CHAPTER 2

# Configuring with the CMM Administration Tool

System administrators can configure their network using the CMM Administration Tool.

This chapter covers:



## Performing Domain Management

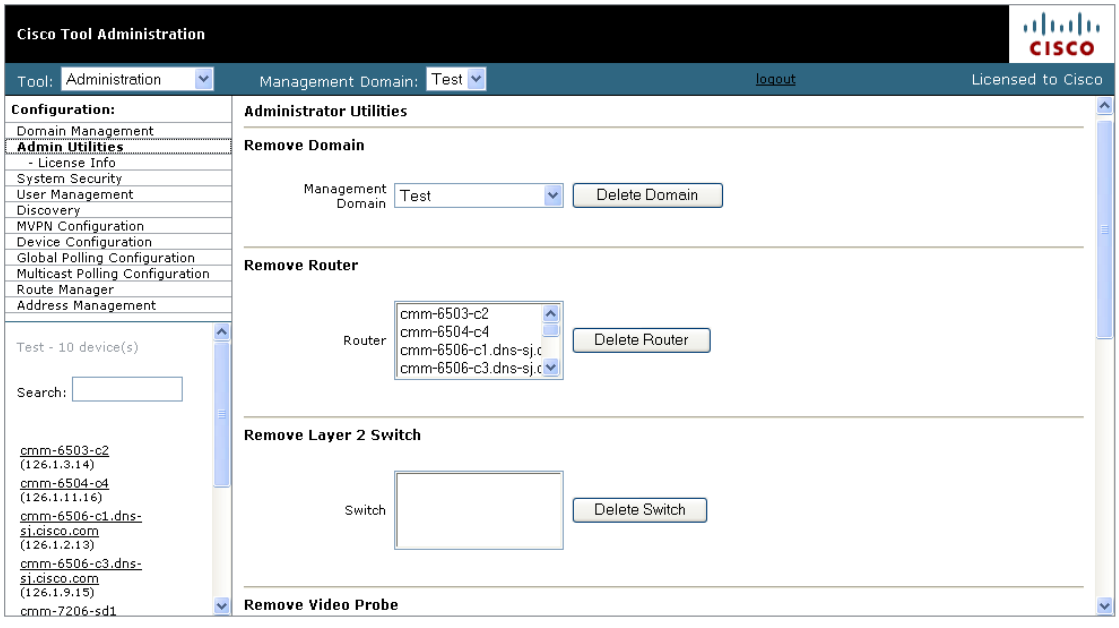
For details on Domain Management, see the "Creating a Domain" section on page 1-3.

## Using Administrative Utilities

The Administrator Utilities page provides maintenance tools for the system administrator.

Figure 2-1 shows the top part of the Administrator Utilities page.

***Figure 2-1 Administrator Utilities Page***



| Field | Description |
|---|---|
| Remove Domain | Removes all data associated with a management domain.<br>**Note** Domains cannot be removed while the polling daemon is running. |
| Remove Router | Removes a specific router from a management domain. However, if the device is being polled, you must remove it from the polling configuration first. |
| Remove Layer 2 Switch | Removes Layer 2 switches from the management database. |
| Remove Video Probe | Removes a video probe from Cisco Multicast Manager. |
| Remove Baseline | Removes a forwarding tree baseline, along with any associated tree change information. |
| Address Management Database | Contains:<br>• **Browse**—Find a CSV file to import.<br>• **Import**—You can import a CSV file into the IP address database. The file should be in the following format:<br>`#import file format`<br>`#this line will be skipped`<br>`239.1.1.1,test group`<br>`192.168.1.1,sourceA`<br>• **Reinitialize**—Restores all reserved multicast addresses to the IP address database.<br>• **Export**—Creates a file in */tmp* called **mmtIPdb.csv** which contains the IP address database in CSV format. |
| Log Files | Contains:<br>• **Clear Server Log**—Truncates the error_log file.<br>• **View Discovery Log**—Shows discovery-specific messages contained in the error_log file.<br>**Note** The error_log file should be rotated along with other system log files.<br>• **View Polling Engine Log**—Displays the contents of the polling log. |

# Configuring System Security

The System Security page provides TACACS login support for Cisco Multicast Manager.

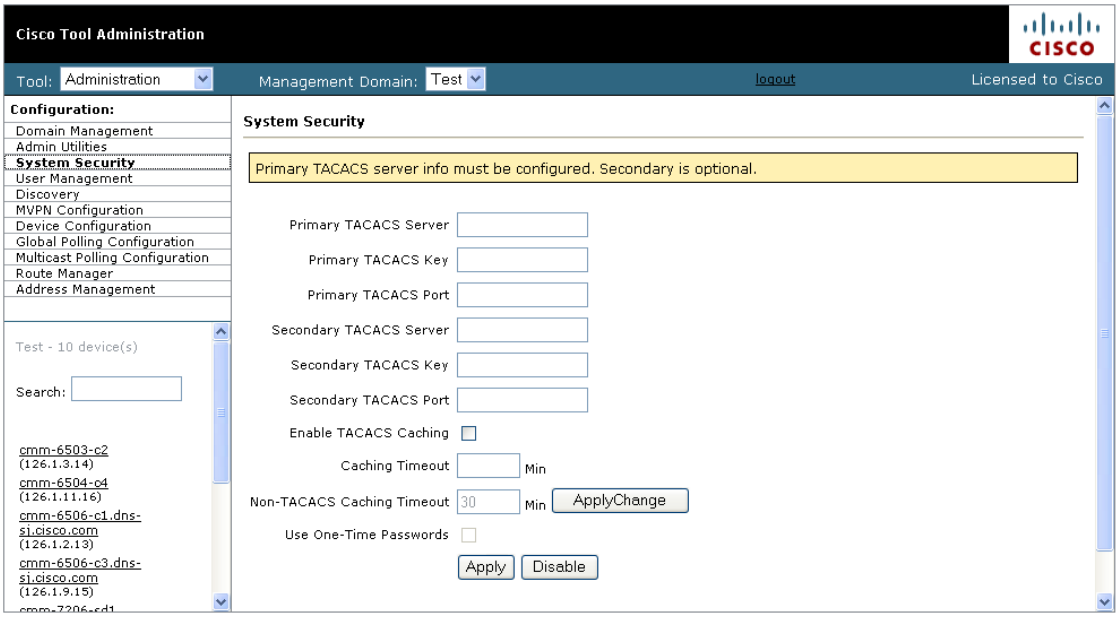
To configure TACACS login support:

**Step 1** Select the **Administration** tool.

**Step 2** From the Configuration menu, select **System Security**.

The System Security page opens, as shown in Figure 2-2.

***Figure 2-2 System Security Page***




**Step 3** Specify the following information for the primary TACACS server:

- **Primary TACACS Server**—Enter the IP address of the TACACS server.
- **Primary TACACS Key**—Enter the primary TACACS key.
- **Primary TACACS Port**—Enter the primary TACACS port number (the default port number is 49).

**Step 4** (Optional) If you want to configure a secondary TACACS server, specify the following information:

- **Primary TACACS Server**—Enter the IP address of the TACACS server.
- **Primary TACACS Key**—Enter the primary TACACS key.
- **Primary TACACS Port**—Enter the primary TACACS port number (the default port number is 49).

**Step 5** If you want to enable TACACS caching, check the Enable TACACS Caching check box and, in the Caching Timeout field, enter a caching timeout value in seconds.

**Step 6** If you want to use passwords that are valid only for one use, check the Use One-time Passwords check box.

**Step 7** Click **Apply**.

## Manually Configuring System Security

If the TACACS keys are configured incorrectly, then you must change them manually in the */opt/RMSMMT/httpd_perl/conf/httpd.conf* file as follows:

```
Tacacs_Pri_Key tac_plus_key
  Tacacs_Sec_Key tac_plus_key

<Sample AAA Server Config>
group = admins {
        service = connection {
                priv-lvl=15
}
group = netop {
        service = connection {}
}
 user = mike {
        member = netop
        login = des mRm6KucrBaoHY
}
user = admin {
        member = admins
        login = cleartext "ciscocmm"
}
</Sample AAA Server Config>
```

# Managing Users and Passwords

The CMM provides two privilege levels: user and admin. You need an administrator account to configure multicast domains, run discovery, create users, create health checks, and use the **Admin Utilities** functions.

You can configure users and passwords using the **User Management** pages:

- Manage Users
- Change Password

## Managing Users

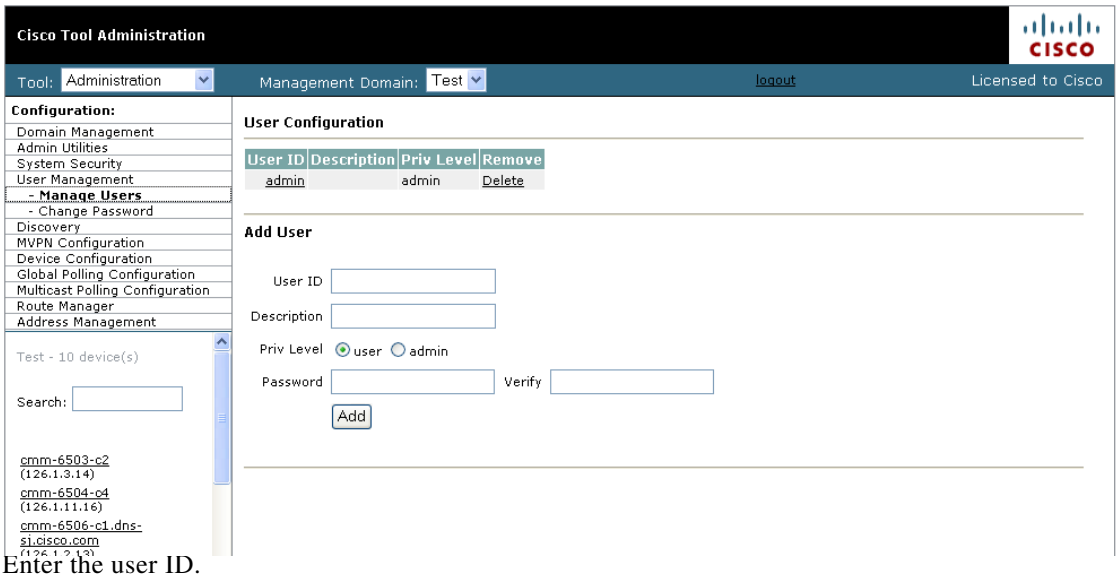
To manage users:

**Step 1** Select the **Administration** tool.

**Step 2** From the Configuration menu, select **User Management > Manage Users**.

The User Configuration page opens, as shown in Figure 2-3.

*Figure 2-3 Manage Users—User Configuration Page*




**Step 3** Enter the user ID.

**Step 4** (Optional) Enter a description.

**Step 5** Choose the appropriate privilege level, **user** or **admin**.

**Step 6** Enter the password into the **Password** and **Verify** boxes.

**Step 7** Click **Add**.

Selecting the User ID link in the table allows you to edit the user's description. Select **Delete** to delete a user (only an administrator can delete users).

**Note** The admin user account cannot be deleted.

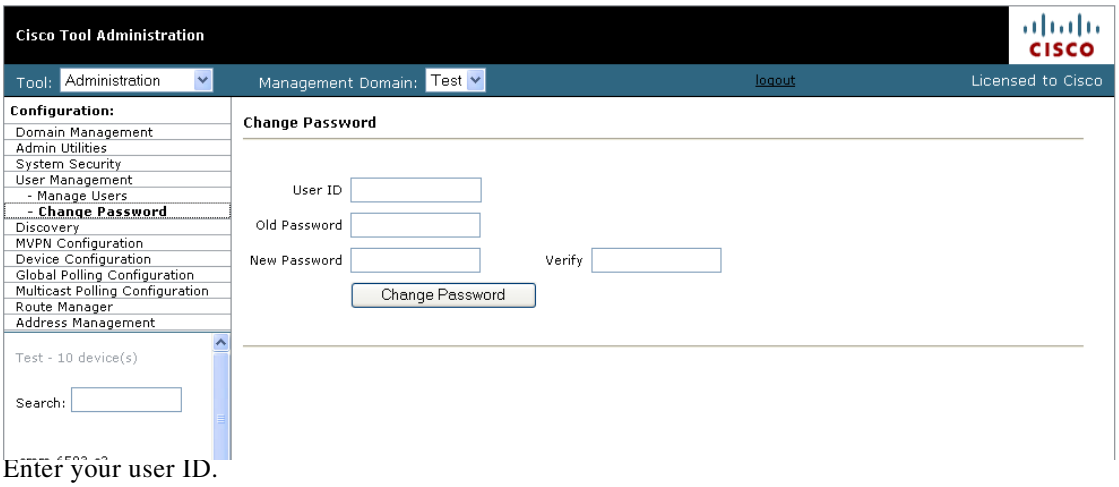
# Changing Your User Password

To change your user password:

**Step 1** On the Configuration Menu, select **User Management > Manage Users**.

The Change Password page opens, as shown in Figure 2-4.

*Figure 2-4 Manage Users—Change Password Page*




**Step 2** Enter your user ID.

**Step 3** Enter your old password.

**Step 4** Enter your new password in the **Password** and **Verify** boxes.

**Step 5** Click **Change Password**.

# Discovering Your Network

For details on Discovery, see Discovering Your Network, page 1-6.

# Configuring Devices and Probes

Using the Device Configuration page, you can:

- Change the SNMP read key of a single device.

  Select a **Router** or **Switch**, then click **Edit Parameters**.

  See Configuring Devices, page 8
- View a list of all available probes and Edit the basic parameters for the probe.

  Select a **Video Probe**, then click **Edit Parameters**.

  See Editing Basic Probe Parameters, page 2-14 for a detailed procedure.

