PMC, refer to the *Cisco IPICS PMC Installation and User Guide.*

Table 2-2 General Tab Fields in Channels Window (continued)

Field	Description
Ops Views	
Belongs To	This drop-down list box allows you to choose the ops view to which you want to associate this channel. See the "Associating PTT Channels to Ops Views" section on page 2-25 for detailed information. **Note** To associate a channel to an ops view, you must belong to the SYSTEM ops view. For general information about ops views, see Chapter 6, "Configuring and Managing Cisco IPICS Operational Views."
Accessible To	This drop-down list box allows you to choose the ops views to which you want this channel to be accessible. See the "Associating PTT Channels to Ops Views" section on page 2-25 for information about how to associate ops views to channels. For general information about ops views, see Chapter 6, "Configuring and Managing Cisco IPICS Operational Views."
Edit button	Click this button to make this channel accessible to other ops views. **Note** This button does not display if there are no additional ops views configured in Cisco IPICS. See the "Associating PTT Channels to Ops Views" section on page 2-25 for more information. For general information about ops views, see Chapter 6, "Configuring and Managing Cisco IPICS Operational Views."

Step 3 To view the PMC details for this channel, click the **PMC** tab.

The PMC tab for the selected channel displays. This window contains PMC information for the selected channel. Table 2-3 provides descriptions of the fields in the PMC tab.

Note Be aware that some options in Table 2-3 apply to all end devices in Cisco IPICS and not only to the PMC.

Table 2-3 PMC Tab Fields in Channels Window

Field	Description
PMC	
RX Mute During PTT	The following values affect how the RX mute functionality is configured on the PMC: • None—When PTT is engaged, the channel is muted. • All—When PTT is engaged, RX (receive transmission) is muted on all channels. • Channel—When PTT is engaged, RX is muted for this channel only. **Note** When you initially assign a channel to the PMC, the RX mute settings that you have configured apply. The PMC user can modify this setting. However, if you change the setting after the channel has been assigned to the user, the changes do not become effective.
Enable Voice Activity Detection (VAD)	When you enable VAD on Cisco IPICS, the PMC only sends voice traffic when it detects a voice packet. When this attribute is set to true (attribute check box is checked) on a channel/VTG, VAD is used by the PMC while communicating with the channel/VTG. By default, this attribute is set to true (attribute check box is checked).

Table 2-3 PMC Tab Fields in Channels Window (continued)

Field	Description
Allow Latch	When set to true (attribute check box is checked) on a channel/VTG, the user can use latch to lock in the channel. By default, this attribute is set to false (attribute check box is unchecked). **Note** If your Cisco IPICS server is running release 2.0(2) and you upgrade to release 2.2(1), any existing channels and VTGs maintain their values for latch, even if set to true.
Listen Only	When set to true (attribute check box is checked), the user can hear, but cannot talk, on the channel.
Channel Color	This attribute specifies a color tag that you can choose from a drop-down list box. This setting uniquely identifies specific channels by using predefined colors for the background text that appears on the channel. You configure the color by choosing from the options in the drop-down list box. **Note** If you do not want the channel to be tagged with a color, you can choose **Not colored** from the drop-down list box.
Channel Region	Choose the channel region that displays on the PMC from the drop-down list box. For information about configuring PMC regions, see the "Managing PMC Regions" section on page 2-176.

Step 4 To view channel associations, click the **Associations** button that displays at the bottom of the window.

Step 5 To view channel associations, from the Associations window take either of the following actions:

- Click the **Users** tab—This tab displays the Cisco IPICS users who are associated to this channel.

The users who are currently associated to this channel display. The Users window lists information about each of the users who are associated to the channel.

Table 2-4 describes the items in the Users window.

Table 2-4 Items in the Users Window

Item	Description
User Name field	This field specifies the unique identification name assigned to the user.
Last Name field	This field specifies the last name of the user.
First Name field	This field specifies the first name of the user.
Status field	This field indicates whether the user is enabled or disabled.
Association Attributes	
Latchable field	This field indicates whether the user can latch (lock in) channels on end devices.
Disable Audio field	This field indicates whether audio is disabled on end devices.
Listen Only field	This field indicates that the user is restricted to listening only on the channel; no transmission is allowed.

Note User association values are appended with a superscript (1) if they are configured as a customized value. See the "Understanding Association Attribute Behaviors" section on page 2-22 for more information about association attribute behaviors.

You can associate additional users to the channel, by performing the steps in the"Associating Users to PTT Channels" section on page 2-26.

- Click the **Virtual Talk Groups** tab—This tab displays the VTGs in which this channel participates.

Step 6 From the Users tab, you can change the PMC status for a user by checking the check box next to selected users.

The Change End Device Status drop-down list box becomes active.

Note The Change End Device Status drop-down list box becomes available only after you have checked the check box next to one or more user names. If you do not check the check box, the Change End Device Status drop-down list box appears dimmed.

Step 7 From the Change End Device Status drop-down list box, choose one of the available options:

- **Allow Latch**—User can latch, or lock in, channels
- **Disallow Latch**—User cannot latch channels
- **Set Listen Only**—User can only listen on the channel; transmission is not allowed
- **Unset Listen Only**—User can listen and transmit on the channel
- **Enable Audio**—Audio is enabled
- **Disable Audio**—Audio is disabled

Note Be aware that when you choose the Disable Audio feature from any location in the Cisco IPICS server, the audio on all end user devices (PMC, IP phones), except for radios, is disabled.

Changing the Status of a PTT Channel

Cisco IPICS allows you to change the status (enable/disable) of a channel from either the main Channels window, or in the individual channel configuration windows.

When you change the status of a channel affects whether the channel is available to the PMC, IP phones, dialed-in users, or whether the channel can connect to a VTG. If the channel is disabled, it cannot be connected to a VTG.

For more information about the PMC, refer to the *Cisco IPICS PMC Installation and User Guide.*

A channel can be configured as enabled or disabled.

You can change the status of a single channel, or you can change the status of several channels at one time.

To determine the current status, access the Configuration drawer, click **Channels**, and look at the information in the Status column for the channel.

To change the status of a channel from the main Channels window, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Channels** window.

Step 2 Take either of these actions:

- Click the link for the channel in the Channel Name column to display the configuration window for the channel, click **Enable** or **Disable**; then, click **Save**.

  The **Enable** or **Disable** button appears at the bottom of the channel configuration window. The name of the button depends on the current status of the channel.

- In the Channels window, check the check box next to each channel for which you want to change the status, then choose the desired action (**Enable** or **Disable**) from the Change Status drop-down list box.

Understanding Association Attribute Behaviors

Users, channels, and VTGs have attributes that control their behavior. In some cases, these resources may have the same attribute behaviors, so that when you associate channels to users, or users to VTGs, the system determines the resulting PMC behavior by how the attributes are configured for each associated resource. For an example of association attribute behaviors, see the "User-Channel Association Example" section on page 2-23.

Cisco IPICS allows you to override the resulting behaviors for specific associations. When you modify channel or user attributes that are part of an association, the resulting behavior depends on the attribute settings for users within the association. Typically, when resources are part of an association, any attribute changes to the resources also apply to the resource and associations within that resource. Resource attributes may have different settings when they are not part of an association.

The following section provides an example of some of the expected system behaviors when you configure user, channel, and VTG associations.

Changes to channel, user, or VTG attributes that are also present in associations, behave differently, depending on the override status. If the association is not overridden you are prompted to remove the overrides. An example of some association attribute behaviors is described below.

Note The example in the "User-Channel Association Example" section on page 2-23 is also applicable to user-VTG associations.

To associate an ops view to a channel, see the "Associating Users to PTT Channels" section on page 2-26.

User-Channel Association Example

The following example describes different user-channel association scenarios that can be performed by a Cisco IPICS operator and a system administrator:

- User A is allowed to latch (the Allow Latch attribute check box is checked).
- Channel A is not allowed to latch (the Allow Latch check box is not checked).
- The Cisco IPICS operator associates User A to Channel A.

  The resulting behavior for this association is that User A is not allowed to latch on Channel A on the PMC. On the server side, the Allow Latch attribute displays as **No** for both the user and the channel for this association, in the Latchable column in the Associations tab.

  Note This behavior results because the Allow Latch setting, for both the user and the channel, must have the same value for latching to be allowed in this association. In this example, the value for Allow Latch must be **Yes**.

- You decide to allow all users to latch on Channel A, so you change the Allow Latch attribute on the channel by checking the Allow Latch check box in the **Channels > PMC** window. Because the association settings have not been customized, Cisco IPICS automatically updates the User A-Channel A association. The PMC updates to allow latching on this channel for this association.
- The operator disallows latch on Channel A by navigating to the Association tab (for Channel A), selecting all of the users, clicking **Change End Device Status**, and selecting the Allow Latch menu item.

  Cisco IPICS marks this attribute as a customized value.

Note A superscript (1) displays next to the value in the Latchable column in the Associations tab, for both the user and the channel. The superscript indicates a customized value, meaning that the previous value of the attribute in the association has been overridden.

  After the PMC updates, users in this association can no longer latch on Channel A.
- You decide to allow all users to latch on Channel A and you check the Allow Latch check box in the PMC tab for the channel. Because the association had previously been marked as a customized value the system prompts you with a message stating that this action overrides the custom PMC settings for Latch.

  If you click OK to the message, the overrides are removed and latching on Channel A, for this association, is allowed on the PMC.

See the "Viewing and Editing Channel Details" section on page 2-8 for more information about the specific channel attributes.

For information about associating a channel to a user or ops view, see the "Associating Users to PTT Channels" section on page 2-26.

For more information about the PMC, refer to the *Cisco IPICS PMC Installation and User Guide.*

Associating PTT Channels to Ops Views

You can associate a channel to an ops view in the General tab of an individual window for a channel. When you associate a channel to an ops view, the channel can be seen by the users who belong to that particular ops view.

For more information about the Accessible To and Belongs To attributes for ops views, see Chapter 6, "Configuring and Managing Cisco IPICS Operational Views."

To associate a channel to an ops view, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Channels** window.

Step 2 In the Channel Name column, click the link for the channel that you want to make accessible to an ops view.

Step 3 In the General tab, click the **Edit** button that appears in the Ops View pane.

The Ops View to Channel Association window displays the following information:

- Available Ops Views—Ops views that can be made accessible to this channel
- Associated Ops Views—Ops views to which this channel is currently accessible

Step 4 Take any of the following actions:

- To move an ops view from one list to the other, click the ops view to highlight it; then, click **>** or **<**, or double-click the ops view.
- To move several ops views from one list to the other at one time, press **Shift+click** or **Ctrl+click** to select the ops views; then, click **>** or **<**.
- To move all ops views from one list to the other at one time, click **>>** or **<<**.

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

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

The ops views that you chose display in the Accessible To: field in the individual window for the channel.

Step 6 To change the ops view to which this channel belongs, choose an ops view from the Belongs To: drop-down list box.

Step 7 Click **Save**.

Associating Users to PTT Channels

You can associate specific users to a channel in the Associations window. When you associate channels with a user, the channels that you choose appear as options on a PMC or a Cisco Unified IP Phone that has been configured for use with Cisco IPICS.

To determine the ops views to which the channels are currently associated, access the Configuration drawer, click **Channels**, and look at the information in the Ops View column for the channels.

Note You can perform this procedure only if users have already been added in Cisco IPICS.

System administrators and operators who belong to an ops view that is associated to a channel can associate other users to the channel, and add the channel to VTGs, as long as the Allow in association to users and Allow use in VTGs check boxes are checked. See the "Adding a PTT Channel" section on page 2-7 for more information.

To associate users to channels, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Channels** window.

Step 2 Take either of these actions to display the Associations window for the channel with which you want to associate users:

- Click the link for the channel in the Channel Name column, then click the **Associations** button, which appears at the bottom of each tab.

- Check the check box to the left of the Channel Name of the channel, then click the **Associations** button at the bottom of the Channels window.

Note The Associations button is dimmed if you do not check a channel or if you check more than one channel.

In the Associations window, make sure that the **Users** tab is selected.

This tab shows a list of the users who are associated with the channel, the status of each user, and information about attributes for devices that the user is using.

Step 3 Click **Add**.

The Search Users window displays. This window allows you to search for users to associate to the channel by choosing criteria based on the following filters:

- User Name field—Specifies the user name of a user
- First Name field—Specifies the first name of a user
- Last Name field—Specifies the last name of a user
- Location drop-down list box—Choose from a list of locations

  See the "Adding Descriptors" section on page 2-82 for detailed information about how to configure locations.
- Role drop-down list box—Choose from a list of Cisco IPICS roles
- Ops View drop-down list box—Choose from a list of ops views

Step 4 To search for a user, enter your search criteria; then, click **Go**. To clear your criteria, click **Clear Filter**.

Note To display all the users in Cisco IPICS, click the **Go** button without entering any search criteria.

The results of your search criteria display in a list.

Step 5 To choose a user to associate to the channel, check the check box to the left of the user name and click **OK**.

The user that you choose displays in the user list in the Users tab.

Step 6 To change the status of an end device for a user, see Step 7 in the "Viewing and Editing Channel Details" section on page 2-8.

Step 7 To delete a user from this channel association, check the check box to the left of the user and click **Delete**.

Step 8 To view the VTGs in which the channel participates, click the **Virtual Talk Groups** tab.

If the channel participates in a VTG, the VTG name and status displays.

Associating Radio Control Signals to PTT Channels

You can associate specific radio control functions to channels in the channel Associations window. When you associate signals to channels, the specific functions that the signals perform appear as options on the PMC for that channel.

Each channel can be associated with one or more signals. Users who are associated with channels can send signals from the PMC.

You can associate signals with a channel that is not associated with a radio, such as another type of tone-controlled device. For example, you could have a Cisco IPICS PTT channel that includes an LMR gateway that is connecting to a tone-controlled device that is not a radio, such as a device that opens a gate. This type of device can interpret tones and perform specific actions.

When the PMC plays the RFC 2833 and RFC 2198 signals, the LMR gateway detects these signals (in this example, the open gate signal) and converts them into audio. This audio gets sent to the devices that open the gate which triggers them to activate. No radio is present in this scenario. The devices are directly connected to the E&M interface on the LMR gateway.

Unlike alerting tones that cannot be restricted to a specific channel, you can associate signals directly with specific channels. This flexibility gives you the ability to control the appearance of and the ability to play out signals to the appropriate channel(s).

Note To view the signals that are defined for a particular channel, users who are associated with the channel must use the radio-centric skin for their PMC clients. For more information, refer to the *Cisco IPICS PMC Installation and User Guide.*

To associate signals to channels, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Channels** window.

Step 2 Take either of these actions to display the Associations window for the channel with which you want to associate users:

- Click the link for the channel in the Channel Name column, then click the **Associations** button, which appears at the bottom of each tab.
- Check the check box to the left of the Channel Name of the channel, then click the **Associations** button at the bottom of the Channels window.

Note The Associations button appears dimmed if you do not check a channel or if you check more than one channel.

Step 3 In the Associations window, click the **Signals** tab.

This tab shows a list of the signals that are associated with the channel, and includes the short name, description, and where it originated.

Step 4 Click **Add**.

The Search Signals window displays. This window allows you to search for additional signals to associate to the channel.

Step 5 To add a signal, check the check box to the left of the signal name; then, click **OK**.

Step 6 To delete a signal from this channel association, check the check box to the left of the signal name and click **Delete**.

Step 7 To view the VTGs in which the channel participates, click the **Virtual Talk Groups** tab.

If the channel participates in a VTG, the VTG name and status displays.

Step 8 To view the users who are associated with the channel, click the **Users** tab.

To associate users to the channel, see the "Associating Users to PTT Channels" section on page 2-26.

Viewing Channel Associations

You can view channel associations by performing the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Channels** window.

Step 2 To view channel associations, take either of these actions:

- Click the link for the channel in the Channel Name column; then, click the **Associations** button, which appears at the bottom of each tab.
- Check the check box to the left of the Channel Name; then, click the **Associations** button at the bottom of the Channels window.

Note The Associations button appears dimmed if you do not check a channel or if you check more than one channel.

Step 3 From the Associations window, you can view the associations for the channel by clicking either of the following tabs:

- **Users**—View users who are associated with this channel and associate other users to the channel.

Note To associate other users to the channel, see the "Associating Users to PTT Channels" section on page 2-26.

- **Virtual Talk Groups**—View the VTGs in which this channel participates.
- **Signals**—View the radio signals that are associated with this channel and associate other signals to the channel.

Note To associate other signals to the channel, see the "Associating Radio Control Signals to PTT Channels" section on page 2-28.

Deleting a PTT Channel

If a PTT channel is no longer needed, you can delete it from Cisco IPICS. You can delete a single channel or you can delete several channels at one time.

To delete a channel, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Channels** window.

Step 2 Check the check box next to each channel that you want to delete.

Step 3 Click **Delete**.

A dialog box prompts you to confirm the deletion.

Step 4 To confirm the deletion, click **OK**.

If you do not want to delete the channel(s), click **Cancel**.

Understanding the Channel Groups Window

The Channel Groups window lists information about each of the channel groups that you have added in Cisco IPICS.

The bottom area of this window displays a list of Cisco IPICS channel groups and general information for each channel group. By default, this area displays all channel groups, but you can choose to display only channel groups that match search criteria that you specify in the top area of the window.

Note You can specify the number of rows of channel groups that display per results page by choosing from the Rows per page drop-down list box at the top right of the window. To navigate between the results pages, click the arrows at the bottom of the window; then click **Go**.

This window also provides you with the ability to perform several channel group management functions.

To display the Channel Groups window, access the Configuration drawer and click **Channel Groups**.

Table 2-5 describes the fields in the Channel Groups window.

Table 2-5 Fields in the Channel Groups Window

Field	Description	Reference
Filter		
Name field	Allows you to display only channel group names that include the character string that you enter (characters are not case-sensitive)	To limit the display of channel groups or to display a certain channel group, enter the desired search criteria in the filter field; then, click **Go**.
Ops View drop-down list box	Allows you to display only channel groups for which the associated ops view matches the information that you choose	
Go button	Displays channel groups by the filters that you choose	
Clear Filter button	Removes filter selections and displays an empty list of channel groups	
Channel Group Information		
Channel Group Name field	Name that is assigned to the channel group	See the "Viewing and Editing Channel Group Details" section on page 2-34 and the "Removing a PTT Channel from a Channel Group" section on page 2-38
Ops View field	Ops view to which the channel group belongs	See the "Associating Ops Views to Channel Groups" section on page 2-39
Add button	Allows you to add a new channel group in Cisco IPICS	See the "Removing a PTT Channel from a Channel Group" section on page 2-38
Copy button	Allows you to copy information from an existing channel group when you add a new channel group	

Table 2-5 Fields in the Channel Groups Window (continued)

Field	Description	Reference
Delete button	Allows you to delete a channel group	See the "Deleting a Channel Group" section on page 2-40
Associations button	Displays the Associations window for a channel group	See the "Associating Ops Views to Channel Groups" section on page 2-39 and the "Viewing Channel Group Associations" section on page 2-37
Display Controls		
Rows per page drop-down list box	Specifies the number of rows of channel groups that are included in a channel groups list page	See the "Navigating Item Lists" section on page 1-16
Page field	Displays channel groups on a specific page	
|< (First page) button	Displays the first page of the channel groups list	
< (Previous page) button	Displays the previous page of the channel groups list	
> (Next page) button	Displays the next page of the channel groups list	
>| (Last page) button	Displays the last page of the channel groups list	

Adding a Channel Group

A channel group enables you to organize channels. You may find it useful to create and name channel groups according to location (for example, South Area Fire Department PTT Channel) or function (for example, Maintenance PTT Channel).

To create a channel group, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Channel Groups** window.

Step 2 In the Channel Groups window, take either of these actions:

- To add a channel group starting with a blank New Channel Group window, click **Add**.
- To copy an existing channel group, check the check box next to the existing channel group; then click **Copy**.

Note The **Copy** button appears dimmed if you do not check an existing channel group or if you check more than one existing channel group.

The New Channel Group window displays. If you clicked Copy, this window includes information from the existing channel group, except for the channel group name.

Step 3 In the General tab, enter information for the channel group as described in the "Viewing and Editing Channel Group Details" section on page 2-34, starting with Step 3.

Note You do not need to perform all of these tasks now. You can enter or update much of this information later.

Step 4 Click **Save** to add the channel group without exiting the current window.

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

For information about how to associate channel groups to a VTG, see the "Managing VTGs" section on page 4-2.

Viewing and Editing Channel Group Details

You can view information about and edit any channel group in your Cisco IPICS network, including adding new channel members to the channel group.

To add a new channel group, see the "Adding a Channel Group" section on page 2-33.

To view and edit channel group details, and add channel members, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Channel Groups** window.

Step 2 In the Channel Group Name column, click the link for the channel group that you want to view or edit.

The General tab for channel groups displays. This window contains general information for that channel group.

Step 3 To view or update general information for a channel group, click the **General** tab. Table 2-6 provides a description of the fields in the General tab.

Table 2-6 General Tab Fields in Channel Groups Window

Field	Description
Channel Group Information	
Channel Group Name	Name of the channel group. The name can include alphanumeric characters, spaces, and any of these characters: ". , – ' # ( ) / :_".
Description	*Optional*. Description of the channel group
Ops View	
Belongs To	Name of the ops view to which you want to associate this channel group. For general information about ops views, see Chapter 6, "Configuring and Managing Cisco IPICS Operational Views."

Table 2-6 General Tab Fields in Channel Groups Window (continued)

Field	Description
Accessible To	Name of the ops view to which you want this channel group to be accessible. For general information about ops views, see Chapter 6, "Configuring and Managing Cisco IPICS Operational Views."
Edit button	Click this button to associate ops views to the channel group. See the "Associating Ops Views to Channel Groups" section on page 2-39 for detailed information. **Note** To associate a channel group to an ops view, you must belong to the SYSTEM ops view.

