User Guide for the Cisco Multicast Manager 2.4

June 2007

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-12466-01

User Guide for Cisco Multicast Manager 2.4

CONTENTS

Preface

This preface describes the objectives, audience, organization, and conventions of the *User Guide for Cisco Multicast Manager 2.4*. It refers you to related publications and describes online sources of technical information.

The Cisco Multicast Manager (CMM) is a web-based software application that requires no client software. With the CMM, you can gather information about the multicast running in your network, monitor multicast networks, and diagnose problems.

This preface includes:

Document Objectives

This guide describes how to use the CMM to monitor, troubleshoot and gather information about multicast networks. Using the information provided in this guide, you can complete the tasks that are necessary to use the CMM in your multicast environment.

Document Audience

This guide is for network administrators or operators who use the CMM software to manage multicast networks. Network administrators or operators should have:

- Basic network management skills
- Basic multicast knowledge

Document Organization

This guide is divided into the following chapters:

- Chapter 1, "Getting Started" describes logging into the CMM, an overview of the CMM interface, and the initial tasks to perform.
- Chapter 2, "Configuring with the CMM Administration Tool" provides information on using the CMM Administration Tool to set up your network for monitoring.
- Chapter 3, "Monitoring with the Multicast Manager Tool" provides information on using the CMM Multicast Manager Tool to view topology and reports.
- Chapter 4, "Diagnostics and Troubleshooting with the Multicast Manager Tool" provides information on using the CMM Multicast Manager Tool to view both global and router-specific diagnostics.
- Chapter 5, "Maintaining and Managing the CMM" describes how to view configuration, log, database, device configuration, and historical data files, and how to include backup directories to maintain and manage the CMM.

Document Conventions

This guide uses basic conventions to represent text and table information.

Command descriptions use the following conventions:

- Commands and keywords are in **boldface** font.
- Arguments for which you supply values are in *italic* font.
- Elements in square brackets ([ ]) are optional.
- Alternate but required keywords are grouped in braces ({ }) and separated by a vertical bar (|).

Examples use the following conventions:

- Terminal sessions and information that the system displays are printed in `screen` font.
- Information that you enter is in **`boldface screen`** font. Variables for which you enter actual data are printed in *italic screen* font.
- Nonprinting characters, such as passwords, are shown in angle brackets (< >).
- Information that the system displays is in `screen` font, with default responses in square brackets ([ ]).

This publication also uses the following conventions:

- Menu items and button names are in **boldface** font.
- Directories and filenames are in *italic* font.
- If items such as buttons or menu options are grayed out on application windows, it means that the items are not available either because you do not have the correct permissions or because the item is not applicable at this time.

Note Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in the manual.

Caution Means *reader be careful*. You are capable of doing something that might result in equipment damage or loss of data.

Tip Means *the following are useful tips*.

Related Documentation

Additional information can be found in the following publications of the CMM documentation set:

- *Installation Guide for Cisco Multicast Manager 2.4*
- *Release Notes for Cisco Multicast Manager 2.4*
- *Documentation Guide and Supplemental License Agreement for Cisco Multicast Manager, 2.4*

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

CHAPTER 1

Getting Started

This chapter covers:

Logging Into Cisco Multicast Manager

Note For details on stopping and starting Cisco Multicast Manager on Solaris and Linux, see the *Installation Guide for the Cisco Multicast Manager 2.4*.

To access CMM, enter the IP address or the name of the server where the software is installed. For example: http://172.16.0.1:8080. The default port of 8080 can be changed as described in the installation instructions.

Figure 1-1 Cisco Multicast Manager Login Page

To enter CMM, click **Login**. You are prompted for a username and a password. The default CMM username is *admin*, and the default CMM password is *rmsmmt*.

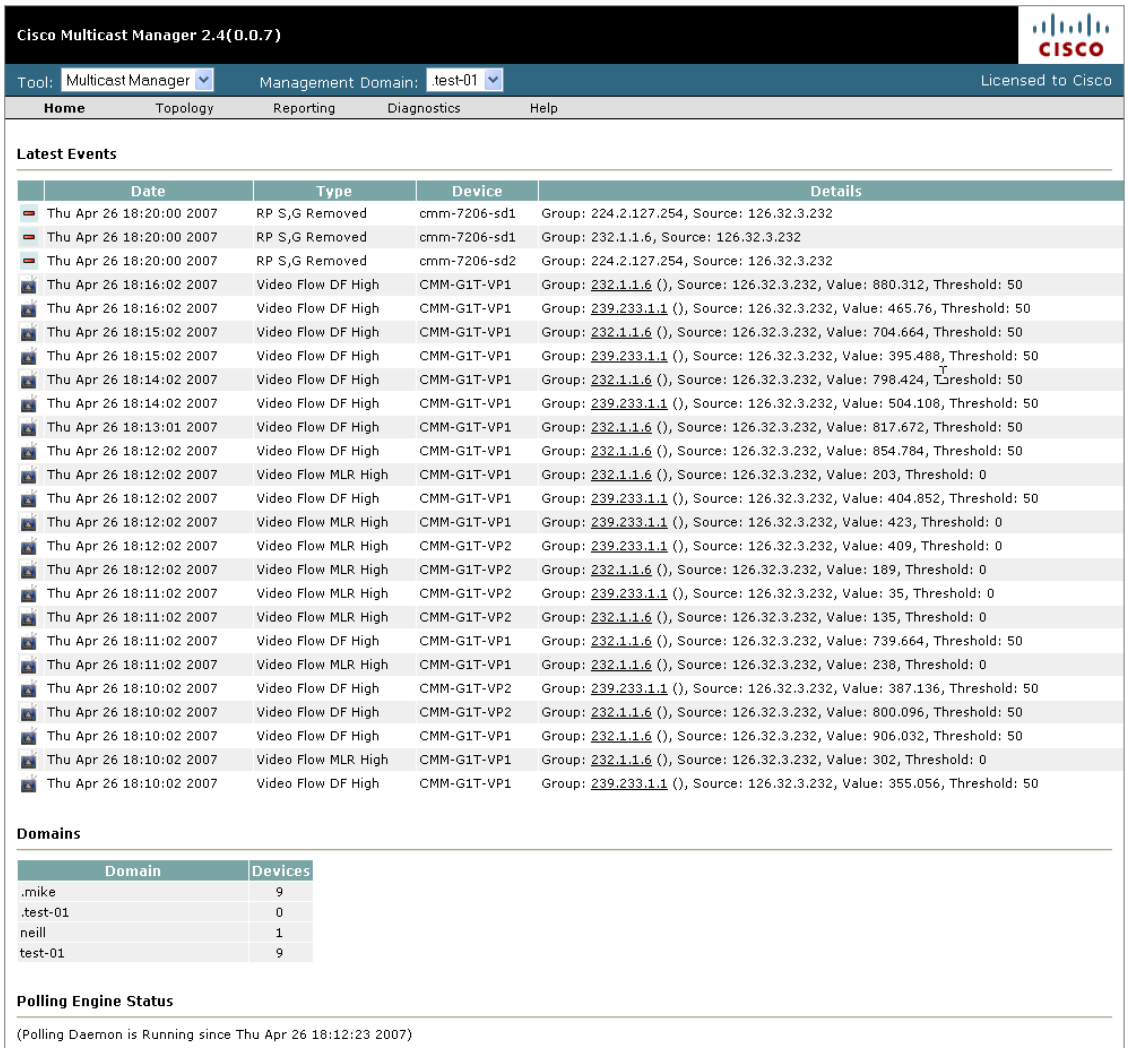
Overview

Cisco Multicast Manager has two main tools: **Administration** and **Multicast Manager**. You can select either tool from the menu at the upper left of Cisco Multicast Manager Web interface. You can perform the following tasks with each tool:

Tool	Tasks	Information
Administration	Manage domains	Creating a Domain, page 1-3
	Use administrative utilities	Using Administrative Utilities, page 2-1
	Configure security	Configuring System Security, page 2-4
	Manage users	Managing Users and Passwords, page 2-5
	Perform discovery	Discovering Your Network, page 1-6
	Configure devices	Configuring Devices and Probes, page 2-7
	Configure global polling	Configuring Global Polling, page 2-16
	Configure multicast polling	Configuring Specific Multicast Manager Polling, page 2-26
	Manage addresses	Managing Device Addresses, page 2-21
Multicast Manager	View events through the **Home** page	• Viewing the Multicast Manager Home Page, page 3-1 • Latest Events, page 3-7
	View **Topology**	Viewing Topology, page 3-2
	Manage **Reporting**	Managing Reports, page 3-6
	Manage **Diagnostics**	Managing Diagnostics, page 4-1
	View **Help**	Viewing User Guide Help, page 4-28

When you first log into Cisco Multicast Manager, the Multicast Manager home page appears.

Figure 1-2 Multicast Manager Home Page



For detailed information on this window, see the "Viewing the Multicast Manager Home Page" section on page 3-1.

Creating a Domain

Before you can begin managing your networks, you must create a domain. A domain is a collection of multicast routers. Multiple domains may exist, and routers can belong to multiple domains. Using Domain Management, you can create and edit domains.

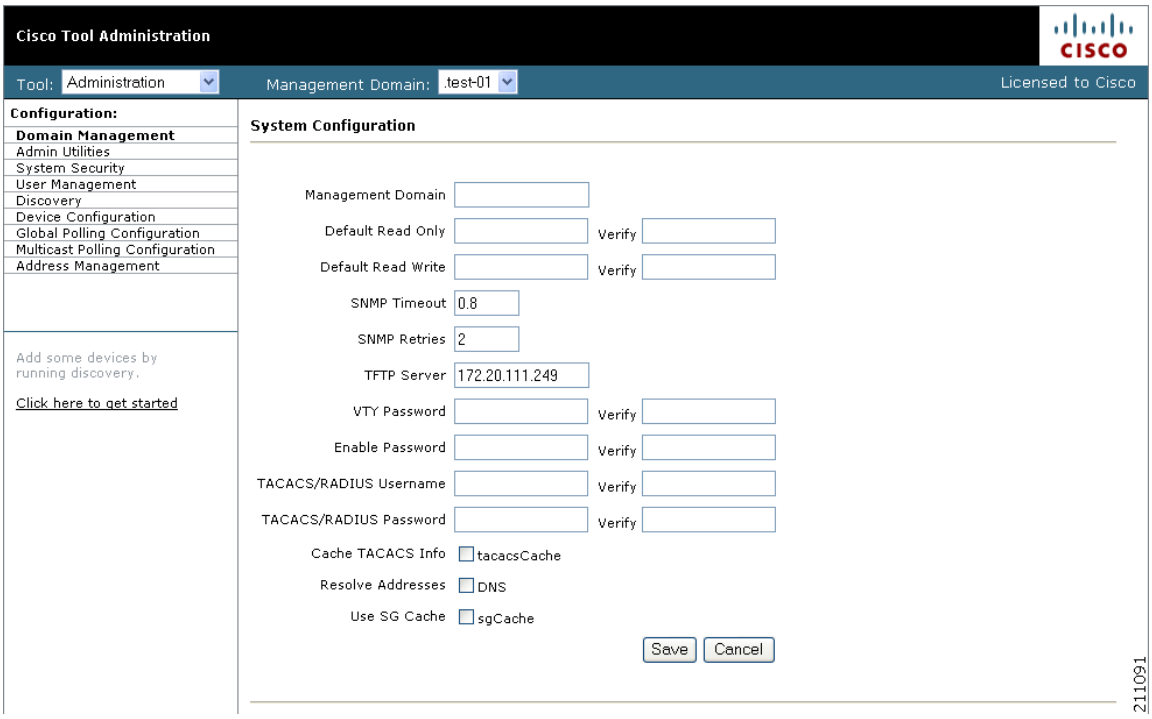
To create a domain:

Step 1 From the Multicast Manager home page, select the **Administration** tool.

Step 2 Select **Domain Management**.

Step 3 Select **add a new domain**. The System Configuration page appears.

Figure 1-3 System Configuration Page



Step 4 Complete the fields in the System Configuration page and click **Save** to continue and create the new domain. Click **Cancel** to exit without creating a domain.

The System Configuration page contains the following fields:

Field	Description
Management Domain	A management domain is defined as a contiguous group of PIM neighbors sharing the same SNMP community string.
Default Read Only	SNMP read-only community string.
Default Read Write	SNMP read-write community string. This is required for retrieving and validating device configurations.
SNMP Timeout	Retry period if node does not respond. Default value is 0.8.
SNMP Retries	Number of retries to contact a node before issuing a timeout. Default value is 2.
TFTP Server	TFTP server IP address. Default is the IP address of Cisco Multicast Manager server.
VTY Password	The VTY password is required if you want to issue show commands from the application. Certain features, such as querying Layer 2 switches, also require this. If TACACS is being used, then a username and password can be supplied instead of the VTY password.
Enable Password	(*Not currently used.*)
TACACS/RADIUS Username	If you are using TACACS/RADIUS then you can enter a username here. See VTY Password above. **Note** If you enter a TACACS/RADIUS username and password here, the application will use these values regardless of who is currently logged in. Users can also enter their own username and password when issuing show commands.
TACACS/RADIUS Password	If you are using TACACS/RADIUS then you can enter a password here. See VTY Password above. **Note** If you enter a TACACS/RADIUS username and password here, the application will use these values regardless of who is currently logged in. Users can also enter their own username and password when issuing show commands.
Cache TACACS Info	If this box is checked, CMM will cache the TACACS username and password until the browser is closed. This eliminates having to enter the username and password each time you issue a router command from the application.

Field	Description
Resolve Addresses	Performs DNS lookups on all sources found. The DNS name appears alongside the IP address on the "Show All Groups" screen. If the server is not configured for DNS, then DO NOT check the box. If the box is checked, you may receive a slower response, due to the fact that the application is trying to resolve names. This option is not recommended if your network contains a large number of S,Gs. The Resolve Addresses option also causes discovery to do a reverse DNS lookup on a device name. The IP address returned by DNS is then used for management purposes. Otherwise, the IP address by which the device is found is used for management purposes.
Use SG Cache	Some networks contain thousands of sources and groups (S,G)s. During discovery, CMM caches all the S,Gs found in the RPs. If this box is checked, CMM reads the SG cache when showing lists of sources and groups, rather then retrieving them again from the RPs in the network. The cache is automatically refreshed if RPs are being polled as described later in this document (see the "RP Polling" section on page 2-26). The cache can also be refreshed manually by clicking the **Refresh Cache** button in the Multicast Diagnostics window (see the "Show All Groups" section on page 4-2). This button appears only if you have the **Use SG Cache** option selected. It is highly recommended to use the SG cache option. If there are no RPs in the domain being discovered, then the SG cache is created by querying all the devices that have been discovered, as would be the case in a PIM Dense-Mode network. In this case, the SG cache is updated only when you click the **Refresh Cache** button.

Discovering Your Network

Note If you are upgrading from CMM 2.3, you must run discovery to access new features.

After you have created a domain, the second step in using Cisco Multicast Manager is to discover your network using one of these choices, found within the **Discovery** menu:

- Adding Layer 2 Switches to Discovery, page 1-7

- Adding Video Probes, page 1-8
- Performing Multicast Discovery, page 1-12
- Adding or Rediscovering a Single Device, page 1-13

The discovery process is multicast-specific and finds only devices that are PIM-enabled. CMM builds a database of all found devices. Discovery adds support for multiple community strings per domain, along with device-specific SNMP timeout and retries.

Note If any new routers or interfaces are added to the network, run discovery again so that the database is consistent with the network topology.

A single router may also be added or rediscovered on the network. A router being added must have a connection to a device that already exists in the database. A router that is being rediscovered is initially removed from the database, along with any neighbors that exist in the database. The router and its neighbors are then added back into the database. This option would be used if a change on a device has caused a change in the SNMP ifIndexes.

Note When possible, use the SNMP **ifindex persist** command on all devices.

Adding Layer 2 Switches to Discovery

Layer 2 switches are not included in discovery and must be added manually. You can add switches individually, or you can import a list of switches in a CSV file.

To add switches individually, enter the switch name or IP address and the community string, then click **Add**.