# Configuring Devices

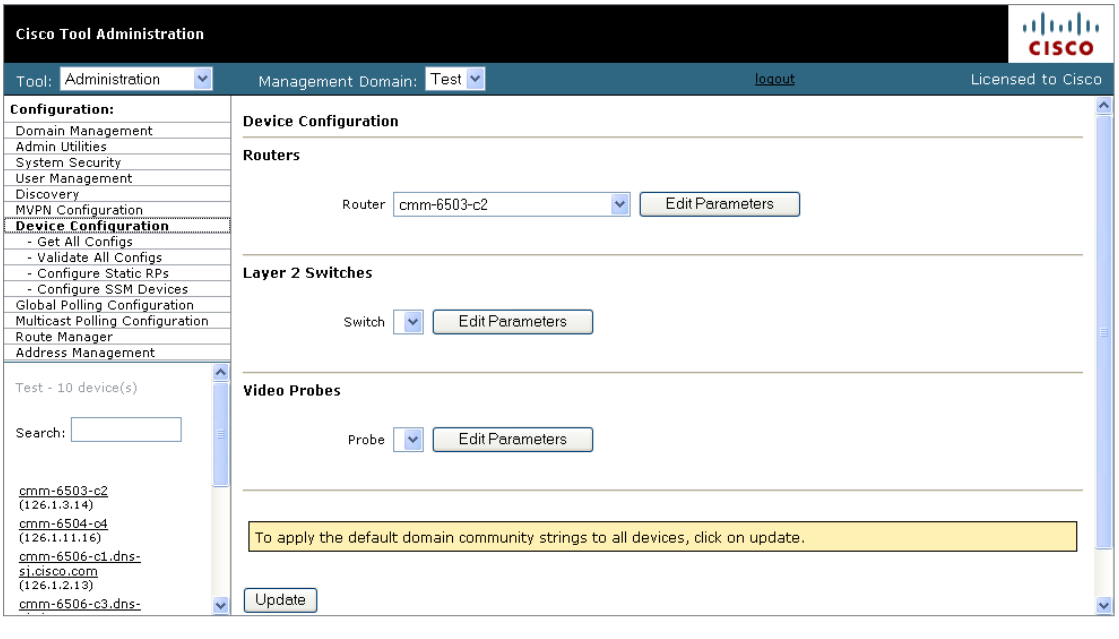
To configure a device:

**Step 1** Select the **Administration** tool.

**Step 2** From the Configuration menu, select **Device Configuration**

The Device Configuration page opens, as shown in Figure 2-6.

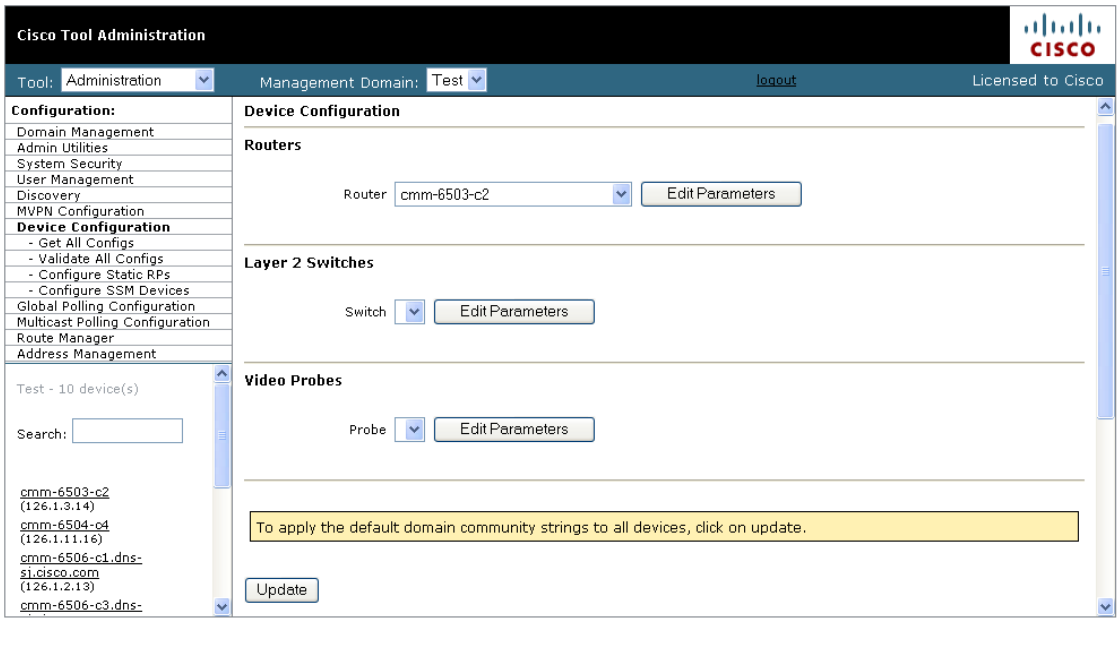
***Figure 2-5 Device Configuration—Edit Parameters***




**Step 3** From the drop-down lists, select a **Router** or **Switch**, then click **Edit Parameters.**

The Edit Parameters section for the specified device appears, as shown in Figure 2-6.

*Figure 2-6 Device Configuration Page for Routers*




**Step 4** Enter the following information:

- **Read Only Community String**—The Read Only Community String for the device.
- **Read Write Community String**—The Read Write Community Screen for the device
- **SNMP Timeout**—The SMMP timeout interval, in seconds.
- **SNMP Retries**—The number of SNMP retries to configure.

**Step 5** Click **Modify**.

# Downloading Router Configurations

If you entered the SNMP write key for the router when you set up the domain, Cisco Multicast Manager can download and display configuration files for the router.

**Note** To use this option, TFTP must be enabled on the server, and the SNMP read-write community string must be supplied. See the *Installation Guide for the Cisco Multicast Manager.*

To download a router configuration:

**Step 1** Select the **Administration** tool.

**Step 2** From the Configuration menu, select **Device Configuration** > **Get All Configs**.

The Get All Configs page opens.

**Step 3** Click **Go**.

The router configuration appears in the Get All Configs page.

This process may take some time, depending on the number of routers in the current domain.

# Validating Router Configurations

Using Cisco Multicast Manager, you can verify if IOS commands exist on a router, either globally, or on a single interface. Router configurations for a domain are verified against a template. Several sample templates are included with the application, or you can create a user-defined template, which must be a text (.txt) file containing a list of IOS commands to check. For example, to check for global commands, start the text file with the word "global." To check interface commands, add the word "interface" and so on. You can check for global and interface at the same time, as in the example:

```
GLOBAL
service timestamps log datetime msec localtime show-timezone
service password-encryption
logging
no logging console
no ip source-route
ip subnet zero
ip classless
INTERFACE
ip pim-sparse-mode
```

**Note** Before you can initiate validation, TFTP must be enabled on the server, and the SNMP read-write community string must be configured in Cisco Multicast Manager.

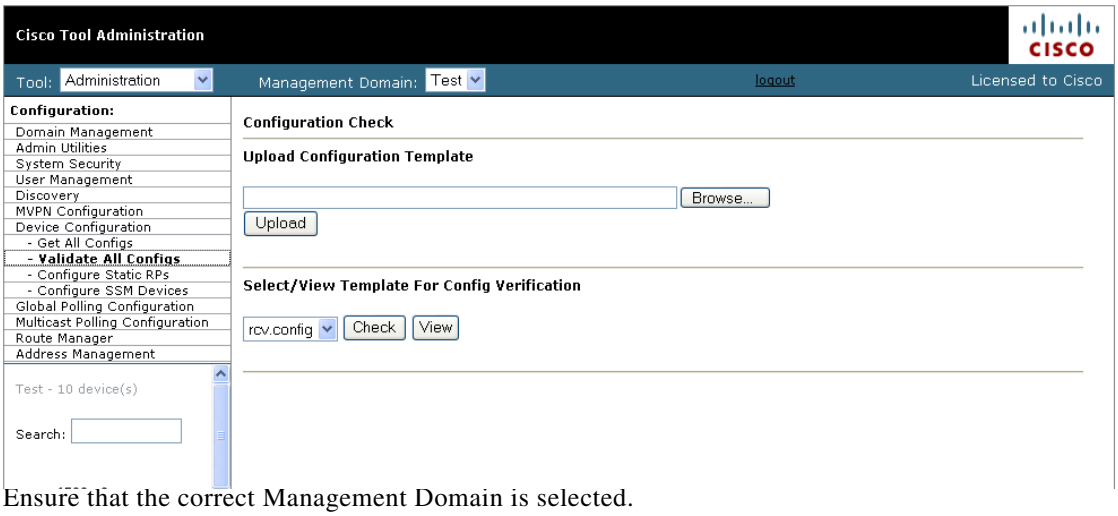
To select a template and initiate validation:

**Step 1** Select the **Administration** tool.

**Step 2** From the Configuration menu, select **Device Configuration** > **Validate All Configs**.

**Step 3** The Configuration Check page opens, as shown in Figure 2-7.

*Figure 2-7 Configuration Check Page*




**Step 4** Ensure that the correct Management Domain is selected.

**Step 5** If you want to upload a user-defined template:

a. Click **Browse**. Open the text (.txt) file you created.

b. Click **Upload**. The user-defined text file appears in the list below.

**Step 6** Select the template you want to use from the list.

**Step 7** (Optional) Click **View** to see the contents of each template.

**Step 8** Click **Check**.

Cisco Multicast Manager checks each router in the database for the existence of the commands in the template you specified. The output display indicates whether the commands have been entered and the corresponding settings have been made.

# Configuring Static RPs

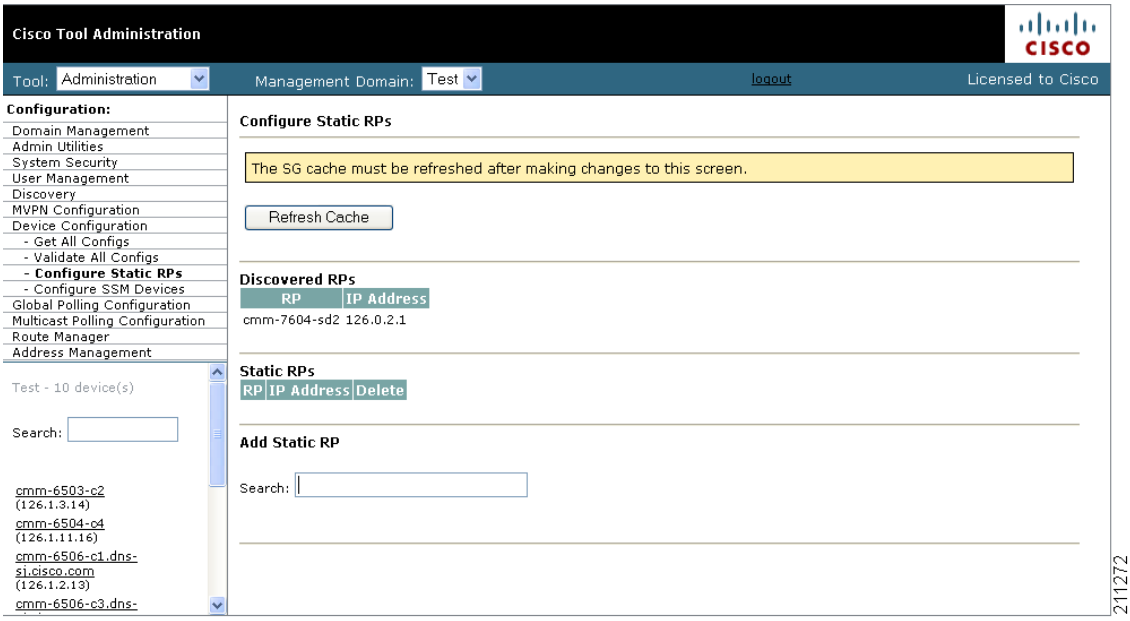
If you have static rendezvous points (RPs) configured, you must configure CMM to find these static RPs, which in turn populates the RP Summary within the Multicast Manager tool Diagnostics section.

To configure static RPs:

**Step 1** Under the **Device Configuration** menu, click **Configure Static RPs**.

The Configure Static RPs page opens, as shown in Figure 2-8.

***Figure 2-8 Configure Static RPs Page***




**Step 2** In the **Add Static RP** field, enter the IP address of the RP. The **Add Static RP** field is address sensitive, so as you type in the IP address, a list of routers appear.

**Step 3** Click **Add** next to the router(s) you want to select. The **Static RPs** table is populated.

# Configuring SSM Devices

The CMM currently supplies you with a list of all active sources and groups when requested (see the "Show All Groups" section on page 4-2). In a network containing RPs, the CMM visits each RP and collates a list to provide this information when requested. This is not possible in a Source Specific Multicast (SSM) network that does not contain RPs. To provide you with a list of all active sources and groups in SSM networks, you can input routers to the CMM that it visits when asked for this information. You can decide which routers are considered RP-type devices that contain most of the active sources and groups in the network, and then specify those routers. When you request to Show All Groups, the CMM visits the specified routers and builds the list from them.

**Note** You can see all active sources and groups on a particular router by viewing the Multicast Routing Table (see the "Managing Router Diagnostics" section on page 4-25).

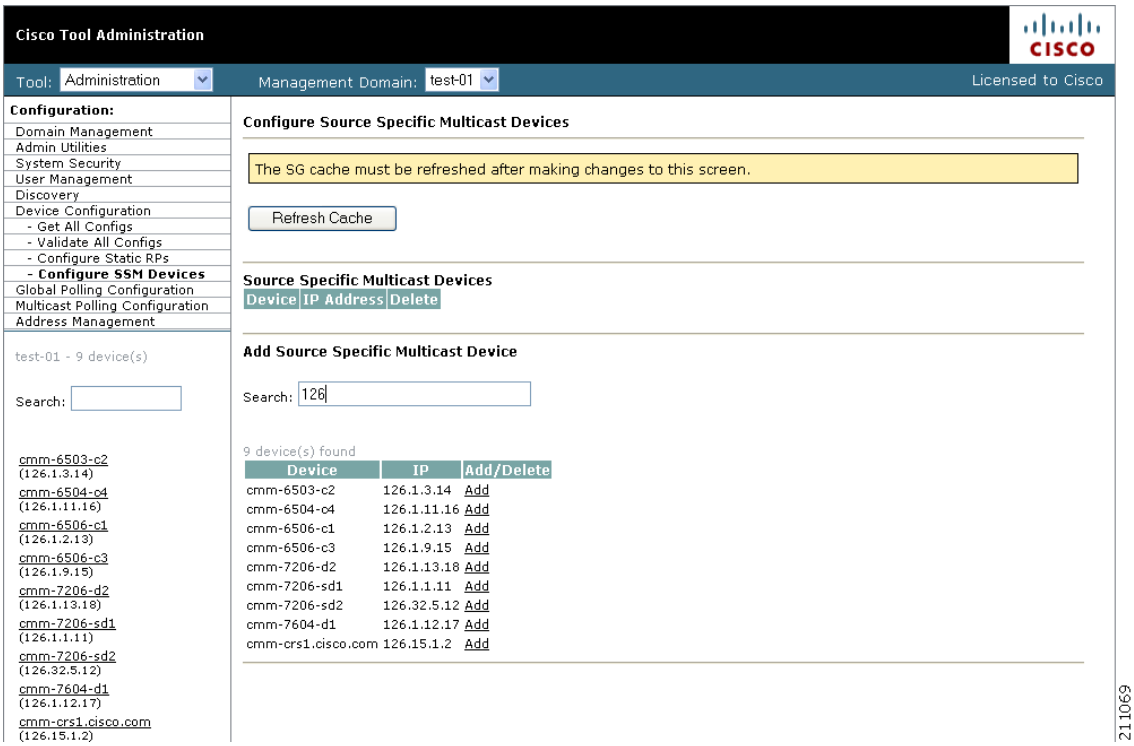
To configure SSM devices:

**Step 1** Select the **Administration** tool.

**Step 2** From the Configuration menu, select **Device Configuration > Configure SSM Devices**.

The Configure Source Specific Multicast Devices page opens, as shown in Figure 2-9.

