Configuring with the CMM Administration Tool

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

This chapter covers:

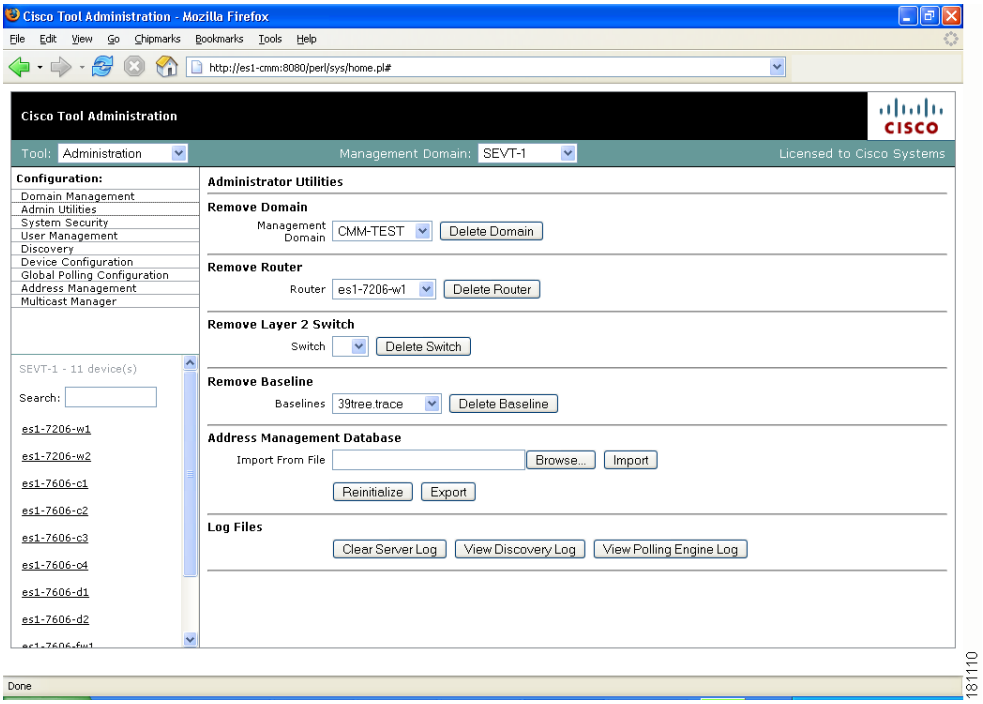
Performing Domain Management

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

Using Administrative Utilities

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

Figure 2-1 Administrative Utilities



Field	Description
Remove Domain	Removes all data associated with a management domain. **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 Baseline	Removes a forwarding tree baseline, along with any associated tree change information.

Field	Description

Address Management Database	Contains:
	• **Browse**—Find a csv file to import.
	• **Import**—You can import a csv file into the IP address database. The file should be in the following format:
	`#import file format`
	`#this line will be skipped`
	`239.1.1.1,test group`
	`192.168.1.1,sourceA`
	• **Reinitialize**—Restores all reserved multicast addresses to the IP address database.
	• **Export**—Creates a file in */tmp* called **mmtIPdb.csv** which contains the IP address database in csv format.

Log Files	Contains: • **Clear Server Log**—Truncates the error_log file. • **View Discovery Log**—Shows discovery-specific messages contained in the error_log file. **Note** The error_log file should be rotated along with other system log files. • **View Polling Engine Log**—Displays the contents of the polling log.

Configuring System Security

The System Security page provides TACACS login support for the CMM.

To configure TACACS login, enter the IP address of the TACACS server within the **Primary TACACS Server** field.

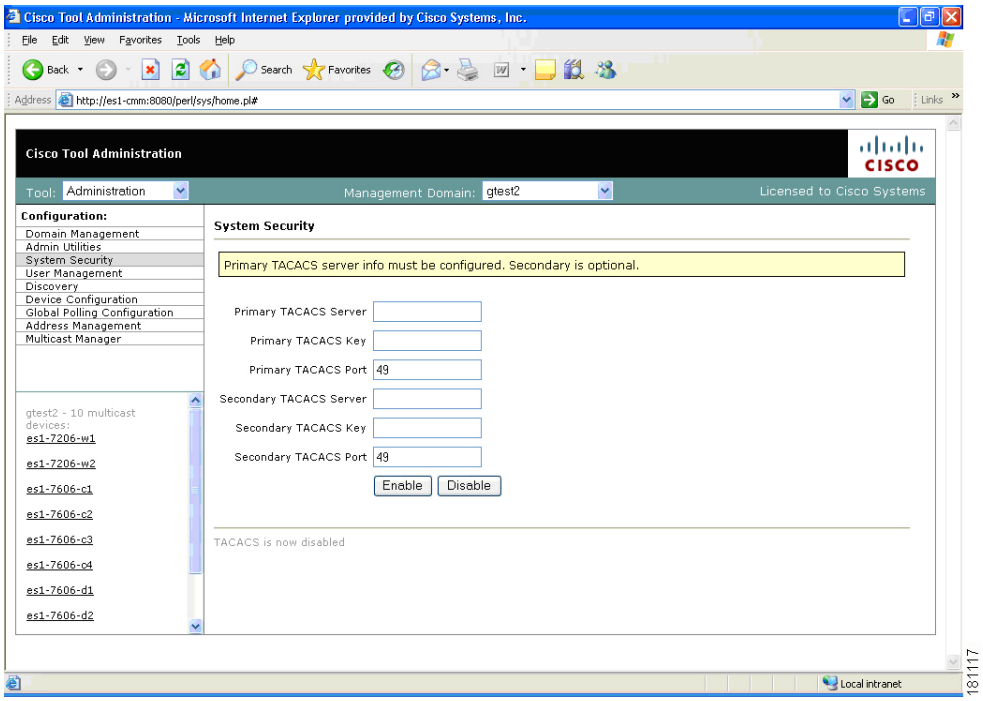
If the keys are configured incorrectly, they will have to be manually changed in the */opt/RMSMMT/httpd_perl/conf/httpd.conf* file as follows:

```
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>
```

Figure 2-2 System Security



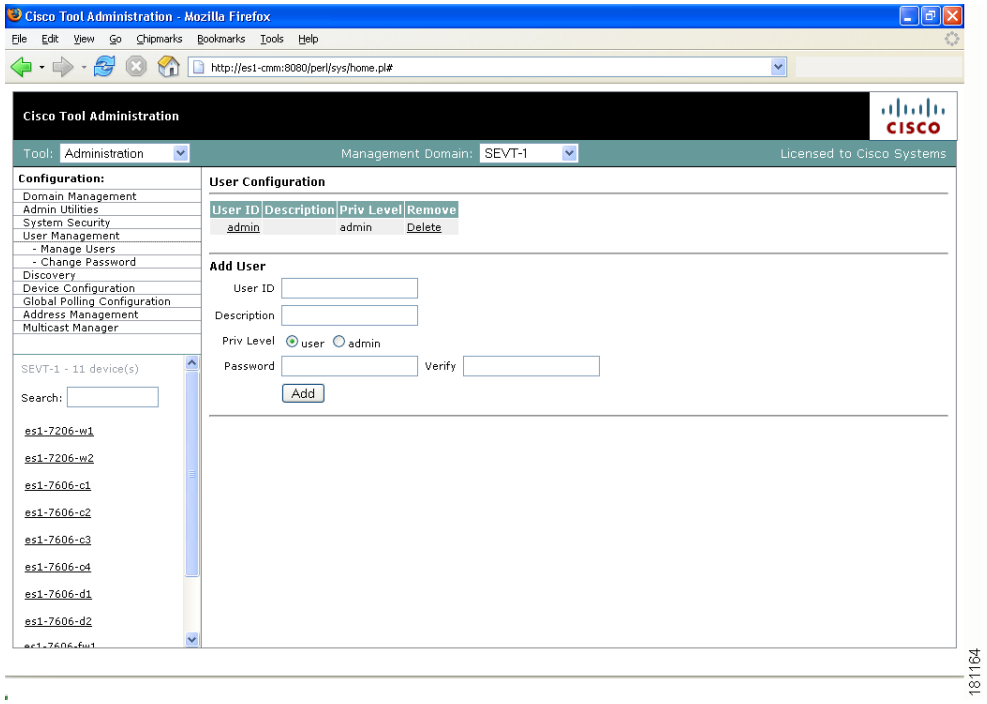
Managing Users and Passwords

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

Figure 2-3 Manage Users—User Configuration



To add a new user:

Step 1 Enter the user ID.

Step 2 (Optional) Enter a description.

Step 3 Choose the appropriate privilege level, **user** or **admin**.

Step 4 Enter the password into the **Password** and **Verify** boxes.