Step 4 To view or update members who are associated with this channel group, click the **Members** tab. Table 2-7 provides a description of the fields in the Members tab.

Table 2-7 Member Tab Fields in the Channel Groups Window

Field	Description
Channel Name	Specifies name of the channel member
Ops View	Specifies ops view to which the channel member belongs
Secure	Indicates whether the channel member is configured as a secure channel
VTG	Indicates whether the channel is configured to be used in a VTG
Users	Indicates whether the channel is configured to be associated with users
Channel Status	Indicates whether the channel is enabled or disabled

Step 5 To add additional channel members to the channel group, click the **Add** button.

The Search Channels window displays. This window allows you to search for channels to add as members by choosing criteria based on the following filters:

- Name field—Allows you to enter a channel name

- Ops View drop-down list box—Allows you to choose from a list of ops views

Step 6 To search for a channel, enter your search criteria; then, click **Go**. To clear your criteria, click **Clear Filter**.

Note To display all the channels in Cisco IPICS, click the **Go** button without entering any search criteria.

You search results display in a list.

Step 7 To choose a channel to add as a member to the channel group, check the check box to the left of the channel name and click **OK**.

The channel that you choose displays in the channel members list in the Members tab.

To view current channel group associations, see the "Viewing Channel Group Associations" section on page 2-37.

Viewing Channel Group Associations

To view channel group associations, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Channel Groups** window.

Step 2 In the Channel Group Name column, click the link for the channel group for which you want to view associations.

The General tab for channel groups displays.

Step 3 To view current channel group associations, take either of the following actions:

- Check the check box of the channel group name; then click the **Associations** button.
- Click the link of the channel group; then click the **Associations** button.

Table 2-8 provides descriptions of the fields in the Associations window.

Table 2-8 Virtual Talk Groups Tab in the Associations Window

Field	Description
VTG Name	VTG to which this channel group is associated
Status	Status of the associated VTG, which includes the following designations: • Active—Channel group is a participant in an active VTG • Idle—Channel group is a member of an inactive VTG

Removing a PTT Channel from a Channel Group

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

To remove a PTT channel from a channel group, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Channel Groups** window.

Step 2 In the Channel Group Name column, click the link for the channel group from which you want to remove a channel.

The General tab of the channel group displays.

Note To view the associations for the channel group, click the Associations button.

Step 3 Click the **Members** tab.

Step 4 Check the check box to the left of each channel that you want to remove from the channel group.

Step 5 Click **Delete**.

Tip To delete all the channels from this channel group, check the check box at the top of the channel list and click **Delete**.

To add channel members to a channel group, see the "Viewing and Editing Channel Group Details" section on page 2-34.

Associating Ops Views to Channel Groups

You can associate specific ops views to channel groups from the Channel Groups window. When you associate an ops view to a channel group, the channel group can be seen by the users who belong to that particular ops view.

For more information about the Accessible To and Belongs To attributes for ops views, see Chapter 6, "Configuring and Managing Cisco IPICS Operational Views."

To determine the ops views to which the channel group is currently associated, access the Configuration drawer, click **Channel Groups**, and look at the information in the Ops View column for the channel group.

To associate ops views to channel groups, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Channel Groups** window.

Step 2 In the Channel Group name column, click the channel group that you want to associate to an ops view.

Step 3 From the General tab in the Ops View pane, click the **Edit** button.

The Ops View to Channel Group Association window displays the following information:

- Available Ops Views—Ops views that can be made accessible to this channel group
- Associated Ops Views—Ops views to which this channel group is currently accessible

Step 4 Take any of the following actions:

- To move an ops view from one list to the other, click the ops view to highlight it; then, click **>** or **<**, or double-click the ops view.
- To move several ops views from one list to the other at one time, press **Shift+click** or **Ctrl+click** to select the ops views; then, click **>** or **<**.
- To move all ops views from one list to the other at one time, click **>>** or **<<**.

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

If you do not want to associate the ops view to the channel group, click **Cancel**.

The ops views that you choose display in the Accessible To: field in the individual window for the channel group.

Step 6 To change the ops view to which this channel group belongs, from the Belongs To: drop-down list box, choose an ops view.

Step 7 Click **Save**.

Deleting a Channel Group

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

To delete a channel group, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Channel Groups** window.

Step 2 Check the check box next to each channel group that you want to delete.

Step 3 Click **Delete**.

A dialog box prompts you to confirm the deletion.

Step 4 To confirm the deletion, click **OK**.

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

Managing Radios

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.

Cisco IPICS also provides support for serial-controlled radios through an integrated radio control service that translates control commands from Cisco IPICS to proprietary serial protocols. Cisco IPICS access serial controlled radios via asynchronous serial ports on the LMR gateway.

Using radio control to manage radios involves the following general steps:

1. Configure hardware as described in the *Solution Reference Network Design (SRND)* (latest version).
2. Create a location that the radio uses for multicast. (See the "Managing Locations" section on page 2-86.)
3. Create and provision a radio descriptor. (See the "Adding Descriptors" section on page 2-82.)
4. Add the radio an assign the desired descriptor to it. (See the "Adding a Radio" section on page 2-52.)

This section contains the following radio management topics:

- Tone Control Radio Overview, page 2-42
- Serial Control Radio Overview, page 2-44
- Understanding How Buttons Display on the PMC, page 2-44
- Radio Frequency Channels, page 2-45

- Configuring Channel Selectors and Control Sequences for Tone Control, page 2-46
- Configuring Channel Selectors and Control Functions for Serial Control, page 2-49
- Understanding the Radios Window, page 2-50
- Adding a Radio, page 2-52
- Viewing and Editing Radio Details, page 2-59
- Associating Users to a Radio From the Radios Window, page 2-61
- Enabling or Disabling a Radio, page 2-64
- Deleting a Radio, page 2-65
- Accessing and Using the Serial Radio Control Interface, page 2-66

You perform the radio management tasks in the **Configuration > Radios** window in the Administration Console. For more information about these windows, including how to access them, see the "Understanding the Radios Window" section on page 2-50.

Tone Control Radio Overview

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. 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.

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 information about channel selectors, see the "Configuring Channel Selectors and Control Sequences for Tone Control" section on page 2-46.

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.

For more detailed information about how to use the tone-controlled radio functionality on the PMC, refer to the *Cisco IPICS PMC Installation and User Guide.*

Channel selector buttons, signals, and commands are defined in descriptor files. The following list describes these descriptor files:

- Radio Descriptor Files—Channel selector buttons that provide the functionality for specific radio types are defined in the radio descriptor files. The radio descriptor file defines the tones and/or events that must be sent to the radio to enable/disable specific capabilities. For more information, see the "Radio Descriptors" section on page 2-70.
- Tone Descriptor Files—Tone descriptor files contain signals and commands. You can associate signals, that are defined in a tone descriptor file, to channels. Commands in a tone descriptor can be reference by any radio descriptor file. See the "Tone Descriptors" section on page 2-72 for more information.

Serial Control Radio Overview

Serial controlled radios can be configured to have channel selectors and control functions. Channel selectors represent buttons that allow a PMC or Administration Console user to select a radio channel or talkgroup and to set up a private or group call. Control functions are buttons that allow a PMC or Administration Console user to invoke functions or modes of operation.

For serial control, Cisco IPICS defines generic control commands that are configured in a radio descriptor. A radio control service that is integrated with Cisco IPICS translates these commands into proprietary commands.

The Serial Radio Control Interface (SRCI) provides access to the channel selectors and control functions that are defined in the radio descriptor. The SRCI also provides feedback from the controlled radio when a channel selector is changed or a control function is invoked. On radios that support these features, the SRCI provides the talker ID for incoming calls and emergency detection. The SRCI is available from the Cisco IPICS Administration Console or from the PMC via a pop-up browser window.

Understanding How Buttons Display on the PMC

When you use tone control, the buttons that display on the PMC get populated from information that the PMC receives from the Cisco IPICS server. Table 2-9 describes how the PMC buttons get populated to display on the PMC, and the sequence of those events:

Table 2-9 How PMC Buttons Get Populated and Displayed

Sequence of PMC Button Population	Position of Buttons on the PMC
1. The Cisco IPICS server performs a one-to-one mapping of the available PMC buttons, and sends it to the PMC. **Note** The PMC can display a maximum of nine channel selector buttons.	The position of the channel selectors display on the PMC flow from left to right and top to down.
2. If buttons are still available on the PMC, the control sequences get mapped.	The position of the buttons display on the PMC flow from left to right and top to down.
3. If a stateful sequence does not fit in the user interface (UI) of the PMC, the Cisco IPICS server checks the next control sequence in the list.	If the sequence fits, it gets placed in the PMC UI.

Table 2-9 How PMC Buttons Get Populated and Displayed (continued)

Sequence of PMC Button Population	Position of Buttons on the PMC
4. Momentary controls get associated to available PMC buttons.	The position of the buttons display on the PMC flow from left to right and top to down.
5. Buttons that are still available get populated with signals.	The position of the signal buttons display on the PMC flow from right to left and bottom to up.

When you use serial control, the PMC displays one button, which is called **CTRL**. Clicking this button displays the SRCI.

For more detailed information about the PMC, refer to the *Cisco IPICS PMC Installation and User Guide.*

Radio Frequency Channels

In Cisco IPICS, a channel can refer to the RF channel (the frequency) to which the radio is actually tuned and on which content is streaming. Be aware of the following RF caveats when you use the PMC:

- A radio frequency alone does not define a channel and the audio content may differ depending on the location of the frequency. For example, a channel that is tuned to one frequency in one location may receive completely different content from the same type of radio that is tuned to the same radio frequency in a different location.
- A channel may appear on more than one frequency, such that the same content may be audible on several different frequencies.
- Any particular radio frequency in a specific location may simultaneously carry multiple different content streams.

You can associate radios and PMC users to enable user access to the specified radio(s). You can also specify channel selector and control permissions to users by choosing the level of permission that pertains to each individual channel selector or radio control button. These permissions determine which channel selector buttons and radio controls the users can use. For example, if you do not configure any channel selector buttons for a user, the user can listen to the channel but cannot change the channels or control the radio.

Some examples of radio control functions include MON (monitor), POW (power level) and Enc (encryption).

See the "Configuring Channel Selectors and Control Sequences for Tone Control" section on page 2-46 for more information about channel selectors and tone control sequences for radios.

Configuring Channel Selectors and Control Sequences for Tone Control

This section describes how to configure channel selectors and tone control sequences and includes the following topics:

- Channel Selector Configuration, page 2-46
- Tone Sequence Configuration, page 2-47
- Caveats for Configuring Default Tone Sequences, page 2-48

Channel Selector Configuration

You select channel descriptors and controls that are available to radio users in the Configuration > Descriptors window. When you configure or update descriptors and controls, the PMC of the any user who is associated to a radio also gets updated.

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

The channel selector attributes include the following elements:

- Label—This field specifies the name of the radio channel selector, as defined in the radio descriptor file. See the "Managing Radio Descriptors" section on page 2-69 for more information about descriptors.

Note When you configure channel selector attributes, be aware that mixing left-to-right (LTR) and right-to-left (RTL) character sets for different languages may cause undesirable behaviors in the server and/or PMC.

- Enabled—If checked, this box indicates whether a PTT channel is allowed to associate to this channel and if this channel selector is available on the radio-centric PMC skin. That is, this channel selector displays in the drop-down list box for the radio connection for the channel and is available on the radio-centric PMC skin.
- Associated Channel—This field displays the name of the currently associated channel and its short name (a condensed name of the channel).

Tone Sequence Configuration

The tone control sequences, which are defined in a radio descriptor file, contain information about how to tune the radio to another channel within that radio. See the "Managing Radio Descriptors" section on page 2-69 for more information.

You can also configure default tone sequences; however, be aware of the caveats that are documented in the "Caveats for Configuring Default Tone Sequences" section on page 2-48 before you configure these sequences.

The control attributes for tone sequences include the following elements:

- Label—This field indicates the name of the tone sequence, as defined in the tone descriptor file. These sequences may include names such as Monitor On/Off or Hi/Medium/Low Power and are used for identification of that particular tone sequence.
- Enabled—If checked, this check box indicates that this control can be made available to the PMC.
- Description—This field indicates a description of the tone control sequence. A tone control can be either a stateful or 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 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.

Note Because of the limitations of tone-controlled radios, you may be able to toggle a feature on, but you may not have any way to know when the feature has been toggled back. For example, even though you can enable monitor mode, this mode can be turned off due to a variety of reasons including pressing the PTT button or changing the radio channel.

For more information about tone and radio descriptors, see the "Tone Descriptors" section on page 2-72 and the "Understanding the Descriptors Window" section on page 2-80.

Caveats for Configuring Default Tone Sequences

Cisco IPICS allows you to configure a default tone sequence that transmits on the last used channel whenever the currently-tuned channel is unknown.

Note Be aware that the channel on which the tone sequence transmits is determined by the capabilities of the specific radio equipment systems that are being used and you should configure the channel based on that information.

You can configure the following options for a default channel:

- Associate to no tones at all
- A tone sequence that instructs that the radio transmits on a default channel, such as F1
- A tone sequence that instructs that the radio transmits on the currently-tuned channel, if that capability is available

Note When some users do not have access to channel selectors and cannot select a channel on which to transmit, the PMC does not know which channel the radio has been tuned to. Therefore, the PMC does not provide the user with any visual indicator and does not allow the user to transmit under those conditions. The channel that gets used is dependent on the configuration and on the radio capabilities as previously described.

Be aware that when you configure a default tone sequence, it may transmit over an unintended channel under the following conditions:

- If you configure the system so that a default tone sequence transmits on the currently-tuned channel, Cisco IPICS uses the last used channel to transmit if the transmission occurs before a specific channel has been selected.
- If a PMC user pushes the PTT button to talk, the tone control sequence may transmit over that specific channel, even if it was not the intended channel to use for transmission.
- If a PMC user begins to transmit while another user attempts to change channels in the same radio, transmission may occur in the channel that was selected by the second user. Or, the channel may not actually be changed but the tone control sequence sent by the attempted channel change may transmit over an unintended frequency.

Note The behavior of the PMC is dependent on the capabilities of the individual radio system that is being used.

Configuring Channel Selectors and Control Functions for Serial Control

This section describes the channel selectors and control functions described in the radio descriptor that are applicable to this radio.

Understanding the Radios Window

The **Configuration > Radios** window, in the Administration Console, lists information about each of the radios that you have added in Cisco IPICS.

Table 2-10 describes the items in the Radios window.

Table 2-10 Items in the Radios Window

Item	Description	Reference
Name field	This field indicates the names of radios that are configured in Cisco IPICS.	See the "Adding a Radio" section on page 2-52 and the "Viewing and Editing Radio Details" section on page 2-59
Radio Type field	This field indicates the radio type for this radio.	
Location field	This field indicates the location of the radios. **Note** Location is used to determine whether the PMC user can reach the radio channel.	
Multicast Address field	This field indicates the multicast address that has been assigned to the radio.	
Status field	This field indicates the status of radios that have been configured in Cisco IPICS. Radios can have one of the following statuses: • Enabled • Disabled • Descriptor Corrupted/Missing • Active • Pending	

Table 2-10 Items in the Radios Window (continued)

Item	Description	Reference
Control Status	This field shows the current state of the serial control radio: • DISCONNECTED— RCS has not initiated connection to LMRG async port. • INITIALIZING—RCS is initializing connection to LMRG async port. • TIMEOUT—No response from RCS connection. • SOCKET_FAILURE—Socket connection to LMRG async port failed. • AUTHENTICATION_FAILURE—Invalid LMRG credentials. • CONNECTED_OFFLINE—No response from connected radio. Check connection. • CONNECTED_ONLINE—Communication has been established with connected radio.	See the "Adding a Radio" section on page 2-52 and the "Viewing and Editing Radio Details" section on page 2-59
Reserved by	This field shows the IPICS user or VTG that has requested control of the radio.	
Add button	Click this button to configure new radios.	See the "Adding a Radio" section on page 2-52
Delete button	Click this button to delete radios from Cisco IPICS.	See the "Deleting a Radio" section on page 2-65
Associations button	Click this button to associate radios to users.	See the "Associating Users to a Radio From the Radios Window" section on page 2-61
Display Controls		

Table 2-10 Items in the Radios Window (continued)

Item	Description	Reference
Rows per page drop-down list box	Specifies the number of rows of radios that are included in a radios list page.	See the "Navigating Item Lists" section on page 1-16
Page field	Displays radios on a specific page.	
|< (First page) button	Displays the first page of the radio list.	
< (Previous page) button	Displays the previous page of the radio list.	
> (Next page) button	Displays the next page of the radio list.	
>| (Last page) button	Displays the last page of the radio list.	

Adding a Radio

When you add a radio it becomes available for use by Cisco IPICS.

Before you add a radio, make sure that you configure locations, as described in the "Managing Locations" section on page 2-86.

To add a new radio, perform the following procedure:

Procedure

Step 1 From the Cisco IPICS Administration Console, navigate to the **Configuration > Radios** window.

Step 2 In the Radios window, click **Add** and designate the type of radio that you want to add by choosing one of these options from the drop-down list that displays:

- **Add Tone Controlled Radio**
- **Add Serial Controlled Radio**

The General tab for a new radio displays. Table 2-11 describes the fields in this tab.

Table 2-11 General Tab Fields in Radios Window

Field	Description for Tone Controlled Radio	Description for Serial Controlled Radio
General Information Area		
Name	Enter the name of the radio.	Enter the name of the radio.
Radio Type	Choose the type of radio from the drop-down list box. The choices that display for radio type are based on the radio types that are in the radio descriptor files. For more information about radio descriptor files, see the "Managing Radio Descriptors" section on page 2-69.	
Description	Enter a description of the radio.	Enter a description of the radio.
Content Source Information Area		
Location	Choose a location for the radio from the drop-down list box. Location is used to determine how the PMC client can reach the radio (via multicast or unicast). **Note** PMC users must login from the same location as the radio to access it. Cisco IPICS supports remote login only if the Cisco IPICS server is configured with an RMS in the same location as the radio. Refer to "Tone-Controlled Radio Caveats" in the *Cisco IPICS PMC Installation and User Guide* for more detailed information. See the "Managing Locations" section on page 2-86 for information about configuring locations.	
Multicast Address	This field specifies the multicast address that is used to transmit audio and tones.	Enter the multicast address that is defined in the dial peer configuration of the LMR gateway.
Multicast Port	This field specifies the multicast port for the radio.	Enter the port number that is defined in the dial peer configuration of the LMR gateway.
Codec	Enter the codec that is defined in the dial peer configuration of the LMR gateway.	Enter the codec that is defined in the dial peer configuration of the LMR gateway.
Secure Radio	Choose **Yes** or **No** from the drop-down list box. **Note** This field defines the security label of the radio only, and not the security of the individual channels that can be carried over the radio.	

Table 2-11 General Tab Fields in Radios Window (continued)

Field	Description for Tone Controlled Radio	Description for Serial Controlled Radio
Voice Delay (msec) (Tone control only)	This field specifies a value, in milliseconds, that is set on the LMR gateway that you must replicate on the server for radio instances that are associated to the router. The value of this parameter on the router determines how long the LMR gateway delays the audio before sending it to the radio. The delay is necessary to ensure that tones do not overlap with audio when the static tone configuration is used in the dial peers. **Note** Make sure that the value that you enter for this parameter is the same that is configured on the LMR gateway. This field must map to the value that is entered in the timing delay-voice tdm CLI command. Refer to the *Solution Reference Network Design (SRND)* (latest version) for more information.	
Hangover Time (msec) (Tone control only)	This field specifies a value, in milliseconds, that is set on the LMR gateway that you must replicate on the server for radio instances that are associated to the router. The value of this parameter on the router determines how long the LMR gateway keeps the radio keyed after the last audio packet is received on a talk spurt. This setting is used to protect the system against packet loss and to accommodate for the configured delay time. Hangover time is usually larger than the delay time to ensure that all the buffered audio is played before unkeying the radio. **Note** Make sure that the value that you enter for this parameter is the same that is configured on the LMR gateway. Refer to the *Solution Reference Network Design (SRND)* (latest version) for more information. Valid values: 0 through 10000	
Ops Views Area		
Ops Views—*Display only*	Indicates that the radio is associated to the System ops view. For general information about ops views, see Chapter 6, "Configuring and Managing Cisco IPICS Operational Views."	
Restrictions Area		
Allow association to users	Check this check box if you want the radio to be available for association with on ore more users.	

Table 2-11 General Tab Fields in Radios Window (continued)

Field	Description for Tone Controlled Radio	Description for Serial Controlled Radio
Allow use in VTGs	Check this check box if you want the radio to be available for use in one or more VTGs. If you do not check this check box, the radio can be used only as a channel media connection.	Check this check box if you want the radio to be available for use in one or more VTGs. If you do not check this check box, the radio can be used only to place private calls to another serial radio.
Control Information Area		
Radio Control Service	—	Value is **local-rcs**.
Connection Information Area		
IP Address	—	Enter the IP address of the LMR gateway to which the radio connects.
Port	—	Enter the port number of the auxiliary or asynchronous line of the LMR gateway to which the radio is physically connected. Determine this port number by adding 4,000 to the line number to which the radio is serially connected. To find the line number, use the **show line** command on the LMR gateway.
User Name	—	*Optional*. Enter the user name of the LMR gateway.
Password	—	*Optional*. Enter the password of the LMR gateway.

Step 3 Click **Save**.

If you do not want to add the radio, click **Cancel**.