***Figure 2-9 Configure Source Specific Multicast Devices Page***




**Step 3** Within the **Add Source Specific Multicast Device** box, enter the IP address of the RP. The **Add Static RP** box is address sensitive, so as you type in the IP address, a list of routers appear.

**Step 4** Click **Add** next to the router(s) you want to select. The **Source Specific Multicast Devices** table is populated.

# Viewing Available Probes

To view all available probes:

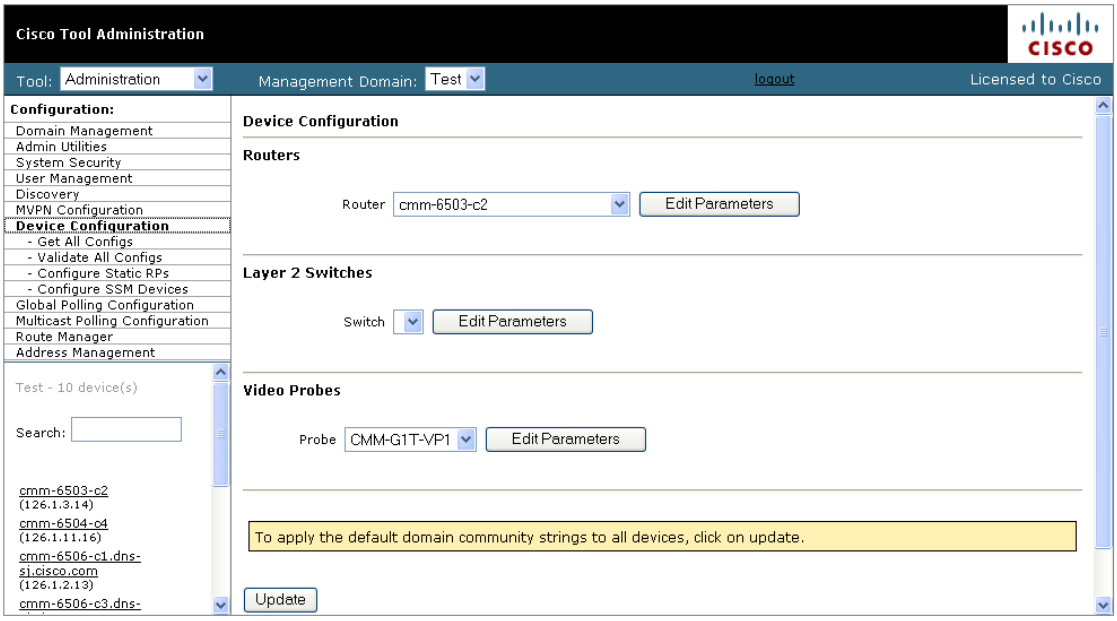
**Step 1** Select the **Administration** tool.

**Step 2** Click **Device Configuration.**

**Step 3** Select the drop-down list in the Probe field.

A list of available probes appears, as shown in Figure 2-10.

***Figure 2-10 Viewing the Available Probes***




# Editing Basic Probe Parameters

To edit the basic parameters for a video probe:

**Step 1** Select the **Administration** tool.

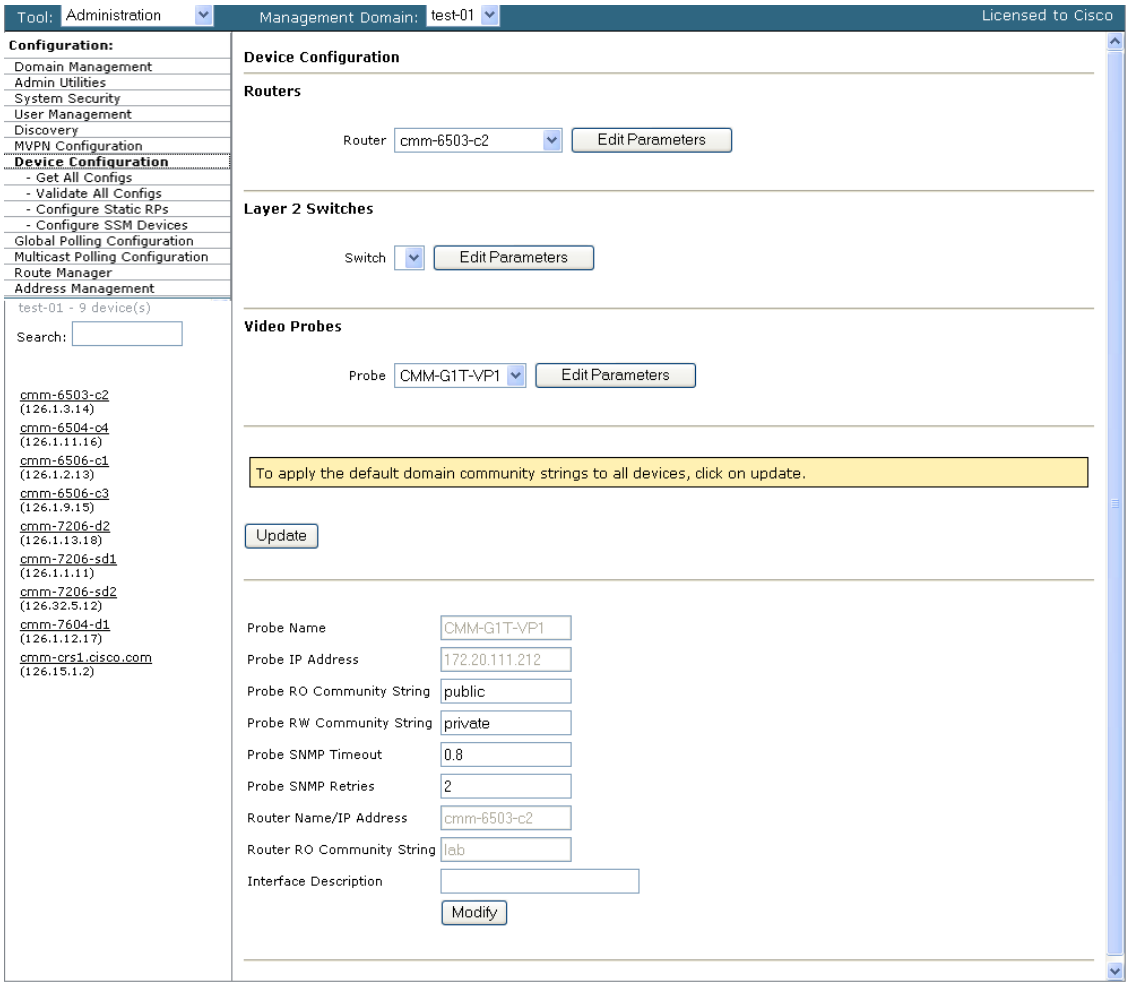
**Step 2** Click **Device Configuration.**

The Device Configuration page appears (shown in Figure 2-10).

**Step 3** From the drop-down list in the Probe field, select a video probe, and then click **Edit Parameters.**

The Edit Parameters section for probes appears, as shown in Figure 2-11.

***Figure 2-11 Editing Basic Probe Parameters***




You can edit the following parameters:

| Parameter | Description |
|---|---|
| Probe RO Community String | The SNMP read-only community string for the probe. |
| Probe IP Address | The IP address of the device on which the probe is installed.<br><br>**Note** Does the probe itself have a separate IP address from the router? |
| Probe RW Community String | SNMP read-write community string for the probe. |
| Probe SNMP Timeout | Retry period if the probe does not respond. Default value is 0.8. |

| Parameter | Description |
|---|---|
| Probe SNMP Retries | Number of retries to contact a probe before issuing a timeout. Default value is 2. |
| Router Name/IP Address | The hostname or IP address of the router on which the probe is running. |
| Router RO Community String | The read only community string for the router. |
| Interface Description | A brief description of the interface that the probe is monitoring. |

**Step 4** Edit the probe parameters as required.

**Step 5** Click **Modify**.

**Note** To set the RW community string and the RO community string to their default values (`public` for the RO community string and `private` for the RO community string, click **Update**.

# Configuring Global Polling

You can configure each polling element to start and stop at specific times. Each element also has its own polling interval. You can configure these values through the Global Polling Configuration page.

**Note** You must restart the polling daemon after making changes on this page.

To configure global polling:

**Step 1** Select the **Administration** tool.

**Step 2** Click **Global Polling Configuration.**

The Global Polling Configuration page appears

Figure 2-12 show the top portion of the page, and Figure 2-13 shows the bottom portion.

*Figure 2-12 Global Polling Configuration Page (Top Portion)*

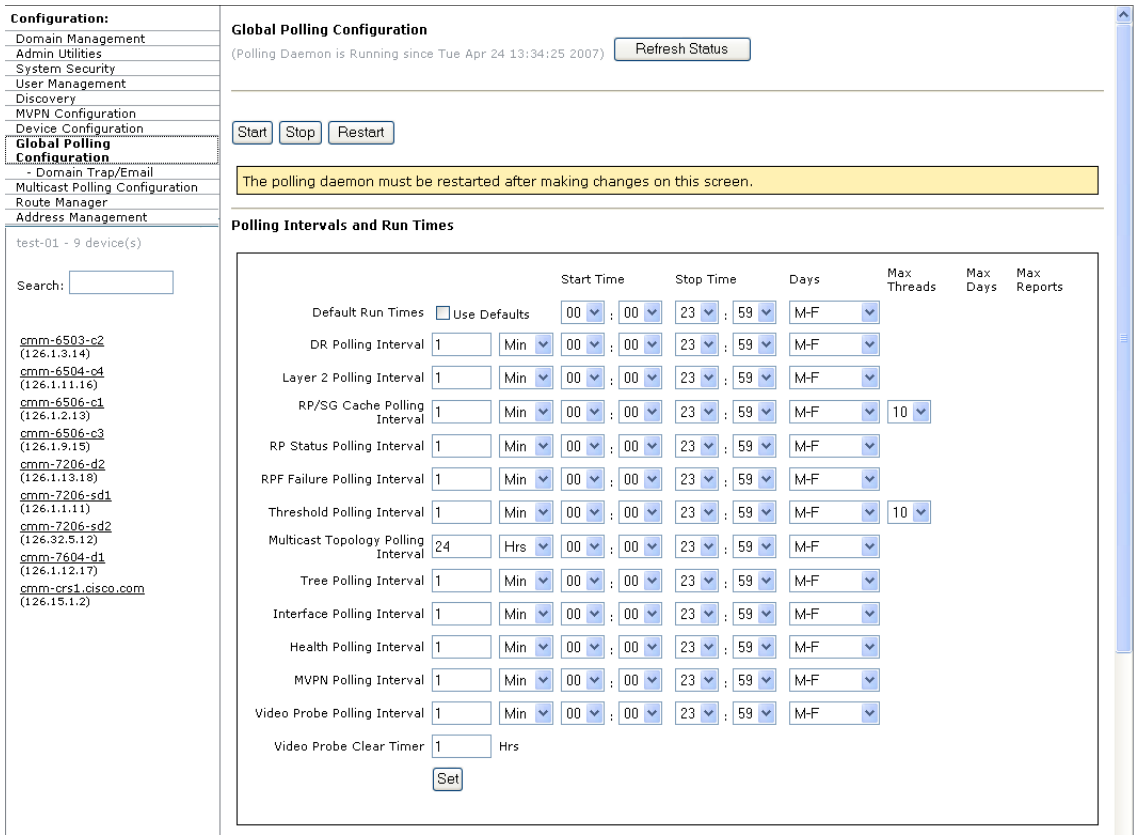
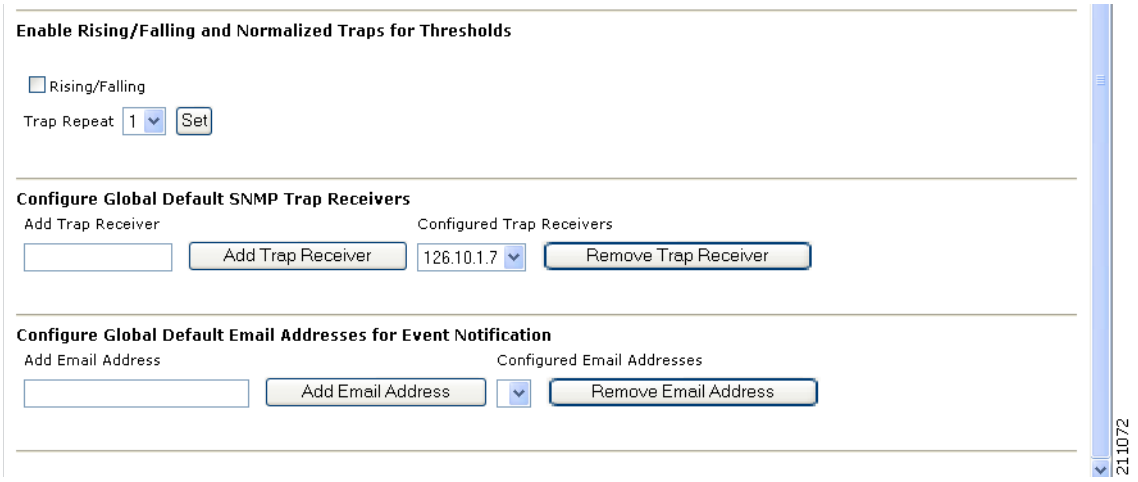