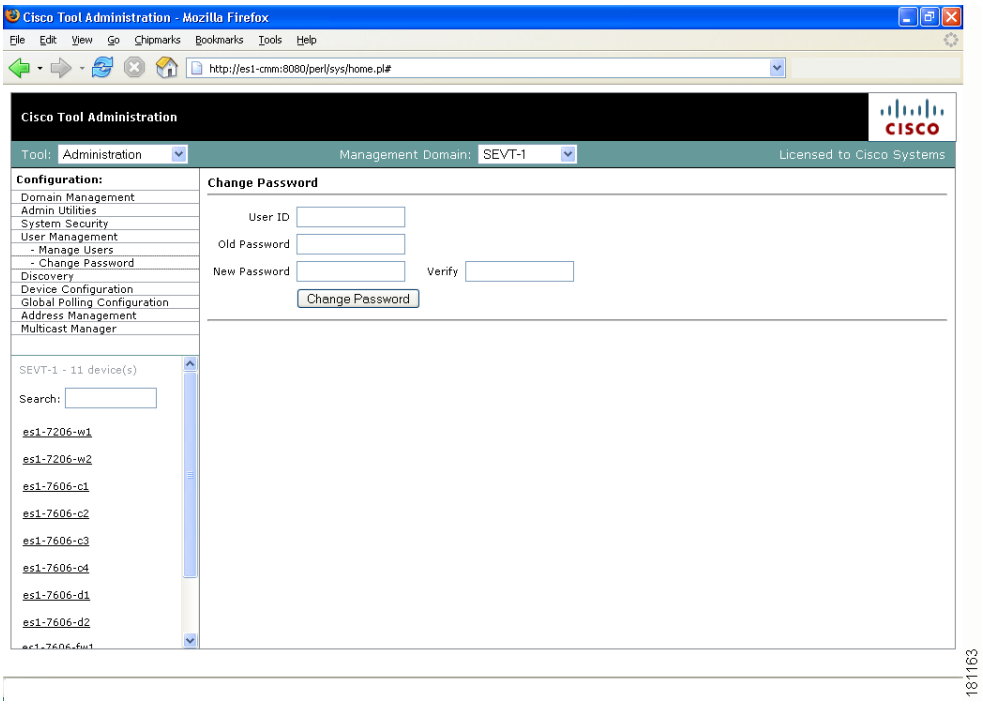
Step 5 Click **Add**.

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.

Users can change their passwords by clicking Change Password.

Figure 2-4 Manage Users—Change Password



To change your password:

Step 1 Enter your user ID.

Step 2 Enter your old password.

Step 3 Enter your new password in the **Password** and **Verify** boxes.

Step 4 Click **Change Password**.

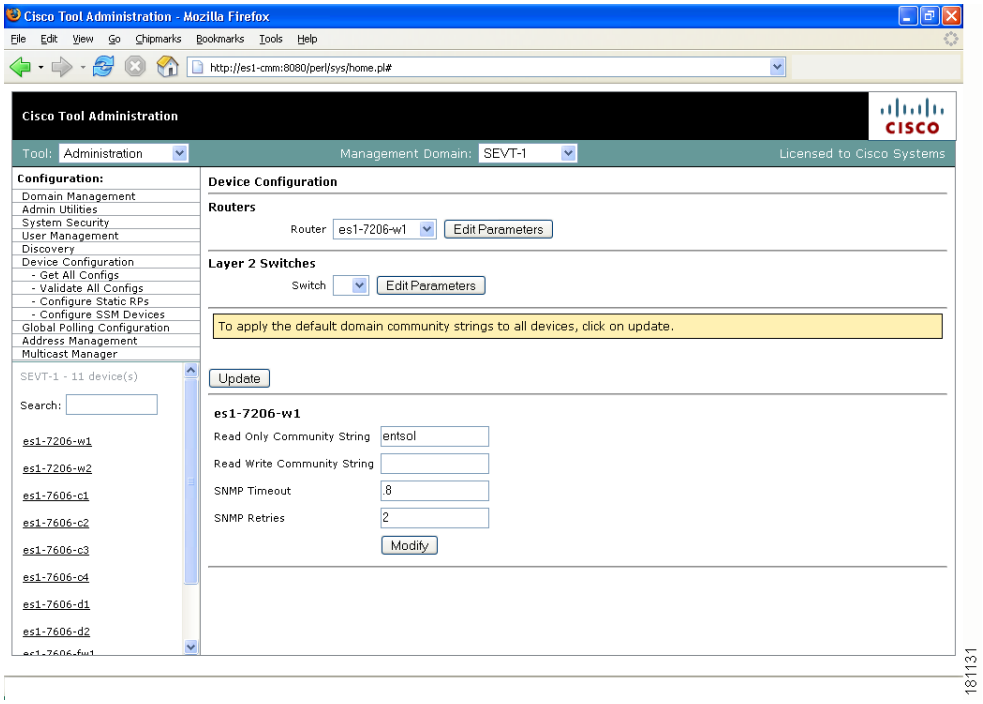
Discovering Your Network

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

Configuring Devices

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**.

Figure 2-5 Device Configuration—Edit Parameters



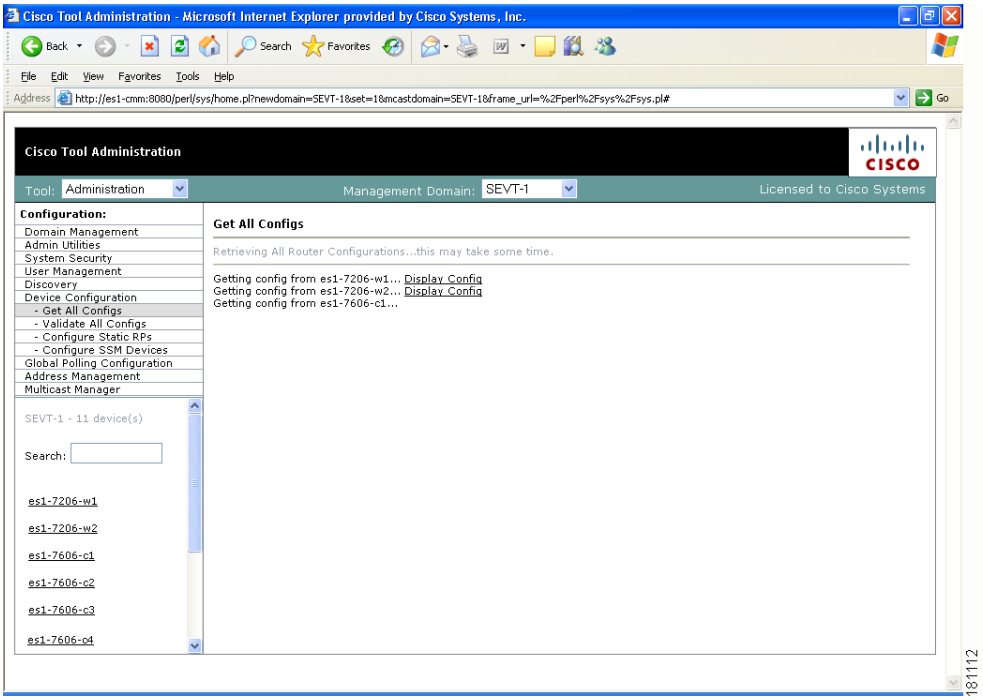
Downloading Router Configurations

You can download the router configurationto the CMM for each router in the database. Under the Device Configuration menu at left, select **Get All Configs**.