To import a list of switches:

Step 1 Create a text file by typing:

```
#import file format switch IP address or switch name
# this line will be skipped
switchA
192.168.1.1, public
switchC
10.10.10.1, public
```

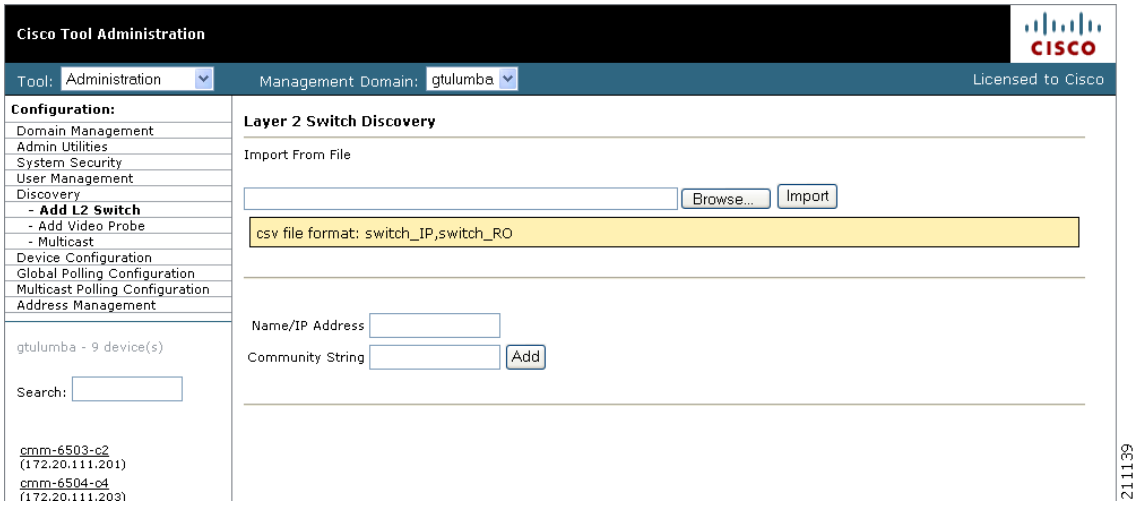
Step 2 Save the file.

Step 3 Within the Administration tool, select **Discovery**.

Step 4 Select **Add L2 Switch**.

The Multicast Layer 2 Switch Configuration page appears.

Figure 1-4 Multicast Layer 2 Switch Configuration



Step 5 Click **Browse**. Open the file you created.

Step 6 Click **Import**.

Adding Video Probes

Configuring a video probe consists of these steps:

1. Gathering the IP addresses and names of the probes.

   Obtain the IP addresses and names of the probes that you will monitor.

2. Inputting a list of probes.

   You can add probes manually, using the Cisco Multicast Manager interface or by importing a CSV that includes a list of the probes that you want to monitor.

   - For information on adding probes manually, see Adding Video Probes Manually, page 1-9.
   - For information on importing probes listed in a text file, see Importing a List of Probes, page 1-11.

3. Setting up monitoring for the probes.

   For information on setting up monitoring for probes, see the following sections in Chapter 2, "Configuring with the CMM Administration Tool."

   - Editing Basic Probe Parameters, page 2-14
   - Configuring Global Polling, page 2-16
   - Video Probe Polling, page 2-48

4. If needed, setting up a trap collector or email alerts.

- For information on setting up a trap receiver and email addresses see, Configuring Domain-Specific Trap Receivers and Email Addresses, page 2-20.

Cisco Multicast Manager can monitor the status and video quality of video streams delivered over the multicast network by using video probes that show activity on specified devices or routes.

You can specify a video probe to monitor in two ways:

- Manually, by entering the probes in the Video Probe Discovery page
- By importing a list of probes contained in a text file.

Note You must compile Cisco Multicast Manager MIBs into your NMS station. The MIBS are located in the following directories:

/opt/RMSMMT - solaris
/usr/local/netman - Linux

RMS-MMT-V1SMI.my
RMS-MMT.mi2
RMS-MMT.my

Adding Video Probes Manually

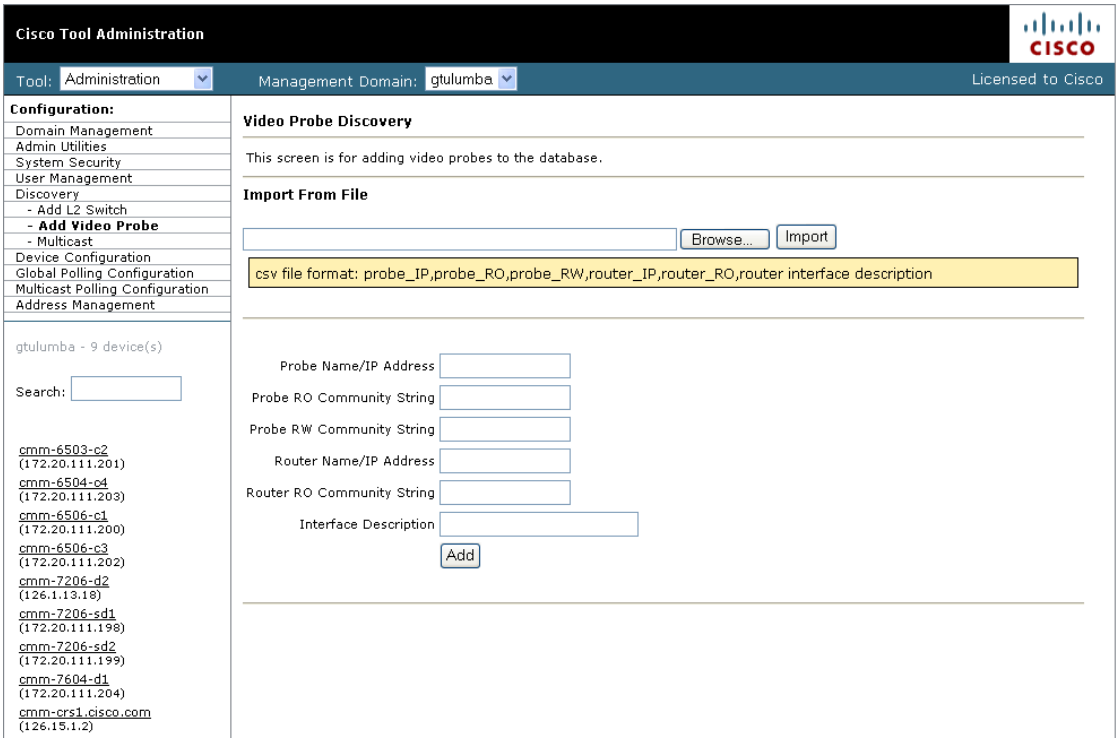
To add a video probe manually:

Step 1 Within the administration tool, select **Discovery**.

Step 2 Select **Add Video Probe**.

The Video Probe Discovery page appears, as shown in Figure 1-5.

Figure 1-5 Video Probe Discovery Configuration Page



Step 3 Complete the fields in the Video Probe Discovery page.

Field	Description
Probe Name/IP Address	Enter the name or the IP address of the video probe.
Probe RO Community String	Enter the read-only (RO) SNMP community string for the probe.
Probe RW Community String	Enter the read-write (RW) SNMP community string for the probe.
Router Name/IP Address	Enter the hostname of the IP address of the router that the probe is monitoring.
Router RO Community String	Enter the RO community string for the router that the probe is monitoring.
Interface Description	Enter a description of the router interface.

Step 4 Click **Add**.

The Cisco Multicast Monitor system starts the probe discovery process, and attempts to contact the router. If the router is contacted successfully, the probe information is added to the Cisco Multicast Manger configuration. If the SNMP community string, router name, or IP address is incorrect, an error message appears.

Importing a List of Probes

To import a list of video probes:

Step 1 Create a comma-separated text file (CSV) in the format:

ProbeIPaddress,Probe-SNMP-RO,Probe-SNMP-RW,Router-IP-Address,Router-SNMP-RO,router-interface-desc

Each entry specifies the following information about a video probe.

Entry	Description
ProbeIPaddress	The name or the IP address of the video probe.
Probe-SNMP-RO	The read-only (RO) SNMP community string for the probe.
Probe-SNMP-RW	Enter the read-write (RW) SNMP community string for the probe.
Router-IP-Address	The hostname of the IP address of the router that the probe is monitoring.
Router-SNMP-RO	The RO community string for the router that the probe is monitoring.
router-interface-desc	A description of the router interface.

Step 2 Save the text file to a directory on the computer where you are running Cisco Multicast Manager.

Step 3 Click **Browse**.

Step 4 Navigate to the directory where the text file is located and select the text file.

The directory path and file name appear in the Input From File text box.

Step 5 Click **Import**.

The Cisco Multicast Monitor system starts the probe discovery process and attempts to discover the specified video probes. If the information in the CSV file is correct, the probes are added to the topology database. If the information in the CSV is incorrect, an error message appears.

Note If the probes are not being added, check that the server CMM is loaded on does have IP connectivity to the probes and the probes have SNMP enabled.

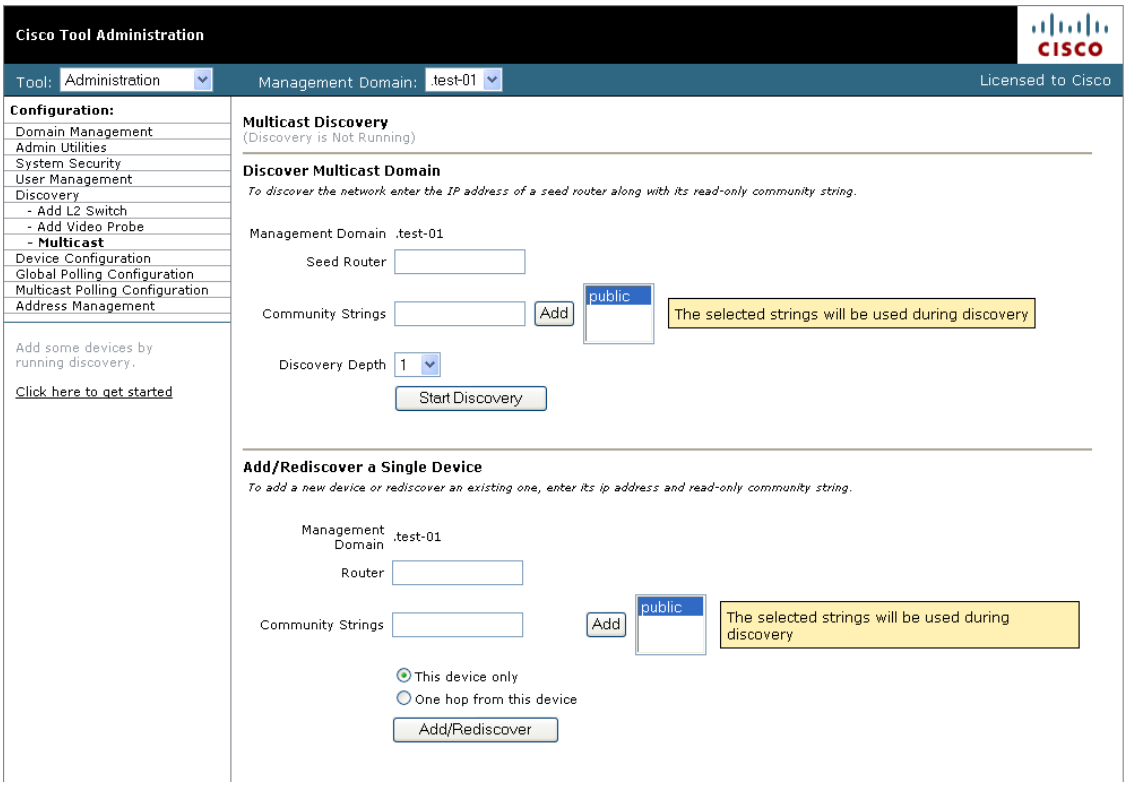
Performing Multicast Discovery

To perform a new multicast discovery:

Step 1 Within the Administration tool, select **Discovery**.

Step 2 Select **Multicast**. The Multicast Discovery page appears, with a **Management Domain** selected.

Figure 1-6 Multicast Discovery Page



Step 3 Complete the fields in the **Discover Multicast Domain** pane and click **Start Discovery** to continue.

The Discover Multicast Domain pane contains the following fields:

Field	Description
Management Domain	(Read-only) Lists the selected management domain.
Seed Router	Enter the IP address of the seed router to start discovery. If you enabled DNS when configuring the domain, enter a name.

Field	Description
Community Strings	You can add additional community strings if required.
Discovery Depth	Number of PIM neighbors Cisco Multicast Manager will discover from the seed router (similar to a hop count).

As routers are discovered, they appear in the browser window.

Step 4 (Optional) To view discovery progress as it is running, click **Refresh Status**.

Note For details on adding or rediscovering a single device, see Adding or Rediscovering a Single Device, page 1-13.

CMM discovers all routers in the network that are multicast enabled and have interfaces participating in multicast routing. If the discovery fails to find any routers, or if there are routers in the network that you expected to discover but did not, check the following:

- Connectivity to the routers
- SNMP community strings on the routers
- Discovery depth setting—is it sufficient?
- SNMP ACLs on the routers

When discovery is complete, the browser window displays the time it took to discover the network and the number of devices discovered:

```
Discovery took 15 seconds
Discovered 5 routers
```

The time the discovery takes depends on the number of routers, number of interfaces, and router types.

If the discovery seems to stop at a particular router, or seems to pause, check that particular router's connectivity to its PIM neighbors. Also, check the PIM neighbor to see if it supports the PIM and IPMROUTE MIBs. Again, because the discovery is multicast-specific, unless these MIBs are supported, the device will not be included in the database. Issuing the **sh snmp mib** command on a router gives this information.

When discovery finishes, you can view the discovered routers in the lower left pane.

Adding or Rediscovering a Single Device

To add or rediscover a single device:

Step 1 Within the Administration tool, select **Discovery**.

Step 2 Select **Multicast**. The Multicast Discovery page appears (see Figure 1-6). A **Management Domain** is selected.

Step 3 Complete the fields in the **Add/Rediscover a Single Device** pane and click **Add/Rediscover** to continue.

The Add/Rediscover a Single Device pane contains these fields:

Field	Description
Management Domain	(Read-only) Lists the selected management domain.
Router	Enter the IP address of the device you want to discover or add.
Community Strings	You can add additional community strings if required.
This device only	Rediscovers this device and updates the current database with the new information.
One hop from this device	Discovers this router and every router within one hop, and updates the current database with the new information.

As devices are discovered, they appear in the browser window.

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

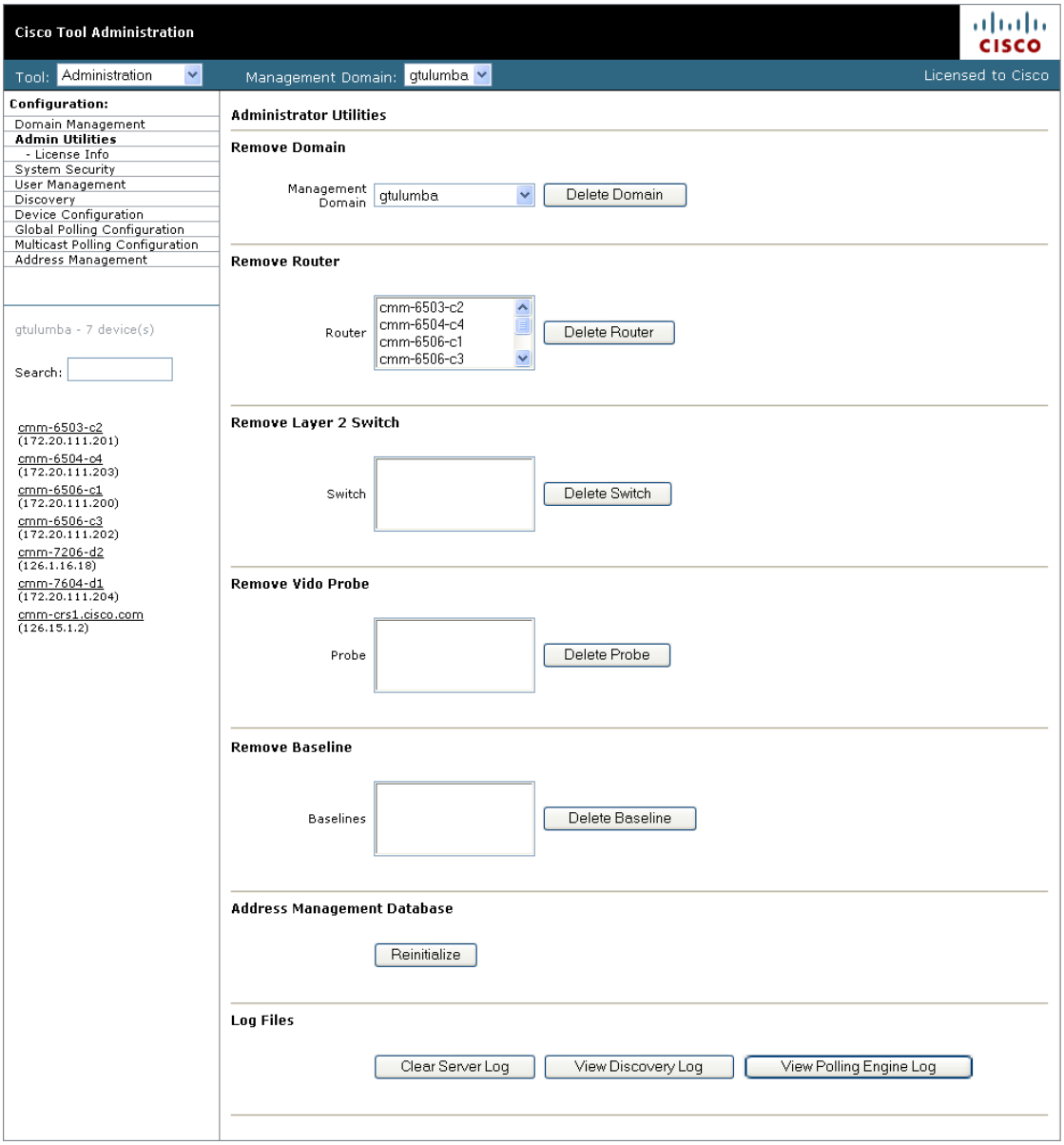
For details on Domain Management, see the "Creating a Domain" section on page 1-3.