*Figure 2-13 Global Polling Configuration Page (Bottom Portion)*




**Step 3** The following table describes the fields and selections on the Global Polling Configuration page:

**Note** Setting any one of these values to less than 1 disables that specific polling feature.

| Field or Button | Description |
|---|---|
| Refresh Status | The status line indicates how long the polling daemon has been running and how it was started. Click **Refresh Status** to update the status information. |
| Start | Starts the polling daemon globally. |
| Stop | Stops the polling daemon globally. |
| Restart | Restarts the polling daemon globally. Each time you change a polling interval, click **Restart**. |
| Default Run Times—Use Defaults | Selecting the Use Defaults checkbox sets all the start/stop times and days to the default values. |
| DR Polling Interval | Checks the status of all DRs in the network. If a user changes a DR, an SNMP trap is sent. |
| Layer 2 Polling Interval | Time between polling of the Layer 2 ports. |
| RP/SG Cache Polling Interval | For certain CMM data, such as the data within the Multicast Diagnostics page (see Show All Groups, page 4-2) the CMM queries each RP, collates a list of active sources, and groups and displays them. There are two ways the CMM can accomplish this: dynamically when the command is entered, or the CMM can build a cache of this information, and when the command is entered, the cache is queried. Caching is enabled on the System Configuration page (see Performing Domain Management, page 2-1) and the RP/SG Cache Polling Interval is the time period that this cache is refreshed.<br><br>Deciding whether caching should be turned on depends upon the number of RPs, sources, and groups. If the Multicast Diagnostics page takes a while to display all groups, you may want to turn caching on.<br><br>The **Max Threads** value controls how many devices are queried simultaneously. Values can be 1-10. Queries used for RP/SG Cache Polling are SNMP getbulk queries that can potentially return large amounts of data. To address timeouts, you can reduce the number of Max Threads and/or adjust the SNMP timeout and retry values on the System Configuration page (see Performing Domain Management, page 2-1). |

| Field or Button | Description |
|---|---|
| RP Status Polling Interval | RP Status Polling queries the sysUpTime of the RPs configured on the RP Polling Configuration page (see RP Polling, page 2-26).<br><br>The purpose of this query is to report availability of the RPs. If the RP responds, an *rpReachable* trap is sent. If the RP does not respond, an *rpUnreachable* trap is sent. Since at least one of these traps is sent at each polling interval, you can also use them to ensure that the polling daemon is up and running. |
| RPF Failure Polling Interval | Time interval that each router will be polled for each source and group configured to check the number of RPF failures. |
| Threshold Polling Interval | Time interval that each router will be polled for the existence of each source and group configured, and CMM will ensure that no thresholds are exceeded. |
| Multicast Topology Polling Interval | Topology polling queries the sysUpTime of each router in the multicast domain to see if it has been reloaded. If it has, the polling daemon launches a Single Router Discovery of that device in the background, to ensure that the SNMP *ifIndexes* have not changed. |
| Tree Polling Interval | Time interval that the monitored trees are drawn and compared with their baselines. |
| Interface Polling Interval | Time interval where the percent of multicast bandwidth per interface is compared to the thresholds. |
| Health Polling Interval | Time interval at which the configured health checks are scheduled to run. |
| Video Probe Polling Interval | Time interval at which Cisco Multicast Manager pools the video probes to examine multicast flows and obtain MDI calculations. |
| Video Probe Clear Timer | Interval after which Cisco Multicast Manager changes a yellow warning indicator to a green OK indicator. |
| Set | Sets the values you enter. |

**Step 4** To enable or disable the continuous sending of PPS threshold traps, use the **Enable Rising/Falling and Normalized Traps for Thresholds** section:

- If the **Rising/Falling** option is not checked (disabled), traps are sent whenever the PPS rate for a monitored S,G exceeds specified thresholds.
- If the **Rising/Falling** option is checked (enabled), a trap is sent only when the PPS rate initially exceeds the high or low threshold. After the PPS rate returns to the specified range, a normalized threshold trap is sent.

- Because SNMP v1 traps are sent unreliably, you can set the **Trap-Repeat** option to allow the initial and normalized traps to be sent anywhere from 1 to 5 times when an event occurs.

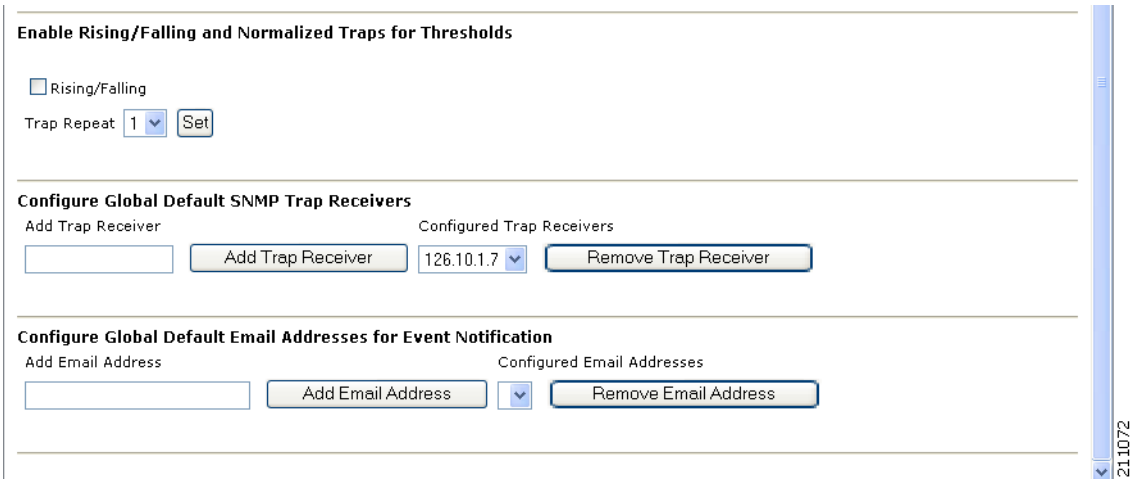
**Step 5** To add or remove trap receivers, use the **Configure Global Default SNMP Trap Receivers** section. The SNMP trap receivers specified here are only used if domain-specific SNMP trap receivers are not specified. Domain-specific trap receivers are specified from the Trap Receiver/Email Polling Configuration page (see Configuring Domain-Specific Trap Receivers and Email Addresses, page 2-20).

**Step 6** To add or remove email addresses, use the Configure Global Default Email Addresses for Event Notification section. Email addresses are notified of SSG exceptions and threshold and existence events. The email addresses specified here are used only if domain-specific email addresses are not specified. Domain-specific email addresses are specified from the Trap Receiver/Email Polling Configuration page (see Configuring Domain-Specific Trap Receivers and Email Addresses, page 2-20).

# Configuring Domain-Specific Trap Receivers and Email Addresses

You can configure the CMM to send domain-specific SNMP trap receivers or emails. Under the **Global Polling Configuration** menu at left, click **Domain Trap/Email**. The Trap Receiver/Email Polling Configuration page appears, as shown in Figure 2-14.

***Figure 2-14 Trap Receiver/Email Polling Configuration***



You can add or remove trap receivers using the **Configure Domain Specific SNMP Trap Receivers** section. The SNMP trap receivers specified here are only used if global SNMP trap receivers are not specified. Global trap receivers are specified from the Configure Global Default SNMP Trap Receivers page (see Configuring Global Polling, page 2-16).

You can add or remove email addresses using the **Configure Domain Specific Email Addresses for Event Notification** section. Email addresses are notified of SSG exceptions and threshold and existence events. The email addresses specified here are only used if global email addresses are not specified. Global email addresses are specified from the Configure Global Default SNMP Trap Receivers page (see Configuring Global Polling, page 2-16).

# Managing Device Addresses

Using the Address Management menu selection page, you can enter multicast group and source addresses into the database with a description. When the CMM displays these sources and groups, the descriptions will be added for easy recognition.

You can also display and manage the addressing information in:

- the Ad Zone database
- the Channel Map database
- the Multiplex Table database

The database is already populated with all the reserved address space.

## Managing IP Addresses

Using the Address Management menu selection page, you can enter multicast group and source addresses into the database with a description. When the CMM displays these sources and groups, the descriptions will be added for easy recognition.

To display the IP address database:

**Step 1** Select the **Administration** tool.

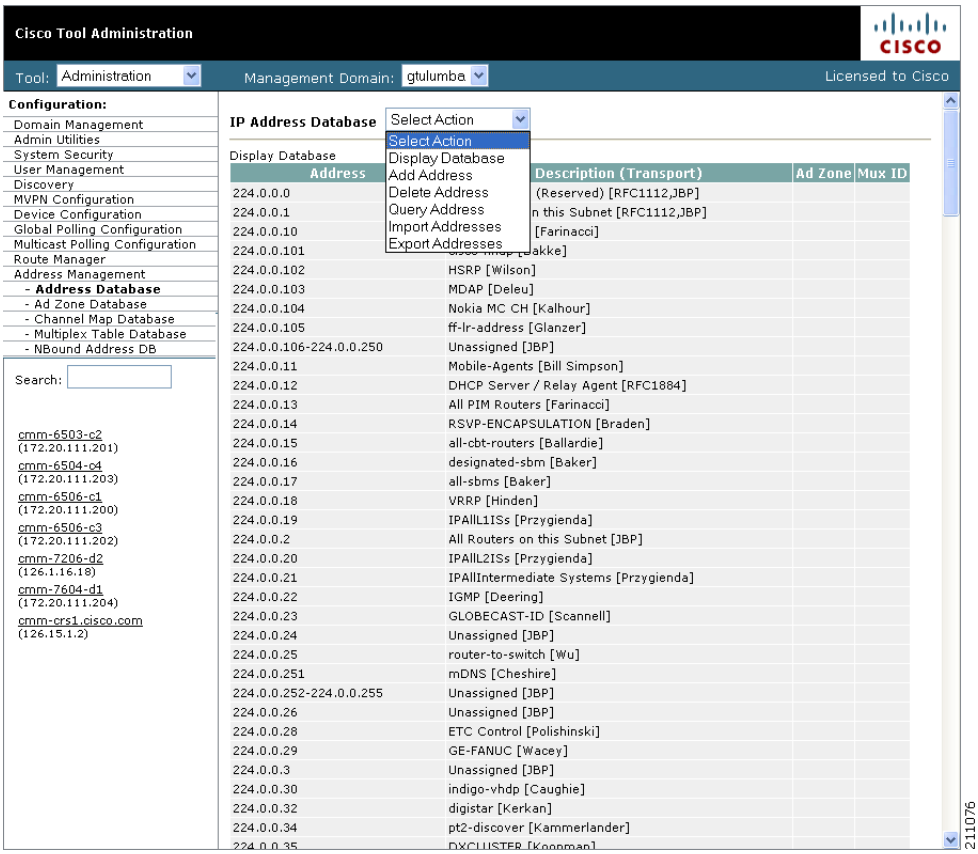
**Step 2** Select **Address Management > Address Database.**

The IP Address Database page opens.

**Step 3** From the drop-down list in the IP Address Database field, select **Display Database**.

The IP Address Database page displays the IP address database, as shown in Figure 2-15.

***Figure 2-15 Address Management***




From the IP Address Database drop-down menu, you can also choose these actions:

| Menu Selection | Description |
|---|---|
| Add Address | Add an address to the IP address database. |
| Delete Address | Delete an IP address from the database. To delete an IP address,<br>1. From the drop-down menu in the IP Address Database field, select **Delete Address**.<br>The Delete Address page appears.<br>2. From the drop-down list in the Address field, select the address to delete.<br>You are prompted to delete the address.<br>3. To delete the address click **OK**. |

| Menu Selection | Description |
|---|---|
| Query Address | To query an IP address:<br>1. From the drop-down menu in the IP Address Database field, select **Query Address**.<br>The Query Address page appears.<br>2. From the drop-down list in the Address field, select the address to query.<br>The Query Address page displays the overlapped IP addresses in the multicast address. |
| Import Addresses | To import addresses from a CSV file,:<br>1. Create a CSV file with this format:<br>`IP Address, Description, Ad Zone Number, Mux ID`<br>2. From the drop-down menu in the IP Address Database field, select **Import Addresses**<br>The Import Address page appears.<br>3. Click the **Browse** button and then browse to CSV file that you created in Step 1.<br>4. Specify one of the following:<br>– To merge the addresses in the import file into the database, click the Merge radio button.<br>– To replace the current database with the addresses in the import file, click the **Replace** radio button.<br>5. Click **Import**. |
| Export Addresses | The Export Addresses selection allows you to export addresses to a CSV file.<br>To export IP addresses:<br>1. From the drop-down menu in the IP Address Database field, select **Export Addresses**<br>The following message appears, indicating the directory and file to which the address file has been exported:<br>`Exported IP Address Database to /tmp/mmtIPdb.csv` |

# Managing the Ad Zone Database

Using the **Ad Zone Database** selection on the Address Management menu, you can manage digital advertising zones (ad zones) in your network.

To manage ad zones:

**Step 1** Select the **Administration** tool.

**Step 2** Select **Address Management > Ad Zone Database.**

The Ad Zone Database page opens.

**Step 3** From the Ad Zone Database drop-down menu, choose one of the following actions:

- **Display Database**—Display the ad zone database.
- **Add Ad Zone**—Enter a Zone Number and a Zone Name to add an ad zone.
- **Delete Ad Zone**—Delete an ad zone from the database.
- **Edit Ad Zone**—Edit an existing ad zone.
- **Query Ad Zone**—Query information about an ad zone.
- **Import Ad Zones**—Import ad zones from a CSV file.

# Managing the Channel Map Database

Using the **Channel Map Database** selection on the Address Management menu, you can manage the channel map database.

To manage the channel map database:

**Step 1** Select the **Administration** tool.

**Step 2** Select **Address Management > Channel Map Database.**

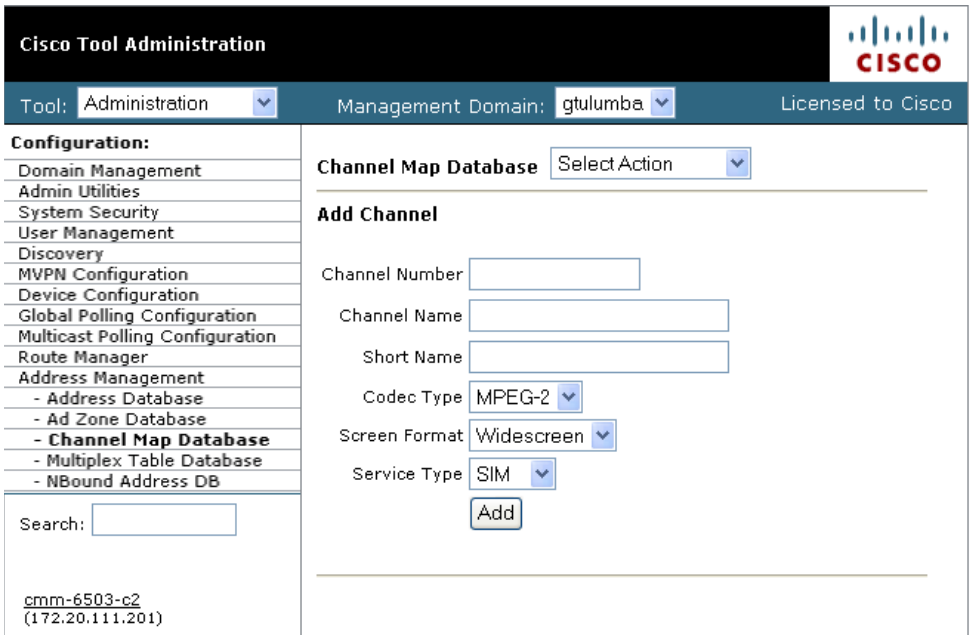
The Channel Map Database page opens.

**Step 3** From the Channel Map Database drop-down menu, choose one of the following actions:

- **Display Database**—Display the channel map database.
- **Add Channel**—Enter a channel from the database.
- **Query Channel**—Query information about a channel
- **Import Channels**—Import channels information from a CSV file.

If you select **Add Channel**, the Add Channel page opens, as shown in Figure 2-16.