If you entered the SNMP write key for the router when you set up the domain, CMM 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.*

Figure 2-6 Get All Configs



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

Validating Router Configurations

Using the CMM, 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
```

To select a template and initiate validation:

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

Step 1 Under the **Device Configuration** menu, click **Validate All Configs**. The Configuration Check page opens.

Step 2 Ensure that the correct Management Domain is selected.

Step 3 If you want to upload a user-defined template:

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

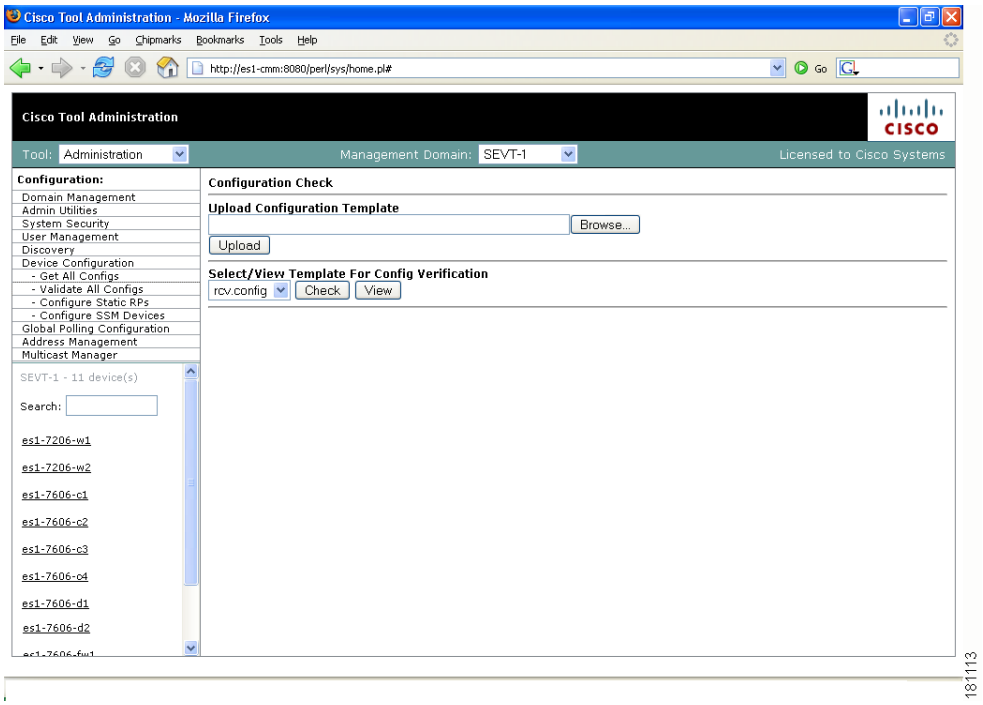
b. Click **Upload**. The user-defined text file appears in the list below.

Step 4 Select the template you want to use from the list.

Step 5 (Optional) Click **View** to see the contents of each template.

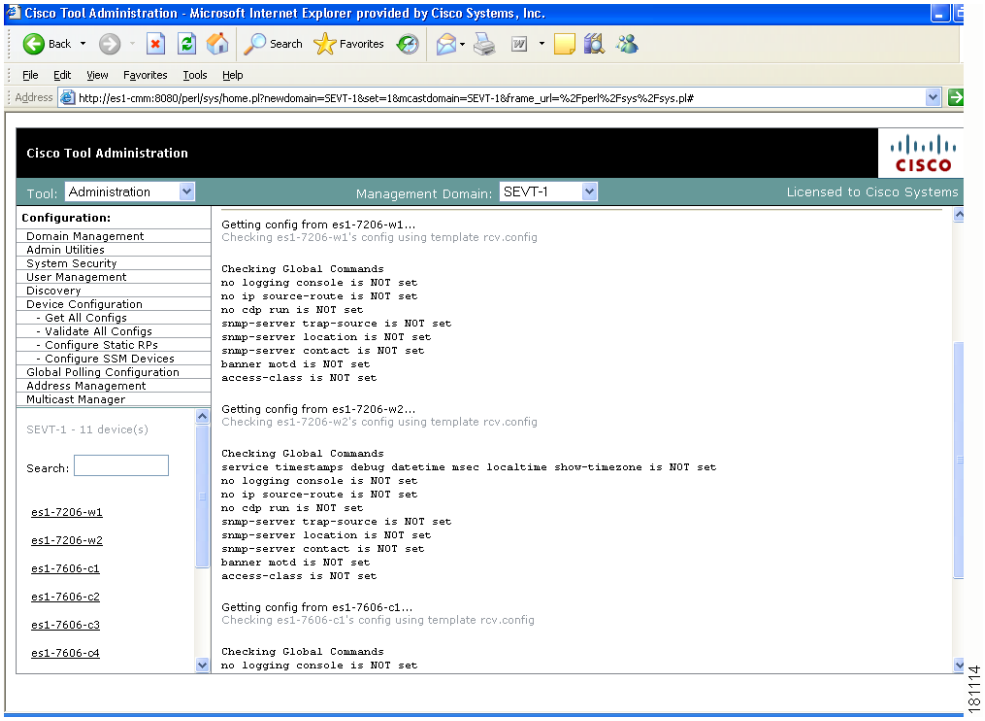
Step 6 Click **Check**.

Figure 2-7 Configuration Check



The CMM checks each router in the database for the existence of the commands in the template you specified. Output looks similar to Figure 2-8.

Figure 2-8 Configuration Check—Output



Configuring Static RPs

If you have static 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.

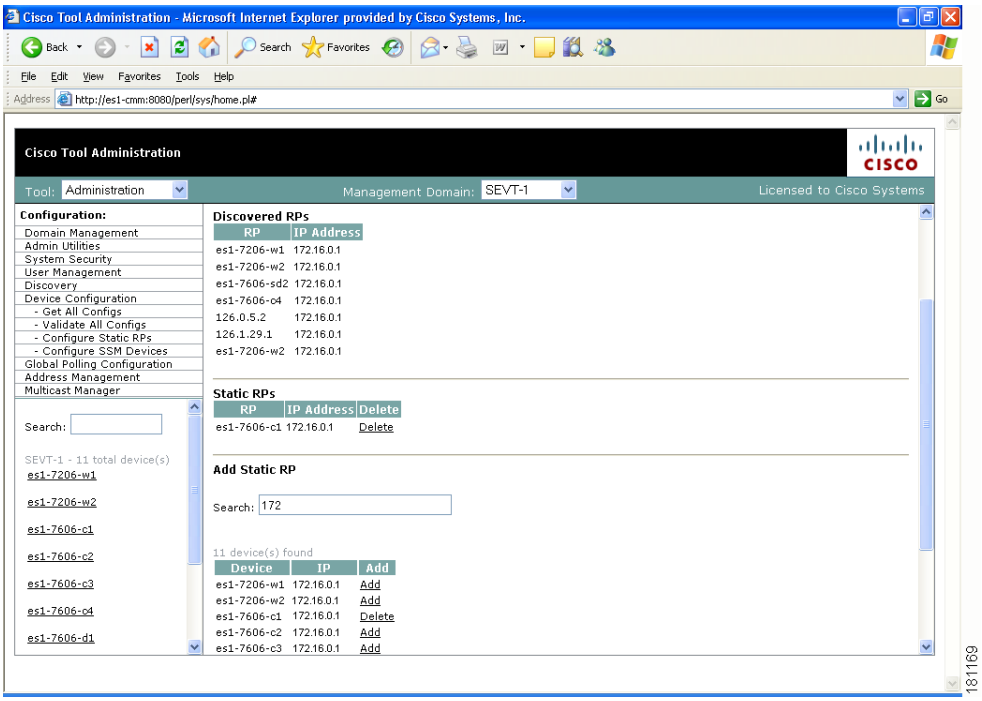
To configure static RPs:

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

Step 2 Within the **Add Static RP** 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 3 Click **Add** next to the router(s) you want to select. The **Static RPs** table is populated.

Figure 2-9 Configure Static RPs



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 4-1). 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 an 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 will visit 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 4-17).

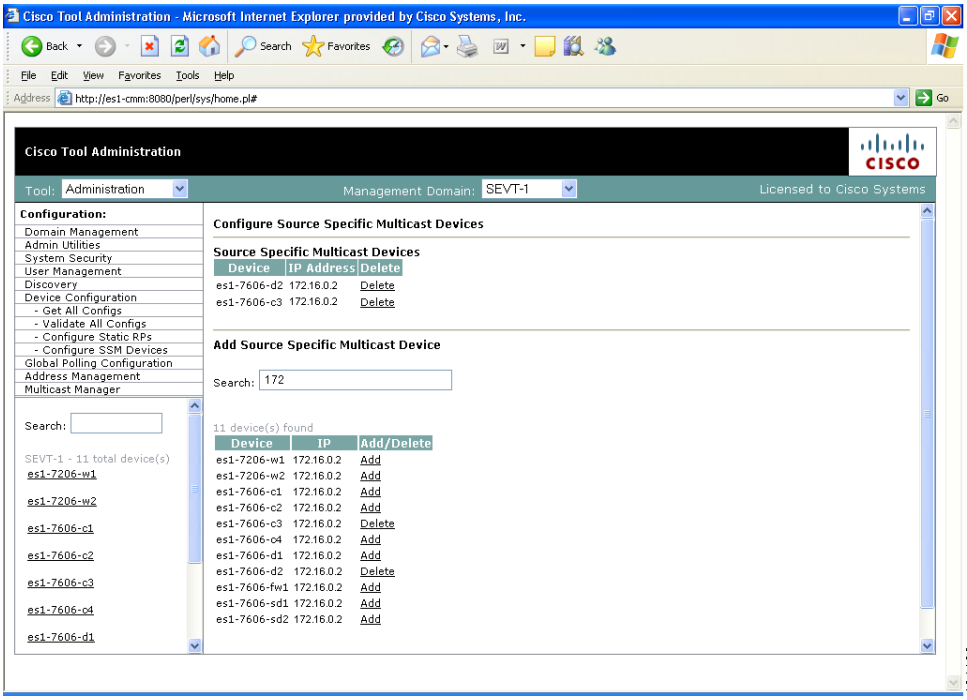
To configure SSM devices:

Step 1 Under the **Device Configuration** menu, click **Configure SSM Devices**. The Configure Source Specific Multicast Devices page opens.

Step 2 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 3 Click **Add** next to the router(s) you want to select. The **Source Specific Multicast Devices** table is populated.

Figure 2-10 Configure Source Specific Multicast Devices Page

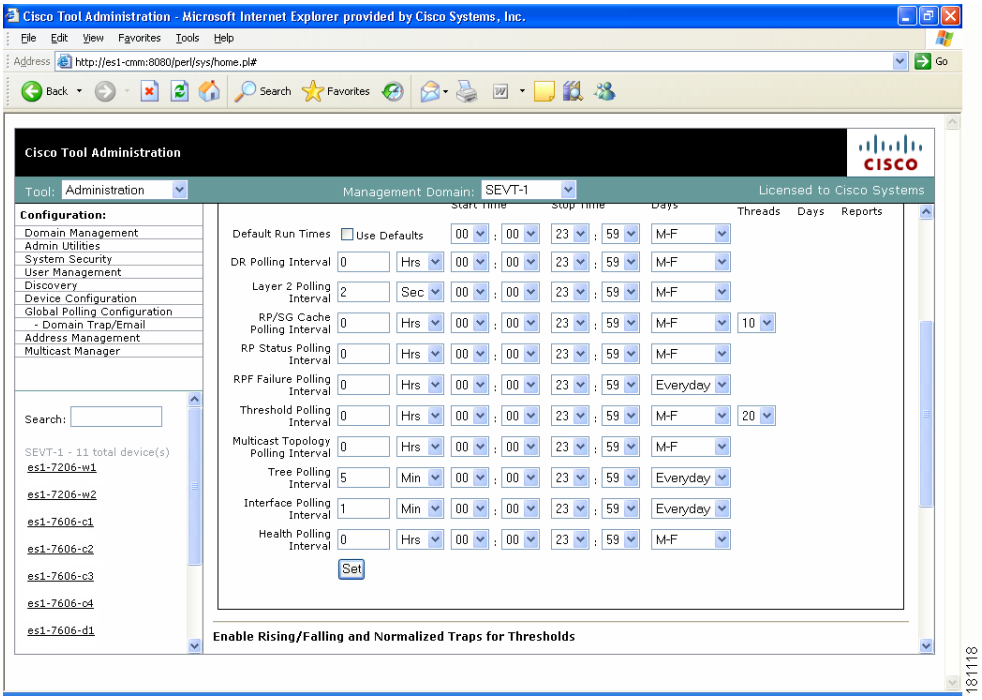


Configuring Global Polling

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.

Figure 2-11 Global Polling Configuration



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.

Field or Button	Description
RP/SG Cache Polling Interval	For certain CMM data, such as the data within the Multicast Diagnostics page (see Show All Groups, page 4-1) 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. 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. 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).
RP Status Polling Interval	RP Status Polling queries the sysUpTime of the RPs configured on the RP Polling Configuration page (see RP Polling, page 2-17). 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.

Field or Button	Description
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.
Set	Sets the values you enter.

You can enable or disable the continuous sending of PPS threshold traps using 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.

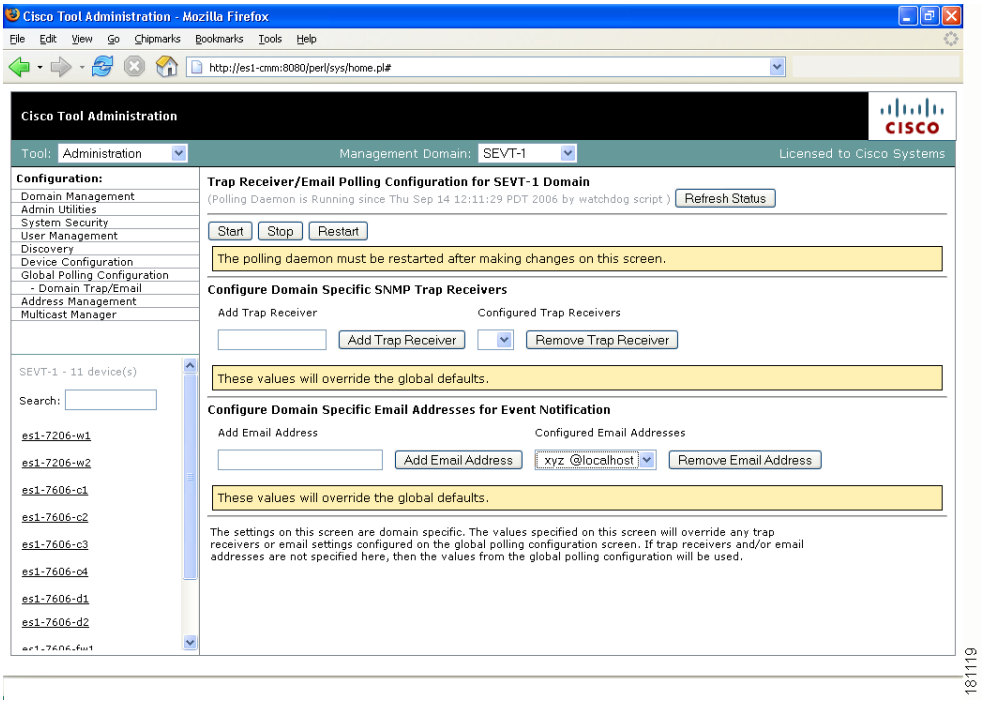
You can add or remove trap receivers using the **Configure Global Default SNMP Trap Receivers** section. The SNMP trap receivers specified here are only used if domain-specific SNMP trap receivers are not specified. Domain-specific trap receivers are specified from the Trap Receiver/Email Polling Configuration page (see Configuring Domain-Specific Trap Receivers and Email Addresses, page 2-15).

You can add or remove email addresses using 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 2-15).

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.

Figure 2-12 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 2-12).

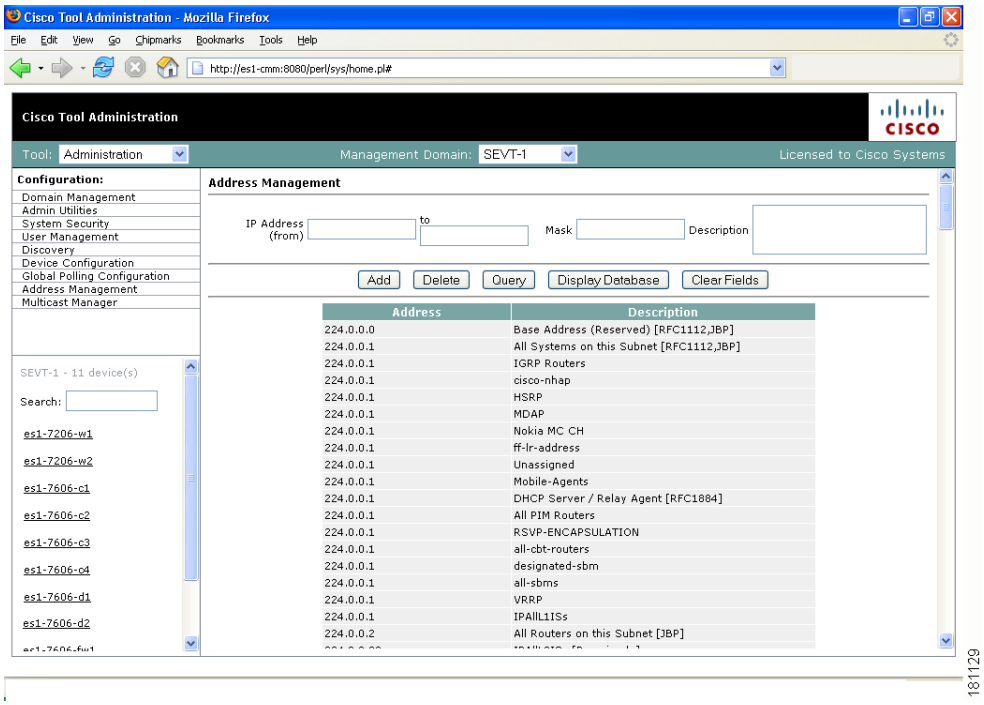