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. **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:
	• **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 Cisco Multicast Manager.

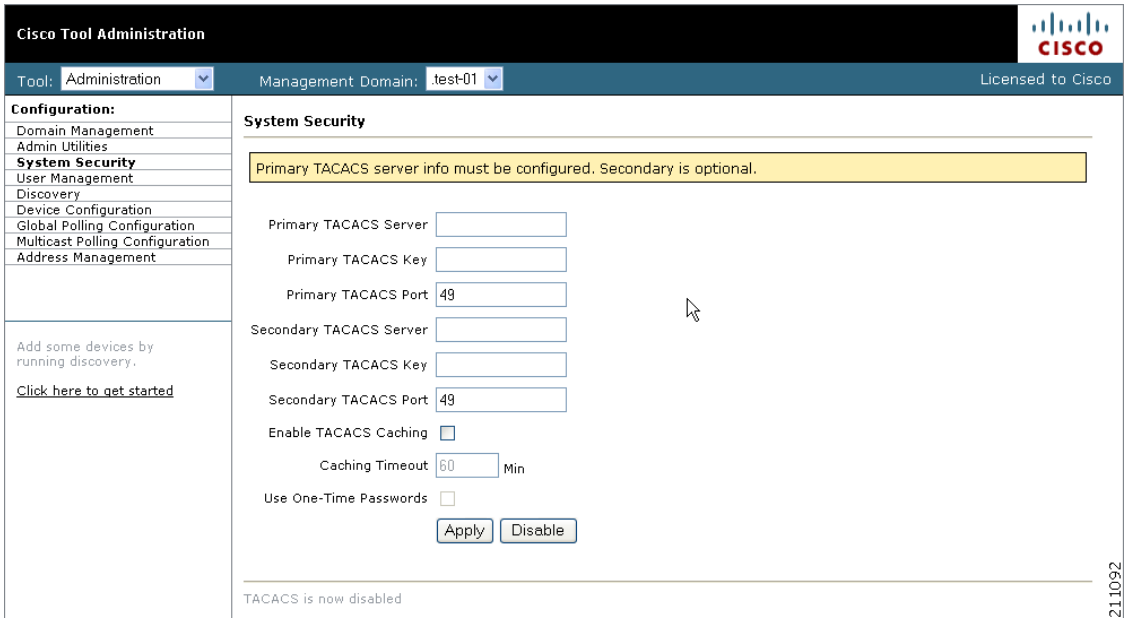
To configure TACACS login support:

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

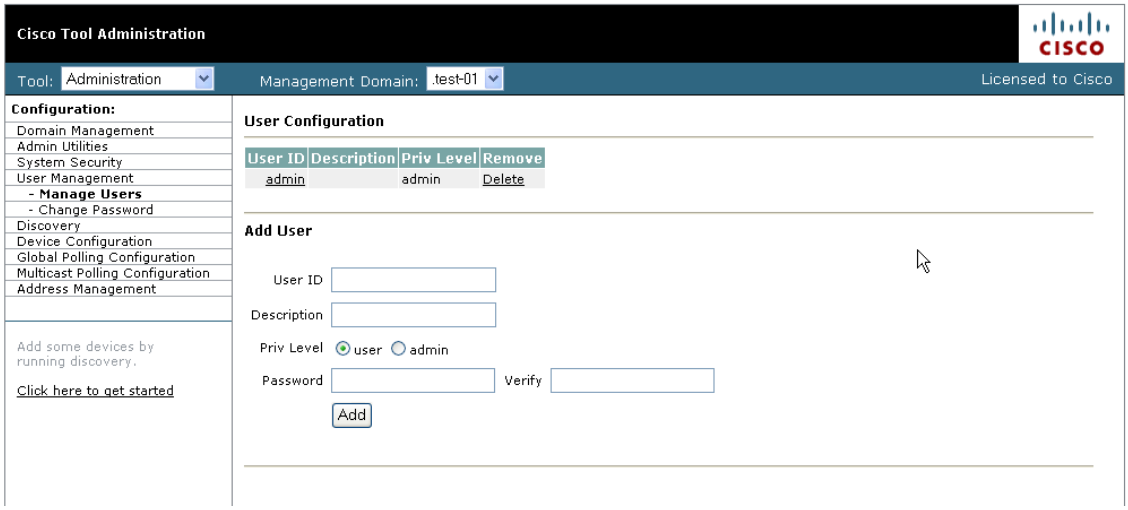
To manage users:

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.

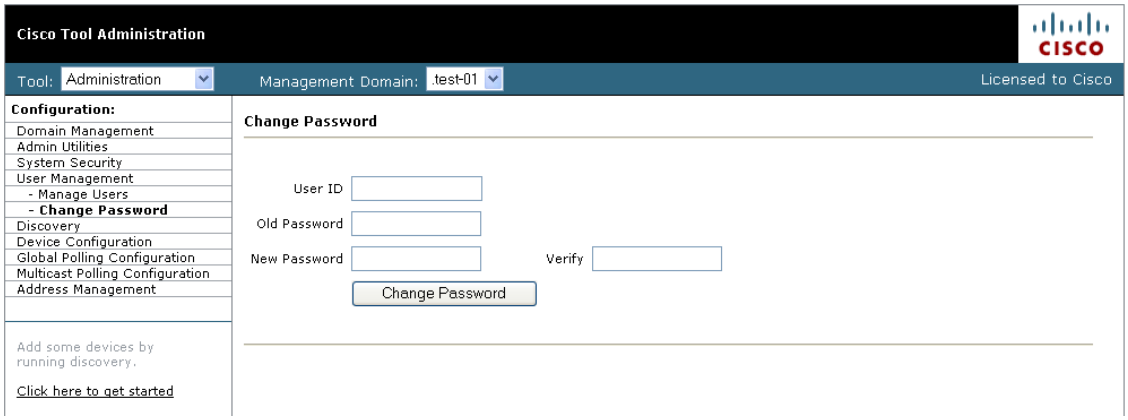
Changing Your User Password

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

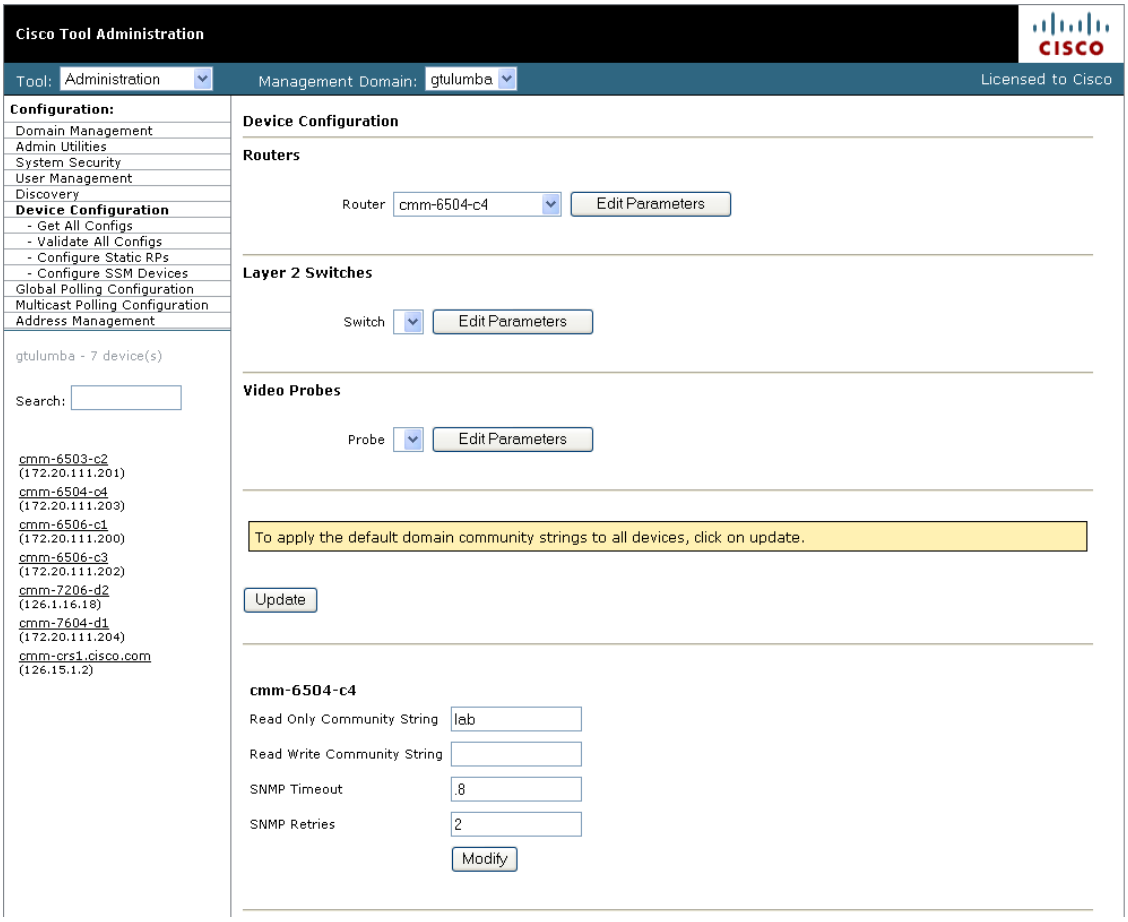
To configure a device:

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.

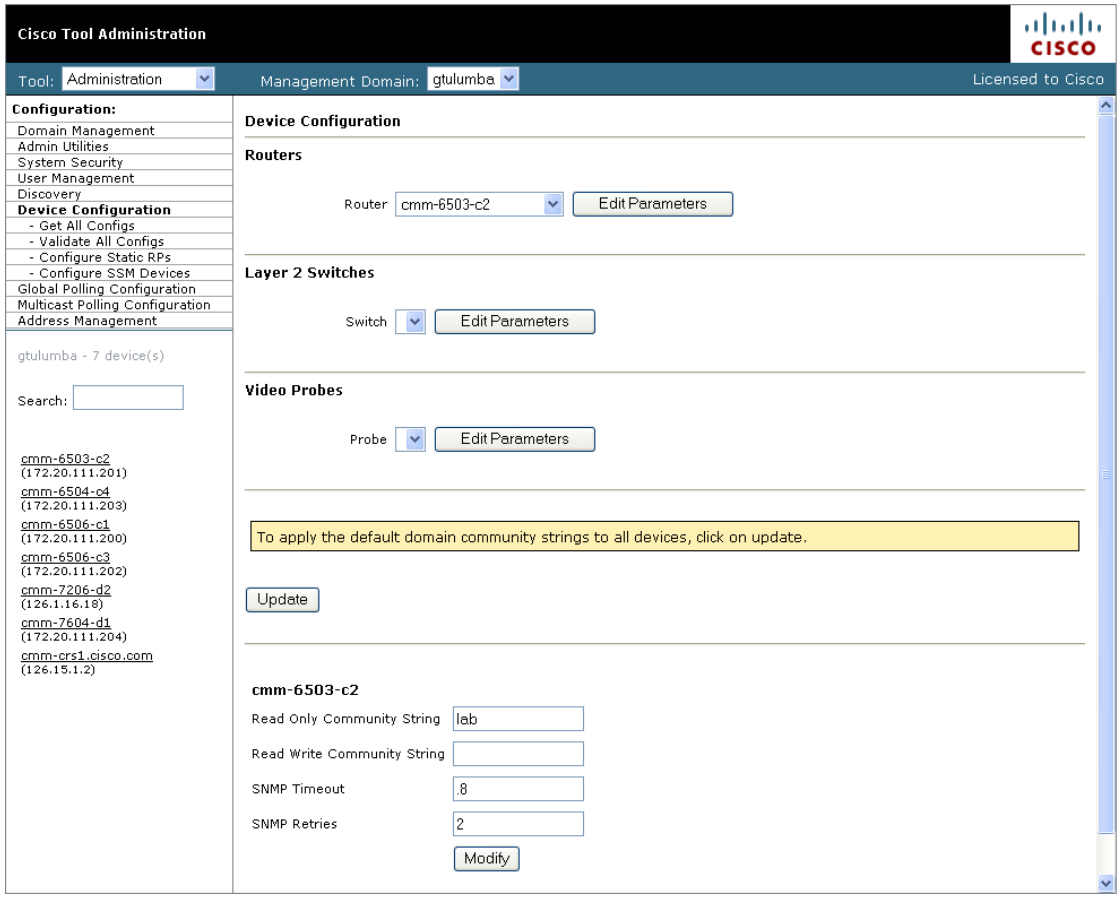
Figure 2-5 Device Configuration—Edit Parameters



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.

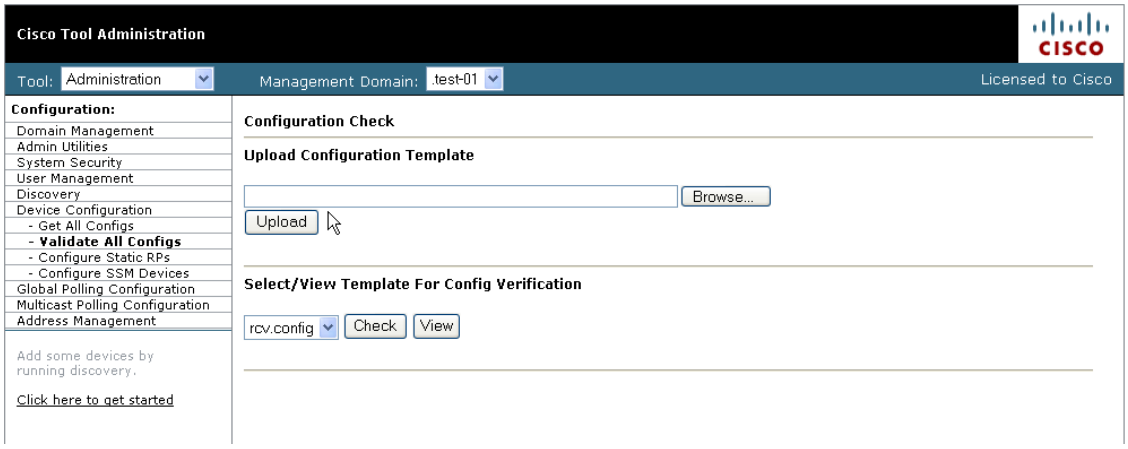
To select a template and initiate validation:

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

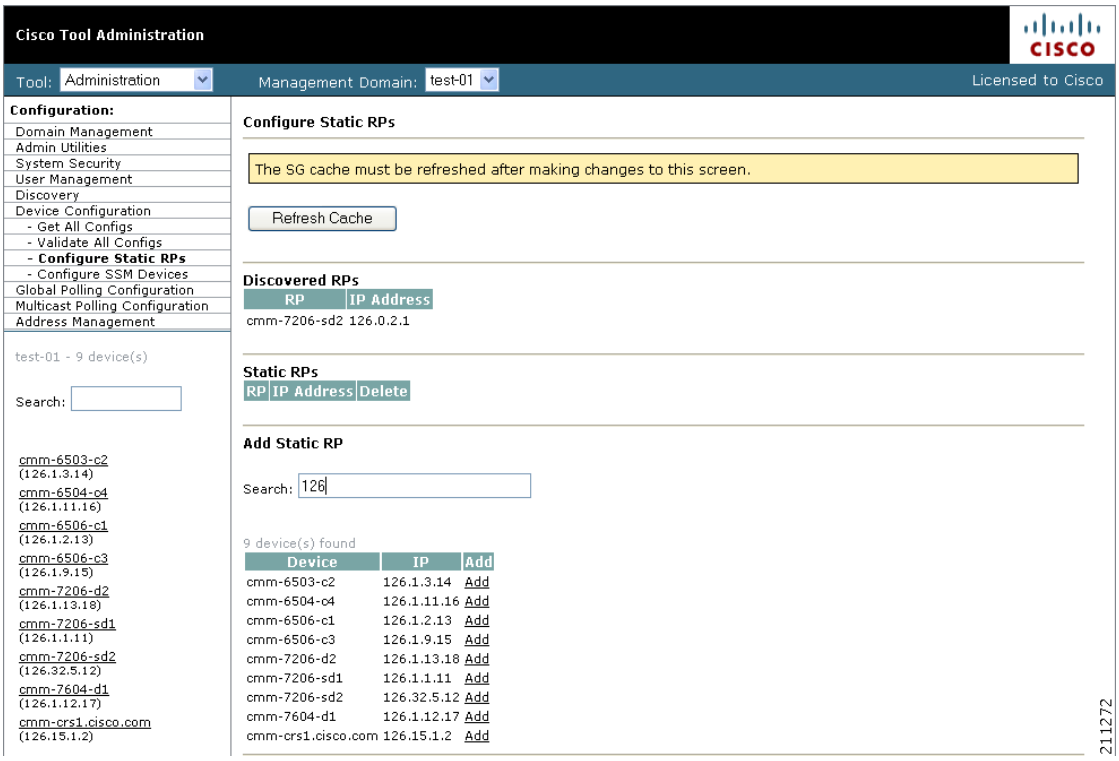
If you have static rendezvous points (RPs) configured, you must configure CMM to find these static RPs, which in turn populates the RP Summary within the Multicast Manager tool Diagnostics section.