***Figure 2-16 Add Channel Page***




**Step 4** If you are adding a channel, specify the following information, then click **Add**:

| Field | Description |
|---|---|
| Channel Number | Enter the channel number. |
| Channel Name | Enter the channel name. |
| Short Name | Enter a short name for the channel. |
| CODEC Type | From the drop-down list in the **CODEC Type** field, select the type of CODEC the channel uses. |
| Screen Format | From the drop-down list in the **Screen Format** field, select the screen format for the channel. |
| Service Type | From the drop-down list in the **Service Type** field, select the service type for the channel. |

## Managing the Multiplex Table Database

Using the **Multiplex Table Database** selection on the Address Management menu, you can manage multiplexers in your network.

To manage multiplexes:

**Step 1** Select the **Administration** tool.

**Step 2** Select **Address Management > Multiplex Table Database.**

The Multiplex Table Database page opens.

**Step 3** From the Multiplex Table Database drop-down menu, choose one of the following actions:

- **Display Database**—Display the Mux ID database.
- **Add Mux ID**—Add a Mux ID.
- **Delete Mux ID**—Delete an Mux ID from the database.
- **Edit Mux ID**—Edit an existing Mux ID.
- **Query Mux ID**—Query information about a Mux ID

# Configuring Specific Multicast Manager Polling

You can configure the following types of multicast polling:



## RP Polling

Using the RP Polling Configuration page, you can enable Cisco Multicast Manager to:

1. Monitor and report all leaves and joins.
2. Set a threshold on the number of groups that can join an RP if this is exceeded, a trap is sent.
3. Find out if a specific RP is available.
4. Create a list of all acceptable sources and groups and send a trap if any rogue sources or groups appear on the RP.

**Note** RP availability is configured within the Global Polling Configuration page (see Configuring Global Polling, page 2-16). A trap is sent if an RP becomes unavailable, and a report is generated within the RP Polling Report page (see RP Polling Report, page 3-7).

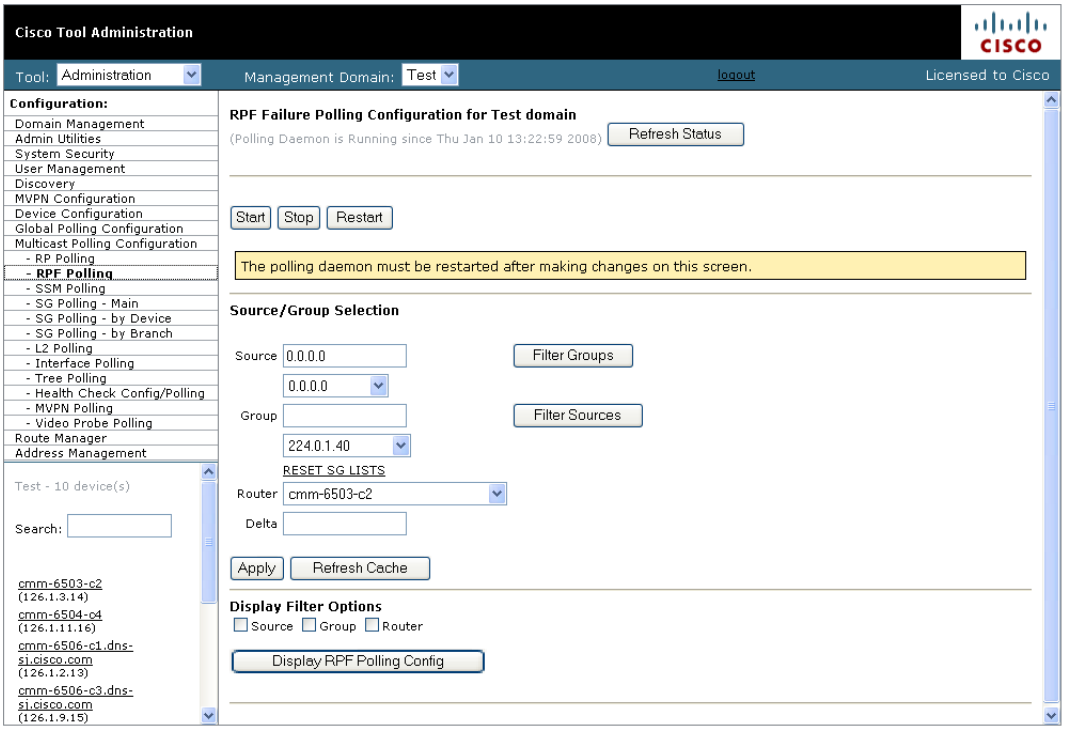
To configure RP polling:

**Step 1** Select the **Administration** tool.

**Step 2** Select **Multicast Polling Configuration > RP Polling.**

The RP Polling Configuration page opens, as shown in Figure 2-17.

***Figure 2-17 RP Failure Polling Configuration Page***



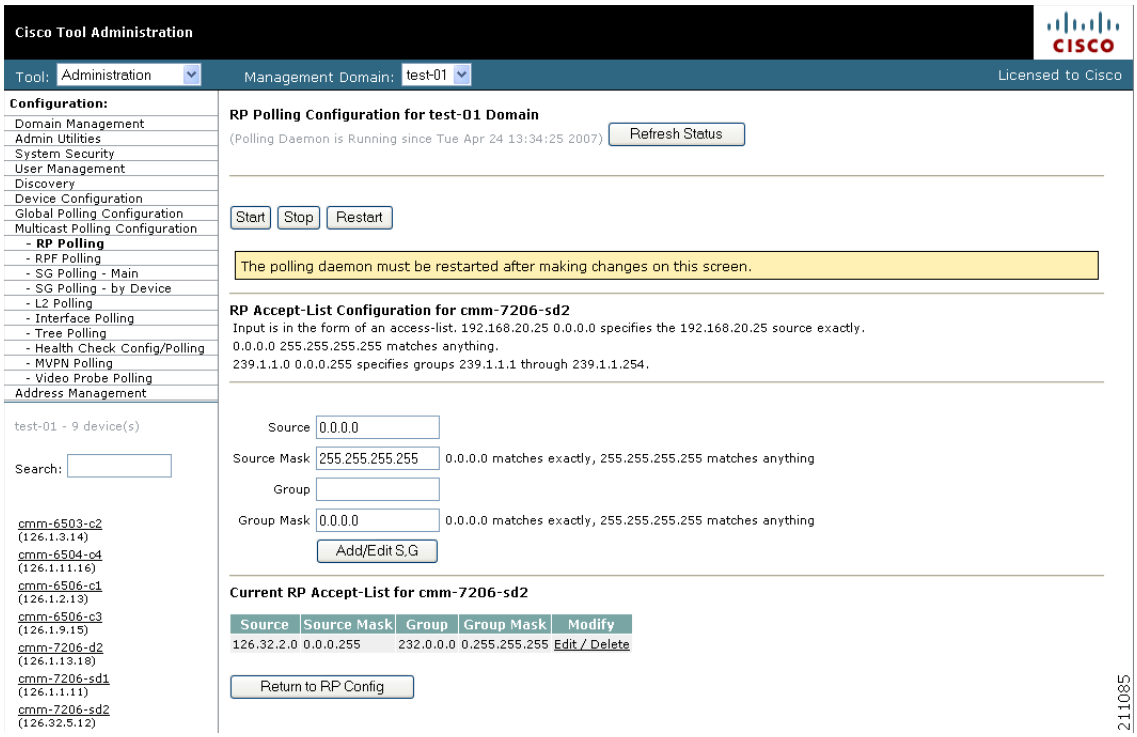
The RP Polling Configuration page contains the following fields and buttons:

| Fields and Buttons | Description |
|---|---|
| Refresh Status | The status line indicates how long the polling daemon has been running and how it was started. Click **Refresh Status** to update the status information. |
| Start | Starts the polling daemon globally. |
| Stop | Stops the polling daemon globally. |
| Restart | Restarts the polling daemon globally. Each time you change a polling interval, click **Restart**. |
| Enable RP Group Add Delete Traps | Click the check box to monitor all leaves and joins, which are then reported within the RP Polling Report page (see RP Polling Report, page 3-7). |
| RP Monitoring | To monitor an RP, select the RP from the box.<br>To monitor a specific number of groups, enter a number in the **Group Limit** box.<br>Click **Monitor RP**.<br>If the group limit is exceeded, a report is generated within the RP Group Threshold Report page (see the "RP Group Threshold Report" section on page 3-8). |
| RPs Being Monitored | Lists:<br>• **RP**—The name of the RP being monitored<br>• **Group Limit**—Number of groups being monitored for that RP.<br>• **Accept-List**—Monitors the sources and groups active on the RP (see the "RP Accept List Configuration" section on page 2-28).<br>• **Remove**—Deletes the RP. |
| Single S, G Monitoring | Enter the group IP address. If more than one source becomes active for this group, a report is generated. |

## RP Accept List Configuration

The RP Accept List Configuration section lets you monitor the active sources and groups on a specific RP.

*Figure 2-18 RP Accept List Configuration*




| Fields and Buttons | Description |
|---|---|
| Source | Enter the sources that are allowed to appear on this RP. |
| Source Mask | Enter the source mask. |
| Group | Enter the groups that are allowed to appear on this RP. |
| Group Mask | Enter the group mask. |
| Add/Edit S,G | Click to save your changes. |
| Return to RP Config | Click to return to the RP Polling Configuration page. |

# RPF Polling

Using Cisco Multicast Manager, you can monitor Reverse Path Forwarding (RPF) failures for a particular source and group on any selected router.

If any monitored source and group begins to experience RPF failures that rise above the delta, then SNMP traps can be sent, and a report generated, which you can view under RPF Failures (see RPF Failures, page 3-9).

You can select the source and group from the list, or you can enter them manually. If there are a lot of sources and/or groups, you can use the filter option to ensure that you are selecting an S,G that actually exists in the network. The filter option displays only the sources for a selected group or only the groups for a selected source. To reset the lists, click **Reset S,G Lists**.

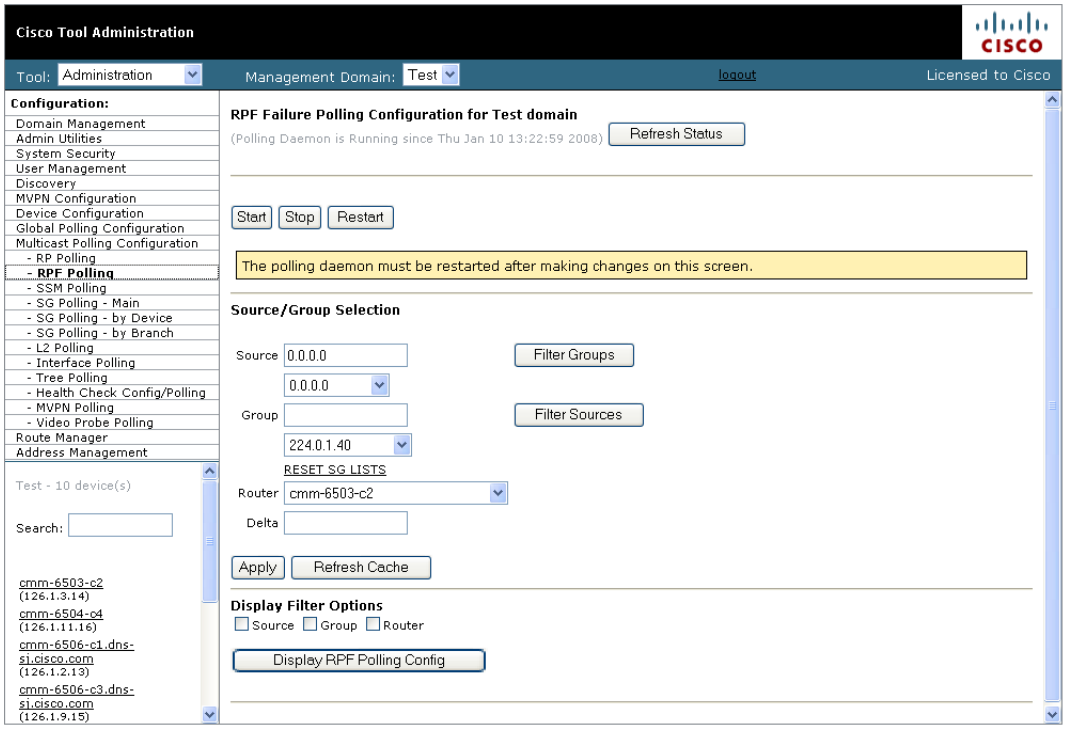
To configure RPF polling:

**Step 1** Select the **Administration** tool.

**Step 2** Select **Multicast Polling Configuration > RPF Polling.**

The RPF Polling Configuration page opens, as shown in Figure 2-19.

***Figure 2-19 RPF Failure Polling Configuration Page***



The RPF Failure Polling Configuration page contains the following fields and buttons:

| Fields and Buttons | Description |
|---|---|
| Refresh Status | The status line indicates how long the polling daemon has been running and how it was started. Click **Refresh Status** to update the status information. |
| Start | Starts the polling daemon globally. |
| Stop | Stops the polling daemon globally. |
| Restart | Restarts the polling daemon globally. Each time you change a polling interval, click **Restart**. |
| Source | Enter or select the IP address of the source to monitor. |
| Filter Groups | Filters the output to contain only the relevant groups. |
| Group | Enter or select the IP address of the group to monitor. |
| Filter Sources | Filters the output to contain only the relevant sources. |
| Reset SG Lists | Clears any entries and refreshes the source and group lists. |
| Router | Enter the router name. |
| Delta | Number of RPF failures per sampling period that trigger a report. |
| Apply | Applies and saves the changes. |
| Refresh Cache | Click **Refresh Cache** to refresh the table of sources and groups. |
| Display RPF Polling Configuration | To display a list of the current RPF Polling configurations:<br>1. Click **Display RPF Polling Configuration** You can filter the configuration display by source, group, or router.<br>A list of the current RPF polling configuration appears.<br>2. To edit a configuration, click **Edit** at the right of the summary row for the configuration.<br>3. To delete a configuration, click **Delete** at the right of the summary row for the configuration. |

# S, G Polling—Main

Using Cisco Multicast Manager, you can poll sources and groups with high and low thresholds.

You can select the source and group from the list, or you can enter them manually. If there are a lot of sources and/or groups, you can use the filter option to ensure that you are selecting an S,G that actually exists on the network. The filter option displays only the sources for a selected group, or only the groups for a selected source.