You can add or remove email addresses using the **Configure Domain Specific Email Addresses for Event Notification** section. Email addresses are notified of SSG exceptions and threshold and existence events. The email addresses specified here are only used if global email addresses are not specified. Global email addresses are specified from the Configure Global Default SNMP Trap Receivers page (see Configuring Global Polling, page 2-12).

Managing IP Addresses

Using the Address Management 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.

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

Figure 2-13 Address Management



Configuring Specific Multicast Manager Polling

You can configure the following types of multicast polling:

- RP Polling, page 2-17
- RPF Polling, page 2-20
- SG Polling—Main, page 2-22
- SG Polling—By Device, page 2-24
- L2 Polling, page 2-26
- Tree Polling, page 2-28
- Health Check, page 2-30

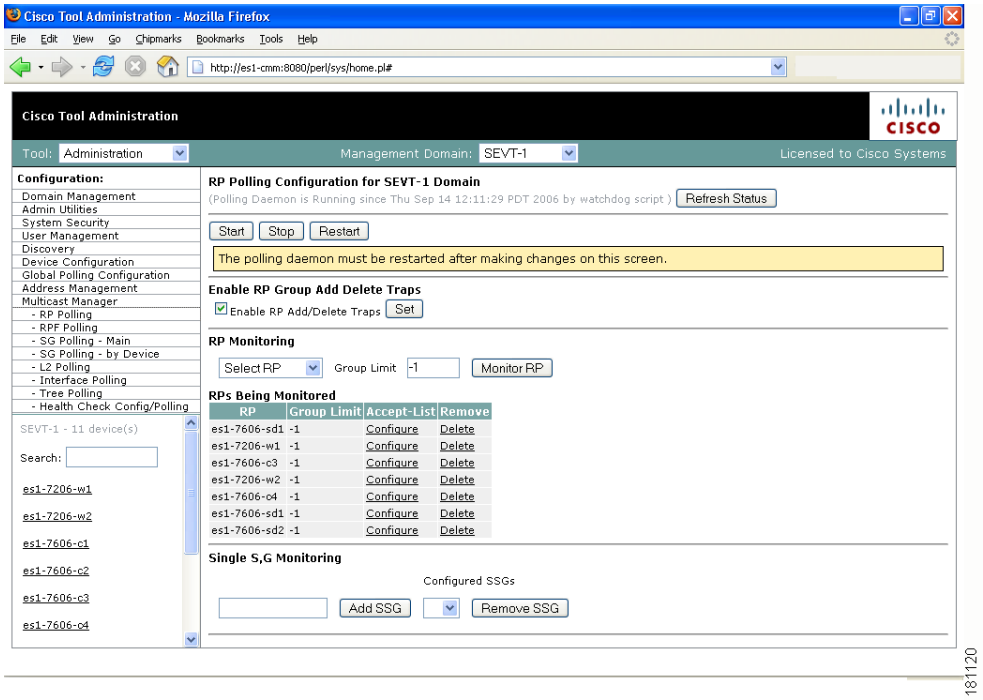
RP Polling

Using the RP Polling Configuration page, you can enable the CMM 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 2-12). 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 3-5).

Figure 2-14 RP Polling Configuration



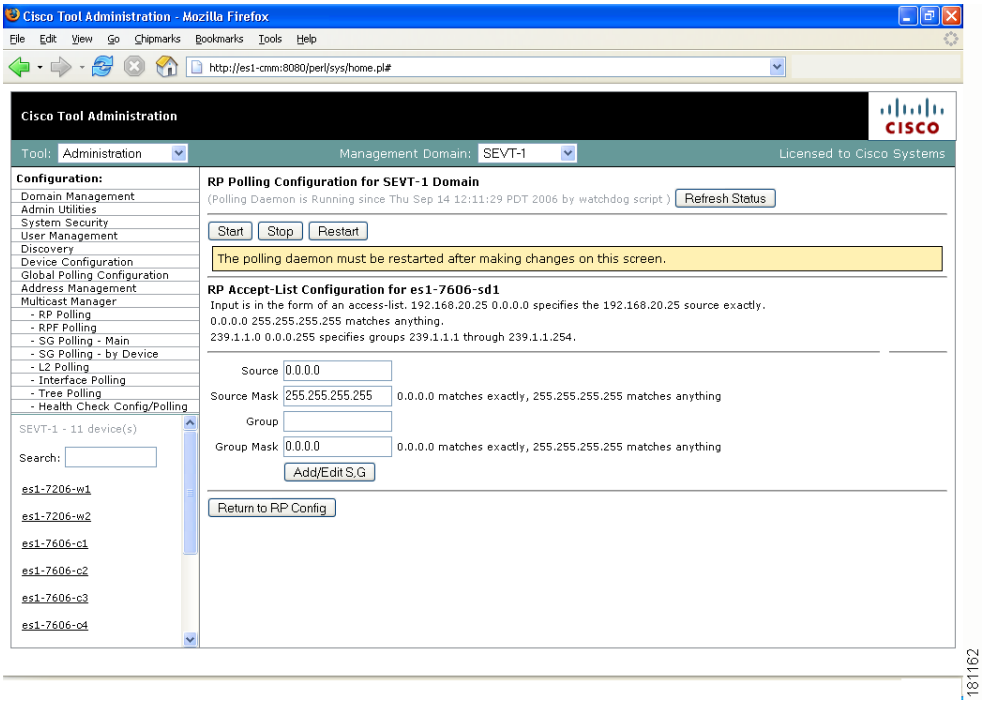
Fields and Buttons	Description
Refresh Status	The status line indicates how long the polling daemon has been running and how it was started. Click **Refresh Status** to update the status information.
Start	Starts the polling daemon globally.
Stop	Stops the polling daemon globally.
Restart	Restarts the polling daemon globally. Each time you change a polling interval, click **Restart**.
Enable RP Group Add Delete Traps	Click the checkbox to monitor all leaves and joins, which are then reported within the RP Polling Report page (see RP Polling Report, page 3-5).

Fields and Buttons	Description
RP Monitoring	To monitor an RP, select the RP from the box. To monitor a specific number of groups, enter a number in the **Group Limit** box. Click **Monitor RP**. 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 3-6).