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).

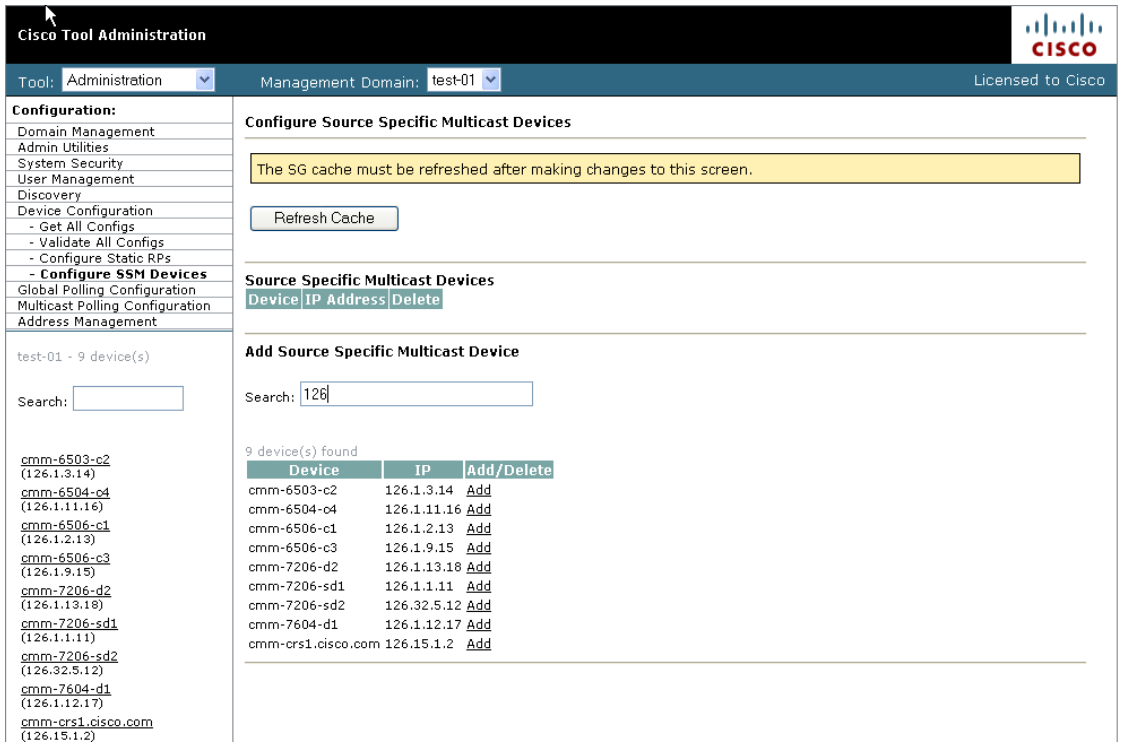
To configure SSM devices:

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:

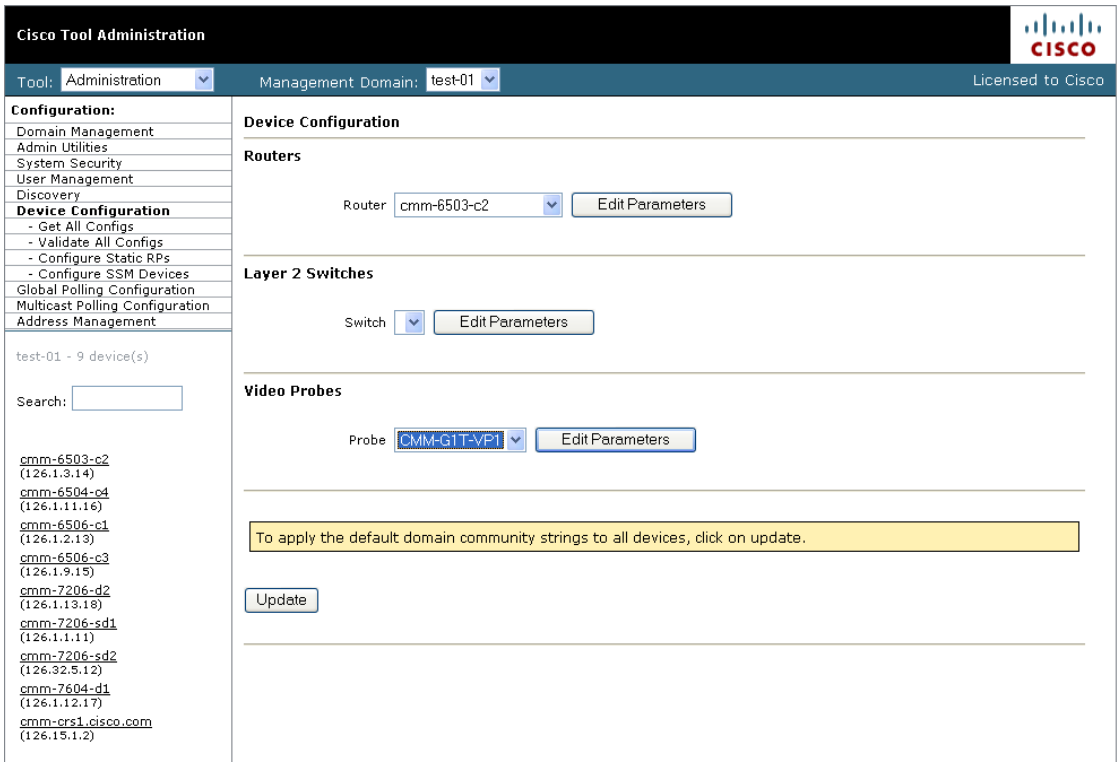
Step 1 Select the **Administration** tool.

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.

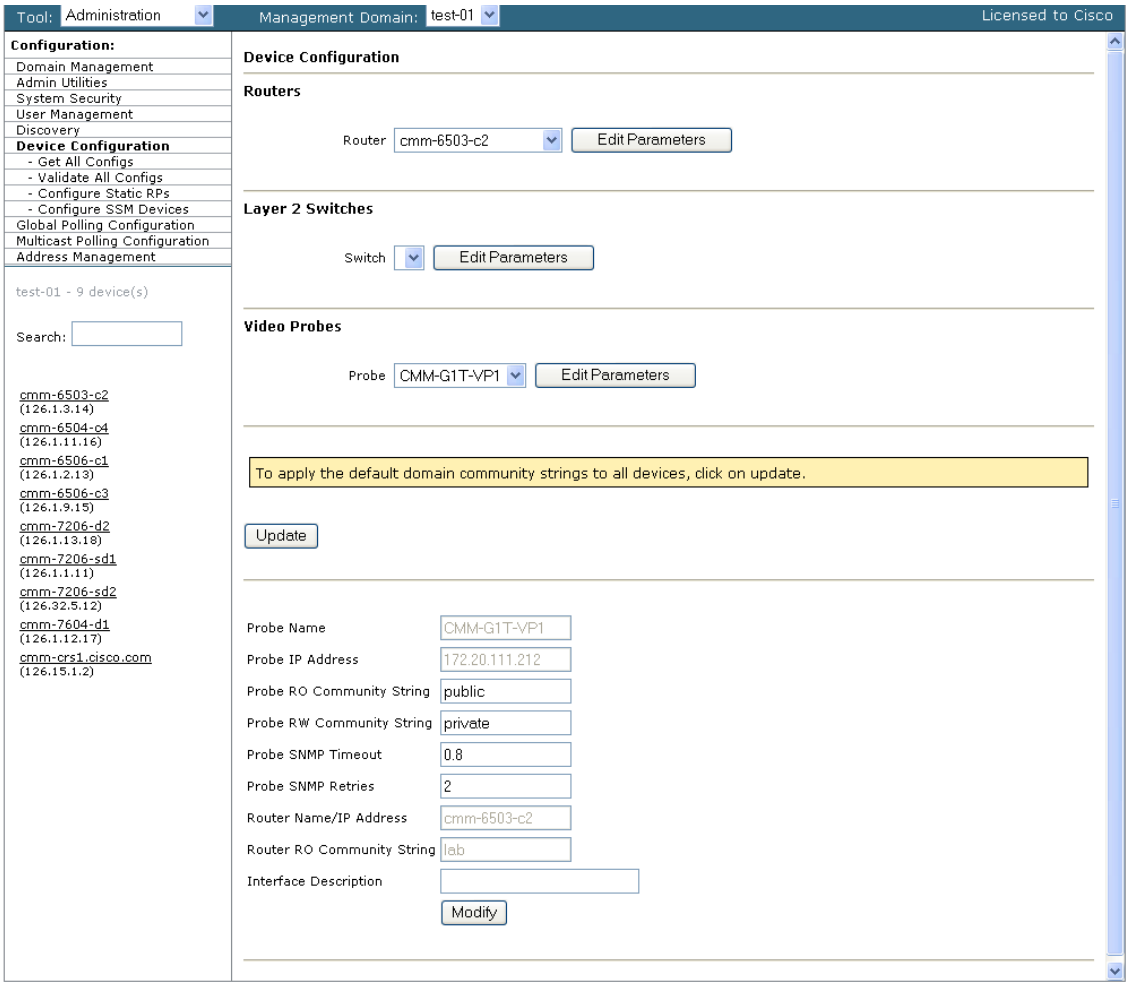
Step 2 Click **Device Configuration.**

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. **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)

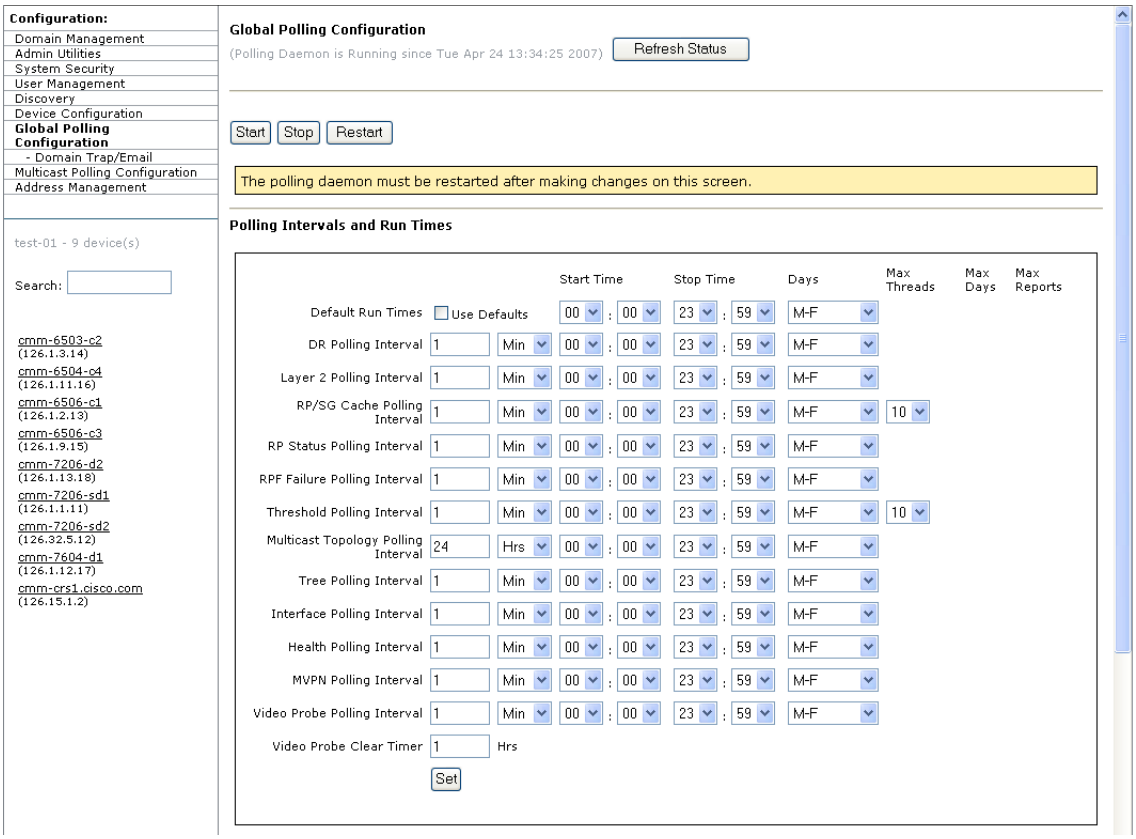
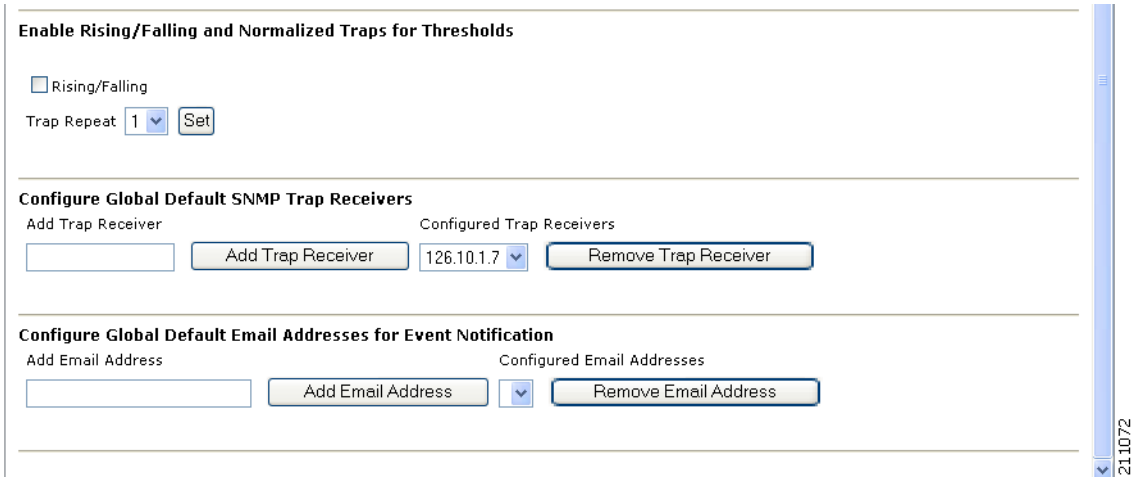


Figure 2-13 Global Polling Configuration Page (Bottom Portion)



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. 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).

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). 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.

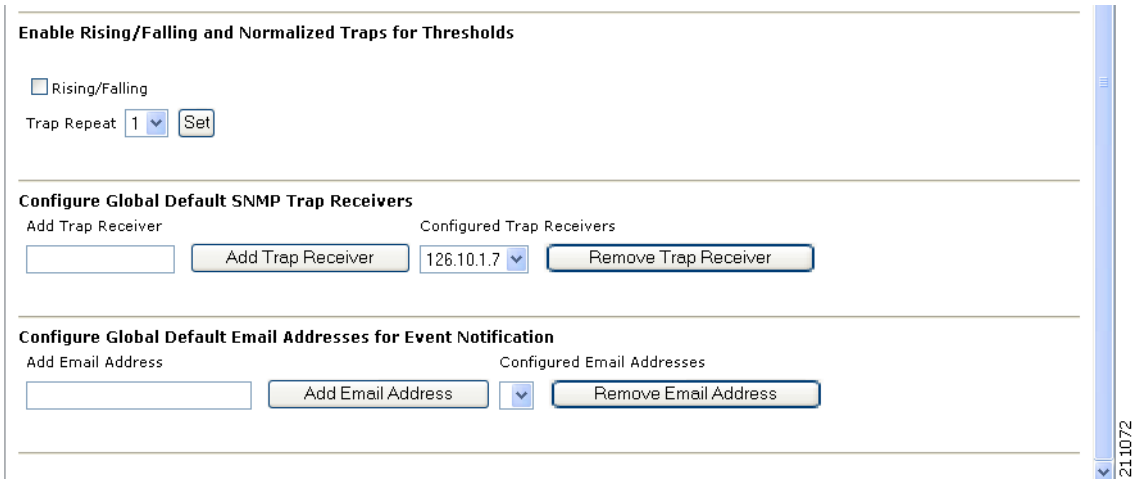
Step 5 To add or remove trap receivers, use the **Configure Global Default SNMP Trap Receivers** section. The SNMP trap receivers specified here are only used if domain-specific SNMP trap receivers are not specified. Domain-specific trap receivers are specified from the Trap Receiver/Email Polling Configuration 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.