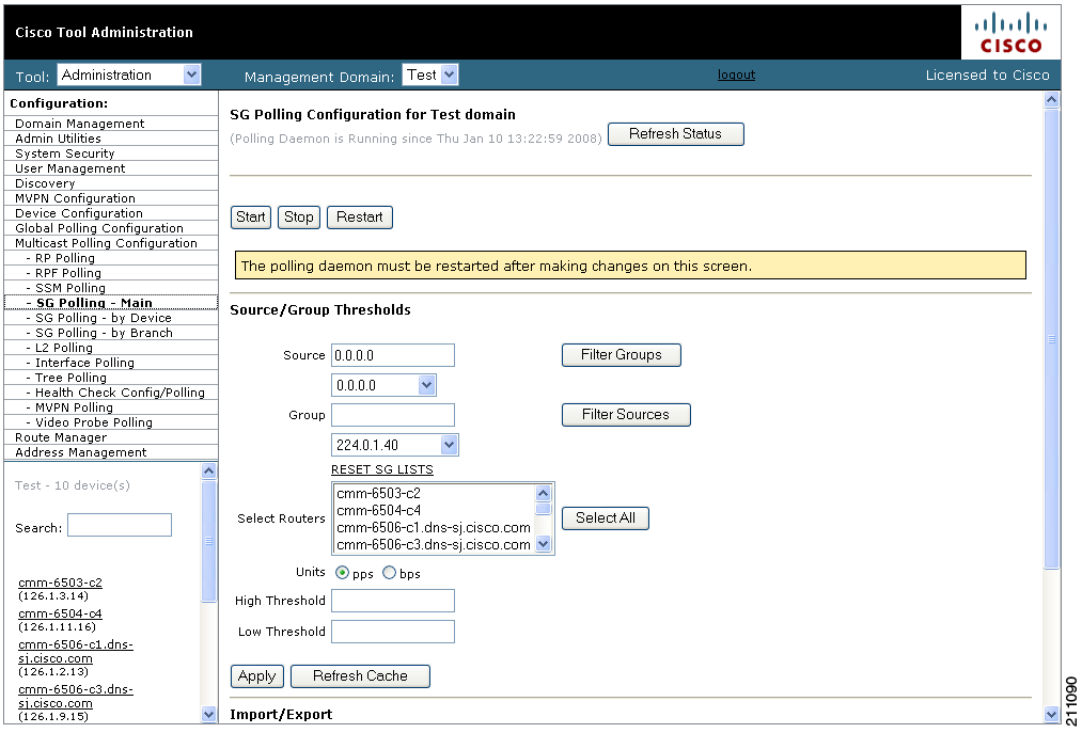
To configure SG polling:

**Step 1** Select the **Administration** tool.

**Step 2** Select **Multicast Polling Configuration > SG Polling - Main.**

The main SG Polling Configuration page opens, as shown in Figure 2-20.

***Figure 2-20 SG Polling Configuration Page***



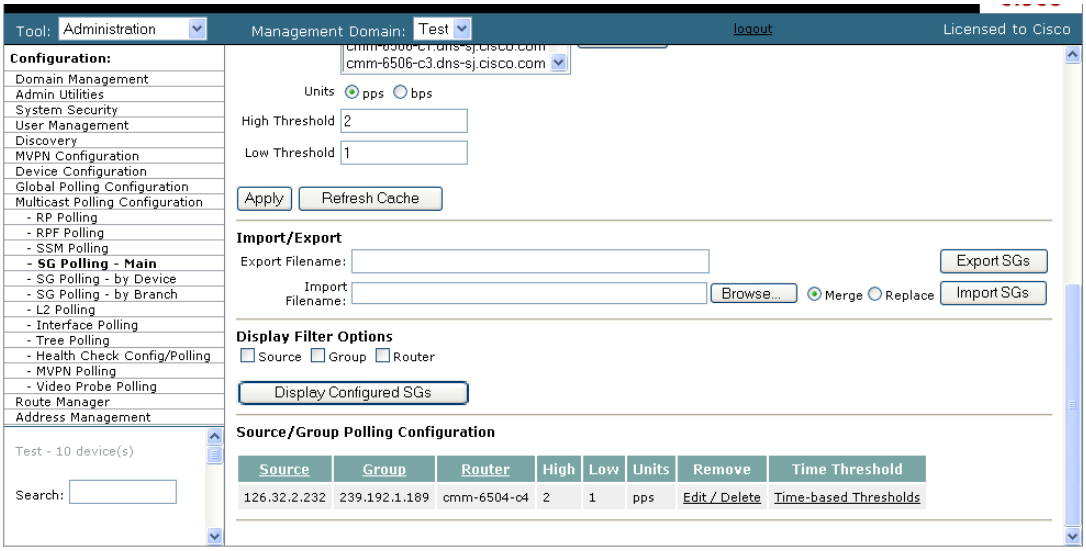
The SG Polling Configuration page contains the following fields and buttons:

| Fields and Buttons | Description |
|---|---|
| Refresh Status | The status line indicates how long the polling daemon has been running and how it was started. Click **Refresh Status** to update the status information. |
| Start | Starts the polling daemon globally. |
| Stop | Stops the polling daemon globally. |
| Restart | Restarts the polling daemon globally. Each time you change a polling interval, click **Restart**. |
| Source | Enter or select the IP address of the source to monitor. |
| Filter Groups | Filters the output to contain only the relevant groups. |
| Group | Enter or select the IP address of the group to monitor. |
| Filter Sources | Filters the output to contain only the relevant sources. |
| Reset SG Lists | Clears any entries and refreshes the source and group lists. |
| Select Routers | Enter the router name. |
| Units | Select either packets per sampling period (pps) or bits per sampling period (bps). |
| High Threshold | Enter the high threshold that, if exceeded, generates a report. |
| Low Threshold | Enter the low threshold that, if exceeded, generates a report. |
| Apply | Applies and saves the changes. |
| Refresh Cache | If you are using S,G caching, the cache contents appear. Click **Refresh Cache** to refresh the table of sources and groups. |
| Display Filter Options | You can filter the list of monitored sources and groups by limiting to source, group, and/or router. |
| Display Configured SGs | Displays all the sources and groups you are currently monitoring (see Current Source/Group Polling Configuration, page 2-34). |

# Current Source/Group Polling Configuration

From the SG Polling Configuration page, select Display Configured SGs to display the sources and groups that you are currently monitoring.

***Figure 2-21 Current Source/Group Polling Configuration***




You can also export (in CSV format) the list of monitored S,G's and use an editor of your choice to change, add, and delete, then import the list back, either replacing the current list, or merging it.

The **Current Source/Group Polling Configuration** section shows you all monitored sources and groups in a tabular format.

- Under the **Modify** column, you can edit or delete a specific source and group.
- Under the **Time Threshold** column, click on **Time-Based Thresholds** to configure up to 50 different time of day high and low thresholds for each source and group. Click the **Set Thresholds** button to save your changes.

Each time a source and group exceeds a threshold, a trap is sent and a report is generated.

# SG Polling—By Device

You can select a particular router using the Device SG Polling Configuration page, and you can configure which sources and routers to monitor on the specific device.

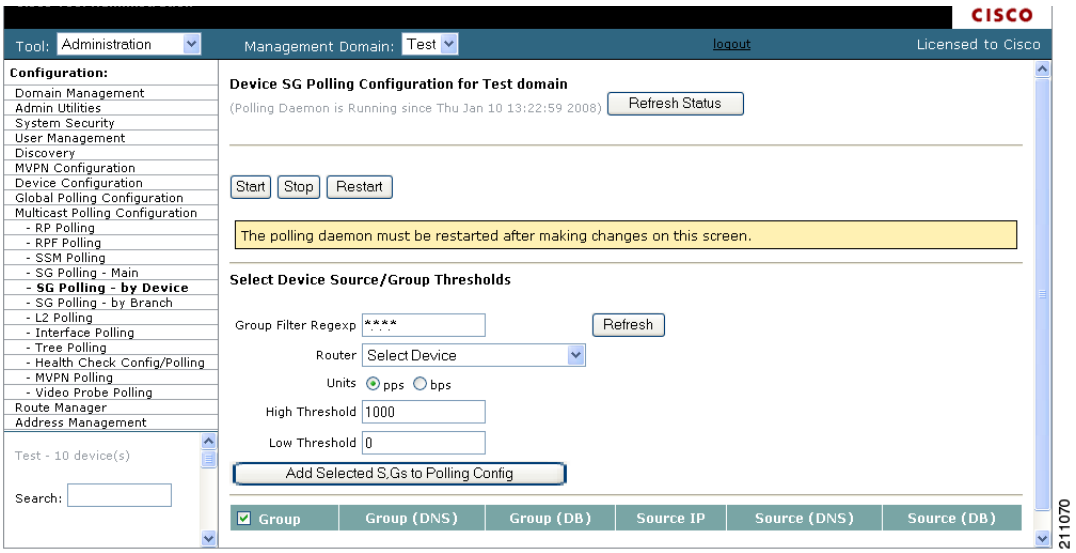
To configure SG polling for a particular device:

**Step 1** Select the **Administration** tool.

**Step 2** Select **Multicast Polling Configuration > SG Polling - by Device.**

The Device SG Polling Configuration page opens, as shown in Figure 2-20.

***Figure 2-22 Device SG Polling Configuration Page***




The Device SG Polling Configuration page contains the following fields and buttons:

| Fields and Buttons | Description |
|---|---|
| Refresh Status | The status line indicates how long the polling daemon has been running and how it was started. Click **Refresh Status** to update the status information. |
| Start | Starts the polling daemon globally. |
| Stop | Stops the polling daemon globally. |
| Restart | Restarts the polling daemon globally. Each time you change a polling interval, click **Restart**. |

| Fields and Buttons | Description |
|---|---|
| Group Filter Regexp | Enter any part of the multicast address. Only those that match appear. |
| Refresh | Clears the Group Filter Regexp previously entered. |
| Router | Select the router name. |
| Units | Select either packets per sampling period (pps) or bits per sampling period (bps). |
| High Threshold | Enter the high threshold which, if exceeded, generates a report. |
| Low Threshold | Enter the low threshold that, if exceeded, generates a report. |
| Add Selected S,Gs to Polling Config | Adds selected sources and groups to the polling configuration. |

**Step 3** From the drop-down list in the **Router** field, select a router.

**Step 4** Select **Units** and enter a **High** and **Low Threshold**.

A table showing the currently configured groups appears.

**Step 5** Within the table, select the groups (and sources) you want to monitor, then click **Add Selected S,Gs to Polling Config**.

# L2 Polling

You can add Layer 2 switches to Cisco Multicast Manager individually, or you can import a list (see Adding Layer 2 Switches to Discovery, page 1-7). Cisco Multicast Manager can monitor the total number of multicast packets inbound and/or outbound from any Layer 2 port.

You can also configure up to 50 different time of day thresholds for each port.

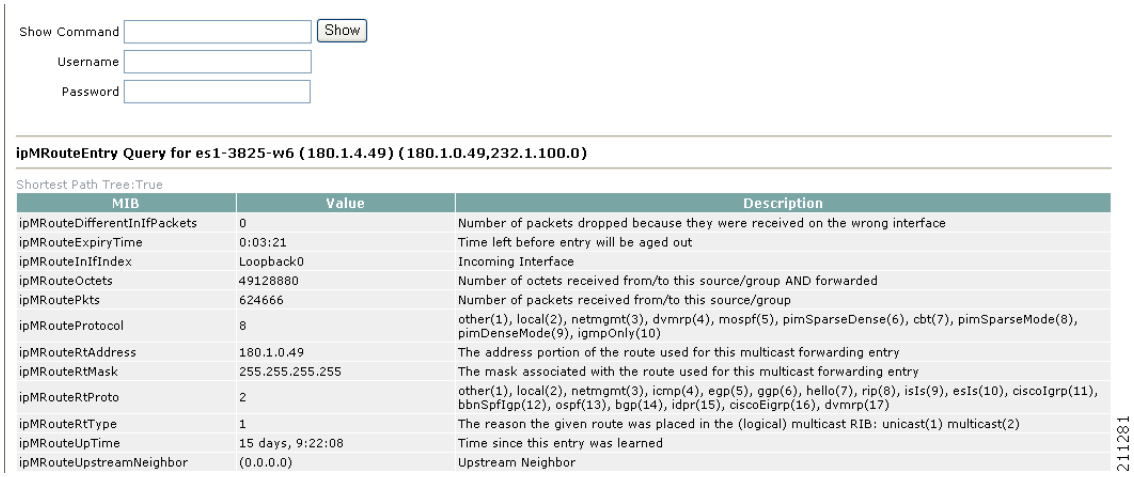
To configure Layer 2 switch polling:

**Step 1** Select the **Administration** tool.

**Step 2** Select **Multicast Polling Configuration > L2 Polling.**

The L2 Polling Configuration page opens, as shown in Figure 2-23.

***Figure 2-23 L2 Polling Configuration***




The L2 Polling configuration page contains the following fields and buttons:

| Fields and Buttons | Description |
|---|---|
| Refresh Status | The status line indicates how long the polling daemon has been running and how it was started. Click **Refresh Status** to update the status information. |
| Start | Starts the polling daemon globally. |
| Stop | Stops the polling daemon globally. |
| Restart | Restarts the polling daemon globally. Each time you change a polling interval, click **Restart**. |
| Select Switch to Monitor | Select the name or IP address of the switch you want to monitor. |
| Direction | Select either inbound packets received at this port, or outbound packets sent from this port. |
| High PPS | Enter the high threshold that, if exceeded, generates a report. |
| Low PPS | Enter the low threshold that, if exceeded, generates a report. |
| Select Port to Monitor | Select the port to monitor. Ports appear in the following format: ifIndex:module/port. |
| Add/Edit | Add the port you want to monitor, or from the list of ports, select edit to edit that entry. |

The **Current Layer 2 Switch Polling Configuration** section shows you all monitored switches and ports in a tabular format.

- Under the **Modify** column, you can edit or delete a specific switch and port.
- Under the **Time Threshold** column, click on **Time-Based Thresholds** to configure up to 50 different time of day high and low thresholds for each port. Click the **Set Thresholds** button to save your changes.

Each time a port exceeds a threshold, a trap is sent and a report is generated.

# Interface Polling

Cisco Multicast Manager can poll any interface on a router and calculate the percentage of bandwidth used by multicast traffic. You can then configure a high and low threshold, and if these are exceeded, a report is generated. This information is also kept for historical purposes.