RPs Being Monitored	Lists: • **RP**—The name of the RP being monitored • **Group Limit**—Number of groups being monitored for that RP. • **Accept-List**—Monitors the sources and groups active on the RP (see the "RP Accept List Configuration" section on page 2-19). • **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 2-15 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.

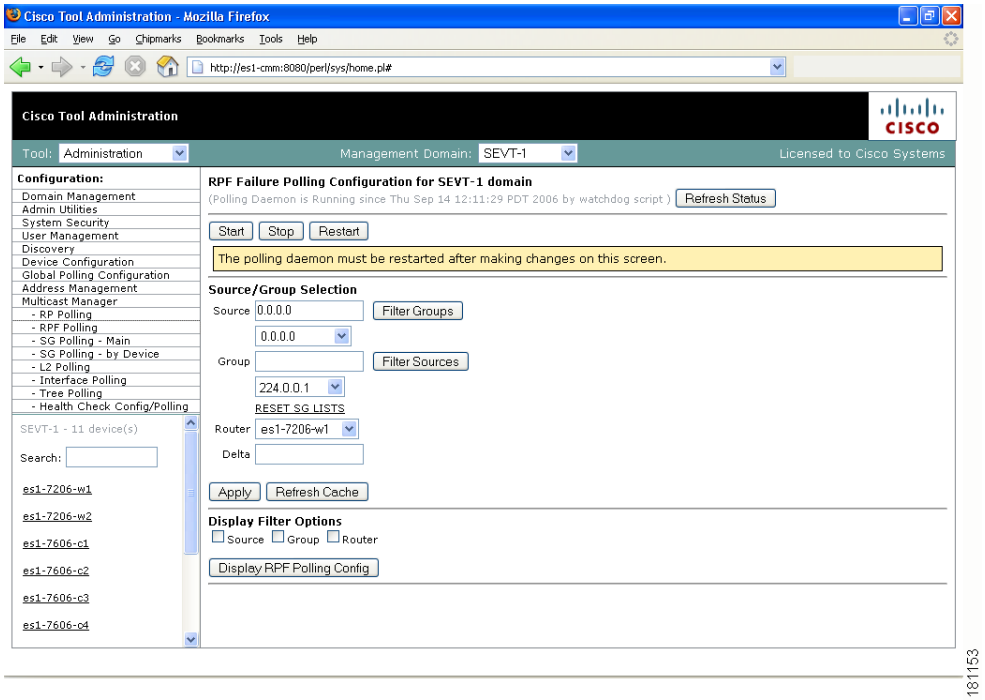
RPF Polling

Using the CMM, you can monitor 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 3-7).

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**.

Figure 2-16 RPF Failure Polling Configuration



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.

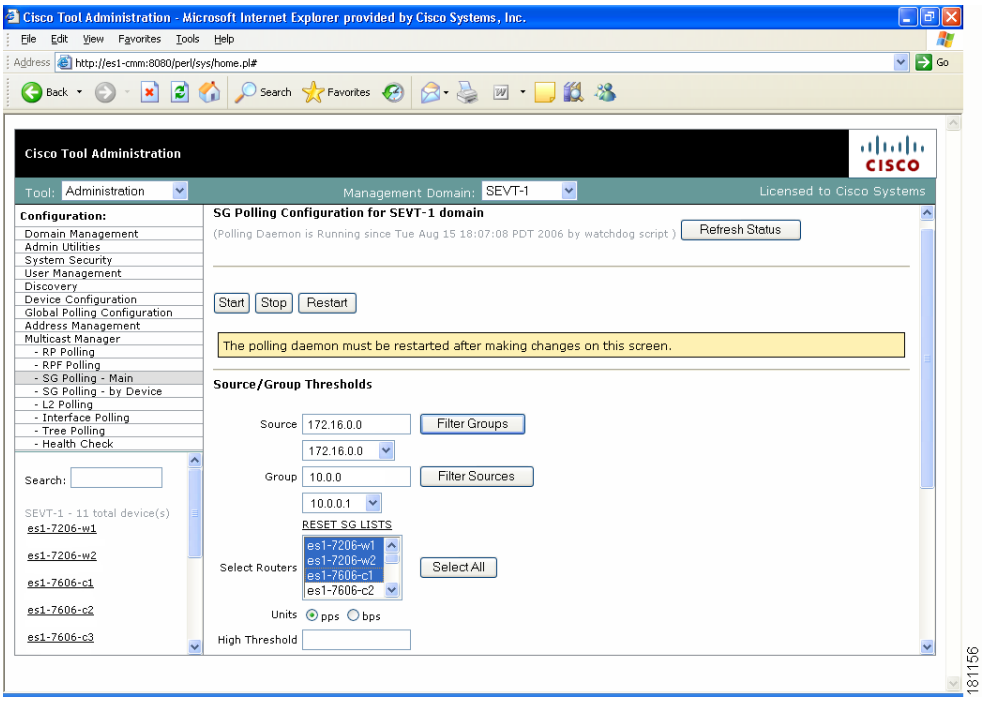
Fields and Buttons	Description
Apply	Applies and saves the changes.
Refresh Cache	Click **Refresh Cache** to refresh the table of sources and groups.

SG Polling—Main

Using the CMM, 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.

Figure 2-17 SG Polling Configuration



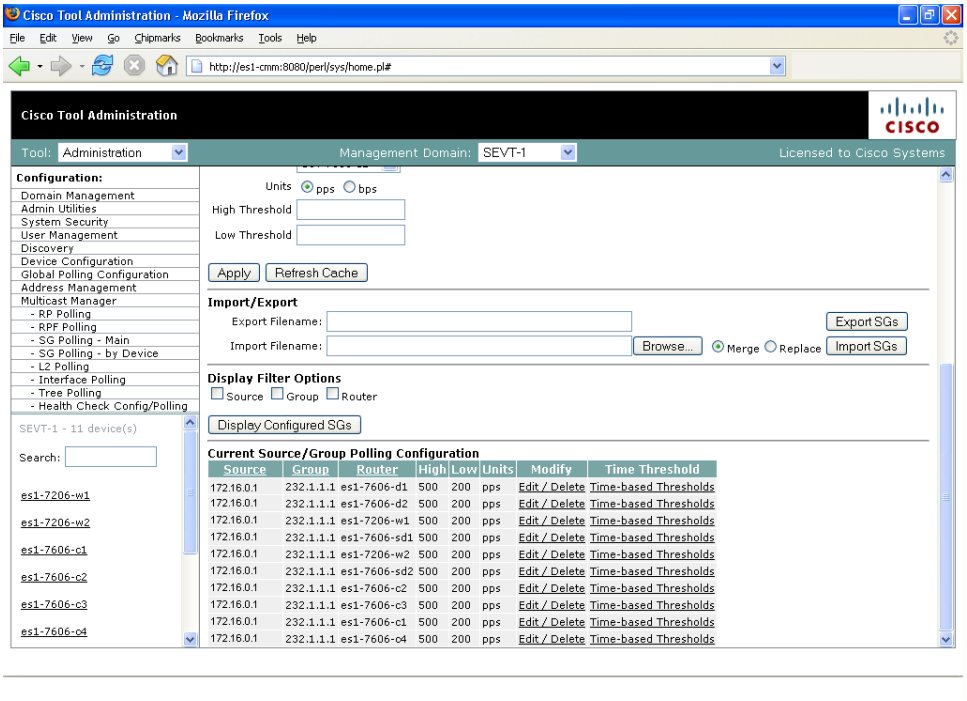
Fields and Buttons	Description
Refresh Status	The status line indicates how long the polling daemon has been running and how it was started. Click **Refresh Status** to update the status information.
Start	Starts the polling daemon globally.
Stop	Stops the polling daemon globally.
Restart	Restarts the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

Fields and Buttons	Description
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 2-23).

Current Source/Group Polling Configuration

The Current Source/Group Polling Configuration section displays all the sources and groups you are currently monitoring.

Figure 2-18 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

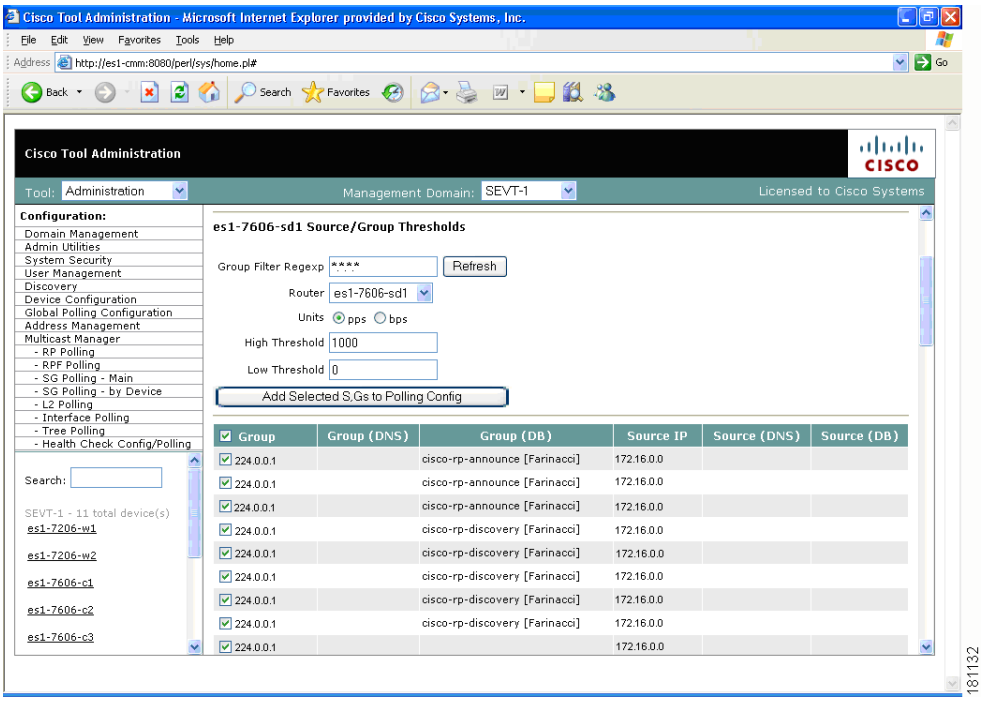
You can select a particular router using the The Device SG Polling Configuration page, and you can configure which sources and routers to monitor on the specific device:

Step 1 Select a **Router**.

Step 2 Select **Units** and enter a **High** and **Low Threshold**.