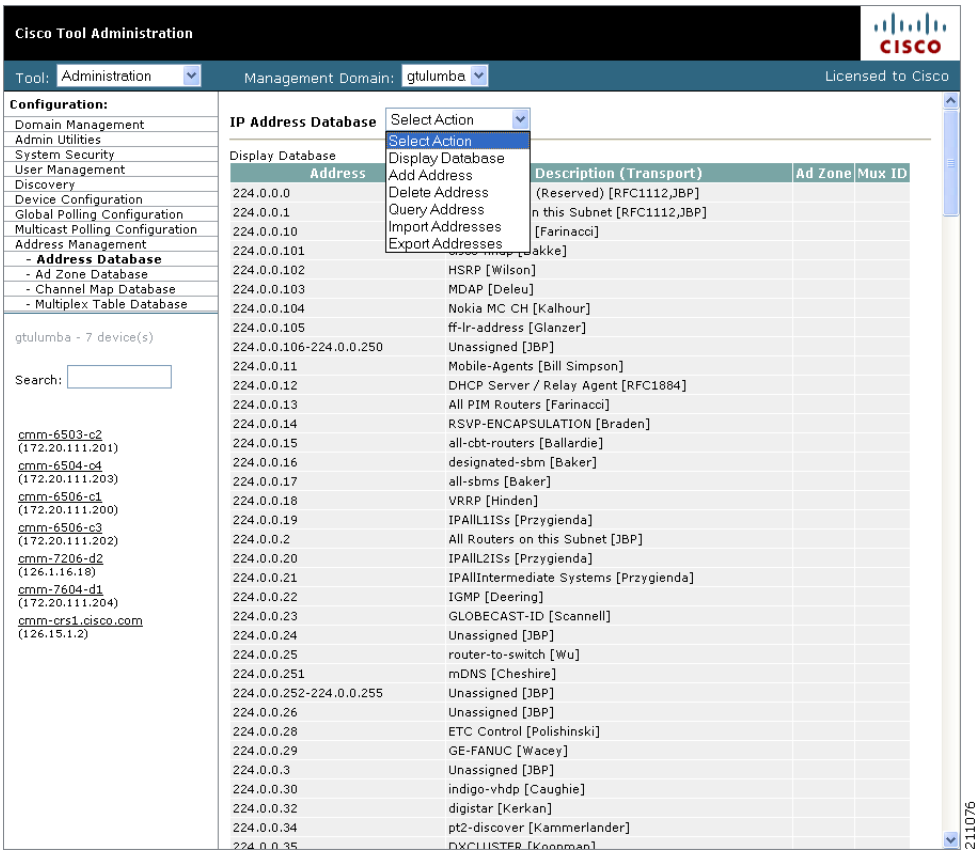
Step 2 Select **Address Management > Address Database.**

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, 1. From the drop-down menu in the IP Address Database field, select **Delete Address**. The Delete Address page appears. 2. From the drop-down list in the Address field, select the address to delete. You are prompted to delete the address. 3. To delete the address click **OK**.

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

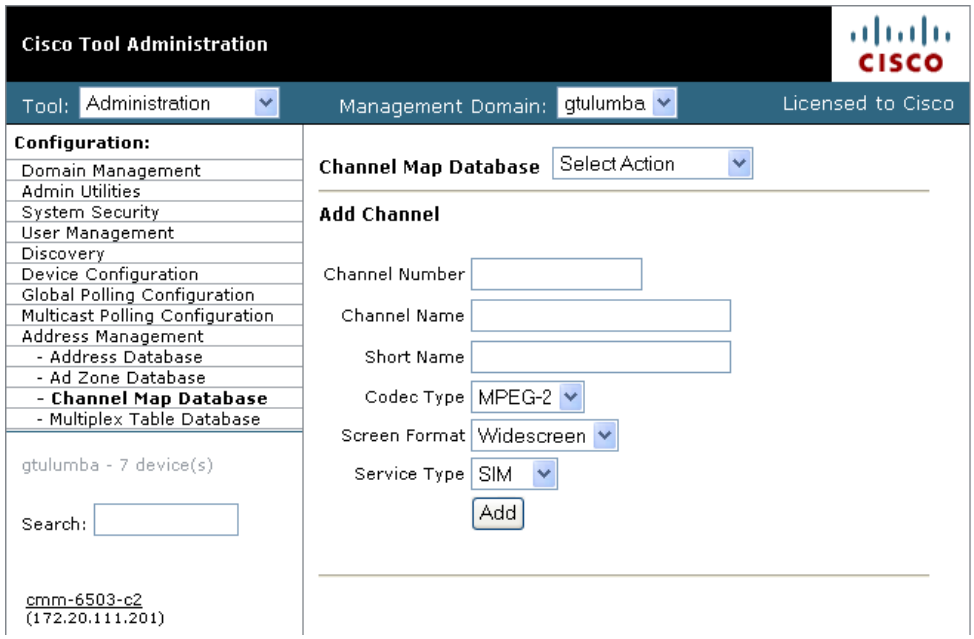
The Channel Map Database page opens.

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).

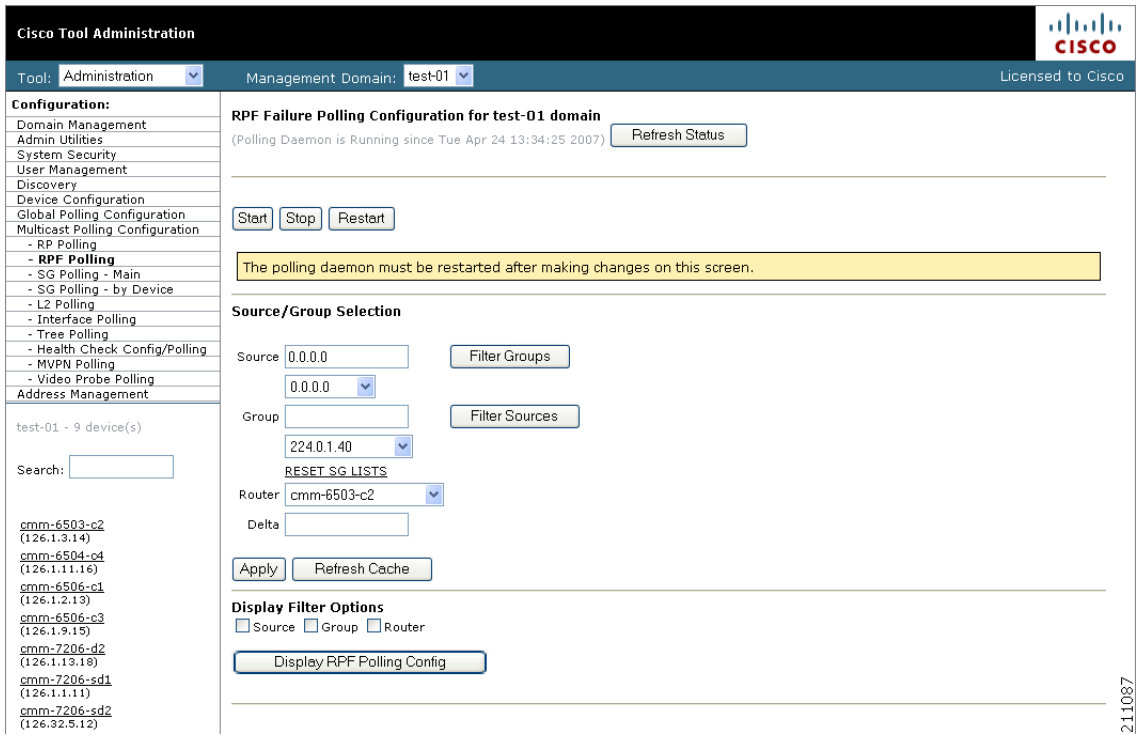
To configure RP polling:

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



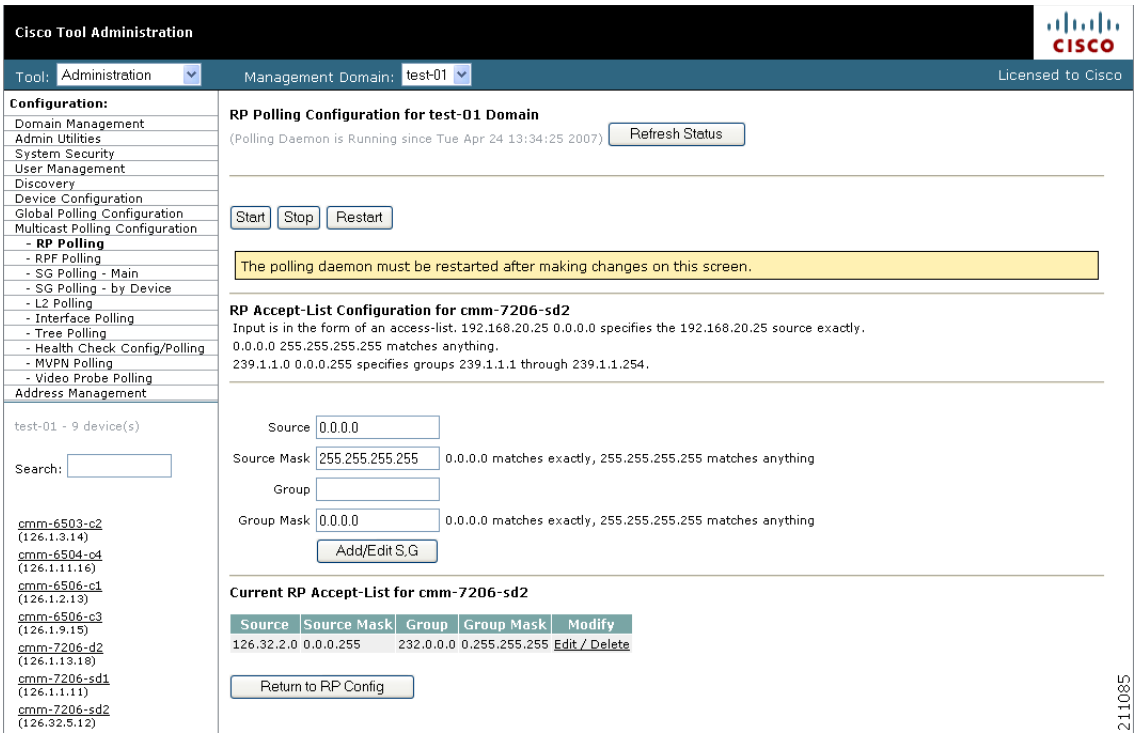
The RP Polling Configuration page contains the following fields and buttons:

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. 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 3-8).
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 2-28). • **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**.

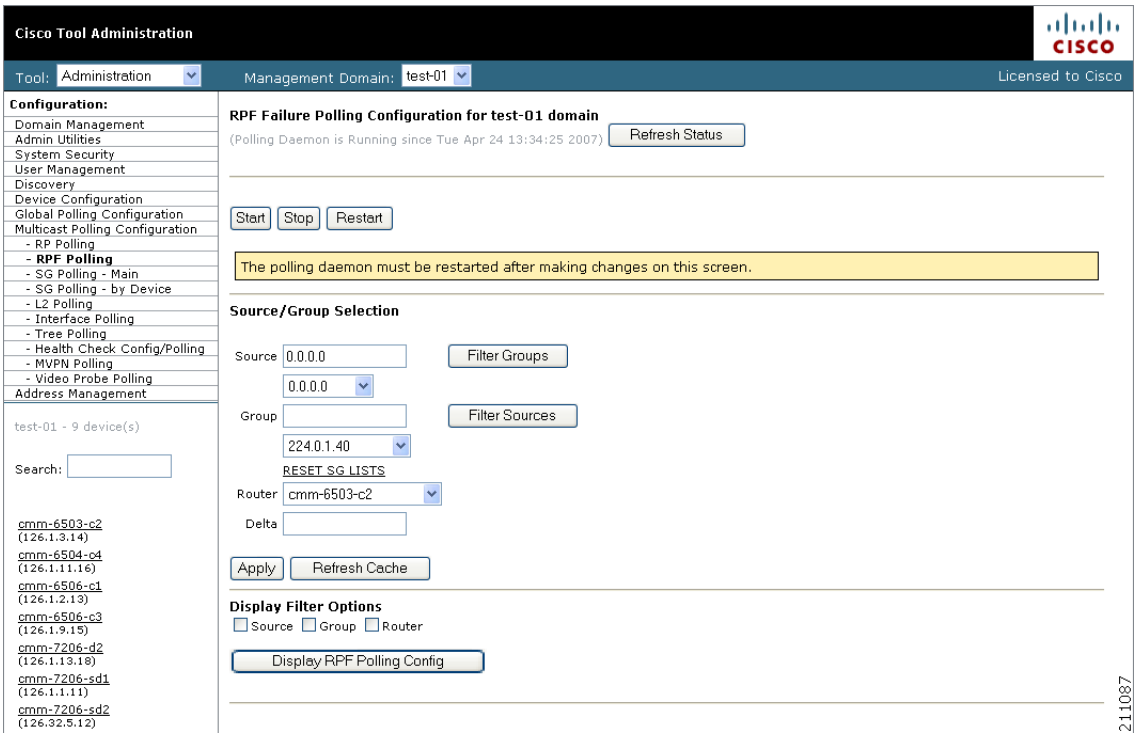
To configure RPF polling:

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: 1. Click **Display RPF Polling Configuration** You can filter the configuration display by source, group, or router. A list of the current RPF polling configuration appears. 2. To edit a configuration, click **Edit** at the right of the summary row for the configuration. 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.

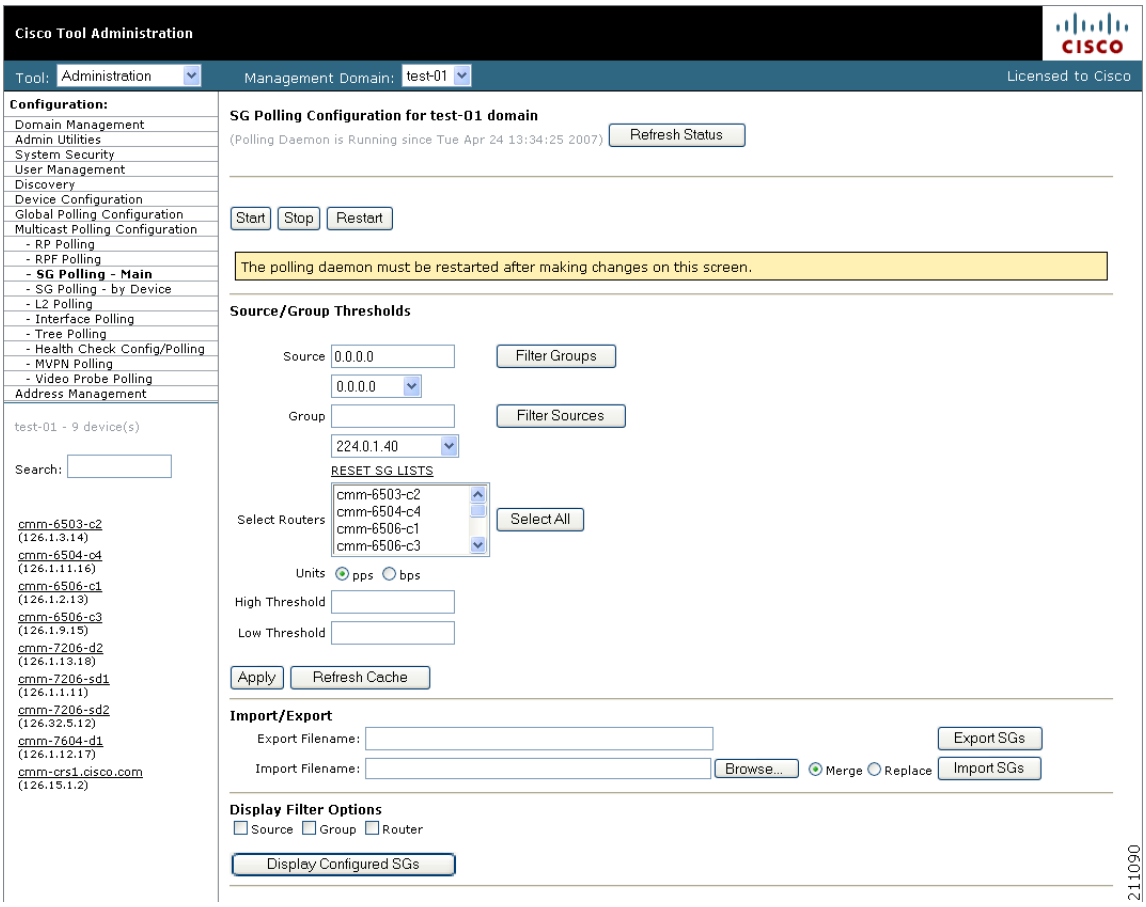
To configure SG polling:

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



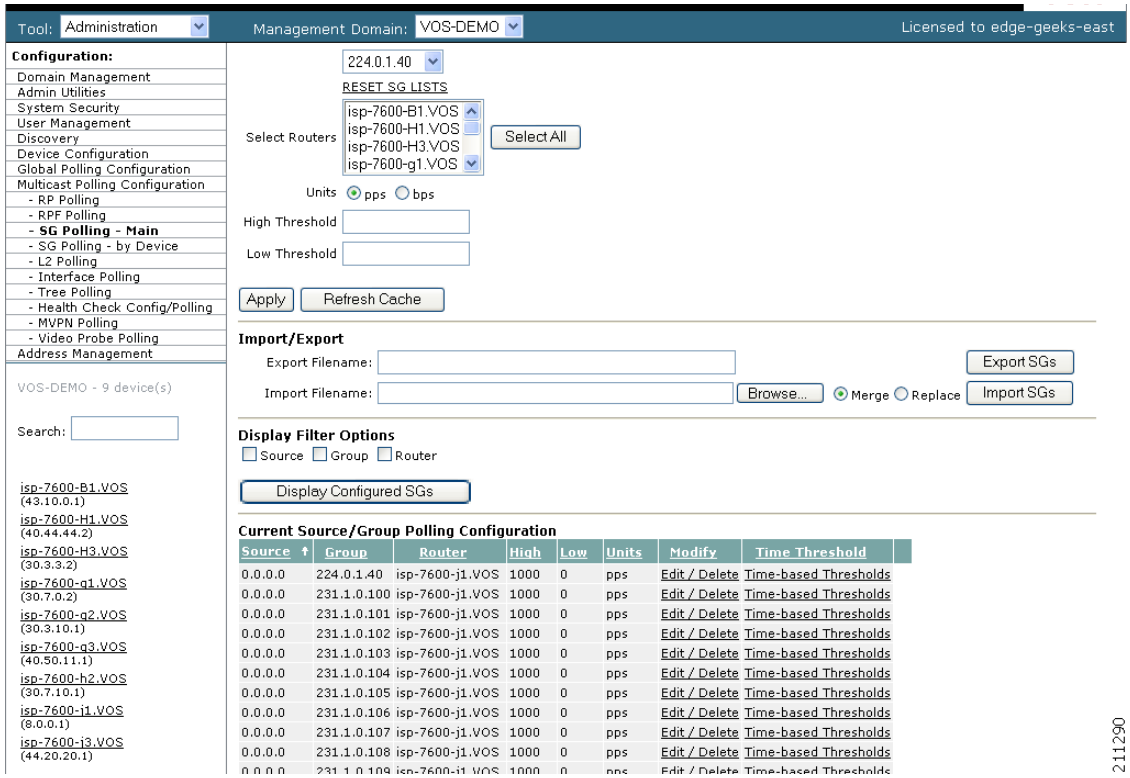
The SG Polling Configuration page contains the following fields and buttons:

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.

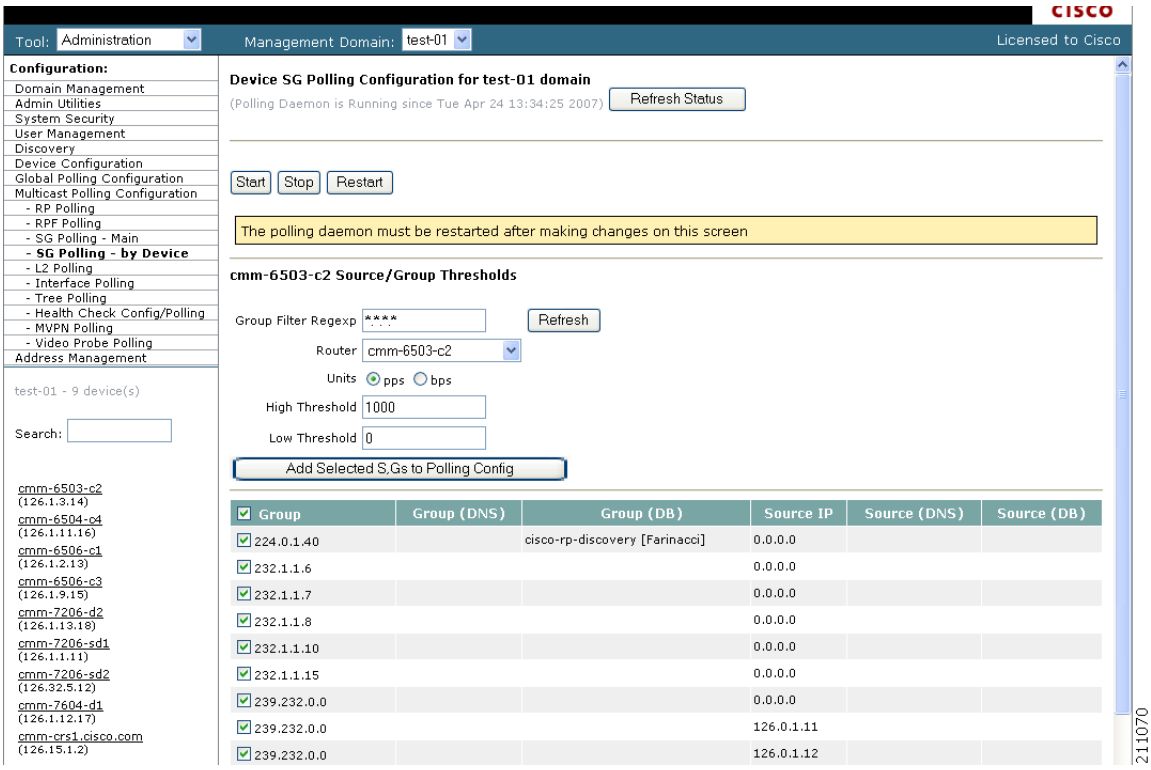
To configure SG polling for a particular device:

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.

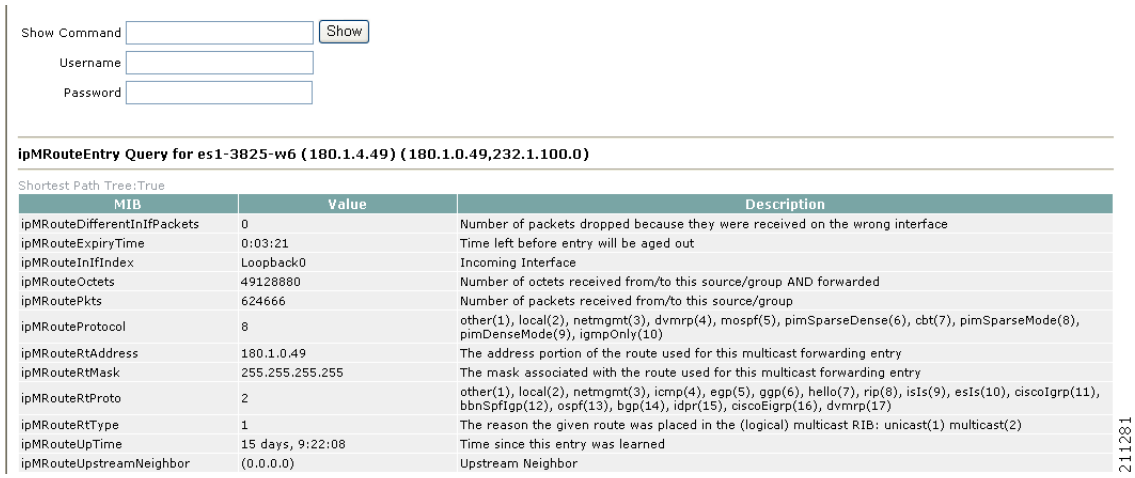
To configure Layer 2 switch polling:

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.

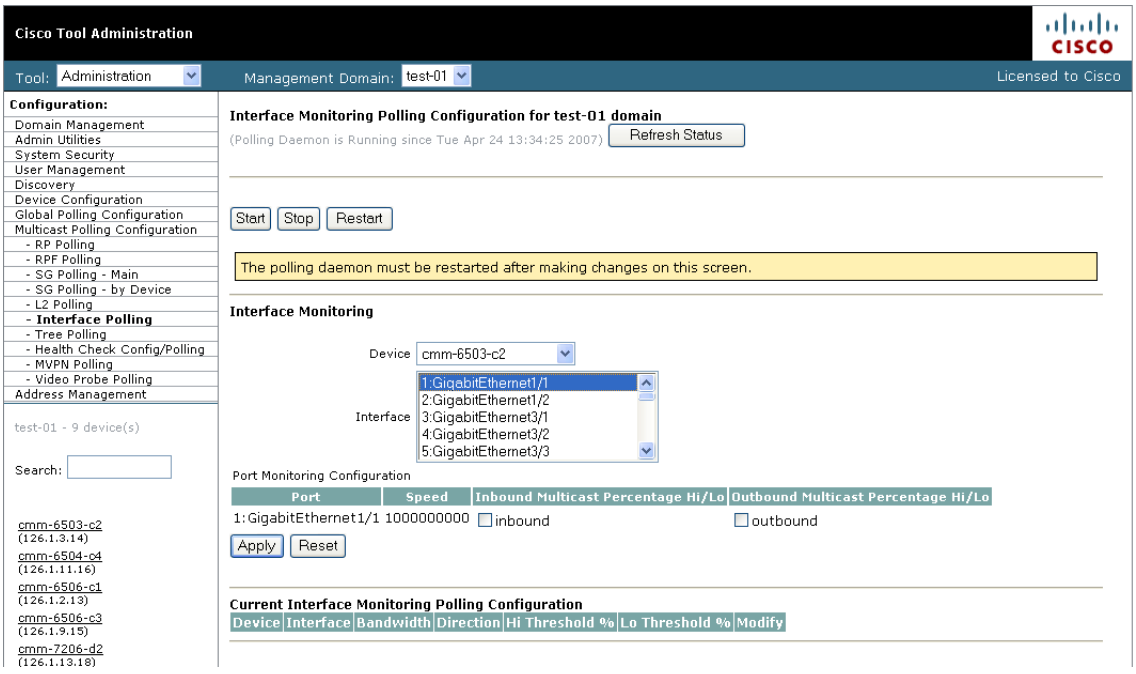
Step 2 Select **Multicast Polling Configuration > Interface Polling.**

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.

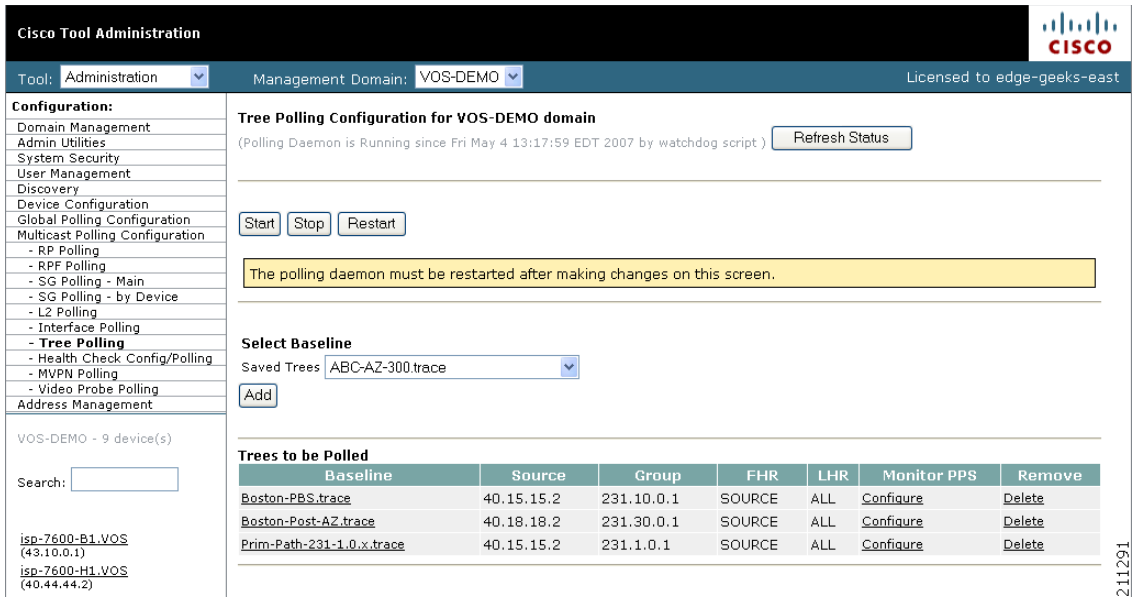
To configure tree polling:

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

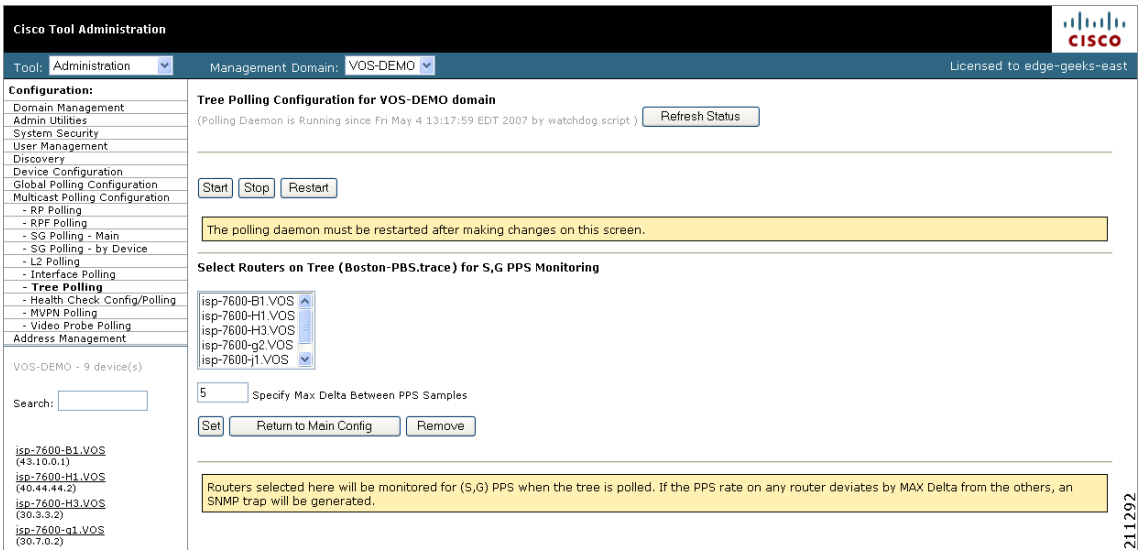
Selecting Trees To Be Polled

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.