To configure multicast bandwidth interface polling:

**Step 1** Select the **Administration** tool.

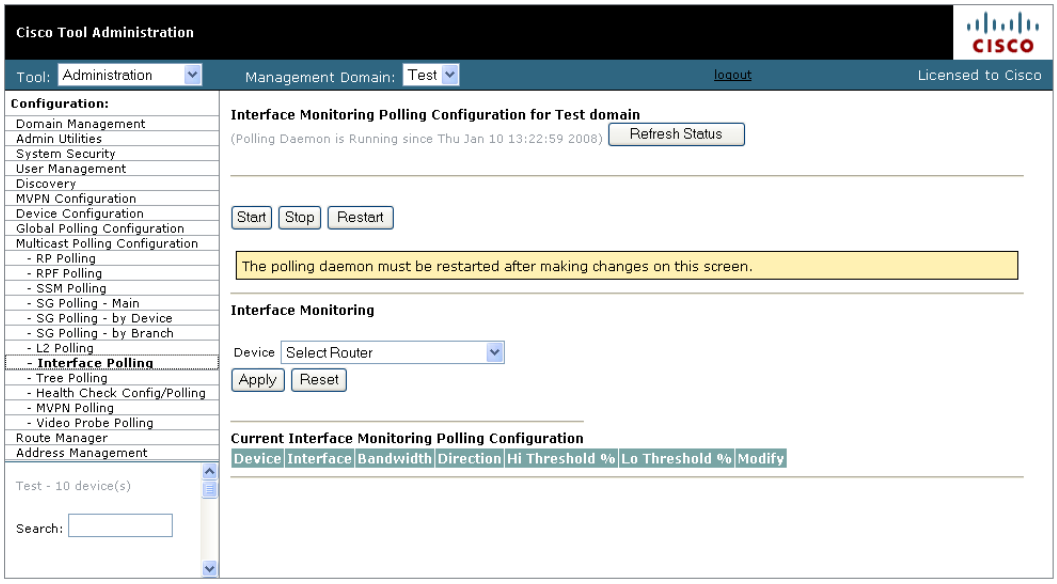
**Step 2** Select **Multicast Polling Configuration > Interface Polling.**

The Interface Monitoring Polling Configuration page opens.

**Step 3** From the drop-down list in the **Device** field, select the device to monitor.

The Interface Monitoring Polling Configuration page displays a list of interfaces on the selected device., as shown in Figure 2-24.

***Figure 2-24 Interface Monitoring Polling Page***



**Step 4** Select the interface to monitor.

**Step 5** Select either inbound, outbound, or both, and enter values in percentages.

**Step 6** Click **Apply**.

# Tree Polling

Before you can monitor a tree using the Tree Polling Configuration page, you must build a multicast tree and save it to the database as a baseline (see Show All Groups, page 4-2).

Once saved, the trees appear in the **Saved Trees** field on the Tree Polling Configuration page.

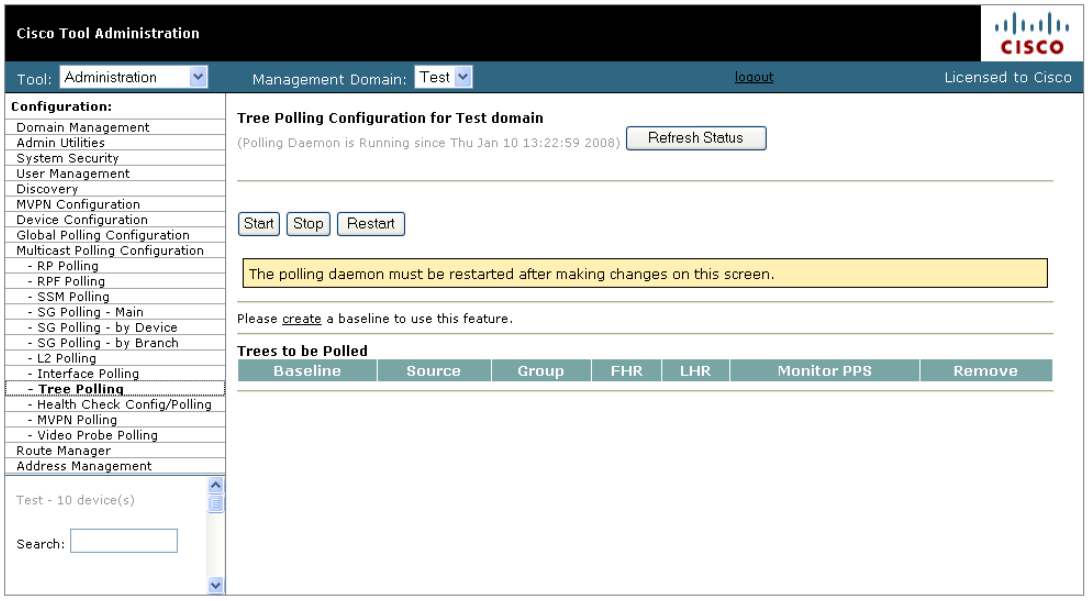
To configure tree polling:

**Step 1** Select the **Administration** tool.

**Step 2** Select **Multicast Polling Configuration > Tree Polling.**

The Tree Polling Configuration page opens, as shown in Figure 2-25.

***Figure 2-25 Tree Polling Configuration Page***




The Tree Polling Configuration page contains the following fields and buttons:

| Fields and Buttons | Description |
|---|---|
| Refresh Status | The status line indicates how long the polling daemon has been running and how it was started. Click **Refresh Status** to update the status information. |
| Start | Starts the polling daemon globally. |

| Fields and Buttons | Description |
|---|---|
| Stop | Stops the polling daemon globally. |
| Restart | Restarts the polling daemon globally. Each time you change a polling interval, click **Restart**. |
| Saved Trees | Lists all the multicast tree baselines that have been saved. |
| Add | Adds the selected tree for monitoring. |

**Step 3** To monitor a tree, from the drop-down menu in the **Saved Trees field,** select the tree name, and click **Add**.

The tree is drawn in the background for every interval that you set up for tree polling (see Configuring Global Polling, page 2-16). This tree is compared with the tree saved in the database. If it is different, a trap is sent, and a report generated

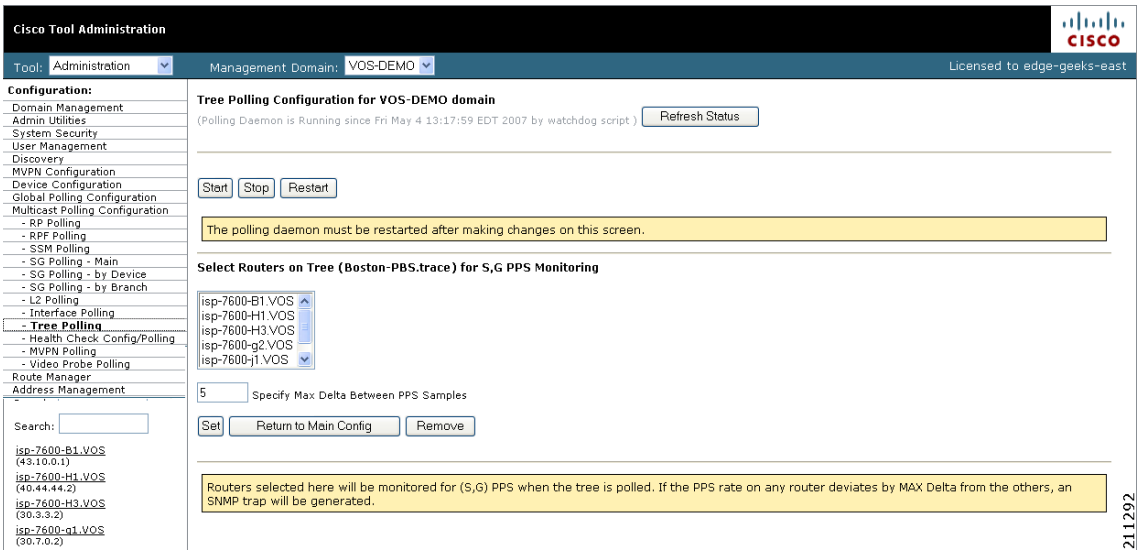
## Selecting Trees To Be Polled

The bottom portion of the Tree Polling Configuration page contains the Trees to be Polled table. Using the Trees to be Polled table, you can:

- View tree details and topology by clicking on a tree name in the **Baseline** column of the Trees to be Polled table.
- Monitor for S,G (PPS) when a tree is polled, and generate SNMP traps for Max Delta deviations by clicking **Configure** under **Monitor PPS**.

  When you click Configure, the Select Routers on Tree pane appears, as shown in Figure 2-26.

***Figure 2-26 Tree Polling Configuration—Configure***



- Select a router and specify a value in **Max Delta Between PPS Samples**, then click **Set**. To remove a router from monitoring, select the router and click **Remove**. You can also return to the main Tree Polling Configuration page.

**Note** You can select multiple routers by holding down the **Ctrl** key.

- Remove a tree by clicking on **Delete** under **Remove**.

# Health Check

Health checks give you an immediate status update on several key multicast network indicators, including:

- Status of selected RPs.
- Multicast Source Discovery Protocol (MSDP) status.
- Existence of S,G entries on selected routers.
- Status of multicast forwarding trees.

You can create several health checks. Once you have created a health check, you can configure it to run at scheduled intervals, and add email alerts that summarize the results of the health check.

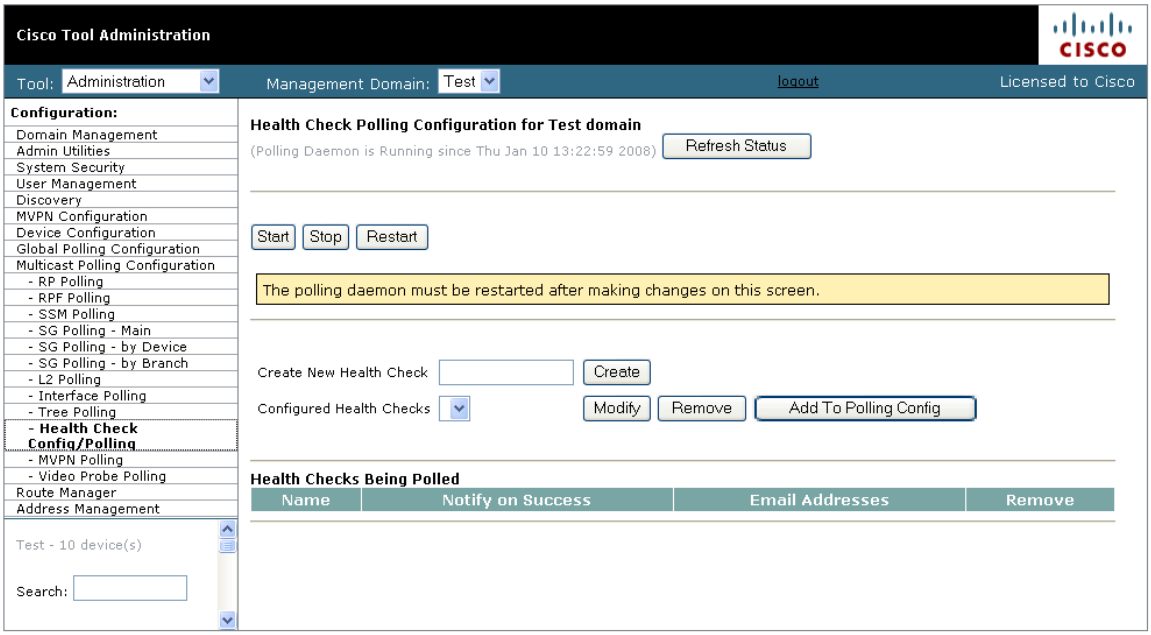
To configure health check polling:

**Step 1** Select the **Administration** tool.

**Step 2** Select **Multicast Polling Configuration > Health Check Config/Polling.**

The Health Check Config/Polling page opens, as shown in Figure 2-27.

***Figure 2-27 Health Check Polling Configuration Page***



The Health Check Config/Polling page contains the following fields and buttons:

| Fields and Buttons | Description |
|---|---|
| Create New Health Check | Type a name for the health check. |
| Create | Creates the new health check. |
| Configured Health Checks | Select the health check you want to modify. |
| Modify | To update a health check, select a health check from the drop-down list of health checks in the Configured Health checks field and then click **Modify**. A summary of the currently configured health checks appears. For detailed information, see Modifying Health Checks, page 2-43. |
| Remove | Removes the existing health check. |
| Add To Polling Config | Schedules this health check to run automatically. |
| Name | Name of the health check. |
| Notify on Success | Generates an email report if the health check completes successfully. |
| Email Addresses | Enter the email addresses to be notified. Click **+** to add an email address. Click **-** to remove an email address. |
| Remove | Click **Remove From Polling** to stop the health check from running at scheduled intervals. |

## Modifying Health Checks

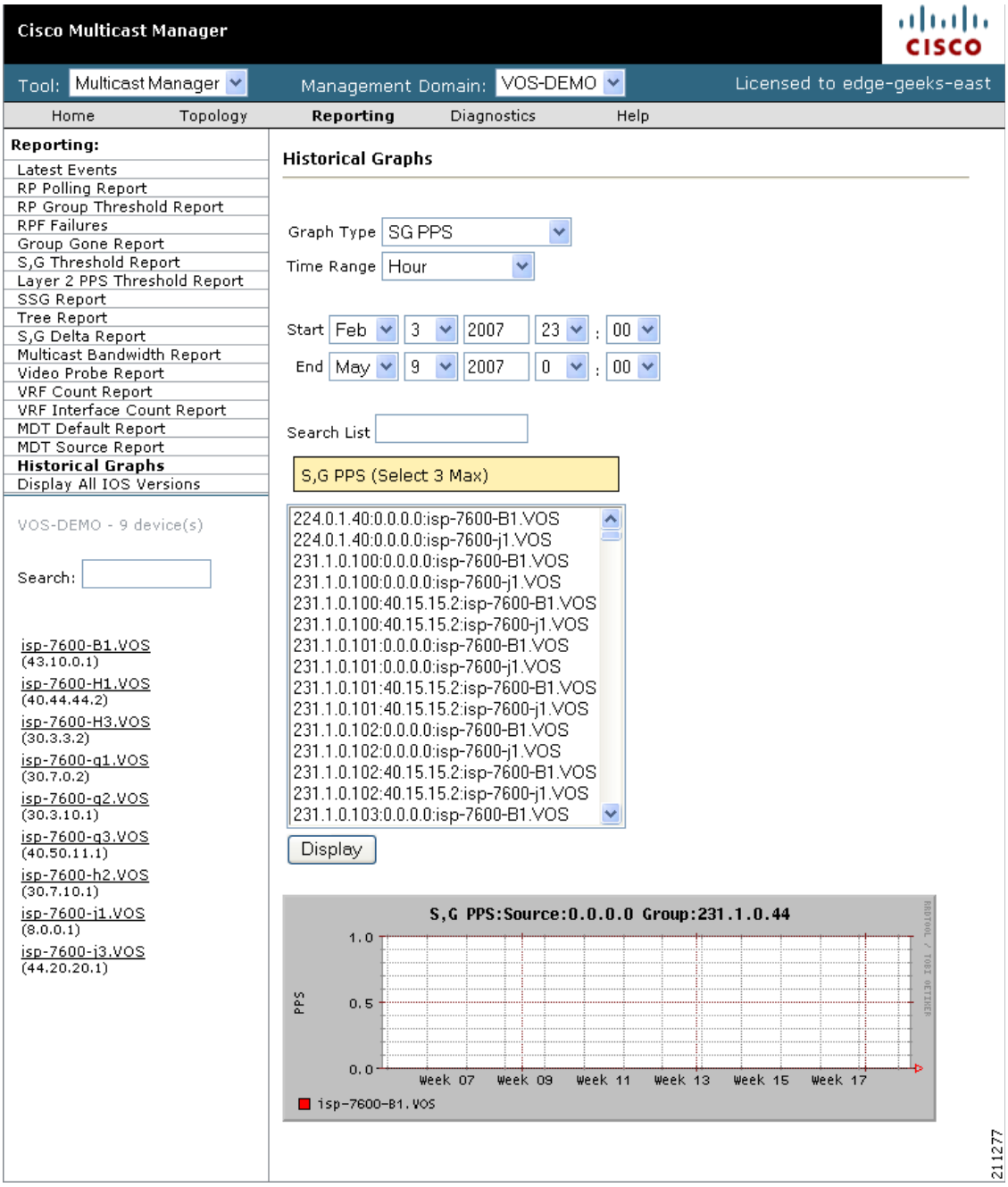
If you click **Modify** on the Health Check Configuration page to select a health check to change, the Health Check Configuration page displays information about the currently configured health checks.