Step 3 Within the table, select the groups (and sources) you want to monitor, then click **Add Selected S,Gs to Polling Config**.

Figure 2-19 Device SG Polling Configuration



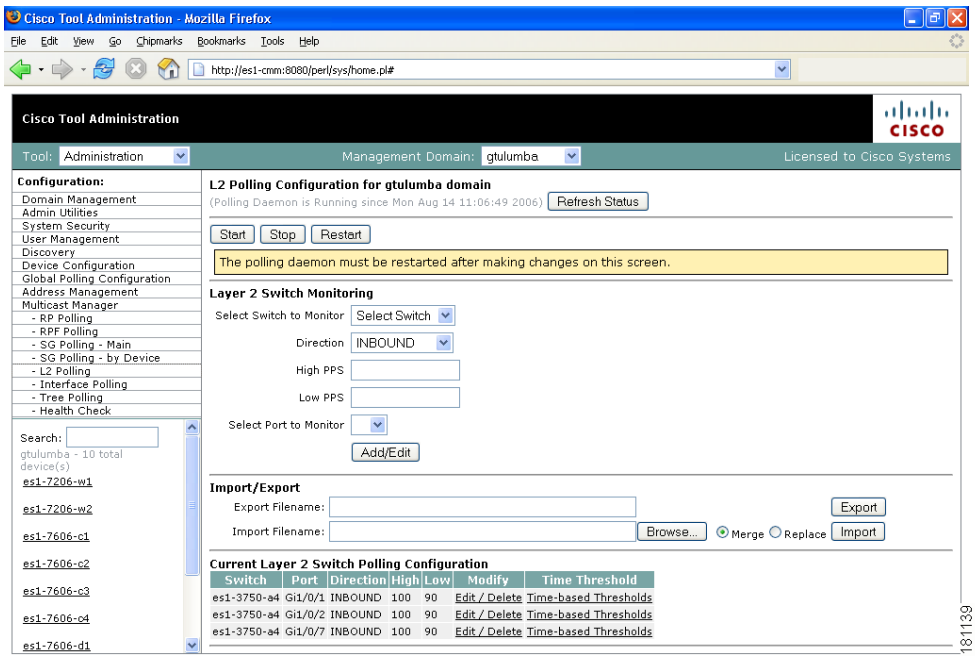
Fields and Buttons	Description
Refresh Status	The status line indicates how long the polling daemon has been running and how it was started. Click **Refresh Status** to update the status information.
Start	Starts the polling daemon globally.
Stop	Stops the polling daemon globally.
Restart	Restarts the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

L2 Polling

You can add Layer 2 switches to the CMM individually, or you can import a list (see Adding Layer 2 Switches to Discovery, page 1-7). The CMM 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.

Figure 2-20 L2 Polling Configuration



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.

Fields and Buttons	Description
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

The CMM 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:

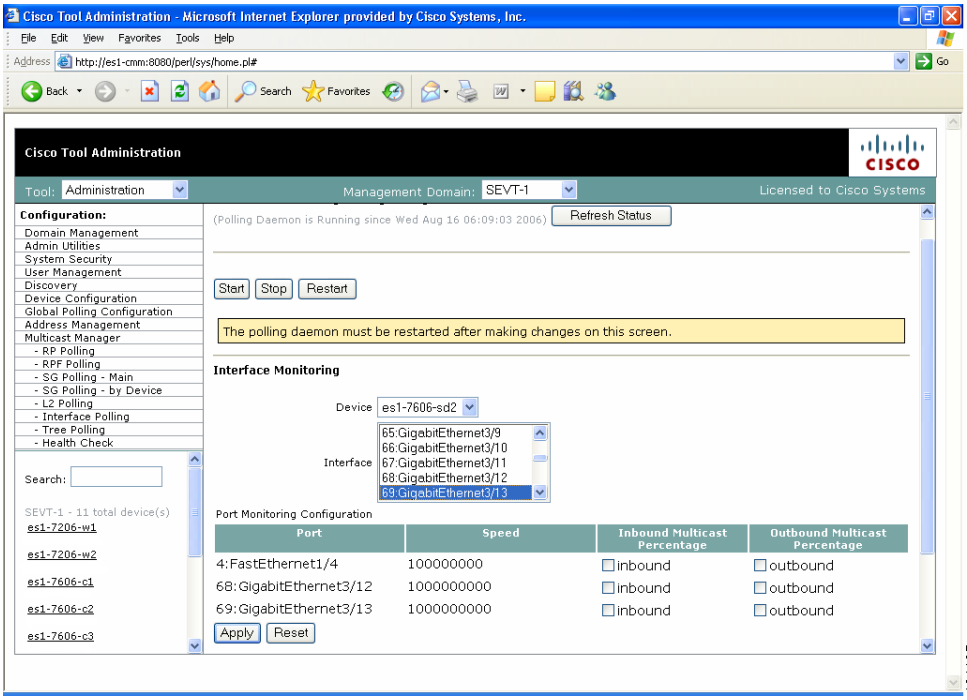
Step 1 Select the device.

Step 2 Select the interface.

Step 3 Select either inbound, outbound, or both, and enter values in percentages.

Step 4 Click **Apply**.

Figure 2-21 Interface Monitoring Polling Page

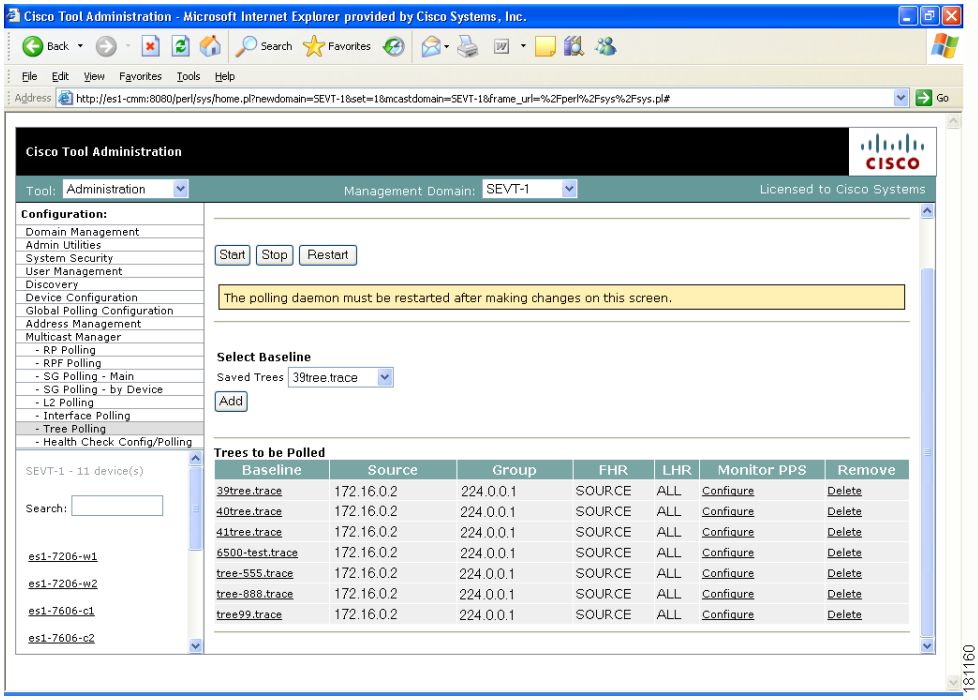


Tree Polling

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 4-1).

Once saved, the trees appear in the **Saved Trees** list of the Tree Polling Configuration page. To monitor a tree, 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 2-12). This tree is compared with the tree saved in the database. If it is different, a trap is sent, and a report generated.

Figure 2-22 Tree Polling Configuration



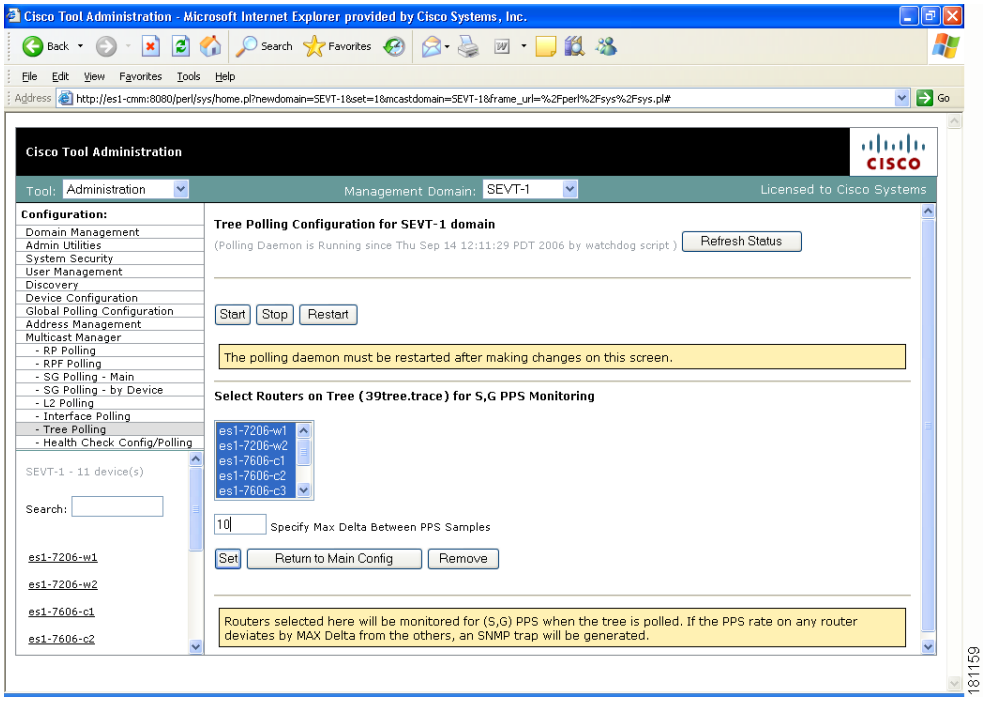
Fields and Buttons	Description
Refresh Status	The status line indicates how long the polling daemon has been running and how it was started. Click **Refresh Status** to update the status information.
Start	Starts the polling daemon globally.
Stop	Stops the polling daemon globally.