Note If you are adding a serial radio and the IP address/port provided in the radio connection section is unreachable, then the radio could take as much as 30 seconds to save. This applies only to serial radios.

Step 4 To configure channel selectors for this radio, take these actions:

a. Click the **Functions** tab.

b. In the Channel Selectors pane, check the check boxes next to the channel selectors that you want to enable.

If you want to check all check boxes at once, check the **Enabled** check box.

Note Channel selectors and radio controls are defined in the radio type descriptors.

c. Click **Save**.

If you do not want to save these configurations, click **Cancel**.

For detailed information about channel selectors, see the "Configuring Channel Selectors and Control Sequences for Tone Control" section on page 2-46 and the Configuring Channel Selectors and Control Functions for Serial Control, page 2-49.

Step 5 To configure controls for this radio, take these actions:

a. Click the **Controls** tab.

b. In the Controls pane, check the check boxes next to the controls that you want to enable.

If you want to check all check boxes at once, check the **Enabled** check box.

Note Radio controls are defined in the radio type descriptors.

c. Click **Save**.

If you do not want to save these configurations, click **Cancel**.

For detailed information about tone control sequences, see the "Configuring Channel Selectors and Control Sequences for Tone Control" section on page 2-46 and the Configuring Channel Selectors and Control Functions for Serial Control, page 2-49.

Step 6 To disable or enable the radio, click the **Disable** or **Enable** button.

Note If the radio is enabled, the **Disable** button displays. If the radio is disabled, the **Enable** button displays. For more information about enabling/disabling radios, see the "Enabling or Disabling a Radio" section on page 2-64.

Step 7 To configure the PMC details for this radio, take these actions:

a. Click the **PMC** tab.

The PMC tab for the selected channel displays. This window contains PMC information for this radio. Table 2-12 provides descriptions of the fields in the PMC tab.

Table 2-12 PMC Tab Fields in Radios Window

Field	Description
PMC Tab	
RX Mute During PTT	This attribute specifies the transmission settings for all radios or only one radio. It controls the audio for the active radios while you are transmitting. The following values affect how the mute functionality is configured on the PMC: • None—When PTT is engaged, the radio is muted. • All—When PTT is engaged, RX (receive transmission) is muted on all channels. • Radio—When radio is engaged, RX is muted for this radio only. **Note** When you initially assign a radio to the PMC, the RX mute settings that you have configured apply. The PMC user can modify this setting, however, if you change the setting after the radio has been assigned to the user, the changes do not become effective.

Table 2-12 PMC Tab Fields in Radios Window (continued)

Field	Description
Allow Latch	When set to true (attribute check box is checked) on a radio/VTG, the user can use latch (lock in radios) on any radio that you specify. **Caution** Use the latch functionality with caution. Be aware that when you latch the PTT button, this action blocks transmissions from half-duplex radios when these devices are attached to the channel or VTG via an LMR gateway. By default, this attribute is set to false (attribute check box is unchecked). **Note** If your Cisco IPICS server is running release 2.0(2) and you upgrade to release 2.2(1), any channels and VTGs that already exist maintain their values for latch, even if set to true.
Listen Only	When set to true (attribute check box is checked), the user can hear, but cannot talk, on the radio.

Table 2-12 PMC Tab Fields in Radios Window (continued)

Field	Description
Radio Color	Color tag that you can choose from a drop-down list box. With this setting, you can uniquely identify specific radios by using predefined colors for the background text that appears on the radio. You configure the color by choosing from the options in the drop-down list box. **Note** If you do not want the radio to be tagged with a color, you can choose **Not colored** from the drop-down list box.
Region	Choose a PMC region from the drop-down list box. When configured, the regions appear as tabs in the PMC display for PMC users who are associated with this radio. **Note** This field is specific to the 36-channel radio console skin on the PMC. To create PMC regions, see the "Adding PMC Regions" section on page 2-178.

b. Click **Save**.

If you do not want to save these configurations, click **Cancel**.

To associate users to a radio, see the "Associating Users to a Radio From the Radios Window" section on page 2-61.

Viewing and Editing Radio Details

You can view and edit information for any radio. Information that you can modify for a radio includes changing the name of a radio, enabling/disabling the channel selectors and tone control sequences, enabling/disabling the radio, and associating the radio to users.

To view or edit radio details, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Radios** window.

Step 2 In the Name column, click the link for the radio for which you want to view or change information.

The General tab for the selected radio displays.

Step 3 Take any of the following actions:

- To view or edit general information, update information in the General tab, then click **Save**.

  For descriptions of the fields in the General tab, see Table 2-11.

- To view or edit PMC information, update information in the PMC tab, then click **Save**.

  For descriptions of the fields in the PMC tab, see Table 2-12.

- To enable or disable channel selectors for the radio, check or uncheck the check boxes next to the channel selectors that you want to modify in the Functions tab, then click **Save**.

- To enable or disable tone control sequences for the radio, check or uncheck the check boxes next to the tone control sequences that you want to modify in the Controls tab, then click **Save**.

Note If you are saving a serial radio and the IP address/port provided in the radio connection section is unreachable, then the radio could take as much as 30 seconds to save. This applies only to serial radios.

Note If radio descriptor files are renamed, deleted, or corrupted, an error message displays in the Radio Management window that includes the affected radio descriptor files and a recommendation of how to proceed.

Step 4 To view or edit the PMC attributes for the radio, make the desired changes in the **PMC** tab, then click **Save**.

For descriptions of the fields in the PMC tab, see Table 2-12.

Step 5 To view or edit radio associations, see the "Associating Users to a Radio From the Radios Window" section on page 2-61.

Associating Users to a Radio From the Radios Window

You can associate specific users to a radio in the Radios window. When you associate radios with a user, the radios that you choose appear as options on a PMC.

When you associate a radio with a user, the user has the permission to change to any enabled channel on that radio. However, you can restrict the channels to which the user can tune by setting radio permissions for that user.

Because the radio permissions are separate from channel permissions, it is possible that a user could have permission to tune a channel on a radio but not have access to the association Cisco IPICS channel.

Note You can perform this procedure only if users have already been added in Cisco IPICS.

You can also associate a radio to a user from the Users window. For information, see the "Associating Radios with a User" section on page 3-34.

To associate users to a radio, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Radios** window.

Step 2 Take either of these actions to display the Associations window for the radio with which you want to associate users:

- Click the link for the radio in the Name column; then, click the **Associations** button, which appears at the bottom of each tab.
- Check the check box to the left of the name of the radio; then, click the **Associations** button at the bottom of the Radios window.

Note The Associations button appears dimmed if you do not check a radio or if you check more than one radio.

The Users tab displays for the radio. This tab displays a list of the users that are associated with the radio and the status of each user.

Step 3 To add a user to be associated with the radio, click **Add**.

The Search Users window displays. This window allows you to search for users to associate to the radio by choosing criteria that is based on the following filters:

- User Name field—Specifies the user name of a user
- First Name field—Specifies the first name of a user
- Last Name field—Specifies the last name of a user
- Location drop-down list box—Choose from a list of locations

  See the "Managing Locations" section on page 2-86 for detailed information about how to configure locations.
- Role drop-down list box—Choose from a list of Cisco IPICS roles
- Ops View drop-down list box—Choose from a list of ops views

Step 4 To search for a user, enter your search criteria; then, click **Go**. To clear your criteria, click **Clear Filter**.

Note To display all the users in Cisco IPICS, click the **Go** button without entering any search criteria.

The results of your search criteria display in a list.

Step 5 To choose a user to associate to the radio, check the check box to the left of the user name and click **OK**.

The user that you choose displays in the user list in the Users tab.

Note You can add multiple users simultaneously by clicking the check boxes next to each user and clicking **OK**.

Step 6 To view or edit radio permissions for a user, select the user by checking the check box next to the user name and choose one of the following options from the Radio Permissions drop-down list box:

- **Channel Selector Permissions**—When you choose this option, a separate window displays for channel selector permissions. In this window, you can configure specific channels that the user can communicate on.
- **Control Function Permissions**—When you choose this option, a separate window displays for radio control function permissions. In this window, you can configure specific radio controls that the user can access to control the radio.

Note The Radio Permissions drop-down list box appears dimmed if you do not have any users checked or if you have more than one user checked.

Step 7 To select the radio permissions on this radio for the user, take any of the following actions in the applicable radio permissions window:

- To move a channel selector/control function from one list to the other, click the item to highlight it; then, click **>** or **<**. Or, double-click the item.
- To move several channel selectors/control functions from one list to the other at one time, press **Shift+click** or **Ctrl+click** to select the items, then, click **>** or **<**.
- To move all channel selectors/control functions from one list to the other at one time, click **>>** or **<<**.

Step 8 Click **Save**.

Note If you are saving a serial radio and the IP address/port provided in the radio connection section is unreachable, then the radio could take as much as 30 seconds to save. This applies only to serial radios.

Step 9 To remove a user from the association to the radio, check the check box to the left of the user name; then, click the **Delete** button.

Note You can remove multiple users from the association at the same time by checking the check boxes that display by the user names of the users that you want to remove and clicking **Delete**.

Enabling or Disabling a Radio

You can enable or disable a radio in Cisco IPICS. If the radio is disabled, you can can still modify the multicast address, location, LLGT, and all of the other attributes of the radio. However, if the radio is enabled, you cannot modify these attributes.

If the radio is part of an active VTG and you disable the radio, it disconnects from the VTG.

Note Once you define a radio, the radio type cannot be changed even if you disable the radio. If you want to change the radio type after you define the radio, you must delete the radio and create a new radio instance. If you only want to modify the types of tones on a radio type, you can upload a new descriptor file for the same radio type and the changes get applied to that radio instance. For more information about descriptors, see the "Managing Radio Descriptors" section on page 2-69.

To enable or disable a radio, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Radios** window.

Step 2 Under the Name column, click the link of the radio that you want to enable/disable.

The General tab displays for the radio.

Step 3 To enable/disable the radio, click the **Enable/Disable** button at the bottom of the window.

Note If the radio is currently enabled, only the **Disable** button displays. If the radio is currently disabled, only the **Enable** button displays.

If you do not want to enable/disable the radio, click **Cancel**.

Deleting a Radio

If a radio is no longer needed, you can delete it from Cisco IPICS. You can delete a single radio or you can delete several radios at one time.

Note Before you delete a radio, you must remove any associated media connections in all of the channels for that radio.

To delete a radio, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Radios** window.

Step 2 Check the check box next to each radio that you want to delete.

Step 3 Click **Delete**.

A dialog box prompts you to confirm the deletion.

Step 4 To confirm the deletion, click **OK**.

If you do not want to delete the radio(s), click **Cancel**.

Accessing and Using the Serial Radio Control Interface

After you configure a serial controlled radio, you can access and use the SRCI from a PMC, as described in *Cisco IPICS PMC Installation and User Guide Release 2.2*, from the Cisco IPICS Administration Console.

To access the SRCI from the Administration Console, perform any of the following actions:

- Navigate to the **Configuration > Radios** window, click the link for the desired radio in the Name column, then click **Controls**, which displays at the bottom of each tab.
- Navigate to the **Configuration > Radios** window, check the check box next to the radio for which you want to access the SRCI, then click **Radio Control**.
- Navigate to the **VTG Management > Virtual Talk Groups** window, and click a VTG name. In the **Participants** tab, double-click a radio in the Participants or Resources box.
- If the radio is associated with a user, navigate to **User Management > Users**, choose a user, click **Associations**, choose the Radio tab, choose the desired radio, then click **Radio Control**.

The SRCI displays in its own page and is organized as follows:

Radio Information

The top area of the SRCI provides the following information and functions:

- Name of the radio, as configured in the Name field in the General tab for the radio.
- Type of the radio, as defined in the radio descriptor.
- Connection status of the radio, which can be any of the following:
  - CONNECTED_ONLINE—Radio is ready for control.
  - CONNECTED_OFFLINE—Radio connection to the LMR gateway is active, but Cisco IPICS cannot communicate with the radio. This situation can occur if the radio is turned off or is not connected to the correct asynchronous line on the correct LMR gateway, or if the connected radio is of the wrong type.

  - AUTHENTICATION_FAILURE—The login credentials provided in the radio details are not correct and IPICS cannot connect to the specified port on the LMR Gateway.
  - SOCKET_FAILURE—Cisco IPICS cannot connect to the LMR gateway IP address and port that are as configured in the General tab for the radio. This situation can occur if the IP address or port number are incorrect, the LMR gateway is turned off, the LMR gateway is disconnected from the network or in an unreachable network, or the LMR gateway is in use and needs to be cleared.
  - DISCONNECTED—Cisco IPICS has not initialized the connection or is in the process of re-initializing the connection because of a SOCKET_FAILURE or AUTHENTICATION_FAILURE situation.
  - RADIO CONTROL SERVICE UNAVAILABLE: The Cisco IPICS Radio Control Service is down and needs to be restarted.

- **Reserve / Release** toggle button—The **Reserve** button allows you to indicate to other users that you would like to use this radio. When you click this button, your Cisco IPICS user name and full name appear in the Reserved By field and the date and time that you clicked it appear in the Reserved On field. In addition, the name of the button changes to **Release**. In this case, other SRCI users see the **Release** button and they see your information in the Reserved By and Reserved On fields.

  This function is provided as a courtesy only and does not block any user from controlling the radio. Any user can click the **Release** button, which clears the Reserved By and Reserved On information and changes the button name to **Reserve**.

  If the radio is in an active VTG, Cisco IPICS disables the **Reserve/Release** button. In addition, the VTG name and the date and time that this radio was added to the VTG appear in the Reserved by field. Along with the date and time this radio was added to the active VTG. (Any user can control a radio that is reserved by a VTG.)

Radio Display and Controls

The second-from-the-top area of the SRCI provides the following information:

- The type of call that is active on the controlled radio, followed by the channel selector name, the private call alias/ID, or the group call name. Call types are indicated as follows:
  - [Channel/TG]—Conventional channel and trunked talkgroup operation

  - [Private Call]—Unit to unit calls (iDEN and Sprint Nextel only)
  - [Group Call]—Dynamic group operation (iDEN and Sprint Nextel only)
- A green LED icon that lights when there is inbound voice traffic on the channel.
- When there is inbound voice to the radio and the radio detects the talker ID, this ID displays below the channel selector for the duration of the inbound voice.
- Configured control functions. Each function appears as a button, and the current state of each function displays above the corresponding button.

Channel Selectors

The third-from-the-top area of the SRCI includes channel selectors. Each configured channel selector displays as a button. Depending on the radio control configuration, a user may be able to press a channel selector button to change the channel/talkgroup on the radio or place a private or group call.

Cisco IPICS Connect

Applies to Nextel radios only.

The bottom area of the SRCI allows you to make private calls, group calls and call alerts (pages). This area applies to Nextel radios only.

Making private and group calls from the channel selector area is a one touch operation. From the IPICS Connect box, you can make ad-hoc private and group calls, including combining users from different pre-defined groups. You can also send a call alert (page) to a predefined participant or ad-hoc participant.

The names that display in the Select From Groups/Users list come from channel selectors for private and group calls that are defined in the serial radio descriptor, and from Cisco IPICS users that are associated with a Nextel radio.

To make a private call, follow these steps:

Step 1 Take either of these actions:

- Enter a direct connect number in the Direct Connector Number field and then click **<<** to move the number to the Participants list.
- Click a name in the Groups/Users list and then click **<<** to move the number to the Participants list.

Step 2 Click **Call** to initiate the private call to the users in the Participants box.

To make a group call, follow these steps:

Step 1 Enter a group name (from 1 to 20 characters) in the Group/User Alias field.

- Enter a direct connect number in the Direct Connector Number field and then click **<<** to move the number to the Participants list.
- Click a name in the Groups/Users list and then click **<<** to move the number to the Participants list. You can specify up to 20 items in the Participants list.

Step 2 Click **Call** to initiate the group call.

To send a call alert, also known as a page, follow these steps:

Step 1 Take either of these actions:

- Enter a direct connect number in the Direct Connector Number field and then click **<<** to move the number to the Participants list.
- Click a name in the Groups/Users list and then click **<<** to move the number to the Participants list.

Step 2 Click **Alert** to initiate the alert to the selected direct connect number, user, or group. You can send a call alert only to one participant at a time.

Managing Radio Descriptors

This section describes radio and tone descriptor management tasks and includes the following topics:

- Radio Descriptors, page 2-70
- Tone Descriptors, page 2-72
- Caveats for PMC Operation, page 2-79
- Understanding the Descriptors Window, page 2-80

- Adding Descriptors, page 2-82
- Updating Radio and Tone Descriptors, page 2-83
- Deleting Radio and Tone Descriptors, page 2-85

Radio Descriptors

Radio descriptors define the controls that a particular type of tone control or serial control radio supports.

Note A radio type may refer to a specific make and model of radio or special tone-controlled hardware, such as a CPI box, which interprets the inband tones and causes the configuration of an attached radio to be changed.

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.

Note When choosing a descriptor type in the Administration Console, be aware that a *Tone Radio* descriptor type refers to a radio descriptor file and a *Tones* descriptor type refers to a tone descriptor file. See the "Adding Descriptors" section on page 2-82 and "Updating Radio and Tone Descriptors" section on page 2-83 for more information.

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 tone control channel selectors and control functions (both stateful and simple), Cisco IPICS supports only RFC 2833 tones. See the "Caveats for PMC Operation" section on page 2-79 for more 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 2-72.

The Cisco IPICS server provides an example radio descriptor file; however, you may need to modify this example and/or create additional radio descriptors that properly model your specific radio hardware. The example file is in the list of descriptors.

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 more information about adding or modifying descriptor files, see the "Managing Radio Descriptors" section on page 2-69. To see examples of valid and invalid descriptor file .xml entries, refer to the *Cisco IPICS Radio and Tone Descriptor File Examples Reference Card.*

See the "Radio Descriptor Format" section on page 2-71 for an example of the format of a radio descriptor.

Radio Descriptor Format

The following example shows the format of a radio descriptor .xml file:

Radio Descriptor File Format

```
<?xml version="1.0" encoding="UTF-8"?>
<ipics:RadioTypeDescriptor... name="CPITestBox">
```

where:

name= represents the name of the radio type that displays in the UI; this name should be unique.

```
<Commands>... </Commands>
```

Commands define “macro-like” tone/event sequences that can be used elsewhere within the radio descriptor.

```
<ChannelSelectors>... </ChannelSelectors>
```

Channel selectors define the available tone sequences needed to use each channel on the radio.

```
<ControlFunctions>... </ControlFunctions>
```

Control functions define the available stateful control sequences and the tones that need to be sent to enable each stateful state.

For more examples of descriptor .xml file entries, refer to the *Cisco IPICS Radio and Tone Descriptor File Examples Reference Card.*

Tone Descriptors

A tone descriptor file is an .xml file that defines 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.

A tone sequence is a list of tones and events that are used to either control a radio or to signal a channel. For more information about tone sequences, see the “Configuring Channel Selectors and Control Sequences for Tone Control” section on page 2-46.

Most tone control radios support a standard set of tone sequences. Some sequences are used to change the RF channel, while other sequences are used to enable the scan functionality on a radio. There are many more tone sequences that are used for tone signaling.

For tone sequences, Cisco IPICS supports both RFC 2833 tone and RFC 2833 event (DTMF) commands. For more information, see the “Caveats for PMC Operation” section on page 2-79.

For some examples of valid and invalid descriptor file entries, refer to the *Cisco IPICS Radio and Tone Descriptor File Examples Reference Card.*

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 0 to 3999 Hz), a decibel (db) level (0 to -63), and a duration in milliseconds. This sequence of tones can be used by different radios. For tone signaling purposes, each telephony event in a sequence is specified by the event type (from 0 to 255), a db level (0 to -63), and a duration in milliseconds.

Note Any RFC 2833 tone or event has a maximum duration of eight seconds. See the "Caveats for PMC Operation" section on page 2-79 for more information.

The Cisco IPICS server provides signaling sequences in an example tone descriptor file called ExampleToneSet.xml; however, you may need to modify this example file and/or create additional tone descriptors that properly model your specific radio hardware. To add or update descriptors, see the "Managing Radio Descriptors" section on page 2-69.

Note If you must modify or create tone descriptors, refer to the documentation that you received with your radio, or other device that you need to control, for the specific signaling sequences that it supports.

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

Note When choosing a descriptor type in the Administration Console, be aware that a *Tone Radio* descriptor type refers to a radio descriptor file and a *Tones* descriptor type refers to a tone descriptor file. See the "Adding Descriptors" section on page 2-82 and "Updating Radio and Tone Descriptors" section on page 2-83 for more information.

For information about the descriptor management functions in the Descriptors window, see the "Understanding the Descriptors Window" section on page 2-80.

Serial Descriptors

This section describes the general steps for creating a serial descriptor for serial radio control.

Step 1: Create the Header

A radio descriptor begins with the element <SerialRadioTypeDescriptor>. This element includes the following attributes:

- name—Contains 1 through 64 characters and specifies the name of the radio descriptor.
- controlType—Always set to SERIAL.
- controlModule—Specifies the type of radio that is controlled. Use “Nextel” for iDEN radios in a Sprint/Nextel or private iDEN network. Use “EFJohnson” for EF Johnson model 5300 mobile radios.

The following is an example of a serial descriptor header:

```
<ipics:SerialRadioTypeDescriptor xmlns:ipics=
       "urn:com.cisco.ipics.RadioDescriptor"
               xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
               xsi:schemaLocation="urn:com.cisco.ipics.RadioDescriptor
../../SerialRadioTypeDescriptor.xsd "
               name="Nextel"
               controlType="SERIAL"
               controlModule="Nextel">
```

Step 2: Create the Body

The body of the radio descriptor has two main sections, <ChannelSelectors> and <ControlFunctions>, each of which define buttons that the SRCI renders.