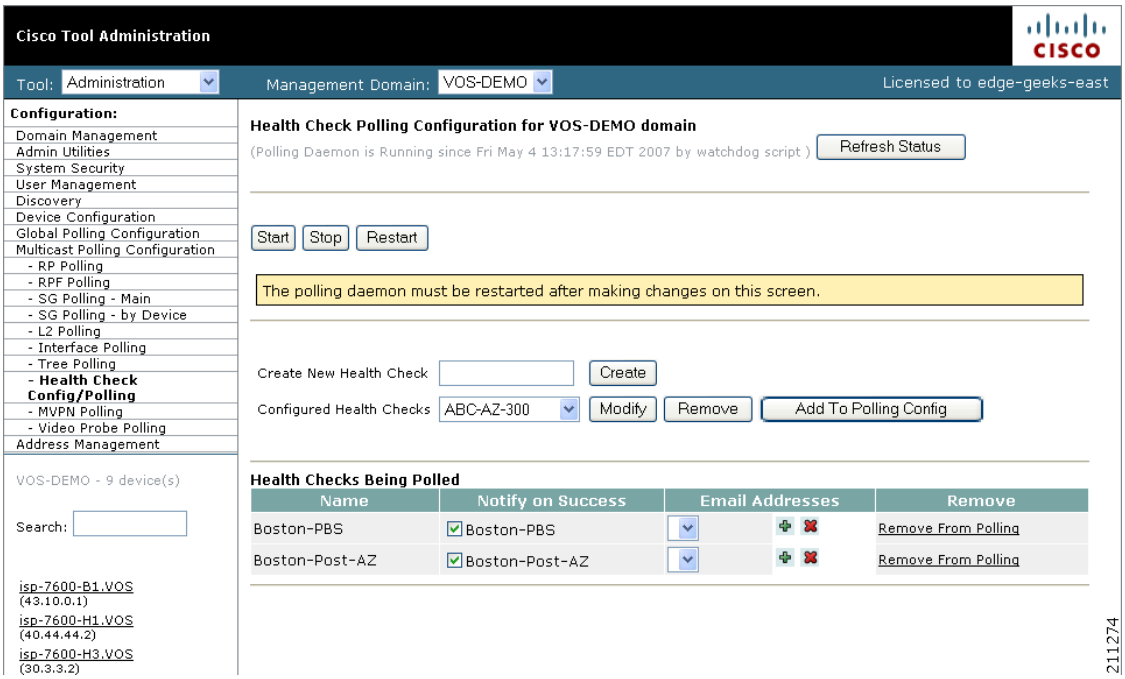
To configure health check polling:

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

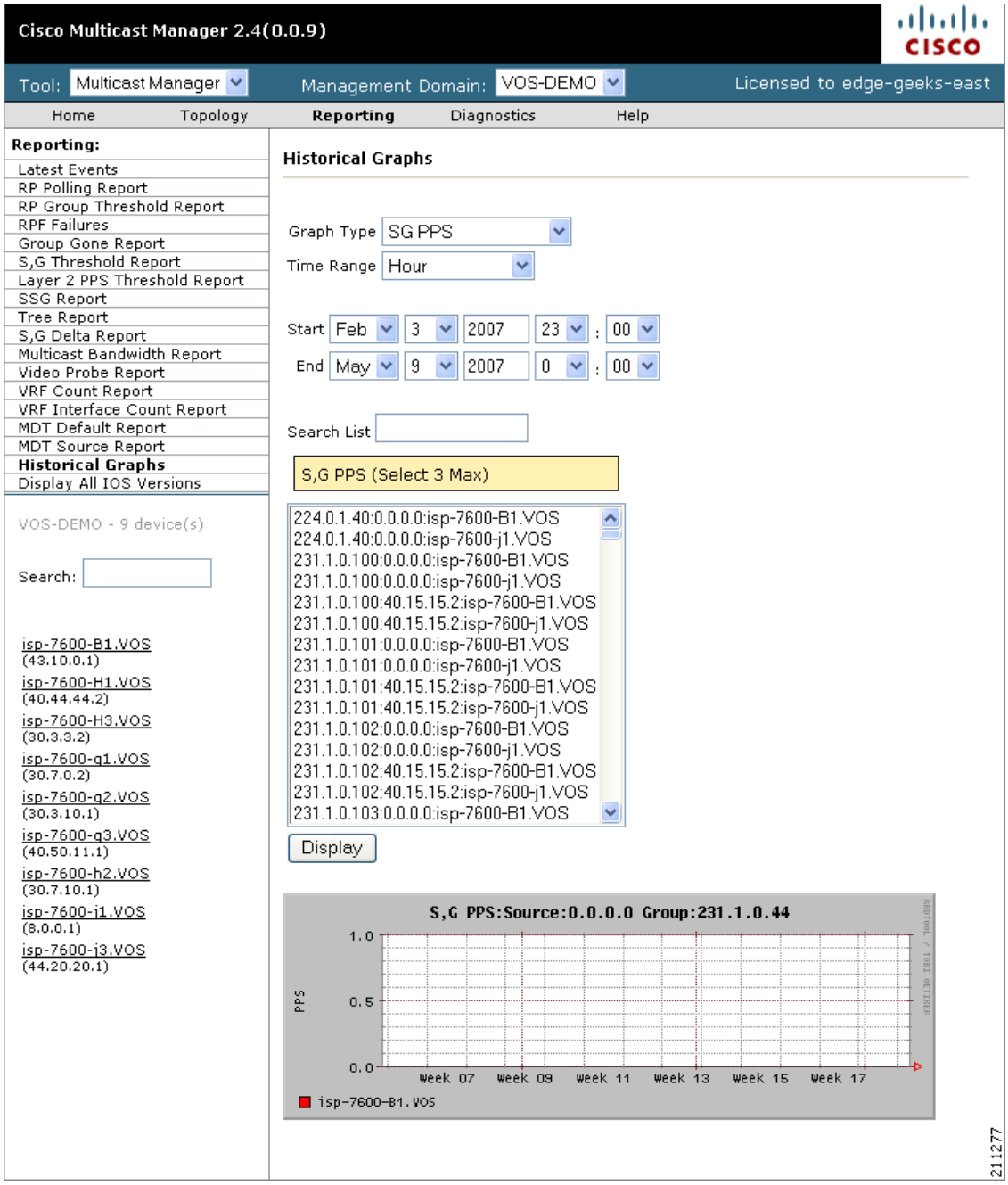
If you click **Modify** on the Health Check Configuration page to select a health check to change, the Health Check Configuration page displays information about the currently configured health checks.

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



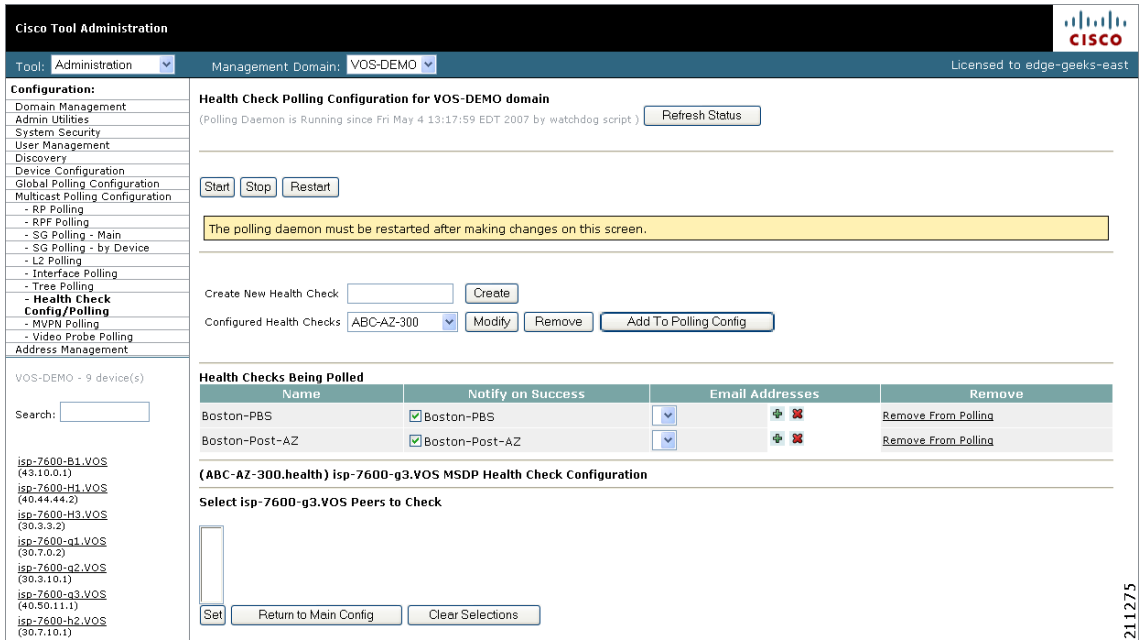
Step 3 From the drop-down list in the Configured Health Checks field, select the RPs that you want this health check to include.:

- 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.

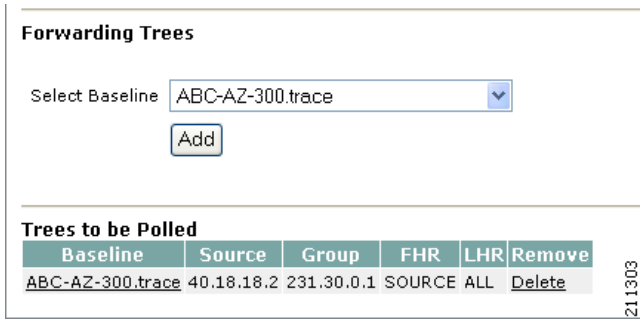
Step 6 Select the sources and groups to check.

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).

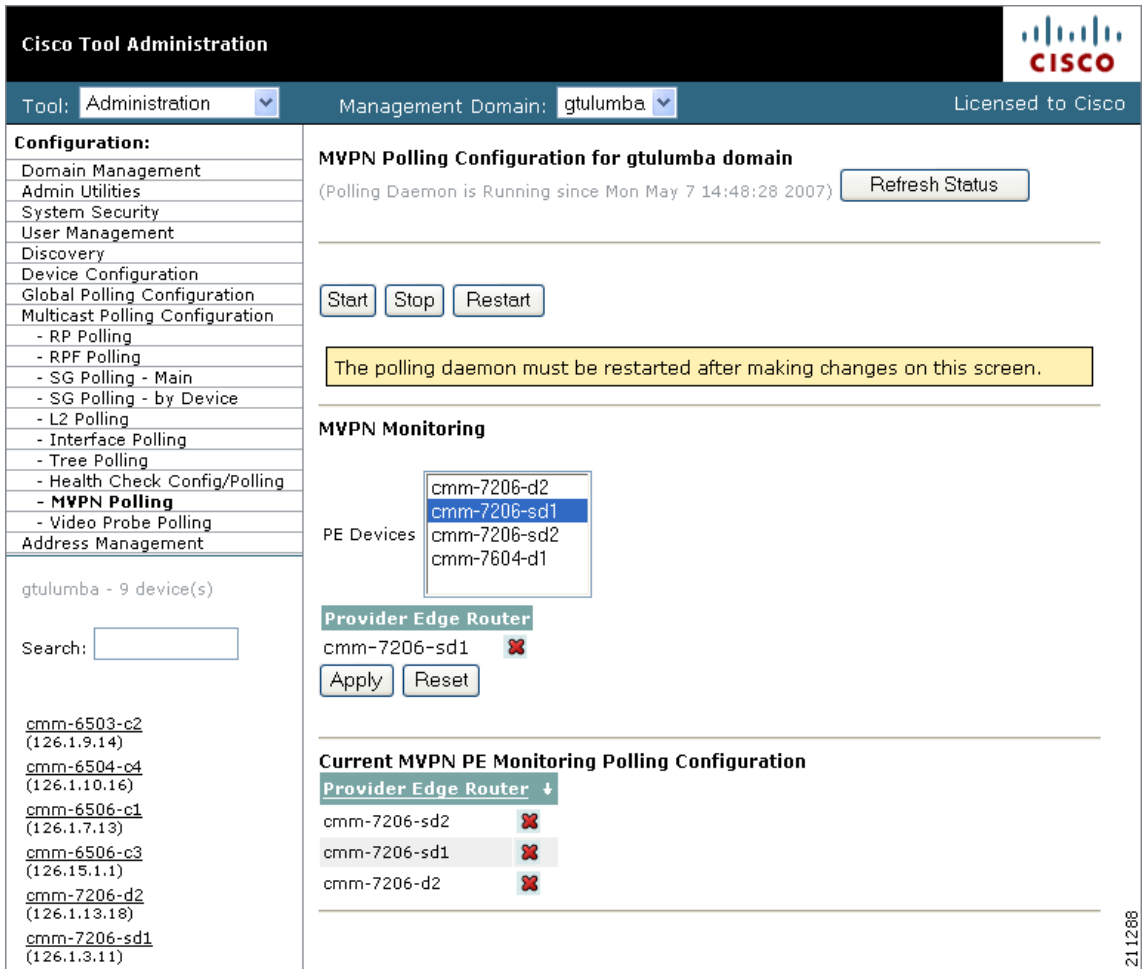
To configure MVPN polling:

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.

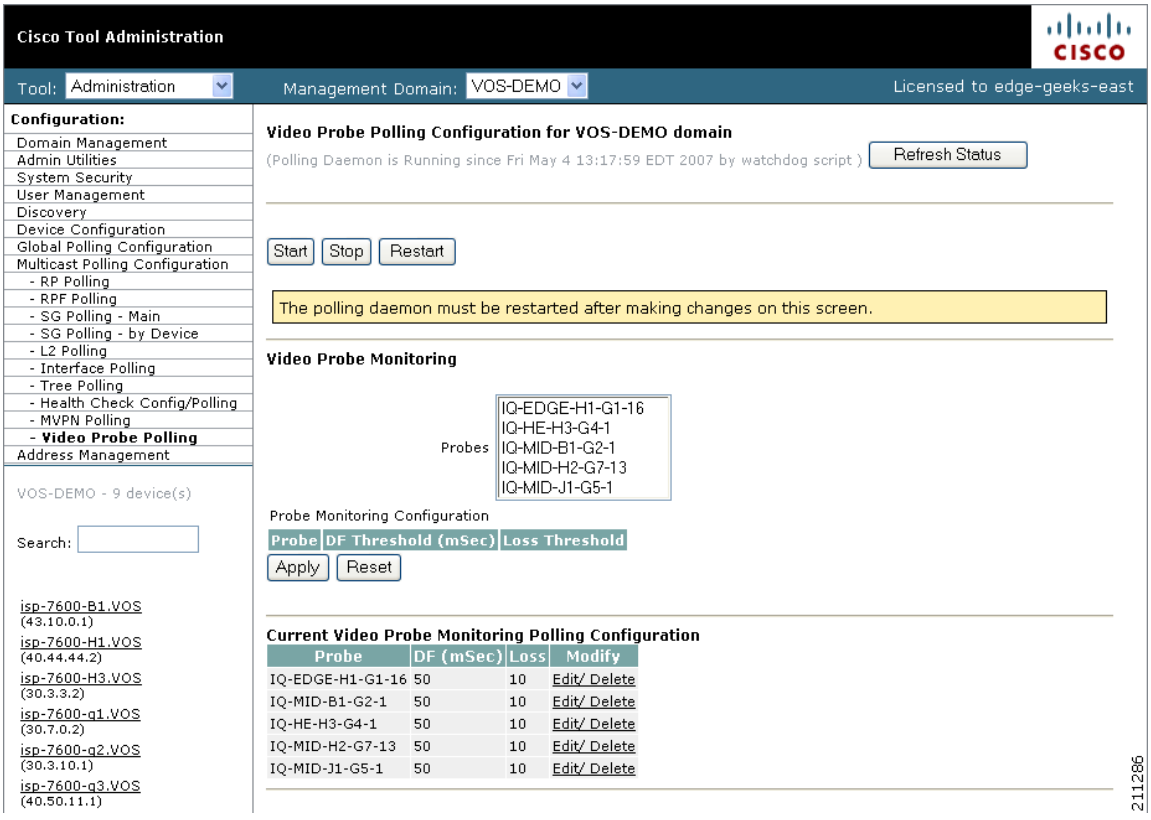
You can configure one video probe or configure several video probes at the same time.

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.

CHAPTER 3

Monitoring with the Multicast Manager Tool

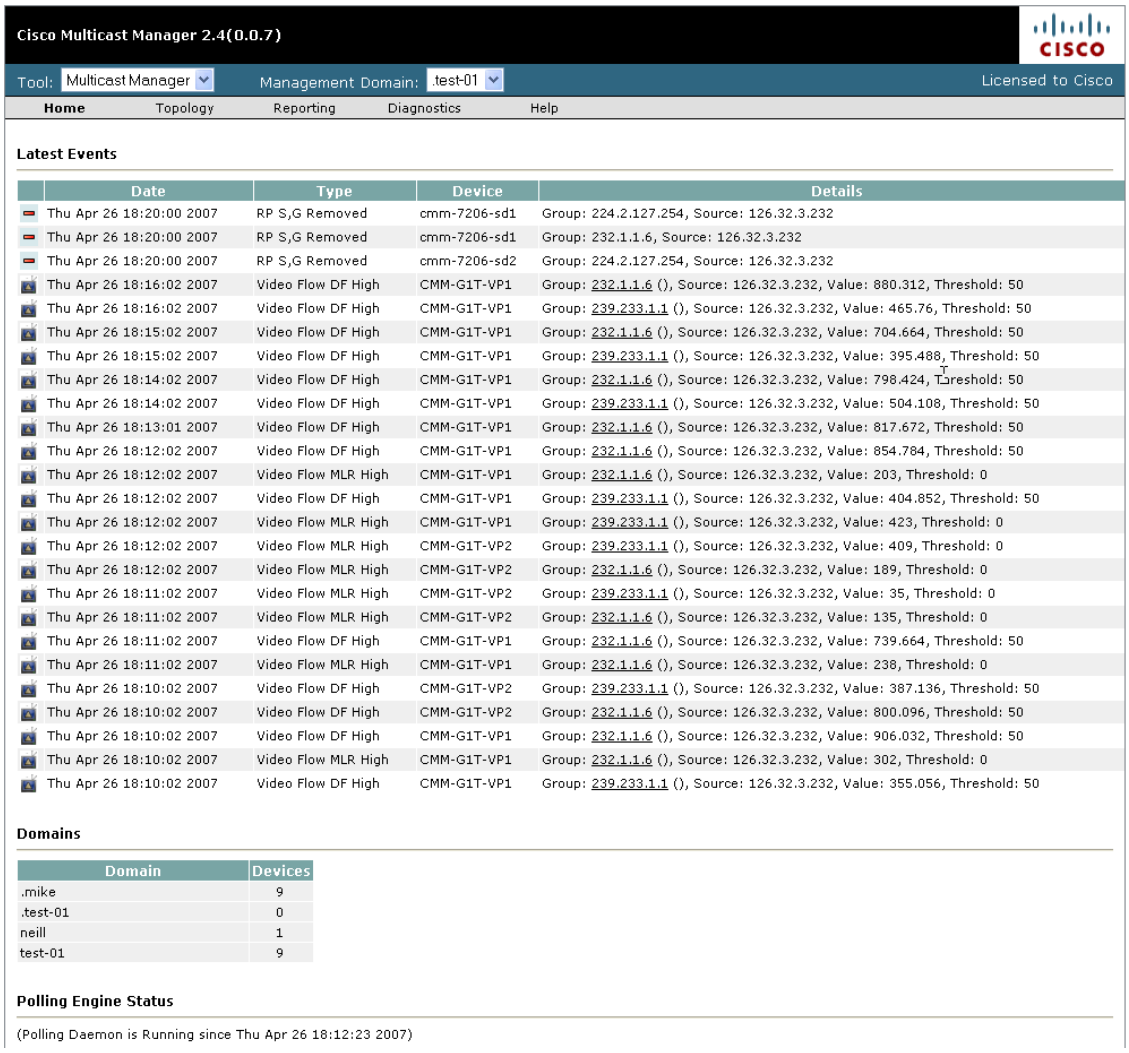
This chapter contains the following sections:

Viewing the Multicast Manager Home Page

When you log into the CMM, the Multicast Manager Home Page opens. To access this page from within the CMM, select the **Multicast Manager** tool, then select **Home**.