Restart	Restarts the polling daemon globally. Each time you change a polling interval, click **Restart**.
Saved Trees	Lists all the multicast tree baselines that have been saved.
Add	Adds the selected tree for monitoring.

Trees To Be Polled

Using the **Trees to be Polled** table, you can:

- View tree details and topology by clicking on a tree name under **Baseline**
- Monitor for S,G (PPS) when a tree is polled, and generate SNMP traps for Max Delta deviations by clicking on **Configure** under **Monitor PPS.**

Figure 2-23 Tree Polling Configuration—Configure



- Select a router(s) 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**.

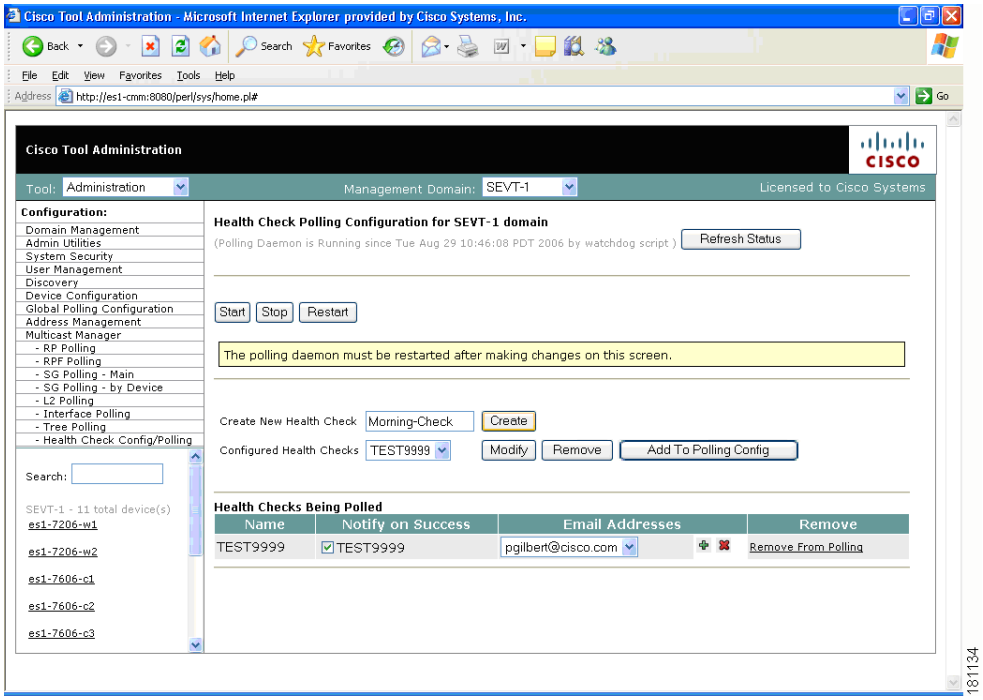
Health Check

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

- Status of selected RPs
- 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.

Figure 2-24 Health Check Configuration



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	Updates the selected health check (see Modifying Health Checks, page 2-31).
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

The Health Check Configuration—Modification section lets you modify a selected health check:

Step 1 Select the RPs that you want this Health Check to check.

Step 2 To check the status of this RPs MSDP peering, click on configure under the RP (see Figure 2-26).

Step 3 Select the sources and groups to check.

Step 4 To check for the existence of multicast trees, select the trees from the **Select Baseline** box and click on **Add**.

Note To run an actual health check, see the "Health Check" section on page 4-14.

Figure 2-25 Health Check Configuration—Modification

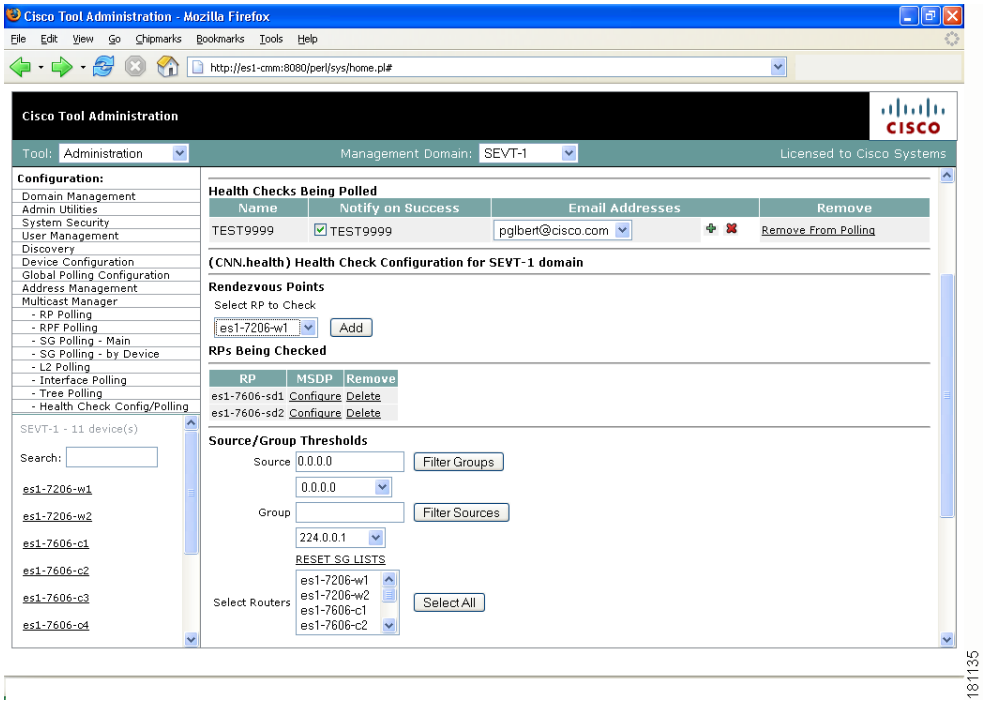
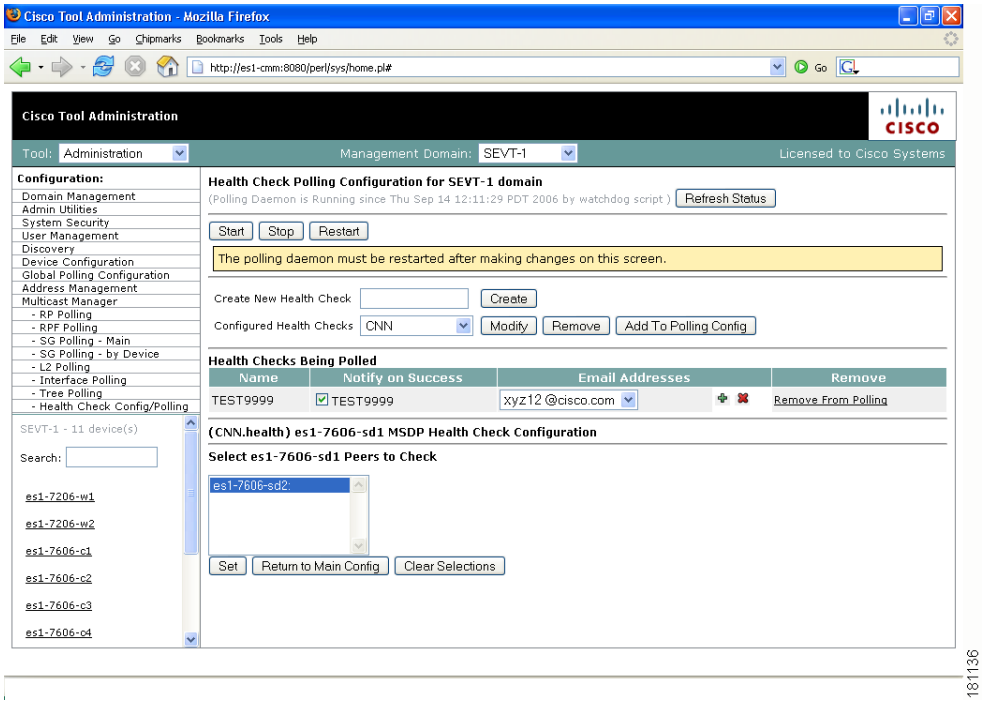


Figure 2-26 Health Check Configuration—Peers



Select the peers you want to check, then click **Set**. You are returned to the Health Check Configuration Modification page. Select the sources, groups and routers to check. To check the status of multicast trees, select the baseline under Forwarding Trees and click **Add**.