Channel Selectors

<ChannelSelector> elements are controls that set up the radio for a specific mode of communication. The controls include selecting a channel/talkgroup on the radio or placing a private or dynamic group all.

Each <ChannelSelector> has a required “label” attribute that is 1 through 12 characters in length and that defines the name of a button that the SRCI renders.

The <Action> element within each <ChannelSelector> includes the “type” attribute. This attribute must be set to “tune” and indicate that this control is communications related.

The <Action> element includes the <Command> element. This attribute specifies the tuning action and can be either <Channel> or <GroupCall>.

Selecting a Channel or Talkgroup

For channel or talkgroup controls, the element within <Command> must be <Channel>. The <Channel> element must include these attributes:

- zone—Must be set to a valid zone in the radio that represents this channel selector.
- channel—Must be set to a valid channel in the radio that represents this channel selector.

iDEN radios do not have the concept of zones and channels. For these radios, always set the zone attribute 1. The channel attribute represents the talkgroup ID and can range from 1 to 200.

The following example shows the use of the <ChannelSelector> element:

```
<ChannelSelector label="CHAN 5">
          <Action type="tune">
                    <Command>
                              <Channel zone="1" channel="5" />
                    </Command>
          </Action>
</ChannelSelector>
```

Setting up a Private Call

This feature applies only to iDEN radios.

To define a channel selector that can set up a private call, the <Command> element must contain a child element called <GroupCall>. The <GroupCall> element includes the “name” attribute, which defines the name of the button that represents this private call. The “name” attribute can contain 1 through 12 characters.

The <GroupCall> element contains the ID of the remote radio that will participate in this call. The radio is represented by the <Call> element and contains an attribute called “number.”

The following example represents an iDEN private call with the direct connect number of the participant in the <Call> element:

```
<ChannelSelector label="W Plinge">
          <Action type="tune">
                    <Command>
                              <GroupCall groupName="W Plinge">
                                        <Call number="123*45678*9" />
                              </GroupCall>
                    </Command>
          /Action>
</ChannelSelector>
```

Setting up a Group Call

This feature applies only to iDEN radios that are in iDEN networks that are capable of dynamic group calls.

To define a channel selector that can set up a group call, the <Command> element contains one or more child elements called <GroupCall>. Each <GroupCall> element includes the “name” attribute, which defines the name of the button that represents this private call. The “name” attribute can contain 1 through 12 characters.

The following example represents an iDEN group call with the direct connect numbers of the participants in <Call> elements:

```
<ChannelSelector label="My Team">
          <Action type="tune">
                    <Command>
                              <GroupCall groupName="My Team">
                                        <Call number="123*45678*9" />
                                        <Call number="123*45678*10" />
                                        <Call number="123*45678*11" />
                                        <Call number="123*45678*12" />
                              </GroupCall>
                    </Command>
          </Action>
</ChannelSelector>
```

Control Functions

Control functions define buttons on the SRCI that can control certain functions of the control radio. Control functions do not exist in iDEN radios. These control functions are listed as <Simple> elements, with the following attributes:

"shortName" is an attribute of a control function. It is 1 through 12 characters in length and defines the name of the control as rendered on the SRCI.

"description" is an attribute of a control function. It describes the nature of the control function.

Each <Simple> element contains an <Action> element, which defines the control functions with the "type" attribute. An <Action> element is always set to a value of "pressed" and contains a <Command> element, which determines the specific command for the control function.

Cisco IPICS provides the following control functions:

- Monitor—When representing a control function to enable or disable monitor mode in the controlled radio, use the following xml within <ControlFunctions>:

```
<Simple shortName="MON" description="Enable/Disable Monitor Mode">
          <Action type="pressed">
                    <Command>
                              <SetMonitorMode value="ON" />
                    </Command>
          </Action>
</Simple>
```

- Secure Transmit Mode—When representing a control function to toggle between secure and clear transmit modes in the controlled radio, use the following xml within <ControlFunctions>:

```
<Simple shortName="SEC" description="Select Between Secure and
    Clear Transmit Modes">
          <Action type="pressed">
                    <Command>
                              <SetSecureTxModevalue="ON" />
                    </Command>
          </Action>
</Simple>
```

- Repeater/Talkaround—When representing a control function to toggle between repeater and talkaround modes in the controlled radio, use the following xml within <ControlFunctions>:

```
<Simple shortName="RTA" description="Select Between Repeater and
    Talkaround Transmit Modes">
          Action type="pressed">
                    <Command>
                              <SetRepeaterTaModevalue="ON" />
                    </Command>
          </Action>
</Simple>
```

- Transmit Power—When representing a control function to toggle transmit power in the controlled radio, use the following xml within <ControlFunctions>:

```
<Simple shortName="PWR" description="Select Between High and Low
    Transmit Power Modes">
          <Action type="pressed">
                    <Command>
                              <SetTxPowerModevalue="ON" />
                    </Command>
          </Action>
</Simple>
```

- Scan—When representing a control function to toggle scan mode in the controlled radio, use the following xml within <ControlFunctions>:

```
<Simple shortName="SCN" description="Enable/Disable Scan Mode">
          <Action type="pressed">
                    <Command>
                              <SetScanModevalue="ON" />
                    </Command>
          </Action>
</Simple>
```

- Emergency Mode—When representing a control function to toggle emergency mode in the controlled radio, use the following xml within <ControlFunctions>:

```
<Simple shortName"EMG" description="Enable/Disable Emergency
    Mode">
          <Action type="pressed">
                    <Command>
                              <SetEmergencyModevalue="ON" />
                    </Command>
          </Action>
</Simple>
```

Caveats for PMC Operation

For Serial Control the CTRL button opens a browser-based UI to control radios. This button is available only on the 36 channel PMC. This applies to tone control only.

If you are using a tone controlled radio, be aware of the following PMC operation caveats when configuring tone sequences in radio and tone descriptor files:

- For tone control sequences (channel selectors and radio control functions), Cisco IPICS supports only RFC 2833 tones (DTMF entries are not supported).
- You cannot enter more than six consecutive RFC 2833 tones in a tone control sequence.

  The following example shows the format of an RFC 2833 tone:

  ```
  <Rfc2833Tone db="0" duration="40" frequency="100" />
  ```

  A tone sequence is a sequence of tones, as shown in the following example:

  ```
  <Rfc2833Tone db="0" duration="40" frequency="100" />
  <Rfc2833Tone db="0" duration="40" frequency="200" />
  <Rfc2833Tone db="0" duration="40" frequency="300" />
  <Rfc2833Tone db="0" duration="40" frequency="400" />
  <Rfc2833Tone db="0" duration="40" frequency="500" />
  <Rfc2833Tone db="0" duration="40" frequency="600" />
  ```

Note The tone sequence in the previous example does not display more than six consecutive RFC 2833 tones ("100" through "600").

- For tone signaling, Cisco IPICS supports both RFC 2833 tone and RFC 2833 event (DTMF) commands.

  You can enter more than six consecutive RFC 2833 tones only if the sixth tone event is separated by a pause entry (such as one ms) or a DTMF digit entry (such as digit one for 200 ms).

Note When you enter DTMF digits, be sure to configure a delay between the digits so that DTMF gets detected, as required by the local specifications. U.S. specifications require a delay of 40 ms.

There is no limit to the number of DTMF entries that are allowed in a signaling tone sequence.

Note You can define a pause by a tone with a frequency of zero, as in the following example:

<Rfc2833Tone db="0" frequency="0" duration="40" />

where:

db="0" frequency="0" represents the pause entry.

- Since tone sequences, whether in signaling or control sequences, are grouped into RFC 2198 packets, a maximum duration gets imposed for some of the tones. For example, if ‘n’ is the total number of tones in the tone sequence, where max(n) = 6, the maximum duration for the first (n-1) tones cannot be more than two seconds.
- The maximum duration for any RFC 2833 tone or event is eight seconds.
- Because preamble tones that are longer than one second compromise the beginning of talk spurts, there is a maximum possible voice delay of one second.

For some examples of valid and invalid descriptor file entries, refer to the *Cisco IPICS Radio and Tone Descriptor File Examples Reference Card.*

Understanding the Descriptors Window

The Descriptors window lists information about each of the radio and/or tone and serial descriptor files that you have added in Cisco IPICS.

This window also enables you to perform several radio and tone descriptor management functions. To display the Descriptors window, navigate to **Configuration > Descriptors** in the Administration Console.

Table 2-13 describes the items in the Descriptors window.

Table 2-13 Fields in the Descriptors Window

Field	Description	Reference
Name field	This field indicates the name of the radio type that Cisco IPICS supports.	See the "Radio Descriptors" section on page 2-70, the "Tone Descriptors" section on page 2-72, and the "Adding Descriptors" section on page 2-82
File Name field	This field indicates the name of the radio/tone descriptor .xml file.	
Type field	This field indicates the type of descriptor. **Note** When choosing a descriptor type in the Administration Console, be aware that a *Tone Radio* descriptor type refers to a radio descriptor file and a *Tones* descriptor type refers to a tone descriptor file.	
File Size (KB) field	This field indicates the size of the descriptor file.	
Last Update field	This field indicates the date and time of the last modified descriptor file.	
Add button	Click this button to add new descriptor files.	See the "Adding Descriptors" section on page 2-82
Update button	Click this button to update existing descriptor files.	See the "Updating Radio and Tone Descriptors" section on page 2-83
Delete button	Click this button to delete descriptor files from Cisco IPICS.	See the "Deleting Radio and Tone Descriptors" section on page 2-85

Table 2-13 Fields in the Descriptors Window (continued)

Field	Description	Reference
Display Controls		
Rows per page drop-down list box	Specifies the number of rows of descriptors that are included in a descriptors list page.	See the "Navigating Item Lists" section on page 1-16
Page field	Displays descriptors on a specific page.	
|< (First page) button	Displays the first page of the descriptors list.	
< (Previous page) button	Displays the previous page of the descriptors list.	
> (Next page) button	Displays the next page of the descriptors list.	
>| (Last page) button	Displays the last page of the descriptors list.	

Adding Descriptors

You can add descriptors to Cisco IPICS in the **Configuration > Descriptors** window in the Administration Console.

For detailed information about descriptors, see the "Radio Descriptors" section on page 2-70 and "Tone Descriptors" section on page 2-72.

For examples of valid and invalid descriptor file .xml entries, refer to the *Cisco IPICS Radio and Tone Descriptor File Examples Reference Card*.

Note When choosing a descriptor type in the Administration Console, be aware that a *Tone Radio* descriptor type refers to a radio descriptor file and a *Tones* descriptor type refers to a tone descriptor file.

To add a new descriptor file, perform the following procedure:

Procedure

Step 1 From the Cisco IPICS Administration Console, navigate to the **Configuration > Descriptors** window.

Step 2 In the Descriptors window, click **Add**.

The New Descriptor window displays.

Step 3 From the Descriptor Type drop-down list box, choose one of the following options:

- **Tone Radio**—Choose this option to add a descriptor file for a tone control radio.
- **Serial Radio**—Choose this option to add a descriptor file for a serial control radio.
- **Tones**—Choose this option to add a tone descriptor file.

Step 4 To locate the descriptor file that you want to add, click **Browse**.

Step 5 In the Choose File window, navigate to the location of the descriptor file that you want to add and highlight the file.

Step 6 Click **Open**.

The File to Upload field gets populated with the descriptor file that you selected.

Step 7 Click **Save**.

If you do not want to add the descriptor, click **Cancel**.

Note If you need to modify an existing descriptor file, follow the steps in the "Updating Radio and Tone Descriptors" section on page 2-83.

Updating Radio and Tone Descriptors

You can update an existing descriptor file in Cisco IPICS in the Descriptors window.

Note When choosing a descriptor type in the Administration Console, be aware that a *Tone Radio* descriptor type refers to a radio descriptor file and a *Tones* descriptor type refers to a tone descriptor file.

When you update a radio descriptor to add new channel selectors and/or control functions, all of the radio instances that are currently using this descriptor get updated accordingly. If there are any PMC users using these radio instances, their PMC clients get updated also.

If you update a tone descriptor, the system checks the newly uploaded file for missing commands that may be in use by the radio descriptor file.

Note If you upload a new file that is missing a command, which is in use by the radio descriptor, the system does not allow the update.

For more detailed information about radio and tone descriptors, see the "Radio Descriptors" section on page 2-70 and the "Tone Descriptors" section on page 2-72.

To update radio and tone descriptors, perform the following procedure:

Procedure

Step 1 From the Cisco IPICS Administration Console, navigate to the **Configuration > Descriptors** window.

Step 2 Click the radio button next to the descriptor that you want to update.

Step 3 Click **Update**.

Step 4 Click the **Browse** button, that is next to the File to Upload field.

Step 5 In the Choose File window, navigate to the location of the descriptor file that you want to use to update and highlight the file.

Step 6 Click **Open**.

The File to Upload field gets populated with the descriptor file that you selected.

Step 7 Click **Save**.

If you do not want to update the descriptor, click **Cancel**.

Note If there are multiple radio descriptor files for the same type of radio, the Cisco IPICS server uses the latest uploaded file. This feature allows you to update the radio descriptor file for a given radio type by uploading a new descriptor file.

Deleting Radio and Tone Descriptors

You can delete radio and tone descriptor files from Cisco IPICS.

Note You cannot delete radio descriptor files that are being used by radios.

For more detailed information about radio and tone descriptors, see the "Radio Descriptors" section on page 2-70 and the "Tone Descriptors" section on page 2-72.

To delete a radio, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Radios** window.

Step 2 Check the check box next to each radio that you want to delete.

Step 3 Click **Delete**.

A dialog box prompts you to confirm the deletion.

Step 4 To confirm the deletion, click **OK**.

If you do not want to delete the radio(s), click **Cancel**.

Managing 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.

If two or more users are connected to the same multicast network (or domain), they are in the same location but not necessarily in the same physical place. If two or more users are in the same location and are using the same multicast channel, they can talk to each other without the need for additional resource configuration.

This section includes the following topics:

- Predefined Cisco IPICS Locations, page 2-86
- Location Associations, page 2-87
- Summary of Access Types and Connections, page 2-91

Predefined Cisco IPICS Locations

In addition to specifically assigning names to locations, Cisco IPICS includes the following 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. The designation of ALL is the sum total of all defined locations.

Note The ALL 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 not applicable to IP phones or RMS components, which are not associated with multicast addresses. The Cisco IPICS server assumes that the multicast address associated with a channel or VTG that is designated with the ALL location can reach all multicast locations; however, this assumption is not always accurate.

- 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 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 each channel 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 An RMS includes digital signal 0 (DS0) resources that are used to connect channels in to VTGs (or VTGs in to VTGs) and to provide SIP-based unicast access to PMC users.

Location Associations

The following Cisco IPICS resources always maintain location associations:

- RMS—Each RMS 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.

- Channels—You can associate a channel with one or more locations. If you associate a user to a channel, the user is assigned the channel configuration that is associated to the current user location. Whenever possible, user access via multicast communication is preferable over SIP to minimize the user of RMS resources.

  The following examples describe the access that is available based on the specified configurations:

  Configuration:

  - Channel 1 is defined with the Alpha location and the Bravo location
  - Channel 2 is defined with the Delta location
  - Channel 3 is defined with the ALL location
  - User 1 is a member of VTG X
  - User 1 is assigned to Channel 1, 2, and 3 and VTG X

  Example 1: PMC User 1 logs in to Cisco IPICS by using the Alpha location

  - User 1 is given access to Channel 1 via the multicast address that is assigned to Channel 1 in the Alpha location.
  - Channel 2 is not included in the current location of User 1 (Alpha), so the server allocates an RMS resource in the Delta location to provide SIP-based connectivity.
  - Channel 3 is defined with the ALL location, so the server enables User 1 for multicast access to Channel 3.
  - VTG X is, by definition of a VTG, in the ALL location, so the server enables User 1 for multicast access to VTG X.

  Example 2: PMC User 1 logs in to Cisco IPICS by using the Delta location

  - Channel 1 is not included in the Delta location, so the server allocates an RMS resource in either the Alpha location or the Bravo location to provide SIP-based access to Channel 1.
  - Channel 2 is included in the Delta location, so the server enables multicast access.

  - Channel 3 is defined with the ALL location, so the server enables User 1 for multicast access.
  - VTG X is defined in the ALL location, so the server enables User 1 for multicast access.

  Example 3: PMC User 1 logs in to Cisco IPICS by using the REMOTE location

  - Channel 1, 2, and 3 and VTG X all require that the server allocate RMS resources for this connection.
  - Channel 1 requires that the server allocates an RMS resource from either the Alpha location or the Bravo location.
  - Channel 2 requires that the server allocates an RMS resource from the Delta location.
  - Channel 3 and VTG X are both defined with the ALL location.

- VTGs—VTGs are always assigned to the ALL location. Each channel that you assign to a VTG uses one RMS resource.
- PMC—During the login process, the PMC user chooses their current location or the REMOTE location.

  When a user chooses the REMOTE location, the server configures all of the user-assigned channels and VTGs for SIP-based access. In this case, the server must allocate one RMS resource for each channel and VTG. If the server has insufficient resources to use in the location that is specified by the channel configuration, the PMC user receives a message to indicate that the channel is not available.

  When the user chooses a location other than REMOTE, the server assigns direct multicast access to each channel that you configure with the same location as the chosen location, and any channel that you configure with the ALL location.

Note The server considers any assigned channels that cannot be accessed directly by using a multicast connection to be in the REMOTE location, which causes Cisco IPICS to allocate RMS resources for each one of those assigned channels.

- IP Phones—Cisco Unified IP Phones support only multicast connections. To use IP phones with Cisco IPICS, you must assign a location that is the same as the dial login default location. The server assigns the configured default location to an IP phone user when the user logs in to Cisco IPICS. (In this case, there is no user selection for location.) IP phone users can access only the associated channels that are assigned to their default location, along with any assigned VTGs. If the configured default location is the ALL location, IP phone users can access only the channels that are assigned to the ALL location. Because of this implementation, Cisco recommends that you do not assign the ALL location as the default location for the IP phone user.
- Dial-in/Dial-out Users—When a user accesses the telephony user interface (TUI), the user connects to the Cisco IPICS dial engine by using unicast communications. The dial engine allows the TUI user to join any VTG or channel to which the user is associated.
  - When the user selects a channel, the server creates a VTG that contains the selected channel and assigns the VTG an address from the multicast pool. For this VTG, the server uses the RMS that is configured with the same location as the channel that the TUI user has selected.
  - When the user selects a VTG, the server creates a VTG that contains the selected VTG and assigns the VTG an address from the multicast pool. For this VTG, the server can use any RMS.

  In both cases, the server establishes a unicast call flow between the TUI user and the dial engine. The dial engine converts the unicast call flow to multicast by using the address that was assigned from the multicast pool. This multicast traffic flows to the RMS where the VTG was activated. When the VTG traffic reaches the RMS it is bridged to the channel or VTG that the user has selected. Therefore, the dial engine must be in the ALL location, or multicast domain.
- Allocation of RMS resources—When multiple eligible RMS components exist, Cisco IPICS allocates resources by using the "least recently used" algorithm to achieve load balancing. The following examples show how this algorithm works:

  Example 1:

  - Channel A is defined in the ALL location
  - RMS 1 is defined in Location 1
  - RMS 2 is defined in Location 2

When the server needs to allocate an RMS resource for Channel A, it determines which RMS is the "least recently used" RMS and allocates the resource in the appropriate RMS.

Example 2:

- Channel B is defined in Location 2
- RMS 1 is defined in Location 1
- RMS 2 is defined in Location 2

In the above example, the server allocates resources from RMS 2 because RMS 1 is defined in a different location.

Summary of Access Types and Connections

Table 2-14 shows a summary of the Cisco IPICS access types and connections, as they pertain to locations.

Table 2-14 Cisco IPICS Access Types and Connections

Access	Type of Connection	Description
IP Phone	Multicast (in all cases)	• Can connect to any VTG that the IP phone user is associated with. • Can connect to any channel that the IP phone user is associated with if the channel is in the same location as the location that is defined in the user dial login default location.
Dial-in	Unicast to the dial engine (in all cases)	• Can connect to any channel or VTG that the dial-in user is associated with.
PMC (remote login)	Unicast	• All channels and VTGs are unicast calls to the appropriate RMS.

Table 2-14 Cisco IPICS Access Types and Connections (continued)

Access	Type of Connection	Description
PMC (non-remote login)	Multicast	• Can connect to any channel via multicast if the user is associated with the channel and the channel is configured with the same location as the location that was chosen by the user at login. • Can connect to any VTG that the user is associated with.
PMC (non-remote login)	Unicast	• Can connect to any channel that is configured with a location that is different from the location that was chosen at login.

You can perform the following location-related management tasks:

- Understanding the Locations Window, page 2-92
- Adding a Location, page 2-93
- Viewing or Editing a Location, page 2-94
- Deleting a Location, page 2-95

Understanding the Locations Window

The Locations window lists information about each of the locations that you have added in Cisco IPICS. It also allows you to perform several locations management functions.

To display the Locations window, navigate to the **Configuration > Locations** link in the Administration Console.

Note By default, location names appear in ascending alphanumeric order.

Table 2-15 describes the items in the Locations window.

Table 2-15 Items in the Locations Window

Item	Description	Reference
Location Name field	Specifies the name that is assigned to the location	See the "Viewing or Editing a Location" section on page 2-94
Add button	Allows you to add a new location in Cisco IPICS	See the "Adding a Location" section on page 2-93
Delete button	Allows you to delete a location	See the "Deleting a Location" section on page 2-95

Adding a Location

You can add locations to Cisco IPICS, as needed.