To modify the health check configuration:

**Step 1** On the Health Check Configuration page, select a health check from the drop-down list of health checks in the **Configured Health Checks** field and then click **Modify**.

**Step 2** The Health Check Configuration page displays the currently configured health checks, as shown in Figure 2-28.

***Figure 2-28 Modifying the Health Check Configuration***



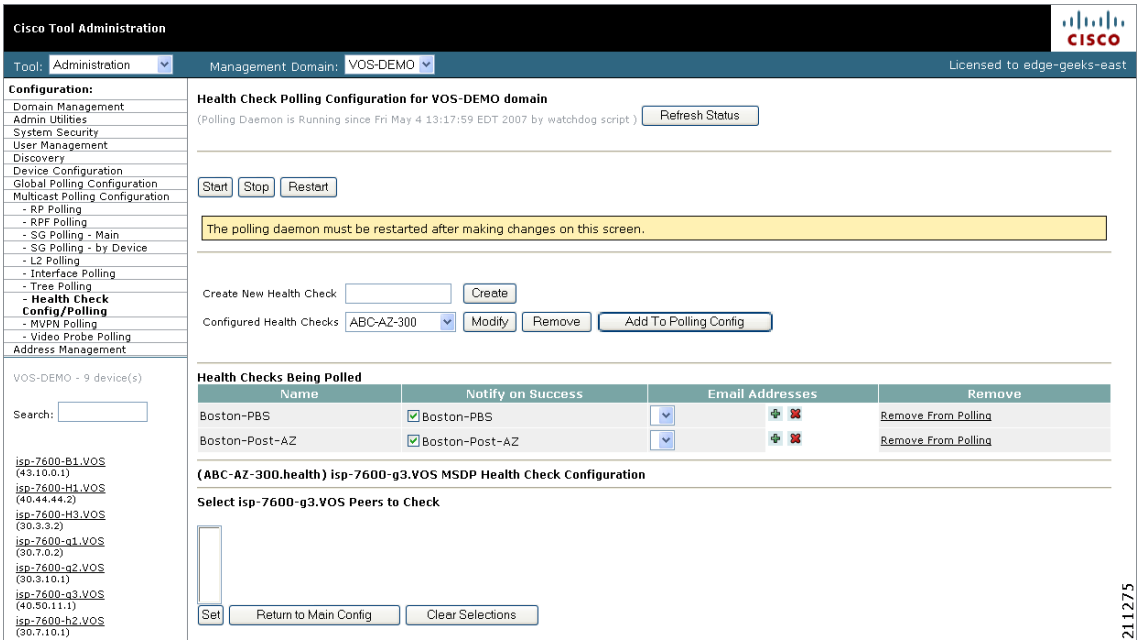

**Step 3** From the drop-down list in the Configured Health Checks field, select the RPs that you want this health check to include.:

- To add an RP to the list, click **Add to Polling Config.**
- To remove an RP from the list, click **Remove**.
- To Modify the configuration, click **Modify**.

**Step 4** To check the status of this RP's MSDP peering, click on **Configure** under the MSDP heading in the list of RPs being checked.

A list of available peers appears, as shown in Figure 2-29.

***Figure 2-29 Health Check Configuration—Peers***




**Step 5** Select the peers you want to check, and then click **Set**.

You are returned to the Health Check Configuration Modification page.

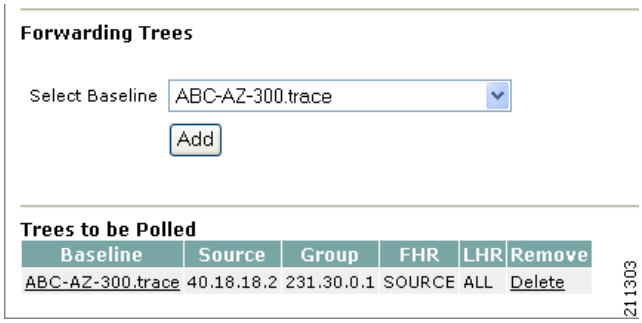
**Step 6** Select the sources and groups to check.

**Step 7** To check for the existence of multicast trees, select the trees from the drop-down list in the **Select Baseline** field (shown in Figure 2-30) and click on **Add**.

The selected tree appears in the list of Trees to be Polled.

Figure 2-30 shows the bottom portion of the page, which includes the **Select Baseline** field and the list of Trees to be Polled.

***Figure 2-30 Selecting a Baseline***




**Step 8** To save your modifications, click **Refresh Status**.

# MVPN Polling

You can configure polling of multicast devices in Multicast Virtual Private Network (MVPN).

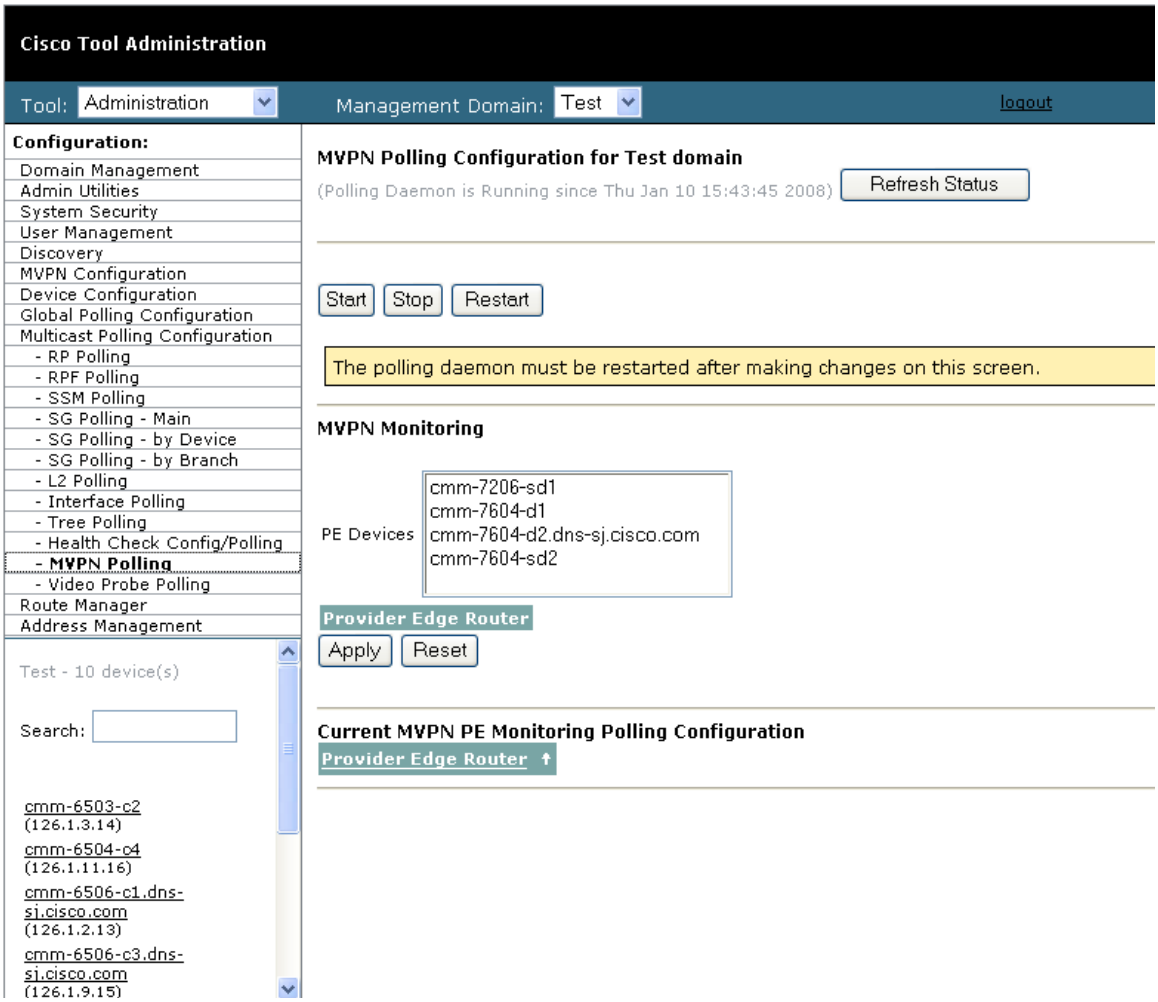
To configure MVPN polling:

**Step 1** Select the **Administration** tool.

**Step 2** Select **Multicast Polling Configuration > MVPN Polling.**

The MVPN Polling Configuration page opens, as shown in Figure 2-31.

***Figure 2-31 MVPN Polling Configuration***



**Step 3** To select a provider edge (PE) device for polling, select the device from the list in the PE devices field.

The PE device appears in the list of Provider Edge Routers.

**Step 4** When you are done selecting PE devices, click **Apply**.

**Note** You must restart the polling daemon before the changes take effect. To restart the polling daemon, click **Start**.

# Video Probe Polling

You can configure the operation of each video probe to specify the probe's delay factor (DF) threshold and the acceptable loss threshold.

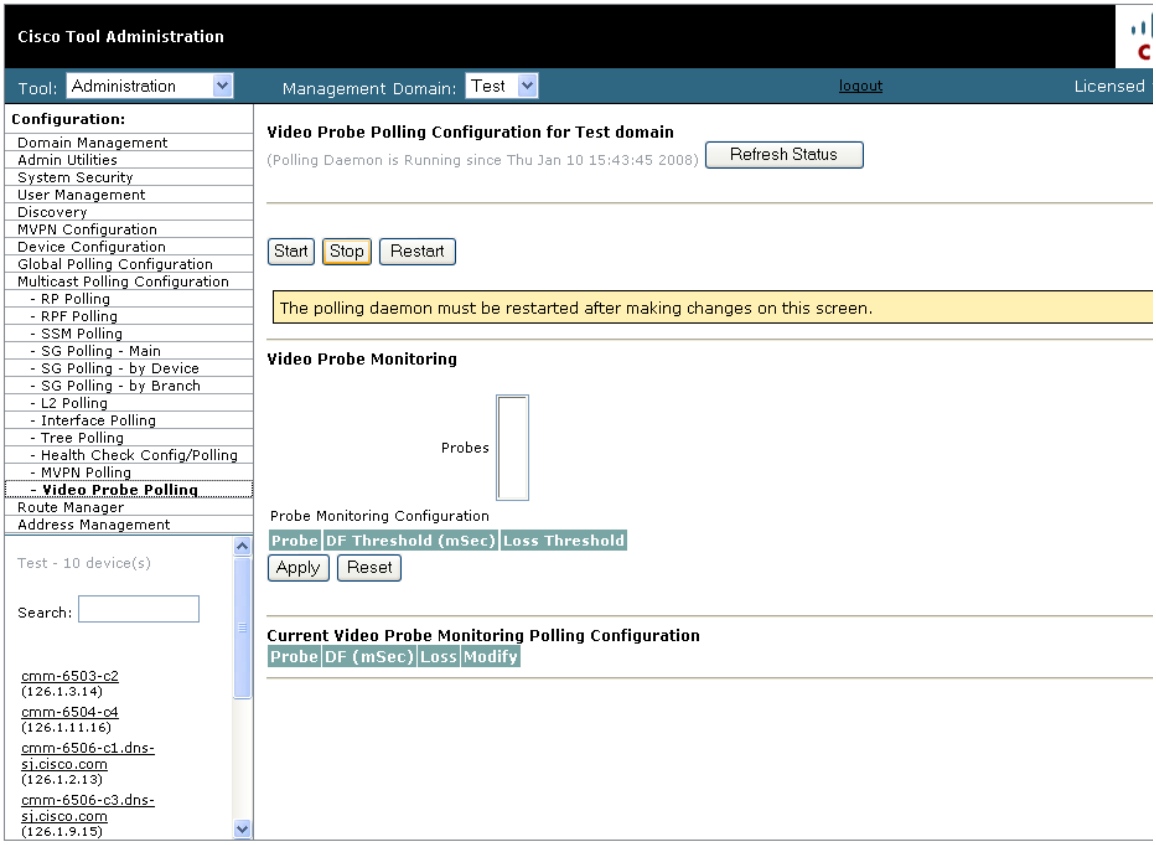
You can configure one video probe or configure several video probes at the same time.

To configure video probe polling:

**Step 1** Select **Administration > Multicast Manager > Video Probe Polling**.

The Video Probe Polling Configuration page appears, as shown in Figure 2-32.

***Figure 2-32 Video Probe Polling Configuration Page***



If one or more probes have been configured already, the Current Video Probe Monitoring Polling Configuration section shows the current probe configurations.

**Step 2** To add a configuration for an unconfigured probe:

**a.** Select one or more probes from the **Probes** pull-down menu.

As you select probes, fields for setting the probe configuration appear in the Probe Monitoring Configuration section.

**b.** To specify a Delay Factor threshold for a probe, check the **DF** check box for the probe and enter a delay factor in milliseconds.

**c.** To specify a Loss threshold for a probe, check the **Loss** check box and enter a loss threshold value in packets per second.

**d.** If you want to clear the values that you have entered, click **Reset**.

**e.** To apply the configuration, click **Apply**.

**Step 3** To edit an existing probe configuration:

**a.** Click **Edit** in the configuration listing in the current polling configuration section.

The current probe configuration appears in the Edit Probe Monitoring Configuration section.

**b.** Modify the existing configuration values as required and then click **Apply**.

**Step 4** To delete an existing probe configuration:

**a.** Click **Delete** next to the configuration listing in the Edit Probe Monitoring Configuration section.

You are prompted to confirm deletion of the probe configuration.

**b.** If you are sure that you want to delete the configuration, click **OK**; otherwise, click **Cancel**.

**Step 5** Restart the polling daemon after making any probe configuration changes.