To add a location, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Locations** window.

Step 2 To add a location, click **Add**.

Step 3 In the Location Name field, enter a name for the location.

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

Note The PMC may truncate the location name if the name includes more characters than the PMC can display.

Tip Remember to assign location names that make sense to you.

Step 4 Click **Save**.

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

Viewing or Editing a Location

You can view or edit a location that is configured in Cisco IPICS.

To view or edit a location, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Locations** window.

Step 2 In the Location Name column, click the link of the location that you want to view or edit.

The window for the location that you choose displays.

Step 3 View or edit the location as desired; then click **Save**.

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

Note The PMC may truncate the location name if the name includes more characters than the PMC can display.

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

To add a location, see the "Adding a Location" section on page 2-93. To delete a location, see the "Deleting a Location" section on page 2-95.

Deleting a Location

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

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

Note You cannot delete the **ALL** or **REMOTE** locations.

To delete a location from Cisco IPICS, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Locations** window.

Step 2 Check the check box next to each location that you want to delete.

Step 3 Click **Delete**.

A dialog box prompts you to confirm the deletion.

Step 4 To confirm the deletion, click **OK**.

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

Managing the Multicast Pool

Cisco IPICS stores multicast addresses in the multicast pool. When you activate a VTG, Cisco IPICS automatically assigns an available multicast address from the multicast pool to that VTG.

Note Multicast addresses are dynamically assigned from the multicast pool to VTGs only; channels are explicitly configured with static addresses.

When a VTG deactivates, its multicast address is released for use by another VTG.

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

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

- Adding Multicast Addresses, page 2-98
- Viewing and Editing Multicast Address Information, page 2-100
- Deleting a Multicast Address, page 2-102

When using multicast communications with Cisco IPICS, Cisco recommends that you follow the guidelines in the "Guidelines for Using IP Multicast Addresses with Cisco IPICS" section on page 2-98.

You perform the multicast pool management tasks in the Multicast Pool window. For more information about this window, including how to access it, see the "Understanding the Multicast Pool Window" section on page 2-96.

Understanding the Multicast Pool Window

The Multicast Pool window lists information about each of the multicast addresses that you have added in Cisco IPICS. It also allows you to perform several multicast pool functions.

Note Cisco strongly recommends that you follow the guidelines in the "Guidelines for Using IP Multicast Addresses with Cisco IPICS" section on page 2-98 when you use multicast communications with Cisco IPICS.

To display the Multicast Pool window, access the Configuration drawer and click **Multicast Pool**.

Each multicast address in the multicast pool window appears on its own row with related information in various columns. By default, rows of information appear in ascending order by multicast address.

Table 2-16 describes the items in the Multicast Pool window.

Table 2-16 Fields in the Multicast Pool Window

Field	Description	Reference
Address field	This field specifies the multicast address and port.	See the "Guidelines for Using IP Multicast Addresses with Cisco IPICS" section on page 2-98
Location field	This field specifies the location that is assigned to this multicast address. The location name can include alphanumeric characters, spaces, and any of these characters: . , – ‘ # ( ) / :_ .	See the "Viewing and Editing Multicast Address Information" section on page 2-100 and the "Deleting a Multicast Address" section on page 2-102 See the "Adding Descriptors" section on page 2-82 for more detailed information about locations.
Status field	Either of the following designations can display in this field: • Active—Address is assigned to an active channel/VTG/radio. • Idle—Address is not assigned to an active channel/VTG/radio.	
Connection Type field	Either of the following designations can display in this field: • Used by Channel—Multicast address is assigned to a PTT channel. • Used by VTG—Address is reserved for use or is in use by a VTG. Cisco IPICS assigns an available multicast address to a VTG automatically. When the VTG ends, the address becomes available for another VTG. • Used by Radio—Multicast address is assigned to a radio.	
Used By field	This field specifies the name of the active channel, VTG, or radio that is using the multicast address, if applicable.	

Field	Description	Reference
Add button	Click this button to add a multicast address.	See the "Adding Multicast Addresses" section on page 2-98
Delete button	Click this button to delete a multicast address.	See the "Deleting a Multicast Address" section on page 2-102

Guidelines for Using IP Multicast Addresses with Cisco IPICS

Be aware of the following guidelines when you use multicast communications with Cisco IPICS:

Cisco IPICS strongly recommends IP multicast addresses that are 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 information, refer to RFC 3171 - Internet Assigned Numbers Authority (IANA) Guidelines for IPv4 Multicast Address Assignment and RFC 2365 - Administratively Scoped IP Multicast.

For additional information about the use of IP multicast addressing, refer to the following URL:

http://www.cisco.com/en/US/tech/tk828/tsd_technology_support_protocol_home.html

Adding Multicast Addresses

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

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

Before you add a multicast address, configure locations, as described in the "Adding Descriptors" section on page 2-82.

To add one or more multicast addresses to the multicast pool, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Multicast Pool** window.

Step 2 Click **Add**.

The New Multicast Pool window displays.

Step 3 In the Address field, enter the multicast address that you want to add.

Be sure to enter a valid multicast address that begins with 239.

Note Cisco strongly recommends that you configure only addresses that are in the 239.192.0.0 to 239.251.255.255 range. For more information, see the "Guidelines for Using IP Multicast Addresses with Cisco IPICS" section on page 2-98.

Step 4 In the Number of Addresses field, enter the number of IP addresses that you want Cisco IPICS to generate.

You can enter a number between 1 and 255.

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

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

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

```
239.195.5.1
239.195.5.2
239.195.5.3
239.195.5.4
```

```
239.195.5.5
```

Note When you generate multicast addresses in this way, Cisco IPICS assigns the port number that you designate to each address. After Cisco IPICS generates the list of addresses, you can change the number or port for any address, and you can delete any addresses that you do not want in the multicast pool. For more information, see the "Deleting a Multicast Address" section on page 2-102.

Step 5 In the Port field, enter the port number for this address.

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

Step 6 Click **Save**.

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

Step 7 If you want to add other individual addresses, repeat Step 3 through Step 6.

Viewing and Editing Multicast Address Information

You can view information for any multicast address, and you can change a multicast address and port number. You do so in the Multicast Pool window.

To view or edit multicast address information, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Multicast Pool** window.

Step 2 To view or edit a multicast address, click the link for the multicast address that you want to view or change.

The Multicast Address Pool Information window for the selected multicast address displays.

Step 3 View or update the information that is described in Table 2-17.

Table 2-17 Multicast Address Details Area Fields

Field	Description
Address	This field represents the multicast address. You add an address, enter a valid multicast address, and make sure to enter all 4 octets of the address. Each octet must be in the range of 0 through 255. **Note** Cisco IPICS strongly recommends addresses that are configured in the 239.192.0.0 to 239.251.255.255 range. For more detailed information, see the "Guidelines for Using IP Multicast Addresses with Cisco IPICS" section on page 2-98.
Port	This field represents the port number assigned to the multicast address. This value must be an even number in the range of 21000 through 65534. **Note** Cisco IPICS does not allow the configuration of any port below 21000 or any odd ports.
Connection Type—*Display only*	This field can include either of the following designations: • Used by Channel—Address is assigned to a PTT channel. • Used by VTG—Address is reserved for use or is in use by a VTG. Cisco IPICS assigns an available multicast address to a VTG automatically. When the VTG ends, the address becomes available for another VTG. • Used by Radio—Address is assigned to a radio.
Status—*Display only*	This field can include either of the following states: • Active—Address is assigned to an active channel/VTG/radio. • Idle—Address is not assigned to an active channel/VTG/radio.

Table 2-17 Multicast Address Details Area Fields (continued)

Field	Description
Location—*Display only*	Location that is assigned to this multicast address. An address for a PTT channel has a specific location, either location ALL or another location name. Regardless of the location in this field, a VTG can contain only channels that are in the same multicast domain as the RMS that is used to mix the channels. See the "Adding Descriptors" section on page 2-82 for more detailed information about locations.
Used By—*Display only*	Name of the active channel, VTG, or radio that is using the multicast address, if applicable.
Last Released—*Display only*	This field displays when the multicast address was last released.

Step 4 Click **Save** to save your changes.

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

Deleting a Multicast Address

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

Note You cannot delete a multicast address that is assigned to an active VTG. You must deactivate the VTG before you can delete the address. You also cannot delete a multicast address that is assigned to a channel. To delete the address in this case, delete the channel, which automatically removes the multicast address from the multicast pool.

To delete a multicast address from the multicast pool, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > Multicast Pool** window.

Step 2 Check the check box next to each multicast address that you want to delete.

Step 3 Click **Delete**.

A dialog box prompts you to confirm the deletion.

Step 4 To confirm the deletion, click **OK**.

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

Managing the RMS

An RMS is a 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.

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

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

- Viewing and Editing RMS Details, Activating an RMS, and Deactivating an RMS, page 2-106
- Adding an RMS, page 2-112
- Viewing and Configuring Loopbacks, page 2-114
- Deleting an RMS, page 2-117
- Managing the RMS Configuration, page 2-118

You perform the RMS management tasks in the RMS window, which is located in the Configuration drawer. For more information about this window, including how to access it, see the "Understanding the RMS Window" section on page 2-104.

Note Cisco IPICS is not intended to provide complete management capabilities for an RMS. Cisco IPICS manages only the voice-specific parameters that are necessary to set up audio services for Cisco IPICS.

Understanding the RMS Window

The RMS window lists the RMS components that are available in your Cisco IPICS network. This window also allows you to perform the RMS management functions.

To display the RMS window, navigate to the **Configuration > RMS** window in the Administration Console.

The Routers pane in the RMS window displays the name of each RMS that is configured in your Cisco IPICS network.

For detailed RMS configuration information, see the Appendix A, "Configuring the Cisco IPICS RMS Component."

Table 2-18 describes the items in the RMS window.

Table 2-18 Items in the RMS Window

Item	Description	Reference
RMS Name field	This field specifies a unique name that is assigned to the RMS.	See the "Viewing and Editing RMS Details, Activating an RMS, and Deactivating an RMS" section on page 2-106 and the "Adding an RMS" section on page 2-112 See the "Managing Locations" section on page 2-86 for detailed information about configuring locations
Location field	This field specifies the multicast domain that contains the multicast addresses that can be accessed by this RMS.	
IP Address field	This field specifies the IP address of the Loopback interface.	
Router Type field	This field specifies the model number of the RMS.	
Status field	This field indicates whether an RMS is operational, configured, stopped, deactivated, or unreachable.	

Table 2-18 Items in the RMS Window

Item	Description	Reference
Available field	Number of DS0s that are available for use in Cisco IPICS.	See the "Viewing and Configuring Loopbacks" section on page 2-114
In Use field	Number of DS0s that are currently being used in Cisco IPICS.	
Reserved field	Number of DS0s that are reserved for non-Cisco IPICS use.	
In Error field	Number of DS0s that are misconfigured.	
Add button	Choose this button to add an RMS component.	See the "Adding an RMS" section on page 2-112
Delete button	Choose this button to delete an RMS component.	See the "Deleting an RMS" section on page 2-117
Configuration drop-down list box	Provides the ability to merge, update, or show configuration information for an RMS component.	See the "Managing the RMS Configuration" section on page 2-118
Display Controls		
Rows per page drop-down list box	Specifies the number of rows of RMS components that are included in a RMS components list page.	See the "Navigating Item Lists" section on page 1-16
Page field	Displays RMS components on a specific page.	
|< (First page) button	Displays the first page of the RMS components list.	
< (Previous page) button	Displays the previous page of the RMS components list.	
> (Next page) button	Displays the next page of the RMS components list.	
>| (Last page) button	Displays the last page of the RMS components list.	

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

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

By default, Cisco IPICS polls the RMS every 10 minutes, using the RMS comparator mechanism. The RMS comparator checks the responsiveness of the RMS if there have been any changes made to the configuration. If there have been changes to the RMS 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. For more information, see the "Managing Cisco IPICS Options" section on page 2-140.)

Tip Because the RMS comparator mechanism can interject delays, you can disable it by navigating to the **Administration > Options** window and checking the **Disable RMS Comparator** check box. You should check this check box if you are connected via a high latency (high delay), low bandwidth connection, such as a satellite link. Be aware that when you disable the RMS Comparator, you must merge the RMS configuration to make sure that the router is synchronized with the server. For information about how to merge RMS configuration, see the "Managing the RMS Configuration" section on page 2-118. For more complete configuration and deployment details, refer to the *Solution Reference Network Design (SRND)* (latest version).

Note Disabling the RMS Comparator affects every router in the network.

Editing or Viewing RMS Details

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

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > RMS** window.

Step 2 In the RMS Name column, click the link of the RMS that you want to view or change.

The General tab for the selected RMS displays.

Step 3 To change any RMS information, except updating the name, configuring loopbacks, or reserving or unreserving DS0s, click **Deactivate**.

This action makes the RMS temporarily unavailable to Cisco IPICS.

Tip Before you make changes, wait until all RMS resources are not in use, or manually disable the channel or deactivate any VTG that uses the resources of this RMS. For more information about how to disable a channel, see the "Changing the Status of a PTT Channel" section on page 2-21. For information about how to deactivate a VTG, "Changing the Status of a VTG" section on page 4-18.

Step 4 To view or update the information in the General tab, see Table 2-19.

Table 2-19 Fields in the General Tab of the RMS Window

Field	Description
Identification	
Name	This field specifies the name of the RMS. The name can include alphanumeric characters, spaces, and any of these characters: . , – ‘ # ( ) / :.
Location	This field specifies the multicast domain that contains the multicast addresses that can be accessed by this RMS. An RMS must be configured with the same location that is configured for the channels that it serves. See the "Managing Locations" section on page 2-86 for detailed information about locations.

Table 2-19 Fields in the General Tab of the RMS Window (continued)

Field	Description
Description	This field specifies a description for the RMS.
	This field specifies a description for the RMS.
Status—*Display only*	This field can include any of the following statuses: • Operational—RMS has at least one loopback configured and that is operating. • Unconfigured—RMS has no loopbacks. • Stopping—RMS has been deactivated but has at least one DS0 in use by Cisco IPICS. The RMS deactivates when Cisco IPICS no longer uses any of its voice ports. **Note** If one or more VTGs are active and you try to deactivate an RMS, the RMS status displays as Stopping. You must deactivate the VTG(s) before the RMS displays a deactivated status. To deactivate a VTG, see the "Changing the Status of a VTG" section on page 4-18. • Deactivated— RMS has been deactivated and has no DS0s in use. **Note** You can change the user name, password, multicast address, or location of the RMS only when it is in the Deactivated state. • Unreachable—RMS cannot be reached by the Cisco IPICS server.
Hardware Settings	
IP Address	This field specifies the IP address of the Loopback interface.
Host Name—*Display only*	This field specifies the host name of the RMS.
User Name	This field specifies the user name that Cisco IPICS uses to access the RMS. This name must have administrator privileges on the RMS.

Table 2-19 Fields in the General Tab of the RMS Window (continued)

Field	Description
Password	This field specifies the password that Cisco IPICS uses to access the RMS.
Router Type—*Display only*	This field specifies the model number of the RMS.
Controllers—*Display only*	This field displays the T1/E1 connections on the RMS. The number in parentheses is the number of ports on the corresponding controller.
Loopbacks—(Click the **Loopbacks** Tab to access the Loopback information)	This field specifies the mappings between two controllers that are physically connected. To change a loopback, choose a pair of controllers from the two Loopback drop-down list boxes and click **Add**. A controller appears in gray if it is in use. Each configured loopback appears in a list near the bottom of this area. To see detailed information about a loopback, click the right arrow next to its name. To see detailed information about all loopbacks, click **Expand All**. To collapse an expanded view of a loopback, click the down arrow next to its name. To collapse detailed information about all loopbacks, click **Collapse All**. For an explanation of the detailed loopback information, see the "Viewing and Configuring Loopbacks" section on page 2-114.

Step 5 If you changed information in the IP Address, User Name, or Password fields, make the corresponding change in the router by using the configuration application of the router.

Step 6 Click **Save** to save your changes.

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

Step 7 If you deactivated the router, click **Activate** to reactivate it.

After you change information for an RMS, it can take up to 10 minutes (by default) for Cisco IPICS to recognize the changes. If you want to cause Cisco IPICS to recognize the changes immediately, see the "Managing the RMS Configuration" section on page 2-118.

Note You can change the default time that Cisco IPICS takes to recognize an RMS by entering a new value in the RMS Polling Frequency field in the **Administration > Options** window. For more information, see the "Managing Cisco IPICS Options" section on page 2-140.

Deactivating or Activating an RMS

When you deactivate an RMS, it goes into the Deactivated state and becomes unavailable for use by Cisco IPICS until you activate it. You should deactivate an RMS when you make certain changes to it, as described in the "Editing or Viewing RMS Details" section on page 2-107.

Note If you deactivate an RMS that has one or more voice ports in use by Cisco IPICS, or if one or more VTGs are active, the RMS goes into the Stopping state. You cannot deactivate an RMS if any VTGs are active. A router that is in the stopping state cannot provide additional support for PMC SIP connections or additional channels that are participants in active VTGs. Existing connections and channels that are supported by the RMS are not affected. The RMS becomes deactivated when Cisco IPICS no longer uses any of its voice ports. To deactivate a VTG, see the "Changing the Status of a VTG" section on page 4-18.

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

To deactivate or activate an RMS, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > RMS** window.

Step 2 In the RMS Name column, click the link of the RMS that you want to deactivate.

Step 3 Click **Deactivate** to deactivate an active RMS, or click **Activate** to activate a deactivated RMS.

Note Activation or deactivation of a VTG requires that the Cisco IPICS server communicate with the RMS. If a VTG is deactivated when the RMS is 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 with, and synchronizes with the RMS.

Adding an RMS

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

- The router must exist on the Cisco IPICS network and it must be configured as described in Appendix A, "Configuring the Cisco IPICS RMS Component"
- At least one location must be defined, as described in the "Managing Locations" section on page 2-86

To add a new RMS in Cisco IPICS, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > RMS** window.

Step 2 Click **Add**.

The **Add** New Router Media Service window displays.

Step 3 In the Add New Router Media Service area, enter the following information:

Note For detailed descriptions of the RMS fields, see Table 2-19.

a. In the IP Address field, enter the IP address of the loopback interface. The IP address of the loopback interface must be configured to support SIP calls.

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

c. In the Password field, enter the password that is required to log in to the RMS.

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

   See the "Managing Locations" section on page 2-86 for more detailed information about locations.

e. Click **Save**.

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

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

   The Router Details area displays the following information for the router that you added:

   – Location—This field specifies the location that is defined for this RMS
   – Status—This field displays unconfigured because you have not yet saved the changes that you made.
   – IP Address—This field specifies the IP address that you entered for this router.
   – Host Name—This field specifies the host name that you configured on the router.
   – User Name—This field specifies the user name that you entered for this router.
   – Password—This field specifies the password that you entered for this router.
   – Type—This field specifies the model number of this router
   – Controllers—This field specifies the T1 connections that the router has available for loopback.

Step 4 In the Name field, enter a name for the RMS if you want to change the name that displays in the list or routers in the Manager Routers window.

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

Step 5 In the adjacent Loopbacks drop-down lists, create a loopback by choosing two controllers that are physically connected on the router; then click **Add**.

Repeat this step as needed to create additional loopbacks.

Step 6 Configure digital signal 0 (DS0s) for each loopback as described in the "Viewing and Configuring Loopbacks" section on page 2-114.

Step 7 Click **Save** to save the configuration for this RMS.

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

After you add an RMS, it can take up to 10 minutes (by default) for Cisco IPICS to recognize the addition. If you want to cause Cisco IPICS to recognize the addition immediately, see the "Managing the RMS Configuration" section on page 2-118.

Viewing and Configuring Loopbacks

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

- Viewing Detailed Information about a Loopback, page 2-114
- Enabling DS0s in a Loopback, page 2-115
- Disabling DS0s in a Loopback, page 2-116
- Removing a Loopback, page 2-117

Viewing Detailed Information about a Loopback

You view loopback information in the **Loopbacks** tab of the RMS window. You can access this tab by navigating to the **Configuration > RMS** window and clicking the **Loopbacks** tab.

For more information about the RMS window, see the "Understanding the RMS Window" section on page 2-104.

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

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

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

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

Enabling DS0s in a Loopback

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

To enable DS0s in a loopback, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > RMS** window.

Step 2 Click the **Loopbacks** tab.

Step 3 Expand each loopback in which you want to enable DS0s by clicking the right arrow next to its name or by clicking **Expand All**.

Step 4 Check the check box next to each DS0 that you want to enable.

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

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

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

Step 5 Click **Enable DS0s**.

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

Step 6 Click **Save**.

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

Disabling DS0s in a Loopback

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

To disable DS0s in a loopback, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > RMS** window.

Step 2 Click the **Loopbacks** tab.

Step 3 Expand each loopback in which you want to disable DS0s by clicking the left arrow next to its name or by clicking **Expand All**.

Step 4 Check the check box next to each DS0 that you want to disable.

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

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

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

Step 5 Click **Disable DS0s**.

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

Step 6 Click **Save**.

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

Removing a Loopback

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

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

Deleting an RMS

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

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

To delete an RMS, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > RMS** window.

Step 2 Check the check box next to the RMS that you want to delete.

Step 3 Click **Delete**.

A dialog box prompts you to confirm the deletion.

Step 4 To confirm the deletion, click **OK**.

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

Managing the RMS Configuration

You can manage the RMS configuration by navigating to the **Configuration > RMS** window.

Merging RMS configuration updates Cisco IPICS with the following router information:

- Host name
- Router type
- Controllers

Merge the RMS configuration if you add or remove controllers on the router or if you change its host name, and you want Cisco IPICS to recognize the change.

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

- You have changed information for an RMS as described in the "Viewing and Editing RMS Details, Activating an RMS, and Deactivating an RMS" section on page 2-106 and you do not want to wait for Cisco IPICS to recognize the changes, which can take up to 10 minutes (by default).
- You have added an RMS as described in the "Adding an RMS" section on page 2-112 and you do not want to wait for Cisco IPICS to recognize the addition, which can take up to 10 minutes (by default).
- You restarted an RMS and are experiencing voice connectivity or voice quality issues. Updating the configuration of the RMS can help to eliminate the router configuration as the source of the problem.
- The RMS has restarted but Cisco IPICS has not yet updated the router configuration with the configuration that is specified in Cisco IPICS.

An RMS that shuts down returns to its default configuration when it restarts. Within 10 minutes—by default—after it restarts, Cisco IPICS compares the current RMS configuration with the RMS configuration in the Cisco IPICS database. If there is a discrepancy, Cisco IPICS refreshes the RMS configuration to match the configuration in the database.

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

To manage the RMS configuration, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Configuration > RMS** window.

Step 2 To manage the RMS configuration, check the check box to the left of the RMS Name of the RMS.

Step 3 From the Configuration drop-down list box, take any of the following actions:

- To merge the RMS configuration, choose **Merge**.
- To update the RMS configuration, choose **Update**.
- To view the RMS configuration, choose **Show**.

  The configuration output displays in a separate window showing the configuration of the voice-ports and dial-peers for this RMS.

Cisco IPICS displays changes in the Edit Router Details area.

Tip You can manage the RMS configuration for all of the RMS components that are configured in Cisco IPICS by checking the check box at the top of the RMS list, and choosing **Merge, Update,** or **Show** from the Configuration drop-down list box.

Managing Licenses

The Cisco IPICS license determines the number of concurrent LMR ports, multicast ports, PMC users, Cisco Unified IP Phone users, dial users, and ops views that are available for your system. The total number of LMR and multicast ports, PMC, IP phone, dial users, and ops views cannot exceed the number that is specified in the license or licenses that you purchased.

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

As a Cisco IPICS system administrator, you can obtain and upload new license files, after you have obtained them, to the Cisco IPICS server so that the new licenses take effect. For instructions, see the "Uploading a License File" section on page 2-126.

You perform the license management tasks in the Administration > License Management window. For more information about this window, including how to access it, see the "Understanding the License Management Window" section on page 2-120.

Understanding the License Management Window

The License Management window provides information about the licenses that you configure for your Cisco IPICS installation. It also allows you to upload new licenses to the Cisco IPICS server after obtaining the licenses. See the "Uploading a License File" section on page 2-126 for information about uploading licenses.

To access the License Management window, navigate to Administration >License Management window in the Cisco IPICS Administration Console.

In this window, the **Summary** tab provides a summary of information about the licenses you have obtained for Cisco IPICS. This tab displays license feature names, the total number of ports, current port usage, and available ports. See Table 2-20 for a description of the licenses that can display in this tab.

The **Usage Per Ops View** tab provides license information per ops view. This tab displays types of licenses, the ops view, and current license usage information. See Table 2-21 for a description of the licenses, per ops view, that can display in this tab and the criteria that Cisco IPICS uses to determine license consumption for ports, PMC, IP phone, policy engine, and ops view usage.

Note The data that displays in the License Management window shows the usage at the time that the license window was last accessed. To view the most current license information, refresh your browser window. Make sure to refresh 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 does not succeed and Cisco IPICS displays an error. If you receive an error, refresh your browser window and retry the operation.

Table 2-20 Summary Tab Fields in the License Management Window

Field	Description
Feature Name	
Concurrent LMR Ports	An enabled channel uses an LMR port license. After a channel is disabled, the server releases the LMR license and makes it available for use. **Note** Each radio channel that you add in Cisco IPICS uses one LMR license. However, each unique channel that you configure within a radio channel, does not use a separate LMR license. Cisco IPICS uses only one LMR license per radio. Cisco IPICS bases license usage for ports on the unique combination of a multicast address and a location. If a channel has two multicast addresses that are assigned to the channel, the single channel uses two licenses. If one of the multicast addresses is removed, the system releases one of the licenses so that the port only uses one license.

Table 2-20 Summary Tab Fields in the License Management Window

Field	Description
Concurrent Multicast Ports	An activated VTG uses a multicast port license. After a VTG is deactivated, the server releases the multicast license and makes it available for use. **Note** Be aware that an inactive VTG uses a license when a policy triggers (activates) that VTG; therefore, if the number of licenses has been exceeded, the policy is not able to activate the VTG. Make sure that the server has a sufficient number of licenses available for the configuration of policies.
Concurrent PMC Users	A PMC user uses a license each time that the user logs in to a PMC session. If the same PMC user logs in to multiple PMC sessions from different PMC client machines, that user uses multiple licenses (one for each PMC session). **Note** If you use all of the available PMC licenses, Cisco IPICS interrupts PMC user access to the system. Make sure that you are aware of the current status of PMC licenses, and that you purchase and install additional licenses immediately if you use all of the available PMC licenses.
Concurrent Cisco Unified IP Phone Users	A Cisco Unified IP Phone user uses a license each time that a user logs in to Cisco IPICS from the phone. If you use all of the Cisco Unified IP Phone licenses, no more Cisco Unified IP Phone users can dial in.

Table 2-20 Summary Tab Fields in the License Management Window

Field	Description
Concurrent Dial Users	Each time that the policy engine performs a dial-in or dial-out action, one license is used. If you use all of the dial user licenses, the policy engine cannot perform additional dial-in or dial-out actions. **Note** To enable dial-in/dial-out functionality in Cisco IPICS, you must have a policy engine base license. After you have purchased the policy engine base license, you are able to access the policy engine-related windows and to perform dial-in/dial-out functions in Cisco IPICS. If you do not have a policy engine base license, the dial-in/dial-out functionality is disabled and you are not able to access the policy engine windows.
Cisco IPICS Ops View	Cisco IPICS uses one license for each ops view that you configure. The number of ops views that are available for use displays in the License Summary pane. **Note** To create additional ops views, you must purchase and install a Cisco IPICS license that includes additional ops view ports.
Cisco IPICS Base Server License	License usage does not apply to this field. This field displays whether you have a base license for Cisco IPICS.
Policy Engine Base License	License usage does not apply to this field. This field displays whether Cisco IPICS policy engine is enabled. When the policy engine is enabled, the Summary tab displays **Licensed**. When the policy engine is not enabled, the Summary tab displays **Not Licensed**.

Note Dial ports can be used for dial-in or dial-out connections. For dial ports that are allocated among the ops view, the dial ports are used by dial-in, according to the pre-assigned dial-in phone number, that is configured in each ops view, that is dialed. For dial-out, the dial ports are used from the ops view, to which the user to be dialed, belongs. See Chapter 6, "Configuring and Managing Cisco IPICS Operational Views" for more information about ops views.

The **Usage Per Ops View** tab provides license information per ops view. This tab displays the types of licenses, the ops view, current license usage, and the allocated ports. See Table 2-21 for a description of the information in this tab.

Table 2-21 Usage Per Ops View Tab in the License Management Window

Field	Description
License Type	
PMC Ports	Ops View—Ops view to which this license belongs Current Usage—Number of PMC ports that are in use for this ops view Allocated Ports—Number of PMC ports that have been allocated to this ops view
LMR Ports	Ops View—Ops view to which this license belongs Current Usage—Number of LMR ports that are in use for this ops view Allocated Ports—Number of LMR ports that have been allocated to this ops view

Table 2-21 Usage Per Ops View Tab in the License Management Window

Field	Description
Cisco Unified IP Phone Ports	Ops View—Ops view to which this license belongs Current Usage—Number of Cisco Unified IP Phone ports in use for this ops view Allocated Ports—Number of Cisco Unified IP Phone ports that have been allocated to this ops view
Multicast Ports	Ops view—Ops view to which this license belongs Current Usage—Number of multicast ports that are in use for this ops view Allocated Ports—Number of multicast ports that have been allocated to this ops view
Dial Ports	Ops View—Ops view to which this license belongs Current Usage—Number of dial ports that are in use for this ops view Allocated Ports—Number of dial ports that have been allocated to this ops view

Understanding Time-bound License Behavior

Time-bound, or evaluation, licenses differ from permanent licenses by the inclusion of a predefined expiration date.

Note Cisco IPICS does not overwrite older license files with newer license files. As a best practice, Cisco recommends that you remove the old license file(s) from the directory where Cisco IPICS stores the license(s).

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

[root]# ***service ipics restart***

For more detailed information and guidelines about time-bound licenses, refer to the *Cisco IPICS Server Installation and Upgrade Guide.*

About 30 days before a time-bound license is to expire, Cisco IPICS displays a warning message to alert you. You can dismiss this warning by clicking the **Dismiss** button.

When a license feature expires, the relevant functionality of that license becomes disabled. If the license is an uncounted license, the feature is disabled; however, if the license is a counted license, the number of ports that correspond to that license type is reduced by the count of the expired license feature. In this case, Cisco IPICS reloads all of the license features when it detects that one or more license features has expired. Expired license features display in the license detail area as flagged items.

Uploading a License File

After you obtain a new Cisco IPICS license file, you must upload it to the Cisco IPICS server before it becomes effective. This procedure copies a license file from the server location where you stored it to the Cisco IPICS server.

Note After you upload the license file, Cisco IPICS places the file in the following directory:
/opt/cisco/ipics/tomcat/versions/5.5.9/webapps/license/

To upload a license file, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Administration > License Management** window.

Step 2 In the License File field, enter the path name and file name of the license file to upload to the Cisco IPICS server.

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

Note If you do not know the path name and file name of the license file, you can click Browse and navigate to the file in the Choose File window.

Step 3 Click **Upload** to upload the file to the Cisco IPICS database.

Step 4 Click **Apply** for the new license to become effective.

Cisco IPICS associates the license file with the server and restarts the license manager.

Note There may be a delay of a few minutes before you can access the Cisco IPICS Administration Console after you click the **Apply** button.

For more information about Cisco IPICS licenses, refer to the *Cisco IPICS Server Installation and Upgrade Guide.*

Viewing Active Users

As a Cisco IPICS system administrator, you can view the activity for users who are logged in to the system via PMC and Cisco Unified IP Phone, and users who are participating in a VTG, by accessing the Administration > Active Users window. This window contains information about each type of user who is logged in to the system, such as the identification of the user, the location of the user, and ops views to which the user belongs. Using this window, you can also manually force logged-in and dialed-in users to log out of Cisco IPICS, if necessary.

To view active users and the associated information for each user, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Administration > Active Users** window.

Step 2 From the View drop-down list box, choose one of following types of users that you want to view:

- **Logged-in Users**—Users who are logged in to Cisco IPICS
- **PMC Users**—Users who are connected to Cisco IPICS via the PMC
- **Cisco Unified IP Phone Users**—Users who are connected to Cisco IPICS via a Cisco Unified IP Phone
- **Dialed-in Users**—Users who are connected to Cisco IPICS by using the dial-in/invite feature

A window displays a list of the type of users that you chose. See Table 2-22 for a description of the fields in the Active Users window.

Note You can specify the number of rows of active users that display per results page by choosing from the Rows per page drop-down list box at the top right of the window. To navigate between the results pages, click the arrows at the bottom of the window; then click **Go**.

Table 2-22 Active Users Window Fields

Field	Description
Logged-in Users	
User	Name or user ID of user who is logged in to the Cisco IPICS system
Date	Date that the user logged in to the Cisco IPICS system
PMC Users	
User	Name or user ID of the active PMC user

Table 2-22 Active Users Window Fields (continued)

Field	Description
PMC ID	Identification of the PMC for the session
Version	PMC version information that the user is using
Address	IP address of the PMC client machine
Location	Location of the user
Belongs To	Ops view to which the active PMC user belongs
Last Activity	Date and time of the last PMC activity of the PMC user
Status	Indicates the status of a PMC The Status column can contain a status of either Logged-in or Logging-out. The Logging-out status means that the PMC has not yet contacted the server to finalize the PMC session. All resources, including licenses and RMS resources, are deallocated immediately when a user is disabled, or when a PMC session is logged out by using the **Logout** button in the PMC tab in the Active Users window. The PMC session is retained until the server can provide detailed information to the PMC about the conditions of the logout. The server removes logging-out sessions in the following conditions: • The PMC contacts the server. • The server periodically checks (every 60 seconds by default) for sessions which have been active for 10 minutes and removes them in the event of a PMC crash or if the PMC is in offline mode. • At the startup of the Cisco IPICS server.
Cisco Unified IP Phone Users	

Table 2-22 Active Users Window Fields (continued)

Field	Description
User	Name or user ID of the active Cisco Unified IP Phone user.
Digit ID	Digit identification number of the active Cisco Unified IP Phone user.
Location	Location of the active Cisco Unified IP Phone user.
Active	Indicates whether the Cisco Unified IP Phone user is currently active.
Remote	Indicates whether the Cisco Unified IP Phone user is dialed in using a remote connection.
Dialed-in Users	
User	Name or user ID of the active dialed-in user.
Dial Number	Number that the user dialed when dialing in to Cisco IPICS.
Digit ID	Digit identification of the active dialed-in user.
Type	Type of talk group. This field is empty if the user is dialed in but has not joined any talk group. Type can indicate one of the following resources: • Channel • VTG
Talk Group	Name of the talk group (channel or VTG) that the user has joined. This field is empty if the user is dialed in but has not joined any talk group.

Table 2-22 Active Users Window Fields (continued)

Field	Description
Status	Status of the dialed-in user and can be one of the following statuses: • Not Joined—The user is dialed in but has not joined a channel or VTG. • Listening—The user is dialed in and has joined a channel or VTG and is listening to that channel or VTG. • Talking—The user is dialed in, has joined a channel or VTG, and is currently talking (pressing the PTT button) on that channel or VTG.

Step 3 To manually disconnect a logged-in, PMC, or dialed-in user from Cisco IPICS, take any of the following actions:

- To log out a logged-in user, click the **Logged-in** tab.
  - Check the check box to the left of each logged-in user that you want to log out and click **Logout**.
- To log out a PMC user, click the **PMC** tab.
  - Check the check box to the left of each PMC user that you want to log out and click **Logout**.

  When you log out a PMC user, the session is ended and the action cleans up all the PMC resources and marks the session accordingly. If the PMC is not running, the cleanup action completes.

  If the PMC is running and connected to the server, the PMC gets the logout update from the server and logs out accordingly, redisplaying the Login dialog.

  If the PMC is running in offline mode, the PMC continues to run. If the PMC uses multicast communications, there are no effects on the channel. If the PMC uses SIP-based communications, the SIP channels become disconnected.
- To log out a dialed-in user, click the **Dialed-in** tab.

– Check the check box to the left of each dialed-in user that you want to log out and click **Logout**.

Tip You can log out all users in each tab by checking the check box at the top of each user list and clicking **Logout**.

Step 4 To refresh the window of any tab, click the **Refresh** button at the bottom of the list.

Managing Activity Logs

The Cisco IPICS logs store a variety of information about activities relating to VTGs, such as the ops view for each channel, user, and VTG, the creator of log entries, and the time that log activities occurred. You can review this information at any time. Log activity information is also used for historical reporting.

In Cisco IPICS, an activity gets logged once and the log entry remains indefinitely. When entities such as users, locations, channels, and VTGs, get deleted from Cisco IPICS, the corresponding log entries do not get deleted from the activity log table to provide a historical record if needed.

You search for and download activity logs in the Activity Log Management window. This window contains a **Logs** tab and an **Archives** tab. See the "Understanding the Activity Log Management Window" section on page 2-133 for more information about the Activity Log Management window.

Cisco IPICS tracks and logs the date and time that certain types of activities occur. For detailed information about the activity types that are logged in Cisco IPICS, and how to specify what activity types get logged per ops view, see the "Managing Activity Log Options Per Ops View" section on page 2-138.

You can choose how to view activity logs:

- By ops view—Ops views to which the resource belongs
- By channel—Users and VTGs that used that PTT channel
- By radio—Channels, users, and VTGs that used that radio
- By user—PTT channels and VTGs in which that user was involved

- By VTG—Users and PTT channels that were participants in that VTG

To view and download activity logs. See the "Viewing and Downloading Activity Logs" section on page 2-134 for more information.

Understanding the Activity Log Management Window

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

The Activity Log Management window contains two tabs, in which you can manage activity log information: the **Logs** tab and the **Archives** tab.

In the **Logs** tab, you can choose to view logs by ops view and resource type (such as channel, radio, user, and VTG), and search for particular logs based on a date range. If you are assigned the system administrator and/or ops view administrator role, you can also apply the date range filter to minimize the logs that get returned from the system. After filtering the activity log resource list by ops view and resource type, you can then choose one of the resources from a single list. For more information about using the search filters, see Chapter 1, "Using Search Windows."

Note Users who are assigned the ops view administrator role can monitor only the activity logs of the ops view to which that user belongs. If a particular ops view is disabled, all the activity logging is done by using the SYSTEM default ops view. The system administrator is allowed to monitor logs of all the ops views. For more information about Cisco IPICS roles, see the "Cisco IPICS Roles" section on page 1-7.

For information about viewing and downloading Cisco IPICS activity logs, see the "Viewing and Downloading Activity Logs" section on page 2-134.

In the **Archives** tab, you can download activity log files that have been archived according to the threshold limits that are configured in the Administration > Options window. For more information about managing Cisco IPICS options, see the "Managing Cisco IPICS Options" section on page 2-140. For information about downloading archived activity logs, see the "Downloading Archived Activity Logs" section on page 2-136.

For information on the display controls, see the "Navigating Item Lists" section on page 1-16.

To open the Activity Logs Management window, navigate to the **Administration > Activity Log Management** window.

Viewing and Downloading Activity Logs

To perform detailed analysis of activities, you can view and download activity logs. You can view activity logs for any channel, radio, user, or VTG, based on ops views and resource type. You view and download activity logs in the Activity Log Management window.

When you download activity logs, Cisco IPICS takes these actions:

- Creates an .xml file that contains all activity logs in the period, ops view, and resource type that you designate
- Downloads the .xml file to the location that you specify on the computer from which you are accessing the Administration Console.

The file includes information about the related log entries for the search criteria that you specify (such as ops view, resource type, and date range).

To view and download activity logs, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Administration > Activity Log Management** window.

Step 2 From the drop-down list box in the **Logs** tab, choose the ops view for the activity logs that you want to view and/or download.

Step 3 From the Resource Type drop-down list box, choose the resource type for the activity logs that you want to view and/or download.

Step 4 To view and/or download only the activity logs for a specific resource, enter the name of the resource of the activity logs in the Resource Name field.

Step 5 From the Sort By drop-down list box, choose one of the following options:

- **Date-and-Time**—This option sorts the logs by the date and time of the logs.

- **Initiator-User-ID**—This option sorts the logs by the user who initiated the log entry.
- **Affected-Source-Resource**—This option sorts by the name of the affected resource.
- **Affected-Target-Resource**—This option sorts by the name of the affected target resource.

Step 6 In the From field, specify the beginning date and time of the of the activity logs that you want to view and/or download.

Step 7 In the To field, specify the ending date and time of the activity logs that you want to view and/or download.

Step 8 Click **Go**.

The activity logs display according to the criteria that you choose.

Note You can specify the number of rows of activity logs that display per results page by choosing from the Rows per page drop-down list box at the top right of the window. To navigate between the results pages, click the arrows at the bottom of the window; then click **Go**.

Step 9 To clear your search criteria, click the **Clear Filter** button.

Step 10 To download the logs to your PC, click **Download Activity Logs**.

Step 11 To open the file immediately, click **Open**. To save the file to your PC, click **Save**.

Note The activity log file is in .xml format.

Step 12 To view the activity logs in Microsoft Excel, save the file to a desired location and perform one of the following actions:

Note The following examples were performed by using Microsoft Office Excel 2003.

- Open the Microsoft Excel application and from the File drop-down menu click **Open**.
  – Navigate to the .xml file, highlight the file and click **Open**.

  - In the Open XML dialog box, click the **As an XML List** radio button.

    Microsoft Excel creates a schema that is based on the .xml file source data.

- Navigate to the location where you saved the .xml file, select the file and right-click it.
  - Choose **Open With** and **Choose Program**.
  - Choose **Microsoft Excel** in the Open With dialog box.

Note If the Excel application does not display in the list of programs, click **Browse** and locate the application.

  - Click **OK**.
  - From the Open XML dialog box, click the **As a read-only workbook** radio button.

Step 13 To view or download archived activity logs, perform the steps in the "Downloading Archived Activity Logs" section on page 2-136.

Downloading Archived Activity Logs

You can download archived activity logs. Cisco IPICS archives the activity logs based on the thresholds that you assigned in the Administration > Options window in the Administration Console. For more information about the Options window, see the "Managing Cisco IPICS Options" section on page 2-140.

To download archived activity logs, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Administration > Activity Log Management** window.

Step 2 Click the **Archives** tab.

Table 2-23 shows the fields in the Archive Status pane.

Table 2-23 Archive WIndow Fields

Field	Description
Archive Time—*Display only*	Time when the activity log files were archived in Cisco IPICS
Archive Status—*Display only*	Indicates whether log files were archived successfully
Archive Count—*Display only*	Number of log entries that were archived during the last archive
Archived Files drop-down list box	The file names of the archived files
Download button	Click this button to download archived Cisco IPICS activity logs

Step 3 From the Archived Files drop-down list box, choose the archived activity log file that you want to download.

Note If no log files have been archived, the Archived Files drop-down list box and the Download button are disabled and display as dimmed.

Step 4 Click **Download**.

Step 5 To open this file immediately, click **Open**. To save the file to your PC, click **Save**.

Note Because Microsoft Excel does not support multi-root .xml documents, you can add the text "<activity_logs>" to the beginning and "</activity_logs>" to the end of the downloaded archived activity log file before opening the file. Adding the text changes the file to have only one root element.

If the name of the downloaded archived activity log file is "ipics_activity.xml.<1-24>", rename the file to "ipics_Activity<1-24>.xml" making sure that the .xml extension appears at the end of the file name, before opening in Microsoft Excel. Renaming the file ensures that Excel recognizes the file as an .xml file.

Managing Activity Log Options Per Ops View

You can specify the activities that you want Cisco IPICS to log, by ops view, in the Activity Log Options window. For example, if you want Cisco IPICS to only log when a VTG gets activated in a particular ops view, and no other activities, you would choose the Resource Creation and Deletion activity type for that ops view.

Table 2-24 describes the types of activities that can be logged in by ops views.

Table 2-24 Activity Log Types By Ops View

Activity Type	Description
Cisco Unified IP Phone Activities	Logs are created whenever Cisco Unified IP Phone activities occur in Cisco IPICS.
Dial-in Activities	Logs are created whenever dial-in activities occur in Cisco IPICS.
Licensable Feature Activities	Logs are created whenever feature activities occur, for features that have been licensed in Cisco IPICS.

Table 2-24 Activity Log Types By Ops View (continued)

Activity Type	Description
PMC Activities	Logs are created whenever PMC activities occur in Cisco IPICS.
Resource Association Activities	Logs are created whenever resources are associated in Cisco IPICS.
Resource Creation and Deletion Activities	Logs are created whenever resources, such as VTGs, users, and channels are created or deleted from Cisco IPICS.
System Activities	Logs are created whenever system activities, such as voice resource activities, occur in Cisco IPICS.
Virtual Talk Group Activities	Logs are created whenever VTG activities occur in Cisco IPICS.

You can access the Activity Log Options window in the Administration Console by navigating to **Administration > Activity Log Options**.

To manage activity logs per ops view, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **Administration > Activity Log Options** window.

Step 2 From the Ops View drop-down list box, choose the ops view for which you want to specify the activities to be logged.

Note All the activity types that are available to be logged in Cisco IPICS are listed in the Unselected Activity Types area. In order to specify particular activity types that you want to be logged in Cisco IPICS, for this ops view, you must move them to the Selected Activity Types list. If you do not move any activity types to the Selected Activity Types list, all activity types are logged in this ops view. If you move an activity type to the Unselected Activity Types list, the previously-logged activities of that type are not deleted from the system but they are prevented from being logged in the future.

Step 3 To select the activity types that you want to log in Cisco IPICS for an ops view, take any of the following actions:

- To move an activity type from one list to the other, click the activity type to highlight it; then, click **>** or **<**. Or, double-click the activity type.
- To move several activity types from one list to the other at one time, press **Shift+click** or **Ctrl+click** to select the activity types; then, click **>** or **<**.
- To move all activity types from one list to the other at one time, click **>>** or **<<**.

Step 4 Click **Save** to save your changes.

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

Managing Cisco IPICS Options

Cisco IPICS provides you with the ability to adjust system preferences and turn on or off certain options in the Options window. Cisco IPICS allows you to restore default settings at any time.

Information in the Options window is contained in the following information tabs:

- **General** tab—Choose this tab to set RMS and activity log options.
- **Passwords** tab—Choose this tab to set the password options for users.
- **PMC** tab—Choose this tab to set PMC configuration options.

Cisco IPICS detects changes that are made to the system options and immediately makes the adjustments for those changes. You do not have to take any further action for the changes to take effect.

You can access the Options window in the Administration Console by navigating to **Administration > Options**.

You can use the options in the Options window in the following ways:

- You can customize the Cisco IPICS option settings by editing the fields in the General, Passwords, and PMC tabs.

  Note Ensure that you click **Save** after each change that you make to the settings.

- To restore all settings to the default values, click **Restore Defaults**.

Table 2-25, Table 2-26, and Table 2-27 describe the fields in the Options window.

Table 2-25 General Tab in the Options Window

Setting	Description	Default Setting
Disable RMS Comparator (in the RMS pane)	The RMS comparator is the mechanism that checks the responsiveness of the RMS and if there have been any changes made to the configuration. If there have been changes to the RMS 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. Because the RMS comparator can interject delays, you can disable it by checking this check box. **Note** If you connect via a high latency, low bandwidth connection, such as a satellite link, you should check this check box.	This check box is unchecked by default. If the Disable RMS Comparator check box is selected, the RMS Polling Frequency field displays as dimmed.
RMS Polling Frequency	The RMS comparator functionality includes a polling mechanism that regularly checks whether the server can reach all of the RMS components that are listed in the RMS window. This setting specifies a value in seconds. To change the default, double-click the current setting and enter a new value. Valid values: 1-32767.	The default interval between checks specifies 10 minutes.

Table 2-25 General Tab in the Options Window (continued)

Setting	Description	Default Setting
Maximum Activity Logs (in the Activity Logs pane)	This setting the maximum amount of database space that may be used by Cisco IPICS activity logs. For more information, see Chapter 10, "Understanding Cisco IPICS Serviceability and Diagnostic Information." This setting specifies a value in megabytes (MB). To change the default, double-click the current value and enter a new value. Valid values: 1-250.	The default maximum space for activity logs specifies 50 MB.
Activity Log Retention Period	This setting specifies the number of days that Cisco IPICS retains activity log entries. When this number has been reached, the logs get written to a rolling archive log. The archive log files are preserved until they get overwritten when the number of rolling files reaches the maximum number of archive files limit that is set by the system. Valid values: 1-365.	The default setting specifies 90 days.
Cisco Unified IP Phone Timeout Period	This setting specifies whether a Cisco Unified IP Phone times out after a configured period of inactivity, forcing a user to log in again. **Note** To disable the timeout period, set the value to 0. This setting specifies a value in minutes. To change the default, double-click the current value and enter a new value. Valid values: 0-99999.	The default setting specifies 30 minutes.

Table 2-25 General Tab in the Options Window (continued)

Setting	Description	Default Setting
Cisco IPICS Session Timeout Period	This setting specifies whether a Cisco IPICS session times out after a configured period of inactivity, forcing a user to log in again. **Note** To disable the timeout period, set the value to 0. This setting specifies a value in minutes. To change the default, double-click the current value and enter a new value. Valid values: 0-99999.	The default setting specifies 30 minutes.
Restrict Operator Role assignments	If you check this box, users with the operator role can grant users (including themselves) the operator, dispatcher, or Ops view administrator roles only.	Not checked.

Table 2-26 Passwords Tab in the Options Window

Setting	Description	Default Setting
Minimum Password Length (in the User Passwords pane)	This setting specifies the minimum number of characters that a user can enter when creating or changing the Cisco IPICS password in the **Home > My Profile** window. See the "Managing Your User Profile" section on page 5-2. Use the drop-down list box to choose a new setting. The minimum length can range from 4 to 20 characters. To ensure a strong password, you must create a password that is at least eight characters long, and includes the following elements: • At least one lower case letter • At least one upper case letter • At least one number • At least one of the following special characters: @ [ ] ^ _ ` ! " # $ % & ' ( ) * + , - . / : ; { < | = } > ~ ? Valid values: 4 through 20.	The default setting specifies 8 characters.
Minimum Digit Password Length	This setting specifies the minimum number of numeric characters that a user can enter when creating or changing the digit password in the My Profile window, in the Home drawer of the Administration Console. Use the drop-down list to choose a new setting. The minimum length can range from 4 to 10 characters. Valid values: 4-10.	The default setting specifies 4 characters.

Table 2-26 Passwords Tab in the Options Window (continued)

Setting	Description	Default Setting
Minimum Lower Case Letter Count	This setting specifies the minimum number of lower case letters that a user can enter when creating or changing the Cisco IPICS login password in the My Profile window, in the Home drawer of the Administration Console. The range of this field is from 0 to whatever number is specified in the Minimum Password Length field. **Note** The total number in this field cannot exceed the number that is set in the Minimum Password Length field. Valid values: 0-20.	The default setting specifies 1 character.
Minimum Upper Case Letter Count	This setting specifies the minimum number of upper case letters that a user can enter when creating or changing the Cisco IPICS login password in the My Profile window, in the Home drawer of the Administration Console. The range of this field is from 0 to whatever number is specified in the Minimum Password Length field. **Note** The total number in this field cannot exceed the number that is specified in the Minimum Password Length field. Valid values: 0-20.	The default setting specifies 1 character.

Table 2-26 Passwords Tab in the Options Window (continued)

Setting	Description	Default Setting
Minimum Numeric Character Count	This setting specifies the minimum numeric character that a user can enter when creating or changing the Cisco IPICS login password in the My Profile window, in the Home drawer of the Administration Console. The range of this field is from 0 to whatever number is specified in the Minimum Password Length field. **Note** The total number in this field cannot exceed the number that is specified in the Minimum Digit Password Length field. Valid values: 0-20.	The default setting specifies 1 character.
Minimum Special Character Count	This setting specifies the minimum special character that a user can enter when creating or changing the Cisco IPICS login password in the My Profile window, in the Home drawer of the Administration Console. The range of this field is from 0 to whatever number is specified in the Minimum Password Length field. Valid values: 0-20.	The default setting specifies 1 character.

Table 2-26 Passwords Tab in the Options Window (continued)

Setting	Description	Default Setting
Password History Count	This setting specifies the number of passwords that Cisco IPICS marks as previously used, and that the user is not able to use again. For example, if the Password History Count is set to 5, the user is not able to use any of the passwords that they have used for the previous five times. **Note** This field does not apply to the ipics or ipicsadmin user IDs. Valid values: 0-999.	The default setting specifies 5 previous passwords.
Apply User Password Expiration (in Password Expiration pane)	This check box specifies whether Cisco IPICS applies the value that is specified in the Password Expiration field. If this check box is unchecked, there is no user password or digit expiration applied. Valid values: true or false.	This check box is unchecked by default. If this check box is not selected, the Password Expiration and Password Expiration Notification fields display as dimmed.

Table 2-26 Passwords Tab in the Options Window (continued)

Setting	Description	Default Setting
Password Expiration	This setting specifies the number of days in which the Cisco IPICS login password and the digit password expires. For example, if the value is 180 days, the password expires after 180 days from the date that the password was created. **Note** To prevent the password from expiring, uncheck the check box in the Apply User Password Expiration setting. The Never Expired message displays in the Password Expiration Date field, in the My Profile window for the user. **Tip** After a Cisco IPICS migration occurs, you may want to require all users to update their login passwords for enhanced password security. To force a login password update after a migration, configure the Password Expiration Days setting to 1; then once that one day has passed you can change the setting back to 180 days, or whatever setting you want to specify. This action forces users who log in to Cisco IPICS during that day (after the migration) to change their login passwords. Valid values: 1-999.	The default setting specifies 180 days.

Table 2-26 Passwords Tab in the Options Window (continued)

Setting	Description	Default Setting
Password Expiration Notification	This setting specifies the number of days before the password expires that the user receives a warning. For example, if the specified number of days is set to 3, the user receives the warning 3 days before password expiration. **Note** This field does not apply to the ipics or ipicsadmin user IDs. **Tip** To expire passwords quickly, set the value to 1 day. The user will be forced to change the password when logging in to Cisco IPICS the following day. Valid values: 1-999.	The default setting specifies 3 days.
Apply User Account Lockout (in the User Account Lockout pane)	This check box specifies whether Cisco IPICS applies the value that is specified in the Maximum Invalid Login Attempts Allowed field. When this check box is checked and a user exceeds the number of invalid login attempts that is specified, the user account is locked and the user can no longer log in to Cisco IPICS until the account is unlocked. For information about how to unlock an account that has been locked, see Chapter 3, "Performing Cisco IPICS Operator Tasks." **Note** This field does not apply to the ipics or ipicsadmin user IDs. If this check box is unchecked, there is no account lockout applied. Valid values: true or false.	This check box is unchecked by default. If this check box is not selected, the Maximum Invalid Login Attempts Allowed and the Failed Password Attempt Expiration fields display as dimmed.

Table 2-26 Passwords Tab in the Options Window (continued)

Setting	Description	Default Setting
Maximum Invalid Login Attempts Allowed	This setting specifies the maximum number of times a user can attempt to log in to Cisco IPICS with invalid login information (user name/password) before the user account gets locked out. The failed login attempts are consecutive. Valid values: 1-999. **Note** The user password invalid attempt count is a separate entity from the digit password invalid attempt count; however, if either password invalid attempt is exceeded, the user account is locked. When the user account is unlocked, both invalid attempt counts is reset to 0. When a user gets locked out of Cisco IPICS, a message displays stating that the user ID has been locked and that the user should contact the system administrator or operator for assistance. To unlock a user account, see Chapter 3, "Performing Cisco IPICS Operator Tasks." You can also re-enable a user account by using the enableuser tool. The enableuser tool clears the value that is specified in the Maximum Invalid Login Attempts Allowed field and unlocks the user account. To re-enable a user ID using the enableuser tool, refer to the *Cisco IPICS Troubleshooting Guide.*	The default setting specifies 5 attempts.

Table 2-26 Passwords Tab in the Options Window (continued)

Setting	Description	Default Setting
Failed Password Attempt Expiration	This setting specifies the number of hours that Cisco IPICS resets the Maximum Invalid Login Attempts Allowed field back to 0 once a user has reached the maximum invalid login attempts. Valid values: 1-999.	The default setting specifies 8 hours.

Table 2-27 PMC Tab in the Options Window

Setting	Description	Default Setting
PMC Update Poll (in the Configuration pane)	This setting specifies the frequency that the PMC uses to poll the server for updates. For more information, refer to the *Cisco IPICS PMC Installation and User Guide.* This setting specifies a value in seconds. To change the default, double-click the current setting and enter a new value. Valid values: 3-3600.	The default polling interval specifies 5 seconds.
Disable PMC Activity Log Upload (in the PMC Activity Logs pane)	When you check this check box, the PMC does not upload logs to the server. **Note** If you connect via a high latency (high delay), low bandwidth connection, such as a satellite link, you should check this check box. Valid values: true or false.	This check box is unchecked by default. If this check box is checked the PMC Log Upload Frequency field and the PMC Send Logs on Rollover fields/check box display as dimmed.

Table 2-27 PMC Tab in the Options Window (continued)

Setting	Description	Default Setting
PMC Log Upload Frequency (PMC to server)	When a PMC client has activity logs ready to upload to the Cisco IPICS server, the PMC application places the logs in a queue. At regular intervals, the PMC client checks the queue and uploads to the server any logs that are waiting to be uploaded. Log files are copied to the **$TOMCAT_HOME/webapps/ipics_server/pmclogs** directory, and are based on user ID and PMC ID. Log files that are not successfully uploaded get put back in to the queue and are uploaded at a later time. This setting specifies the interval between these checks. For more information, refer to the *Cisco IPICS PMC Installation and User Guide.* This setting specifies a value in seconds. To change the default, double-click the current setting and enter a new value. **Note** Cisco IPICS archives or deletes PMC log files that have been uploaded to the server, such as debug logs, by using an archive utility. This utility runs once a day and checks for log files that are older than 14 days old and deletes them. If the total file size of the files is over 5GB, the oldest files are deleted until the total size drops below 5GB. For detailed information about PMC log files, see "Managing an End Device from the PMC Tab" section on page 3-19. Valid values: 60-32767.	The default upload frequency specifies 600 seconds (10 minutes).

Table 2-27 PMC Tab in the Options Window (continued)

Setting	Description	Default Setting
PMC Send Logs on Rollover	Cisco IPICS defines the PMC UserInterface.log, Authentication.log, and ChannelStatistics.log log files based on a maximum size of 1MB. When any one of these log files reaches this predefined limit, the system creates a new log file. When you enable this option, the Cisco IPICS server retrieves the log files from the PMC based on file size rollover and renames the uploaded log file to reflect an archive copy. If you do not enable this option, the PMC deletes the log files when they reach their maximum size limit. Be aware of the following caveats: • The DebugLog.txt file does not have a size limit of 1MB, and is only uploaded to the server on request or when the PMC is started if this check box is checked (set to true). If this check box is unchecked, the DebugLog.txt file is not uploaded. • The ChannelActivity.log file is uploaded to the server every 10 minutes (or the interval that you configure in the PMC Log Upload Frequency field). Valid values: true or false.	The PMC uploads files on rollover (the check box is checked).

Table 2-27 PMC Tab in the Options Window (continued)

Setting	Description	Default Setting
PMC Activity Log Update	The Cisco IPICS server gathers activity logs from the PMC client machines and updates the database with this information at regular intervals. In the Cisco IPICS database, this data is parsed, organized, and made available for queries from the Activity Log window of the Administration Console. This setting specifies a value in seconds. To change the default, double-click the current setting and enter a new value. Valid values: 30-32767.	The default update frequency specifies 600 seconds (10 minutes).

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 you can upload to the Cisco IPICS server.

These updates of the PMC application add features and resolve issues. Users can upgrade their PMC clients at their convenience by downloading the current version of the PMC utility, as described in the "Downloading the PMC" section on page 5-19.

Note You must perform the PMC configuration procedures that are in this section before users can download and install a PMC on their PC clients.

When you initially install Cisco IPICS, a PMC package is included with the server. You must configure the PMC download configuration and generate the PMC Installer for that version to be available for download to PMC users.

When you upgrade the Cisco IPICS server software, you install the new version of the PMC to the older version of the server. For more information about upgrading the Cisco IPICS server software, refer to the *Cisco IPICS Server*

Installation and Upgrade Guide. For information about how to install a new PMC version for an upgrade, see the "Installing a New PMC Version Before You Upgrade Your Cisco IPICS Server" section on page 2-161.

When subsequent versions of the PMC becomes available, you upload the new PMC package to the Cisco IPICS server making it available for the PMC users to download to their PMC clients. PMC packages are contained in .zip files and can include alert tones and skins.

Each PMC client polls the Cisco IPICS server regularly. As part of this process, the PMC client determines whether there is a new version of a PMC upgrade package to which it can or must update. You configure the recommended PMC versions to designate the PMC version that is available for this update, and to designate whether an update is required or recommended. For more information about configuring the PMC versions, see the "Changing the State of PMC Versions" section on page 2-159.

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

- Uploading PMC Versions to the Cisco IPICS Server, page 2-158
- Changing the State of PMC Versions, page 2-159
- Installing a New PMC Version Before You Upgrade Your Cisco IPICS Server, page 2-161
- Deleting PMC Versions, page 2-163

You perform the PMC version update tasks in the PMC Versions window. For more information about this window, including how to access it, see the "Understanding the PMC Versions Window" section on page 2-156.

Understanding the PMC Versions Window

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

The PMC Versions window lists information about each of the PMC versions that have been uploaded to the Cisco IPICS server.

To display the PMC Versions window in the Administration Console, navigate to **PMC Management > PMC Versions**.

Table 2-28 describes the items in the PMC Versions window.

Table 2-28 Item in the PMC Versions Window

Item	Description	Reference
Upgrade Package field	This field contains the PMC version to be uploaded to the Cisco IPICS server.	See the "Uploading PMC Versions to the Cisco IPICS Server" section on page 2-158 and the "Installing a New PMC Version Before You Upgrade Your Cisco IPICS Server" section on page 2-161
Browse button	Click this button to browse to the location that contains the PMC version upgrade package that you can upload to the Cisco IPICS server.	
Upload button	Click this button to upload a new PMC version to the Cisco IPICS server.	
Name field	This field allows you to assign a unique identification to the PMC version upgrade package.	
Version field	This field specifies a unique version number that is assigned to the PMC version upgrade package.	
State field	This field specifies the priority (state) that is assigned to the upgrade package.	See the "Changing the State of PMC Versions" section on page 2-159
Delete button	Click this button to delete a PMC version from the Cisco IPICS server.	See the "Deleting PMC Versions" section on page 2-163

Table 2-28 Item in the PMC Versions Window (continued)

Item	Description	Reference
Drop-down list box for PMC version states	Choose from this list box to configure the state for the PMC versions.	See the "Changing the State of PMC Versions" section on page 2-159
Change State button	Click this button to change the state of the PMC version.	

Uploading PMC Versions to the Cisco IPICS Server

When you upload a new PMC version, the upgrade package file is copied from the stored location on your PC to the Cisco IPICS server.

To upload a PMC upgrade version to the Cisco IPICS server, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **PMC Management > PMC Versions** window.

Step 2 To locate the PMC version upgrade package that you obtained from Cisco click **Browse**.

Step 3 In the Choose File window, browse to the PMC version that you want to upload and click **Open**.

The file that you choose displays in the Upgrade Package field.

Step 4 Click **Upload**.

Cisco IPICS uploads the file from your PC to the Cisco IPICS server. The PMC version displays in the PMC Versions list.

Note All new PMC versions are saved, by default, in a non-operational state. This means that the PMC users cannot download the version until you change the state. See the "Changing the State of PMC Versions" section on page 2-159 for more information.

Changing the State of PMC Versions

The PMC Versions window enables you to designate the PMC versions that are used for an automatic update by changing the state of the versions. When you specify a PMC version for the automatic update, be aware of this information:

- If you want to force PMC clients to update as soon as possible, choose **Recommended** from the drop-down list box. When you choose this state, the next time that a PMC client polls the server, it compares the PMC version that it is running with the recommended PMC version. If the PMC client does not match the recommended or operational versions, it automatically downloads the PMC version that is specified in the drop-down list box, automatically updates to that version, and automatically restarts.
- To force updates immediately, choose **Not Supported** from the drop-down list box. When you choose this state, PMC users who are running this version are forced to restart and download a newer version.

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

- You must upload a PMC version to the Cisco IPICS server before it becomes available in any of the fields in the PMC Versions window.

For more detailed information about the PMC, refer to the *Cisco IPICS PMC Installation and User Guide.*

To change the state of PMC versions for automatic updates, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **PMC Management > PMC Versions** window.

Step 2 Check the check box next to the PMC version that you want to change.

Step 3 From the drop-down list box, choose any of the following states:

- **Recommended**—This version represents the recommended software version that should be run on the PMC. The server notifies the PMC of this recommended version and displays a message to inform 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 the discretion of the administrator. The server sends this version to the PMC for download but the PMC does not install it until the administrator changes the state of this version to recommended or operational. At that time, the PMC may install the new version after the PMC user responds positively to the message prompt or if other installed versions are not installed.

  By using the Staged version, the PMC can download the version without installing it. The PMC may download this version but does not install it until the server configuration has been updated to reflect this version as recommended or operational.
- **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.

- **Not Supported**—This version represents an unsupported PMC software version. The server does not send this version to the PMC so that the PMC users cannot choose an unsupported version from the drop-down list box in the location dialog box.

Note The server forces an upgrade on any PMC that has installed an unsupported version of software.

Step 4 Click the **Change State** button.

Installing a New PMC Version Before You Upgrade Your Cisco IPICS Server

Before you upgrade the Cisco IPICS server software, you can set up a new version of the latest, supported PMC, thereby allowing you to stage the PMC download process. Staging the PMC download alleviates the burden of long PMC downloads to all users at one time. When the PMC users log in and connect to the server, the latest PMC version is automatically downloaded. After you upgrade the server and change the PMC state to recommended, the latest PMC becomes available for use.

To install the latest PMC version, you must have the Cisco IPICS server software installation CD for the release to which you are upgrading.

To install the latest PMC version before you upgrade the server software, perform the following procedure:

Procedure

Step 1 Log in to the server by entering the root user ID in the *hostname* **login**: field in the terminal console; then press **Enter**.

Cisco IPICS prompts you for the password for the root user.

Step 2 Enter the password that you created for the root user when you initially installed the Cisco IPICS operating system.

Refer to the *Cisco IPICS Server Installation and Upgrade Guide* for more information.

The Cisco IPICS operating system logs you in as the root user.

Step 3 Mount the contents of the upgrade CD onto the server by entering the following command:

```
[root]# mount /mnt/cdrom
```

Step 4 To navigate to the CD location, enter the following command:

```
[root]# cd/mnt/cdrom
```

Step 5 To view the installer file, enter the following command:

```
[root]# ls -l
```

The directory of the CD displays.

Step 6 Locate the installer file in the directory listing.

The Cisco IPICS installer file displays in the list with a .run file extension.

Step 7 To install the new PMC version on the server for staging, enter the following command:

```
[root]# bash install-ipics-<version>.run -- -i pmc
```

where:

<*version*>**.run** specifies the name of the installer file that you located in Step 6.

This command uploads the latest PMC version to the Cisco IPICS server.

The system prompts you to restart the Cisco IPICS server to complete this operation.

Note To terminate the installation process at any time, press **Ctrl+C**.

Step 8 Enter **Yes** to restart the server now.

Note Be aware that a server restart automatically logs all users out of Cisco IPICS. Therefore, Cisco recommends that you perform this activity during maintenance window or other offpeak time.

When you enter **Yes** to restart the server, the system automatically initiates the PMC download.

Step 9 To change the state of the PMC version, in the Administration Console, navigate to the **PMC Management > PMC Versions** window.

Note If you are already logged in to Cisco IPICS, you must restart your Administration Console session by logging in to Cisco IPICS again.

Step 10 To change the state of the previous PMC version to operational and the latest PMC version to staged, check the check box next to each version and choose the appropriate state from the drop-down list box.

For more information about how to change the state of the PMC versions, see the "Changing the State of PMC Versions" section on page 2-159.

When the PMC users log in to the PMC, the previous PMC version remains available for use and the latest PMC version becomes available for download.

Step 11 Upgrade your Cisco IPICS server software.

For more information, refer to the *Cisco IPICS Server Installation and Upgrade Guide.*

After you perform the upgrade, the system reflects the state of the previous PMC as Not Supported and marks it as being unavailable for use. The latest PMC version displays as the Recommended version and is available for PMC users who connect to the server.

Note When PMC clients log in, only the latest PMC version displays as available in the drop-down list box (if this version has already been downloaded by the PMC user). If the PMC user has not downloaded the latest PMC version, the server forces a download.

Deleting PMC Versions

To delete PMC versions, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **PMC Management > PMC Versions** window.

Step 2 Check the check box of the PMC version that you want to delete.

Step 3 Click **Delete**.

A message displays asking if you want to delete the selected version.

Step 4 Click **OK** to delete the PMC version.

This version of the PMC is completely removed from the server.

If you do not want to delete the PMC version, click **Cancel**.

Managing PMC Alert Tones

PMC tone broadcast wave (.wav) files contain alerting tones, hereafter referred to as *alert tones*, that can be broadcast to a variety of Cisco IPICS users at the same time. Cisco IPICS stores alert tones in a set on the server. The alert tone set is packaged in a .zip file that you can upload to the server, and that PMC users can then download on to their client machines.

An alert tone set is associated with an ops view; therefore, each PMC user can see only one tone set based on the ops view association. For more information about ops views, see Chapter 6, "Configuring and Managing Cisco IPICS Operational Views."

Note The PMC alert tone feature requires the use of compatible alerting tone files. These files must be .wav files that are encoded in Pulse Code modulation (PCM), which is a sampling technique that digitizes analog signals. These .wav files must be encoded in PCM format with 8 bits monaural samples at 8000 Hz sampling rate, for a total of 64 kbps. While higher and lower bit rates may seem to work, Cisco IPICS does not support the use of any other encoding or bit rates, as they may produce inferior sound quality. (Any file that is used with the G.729 codec may sound inferior due to its encoding algorithms; for more information, refer to the *Cisco IPICS PMC Installation and User Guide.*) 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.

As a Cisco IPICS system administrator, you can perform the following alert tone management functions:

- Creating a PMC Alert Tone Set, page 2-165
- Adding PMC Alert Tone Sets, page 2-167
- Viewing or Editing PMC Alert Tone Sets, page 2-168
- Associating an Alert Tone Set to an Ops View, page 2-169
- Deleting PMC Alert Tones, page 2-170

Creating a PMC Alert Tone Set

To provide the alert tones that get downloaded to the PMC, you must first create a PMC alert tone set and upload it to the Cisco IPICS server. To create the tone set, perform the following procedure:

Procedure

Step 1 From any PC on which the Cisco IPICS PMC is installed, navigate to the following directory:

C:\Program Files\Cisco Systems\Cisco IPICS\PMC\Components

Step 2 Create a new empty directory and extract the sample alert tone set zip file, and all its contents, in to the new directory.

Step 3 Add any desired sound files in .wav format to this directory.

Note These files should be normalized to -2 db and should be encoded by using 8 bit PCM at 8000 Hz.

Step 4 Open the sample alert tone .xml file by using Notepad.

Note The order in which the .wav files appear in the .xml file determine the order in which the alert tones display on the PMC.

Step 5 In Notepad, add new alert tones or delete existing alert tones by following the example below:

```
<file item="1" name="stop.wav" displayName="STOP" type="tone"
priority="required" />
<file item="2" name="message.wav" displayName="Message" type="tone"
priority="required" />
<file item="3" name="siren.wav" displayName="Siren" type="tone"
priority="required" />
<file item="4" name="alert.wav" displayName="Alert" type="tone"
priority="required" />
<file item="5" name="urgent.wav" displayName="URGENT" type="tone"
priority="required" />
```

where:

"*name*" represents the .wav file to be played, and "*displayName*" is the text that displays on the PMC.

Note The PMC displays a maximum of 8 characters for the display name.

Step 6 Save the example tone set .xml file and rename the .xml file to an appropriate file name.

Note You must save the .xml file in UTF-8 format. If you are using Notepad, choose UTF-8 from the Encoding drop-down menu in the Save As dialog box.

Step 7 Delete any files from the directory that you do not want.

Step 8 Using file explorer, navigate to the directory that contains the .xml and .wav files and select all of the .wav files and the .xml file.

Tip You can select all of the files by clicking **Ctrl+A**.

Step 9 Right-click the selected files and choose **Send To > Compressed Folder**.

Tip You can also use WinZip or a similar utility to compress the files.

Step 10 To enable the PMC user to press a button on the PMC to stop an alert tone from playing, for displayName enter the name "*STOP*" but give the name an invalid file name, such as "*stopplayout.wav*," then edit the alert tone file with this information, as if it were a real alert tone.

Step 11 You can now upload the compressed PMC alert tone set to the Cisco IPICS server. See the "Associating an Alert Tone Set to an Ops View" section on page 2-169 for information about how to upload a tone set.

Note You can use Windows Sound Recorder to save .wav files in the required format.

Adding PMC Alert Tone Sets

To add a new PMC alert tone set, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **PMC Management > Alert Tones** window.

Step 2 Click **Add**.

A blank alert tone detail window displays.

Step 3 To locate and upload the alert tone set that you want to add, click **Browse**.

Tip The Stop alert tone should be uploaded to the Cisco IPICS server. This alert tone allows users to press the Stop alert tone to stop an alert tone that is currently playing. You should ensure that the Stop alert tone is included in an alert tone set that you upload to the Cisco IPICS server. If your tone set does not contain a .wav file called Stop, you can use an alert tone that is named something similar, such as Silence. See the "Creating a PMC Alert Tone Set" section on page 2-165 for information about how to create an alert tone set.

Step 4 In the Set Name field, enter a name for the alert tone set.

Step 5 In the Description field, enter a description for the alert tone set.

Step 6 Click the **Browse** button to upload the alert tone set.

Step 7 Click **Save**.

The tone set gets uploaded to the server and is available for use by PMC users.

The alert tone set name, file size, and MD5 summary information of the new alert tone set also displays.

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

Step 8 To associate an alert tone set to an ops view, click the Ops View tab and follow the steps in the "Associating an Alert Tone Set to an Ops View" section on page 2-169.

Viewing or Editing PMC Alert Tone Sets

To view or edit the PMC alert tone sets that are available for use in Cisco IPICS, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **PMC Management > Alert Tones** window.

Step 2 Click the link in the Name column for the alert tone set that you want to view or edit.

An alert tones detail window displays current information about the tone set that you chose.

Step 3 To download the alert tone set without making any changes, click the **Download** button.

Step 4 To edit the information for the alert tone set, take any of the following actions:

- In the Name field, enter a new name for the alert tone set.
- In the Description field, enter a new description for the tone set.
- Click the **Browse** button to upload and overwrite the existing tone set.

Step 5 Click **Save**.

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

Step 6 To associate an alert tone set to an ops view, click the Ops View tab and follow the steps in the "Associating an Alert Tone Set to an Ops View" section on page 2-169.

Associating an Alert Tone Set to an Ops View

You can associate an alert tone set to an ops view while you are adding a new alert tone set, or you can associate an ops view to an existing tone set. Associating an alert tone set to an ops view ensures that PMC users can see only the tone set that is associated with the ops view to which they belong.

To associate an alert tone set to an ops view, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **PMC Management > Alert Tones** window.

Step 2 In the Name column, click the alert tone set link that you want to associate with an ops view.

Step 3 Click the **Ops Views** tab.

Step 4 Take any of the following actions:

- To move an ops view from one list to the other, click the ops view to highlight it; then, click **>** or **<**. Or, double-click the ops view.
- To move several ops views from one list to the other at one time, press **Shift+click** or **Ctrl+click** to select the ops views; then, click **>** or **<**.
- To move all ops views from one list to the other at one time, click **>>** or **<<**.

Step 5 Click **Save** to save the ops view that you want to associate to the alert tone set in the Associated Ops Views list.

PMC users can now only see the alert tone set that is in the ops view to which they belong.

Note The user(s) that you want to have access to the tone set must be assigned the appropriate permissions in Cisco IPICS to see the tone set, and must also belong to the same ops view to which the tone set is associated.

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

Deleting PMC Alert Tones

To delete PMC tones, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **PMC Management > Alert Tones** window.

Step 2 Check the check box to the left of the name of the tone that you want to delete.

Step 3 Click **Delete**.

The alert tone that you deleted is no longer available for use by the PMC users.

Note If you want to delete all of the existing alert tones, check the check box at the top of the alert tones list and click **Delete**.

Managing PMC Skins

Cisco IPICS supports several different skins that PMC users can use on their PMC. Skins are files, that you create and manage, that are packaged in sets (zip files) that can be downloaded to a PMC, and that form the appearance of the PMC. Once the skin sets are downloaded, PMC users can unpack them and choose from the individual skins, that were contained in the package, to use on their PMCs.

Skins are customizable in Cisco IPICS and are available in various options, including 4, 6, and 18-channel mouse skins and 4 and 8 channel touch screen skins. You control whether PMC users can download only selected PMC skins, or customizable skins.

Cisco IPICS supports only 18 channels to be viewed at a time, and several different skins from which PMC users can choose for the PMC. For more information about using the PMC, refer to the *Cisco IPICS PMC Installation and User Guide.*

Cisco IPICS enables you to upload and manage skin sets that are available to the PMC users. The information about the skin sets, contained in the Skins window, includes the name of the skin set, files size, and the MD5 summary of each skin set. You can use the MD5 summary field to determine whether skin sets get properly uploaded to the server.

Note The MD5 value should never be empty after the skin set has been uploaded to the server. It only displays as blank prior to adding the skin set because the server must process the file before producing the MD5 value.

You can access all skin sets that are currently available on the server by navigating to the PMC Management drawer in the Cisco IPICS Administration Console and clicking the **Skins** link.

You can view and edit existing skin sets, as well as add and delete skin sets, as described in the following procedures:

- Adding PMC Skins, page 2-172
- Viewing or Editing PMC Skins, page 2-172
- Deleting PMC Skins, page 2-173

Adding PMC Skins

To add a new PMC skin set, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **PMC Management > Skins** window.

Step 2 Click **Add**.

A blank New Skin detail window displays.

Step 3 To locate and upload the skin set that you want to add, click **Browse**.

Step 4 In the Skin Name field, enter a name for the skin set.

Step 5 In the Description field, enter a description for the skin set.

Step 6 Click the **Browse** button to upload the skin set.

Step 7 Click **Save**.

The skin set gets uploaded to the server and is available for download by PMC users.

The skin name, file size, and MD5 summary information of the new skin set also displays.

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

Viewing or Editing PMC Skins

To view or edit the PMC skins that are available for use in Cisco IPICS, perform the following procedure.

Note To add a new skin set, see the "Adding PMC Skins" section on page 2-172.

Procedure

Step 1 From the Administration Console, navigate to the **PMC Management > Skins** window.

Step 2 In the Skin Name column, click the link for the skin set that you want to view or edit.

A skin detail window displays current information about the skin set that you chose.

Step 3 To download the skin set without making any changes, click the skin name link.

Step 4 To edit the information for the skin set, take any of the following actions:

- In the Skin Name field, enter a new name for the skin.
- In the Description field, enter a new description for the skin.
- Click the **Browse** button to upload and overwrite the existing skin.

Step 5 Click **Save**.

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

Deleting PMC Skins

To delete PMC skins, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **PMC Management > Skins** window.

Step 2 Check the check box to the left of the Skin Name of the skin set that you want to delete.

Step 3 Click **Delete**.

The skin set that you deleted is no longer available for use by the PMC users.

Note If you want to delete all of the existing skins, check the check box at the top of the skins list and click **Delete**.

Managing the PMC Installer

Before PMC users can download new PMC versions to their clients, you must configure the PMC Installer.

The PMC Installer installs the PMC on to PMC client machines. The PMC package downloads to a PMC client when a PMC user clicks the **Download PMC** link in the Home drawer, as described in the "Downloading the PMC" section on page 5-19.

As a Cisco IPICS system administrator, you can upload a new PMC package, as well as generate the PMC Installer as described in the "Generating the PMC Installer" section on page 2-175.

You perform these tasks in the PMC Installer window. For more information about this window, including how to access it, see thee "Using the PMC Installer Window" section on page 2-174.

Using the PMC Installer Window

The PMC Installer window contains configuration information that is necessary in order to generate a PMC installer.

To display the PMC Installer window, navigate to the PMC Management drawer in the Cisco IPICS Administration Console and click the **PMC Installer** link.

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

Generating the PMC Installer

Generating a PMC Installer installs a new PMC version package, and makes it available for download from the **Download PMC** link in the Home drawer, as described in the "Downloading the PMC" section on page 5-19.

To configure additional PMC options, see the "Managing Cisco IPICS Options" section on page 2-140.

To configure a PMC and generate a PMC Installer, perform the following procedure from the PC on which you stored the PMC version package:

Procedure

Step 1 From the Administration Console, navigate to the **PMC Management > PMC Installer** window.

Step 2 To choose the IP address that is listed for Server Address, click the radio button next to the IP address that displays.

This address is the IP address that the PMC uses to contact the server. The IP address or hostname of the connected NIC hardware should display as a choice.

Step 3 To configure a different IP address for the PMC, click the **Other** radio button and enter the IP address that you want the PMC to use.

Note If you choose another IP address instead of the configured IP address, that IP address should be tested in the network domain that is supported with that server. This is in case the PMC cannot connect to the server due to NAT or firewall restrictions.

Step 4 In the HTTP Port field, enter the port number that is used for non-secure HTTP communication between the PMC and the server.

Step 5 In the HTTPS Port field, enter the port number that is used for secure HTTPS communication between the PMC and the server.

Note 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 PCs. If you need to change these values, Cisco recommends that you notify all users that they need to download and reinstall the PMC using the new pmcsetup.exe that is generated after you save the changes to these values.

Step 6 In the PMC Version To Be Used For The PMC Installer drop-down list box, choose the version number of the PMC that you want the users to download.

The drop-down list box should be populated with the version numbers of the pmcinst.exe files that have been uploaded to the Cisco IPICS server. See the "Managing PMC Versions" section on page 2-155 for more information.

Note There is only one PMC installer and all PMC users who use that installer automatically receive a complete application of that PMC version.

Step 7 Click **Save**.

PMC users can now download a new version of the PMC application, as described in the "Downloading the PMC" section on page 5-19.

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

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 (radios) are divided among regions. Channels, radios, and VTGs are configured to belong to a particular region when they are created.

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

You create regions in the **PMC Management > PMC Regions** window in the Administration Console.

You can add new PMC regions, as well as edit and delete existing regions, as described in the following procedures:

- Understanding the PMC Regions Window, page 2-177
- Adding PMC Regions, page 2-178
- Viewing or Editing PMC Regions, page 2-179
- Deleting PMC Regions, page 2-179

Understanding the PMC Regions Window

The PMC Regions window allows you to create new PMC regions that display on the PMC. You can also edit and delete existing PMC regions in this window.

The PMC Versions window lists information about each of the PMC regions that have been created in the Cisco IPICS server.

To display the PMC Regions window, navigate to the **PMC Management > PMC Regions** window.

Table 2-29 describes the items in the PMC Regions window.

Table 2-29 Item in the PMC Versions Window

Item	Description	Reference
Name field	This field specifies the name of the PMC regions.	See the "Adding PMC Regions" section on page 2-178 and the "Viewing or Editing PMC Regions" section on page 2-179
Short Name field	This field specifies the shortened name of the regions.	
Position field	This field specifies the position of the regions on the PMC display.	

Table 2-29 Item in the PMC Versions Window (continued)

Item	Description	Reference
Add button	Click this button to add a new PMC region to the Cisco IPICS server.	See the "Adding PMC Regions" section on page 2-178
Delete button	Click this button to delete a PMC region.	

Adding PMC Regions

To add a new PMC region, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **PMC Management > PMC Regions** window.

Step 2 Click **Add**.

A blank New PMC Region detail window displays.

Step 3 In the Name field, enter a name for the region.

Step 4 In the Short Name field, enter a condensed name for the region.

Tip The short name can be a shortened version of the full name or the same as the region position.

Step 5 From the Position drop-down list box, choose a position for the region.

Step 6 In the Description field, enter a description of the region. This field is optional.

Step 7 Click **Save**.

The region displays in the list of PMC regions and is available to assign to a channel/VTG while creating/updating channel/VTGs. See the "Adding a Radio" section on page 2-52

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

Viewing or Editing PMC Regions

To view or edit the PMC regions that are available for use in Cisco IPICS, perform the following procedure.

Note To add a new region, see the "Adding PMC Regions" section on page 2-178.

Procedure

Step 1 From the Administration Console, navigate to the **PMC Management > PMC Regions** window.

Step 2 In the Name column, click the link for the PMC region that you want to view or edit.

A region detail window displays current information about the region that you choose.

Step 3 To edit the information for the region, take any of the following actions:

- In the Name field, enter a new name for the region.
- In the Short Name field, enter a new condensed name for the region.
- In the Description field, enter a new description for the region.

For a description of the fields in this window, see the "Adding PMC Regions" section on page 2-178.

Step 4 Click **Save**.

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

Deleting PMC Regions

To delete PMC regions, perform the following procedure:

Procedure

Step 1 From the Administration Console, navigate to the **PMC Management > PMC Regions** window.

Step 2 Check the check box to the left of the region that you want to delete.

Step 3 Click **Delete**.

The region that you deleted is no longer available for use by the PMC users.

Tip If you want to delete all of the existing regions, check the check box at the top of the region list and click **Delete**.

Note When you delete a PMC region, any associated channels/VTGs are moved to the default region.