The **Home** page shows the last 20 events (see the "Latest Events" section on page 3-7).

Figure 3-1 Multicast Manager Home Page



Viewing Topology

Using **Topology**, you can display routers and their multicast information in the database, on an individual basis, or by showing the complete database.

If you are using video probes in your installation, the Cisco Multicast Manager home page displays threshold exceeded alerts that the probes generate. You can click on the group information in the alert (an underlined IP address) to launch the Diagnostics tool and view detailed information about the multicast, which includes a display of the network topology that includes both routers and probes.

This section contains:

Viewing Router Topology and Multicast Information

To view router topology and multicast information:

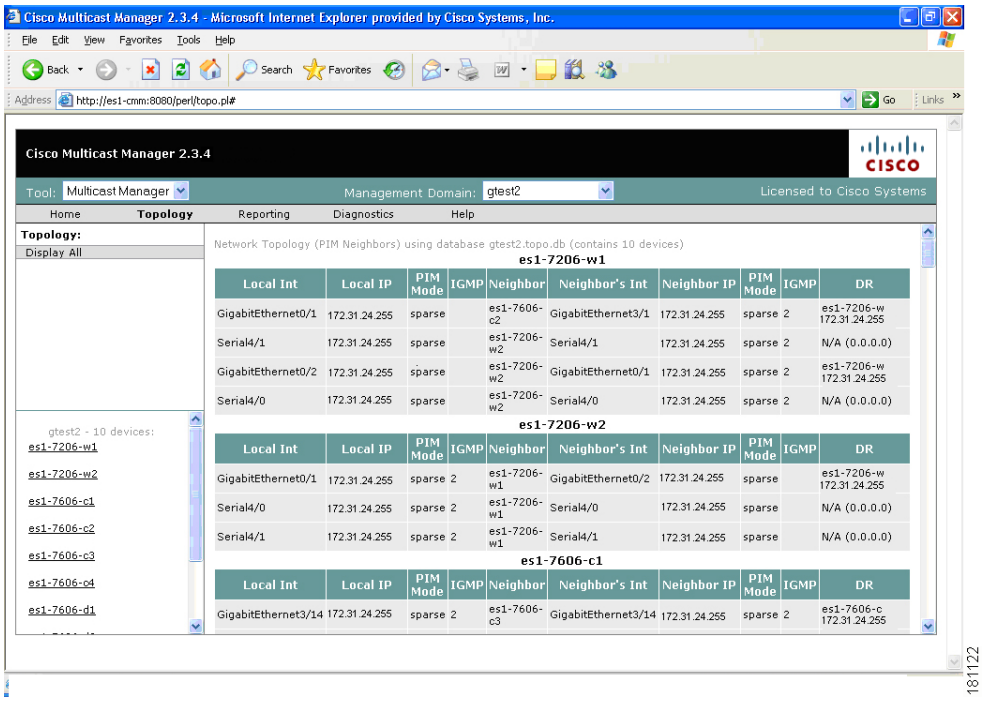
Step 1 Select the **Multicast Manager** tool.

Step 2 Click **Topology**.

Step 3 To see the complete database, select **Display All**.

A network topology table appears, as shown in Figure 3-2. Router names appear at the top of each table.

Figure 3-2 Topology Display All

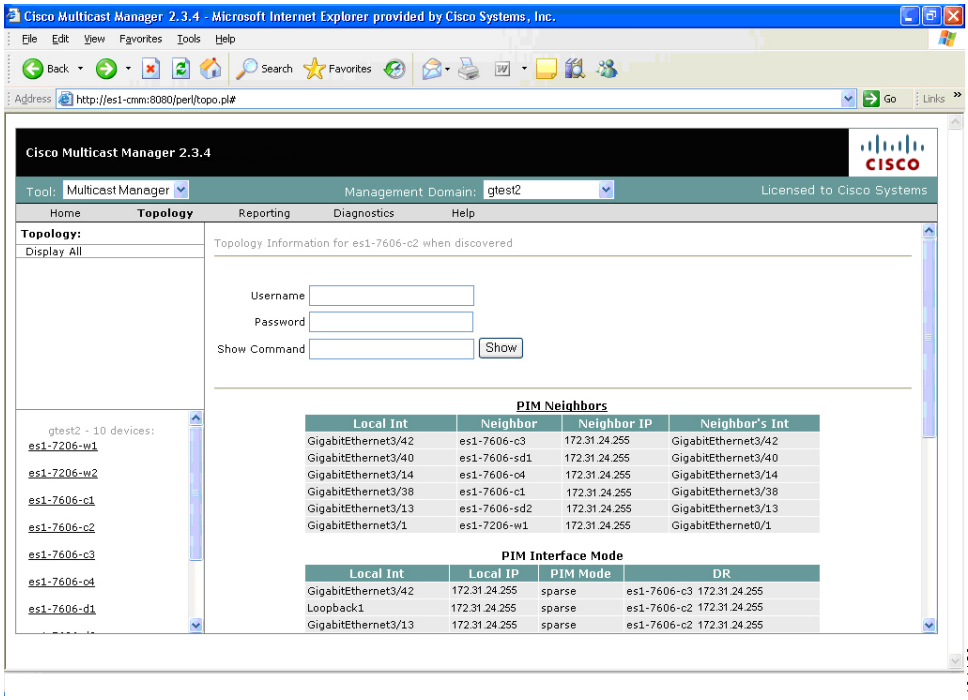


For each device, the table shows the following information:

Field	Description
Local Int	Interfaces running multicast.
Local IP	IP address of the interfaces.
PIM Mode	PIM Mode, can be sparse or dense.
IGMP	IGMP version.
Neighbor	PIM neighbor name.
Neighbor's INT	PIM neighbor's interface.
Neighbor IP	PIM neighbor's IP address.
PIM Mode	PIM neighbor's mode, can be sparse or dense.
IGMP	IGMP version of PIM neighbor.
DR	DR information.

Step 4 To see topology for an individual router, click a router from the list pane at the lower left of the interface. Topology information for the selected device appears, as shown in Figure 3-3.

Figure 3-3 Topology for an Individual Router



The topology display contains these fields and buttons:

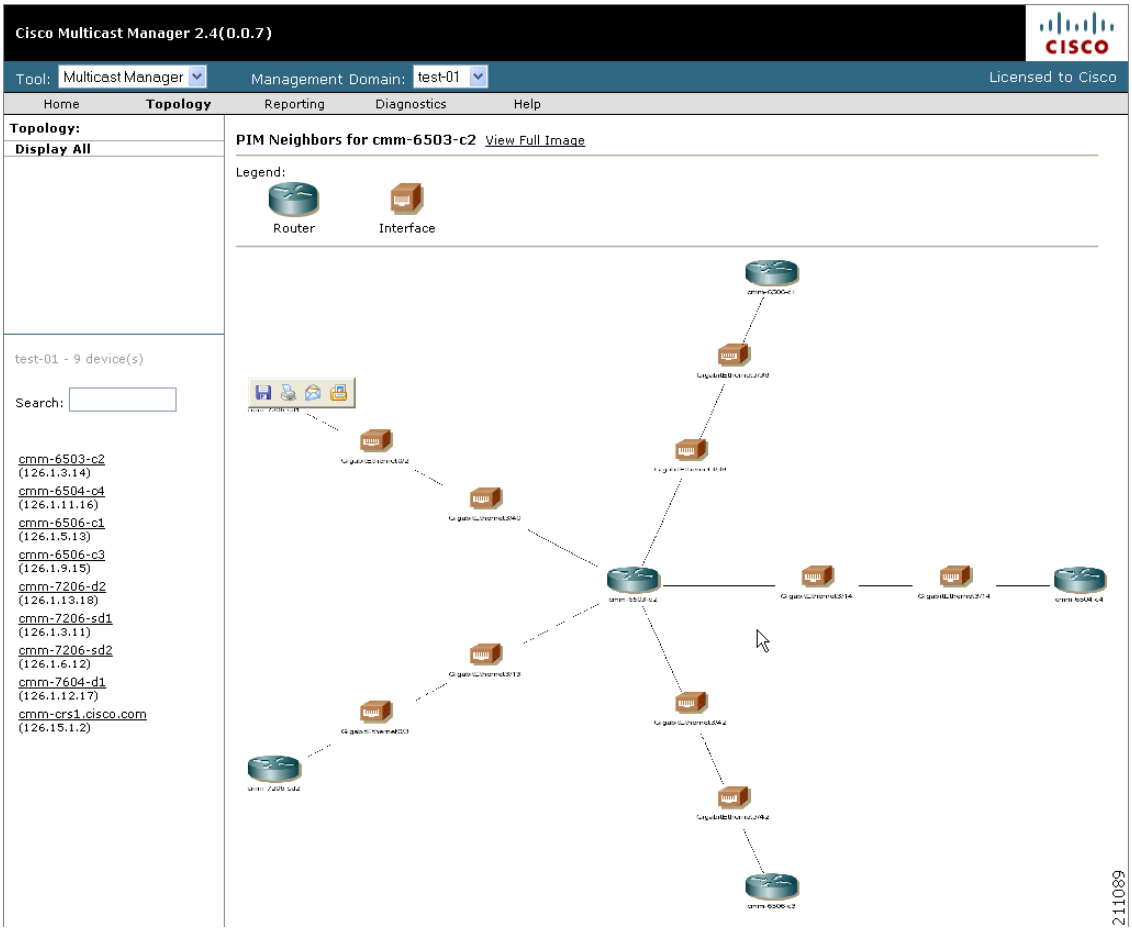
Field or Button	Description
Username	Enter your username.
Password	Enter your password.
Show Command	Enter any show commands on the router.
Show	Click **Show** to run the selected command.
PIM Neighbors	PIM neighbor name.

Note For details on the columns within this table, see the descriptions for the Topology Display All window.

Step 5 To see a topological display of the routers, select **PIM Neighbors**.

A topological display appears, as shown in Figure 3-4.

Figure 3-4 PIM Neighbors



The topology display shows:

- Each router and its local interfaces.
- The interfaces on each of the router's PIM neighbors.
- The names of the routers and their PIM neighbors.

Viewing Topology Including Probe Information

You can view topology information that shows probes and probe status from the Cisco Multicast Manager home page and from the Diagnostics tool.

The multicast diagnostic information shown on the home page includes:

- The source, group, and channel association that you are troubleshooting.
- A graphical topology tree that clearly shows all of the routers that form the tree, and their input and output interfaces. along with IP addresses and interface descriptions

- The packets per sampling period being received at each point in the tree (sampling periods range from 5 seconds to 30 and are configurable).
- The packet input, output and discard errors being received at each interface.
- A text representation of the tree, which is invaluable when troubleshooting large multicast trees.

Note For detailed information on using the Diagnostic tool to troubleshoot video multicast flows and viewing a topology tree that shows the multicast topology, see Video Probe Status, page 4-15.

Managing Reports

To start managing reports, within the **Multicast Manager** tool, click on **Reporting**.

Within Reporting, you can view:

- A record of the latest SNMP traps sent.
- Historical graphs or trends.
- Routers in the database IOS versions.
- Video probe reports.
- Reports on VPN routing/forwarding instances (VRFs).

Reporting Options
Latest Events, page 3-7
RP Polling Report, page 3-7
RP Group Threshold Report, page 3-8
RPF Failures, page 3-9
Group Gone Report, page 3-9
S,G Threshold Report, page 3-10
Layer 2 PPS Threshold Report, page 3-10
SSG Report, page 3-10
Tree Report, page 3-10
S,G Delta Report, page 3-12
Multicast Bandwidth Report, page 3-12
Video Probe Report, page 3-12
VRF Count Report, page 3-14
VRF Interface Count Report, page 3-14
MDT Default Report, page 3-15
MDT Source Report, page 3-15
Historical Graphs, page 3-15
Display All IOS Versions, page 3-17

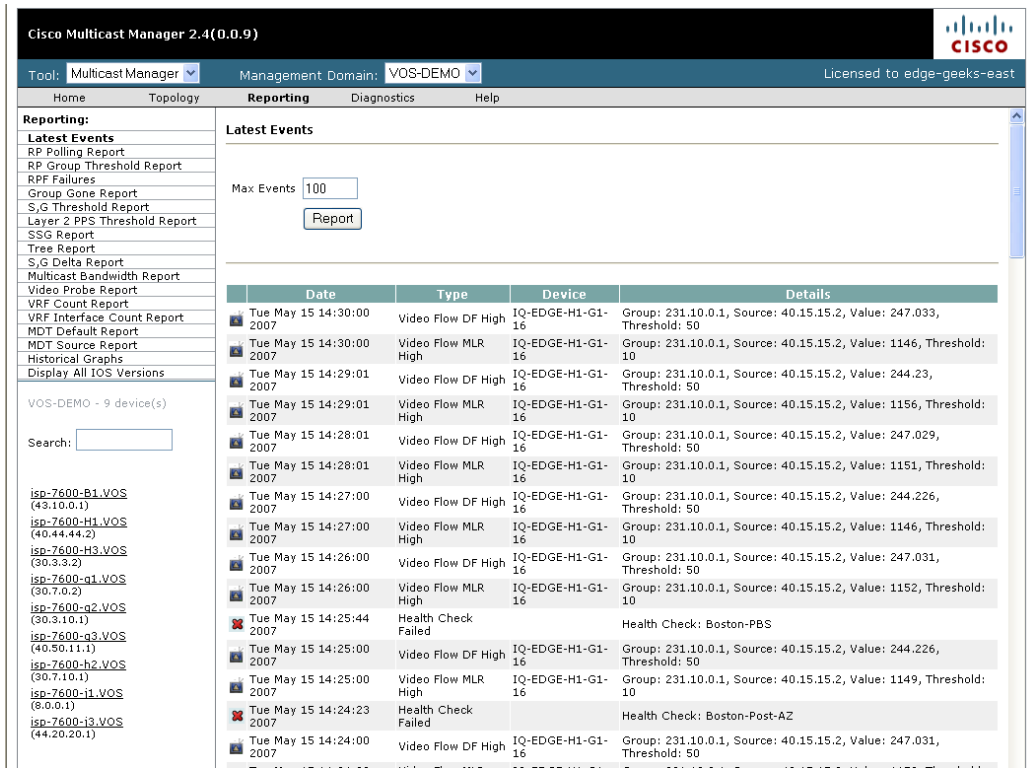
Note The information shown for each type of report, with the exception of Historical Graphs, spans only the previous 24 hours. There may be more information available in the log file. However, it is recommended that the events.log file be rotated every 24 to 48 hours, depending on event activity.

Latest Events

Using the **Latest Events** page, you can set a configurable amount of the latest events generated by the CMM. Clicking **Report** lists the traps in time order.

Figure 3-5 shows the Latest Events page.

Figure 3-5 Latest Events



RP Polling Report

Using the **RP Polling Report**, you can monitor:

- All leaves and joins for the selected RP (if the Enable RP Add/Delete Traps option is selected, see the "RP Polling" section on page 2-26).
- If the selected RP becomes unavailable.
- Any rogue source or group that joins the selected RP.

To generate an RP Polling report:

Step 1 Select the **Multicast Manager** tool.

On the Reporting menu, select **RP Polling Report**.

The RP Polling Report page opens.

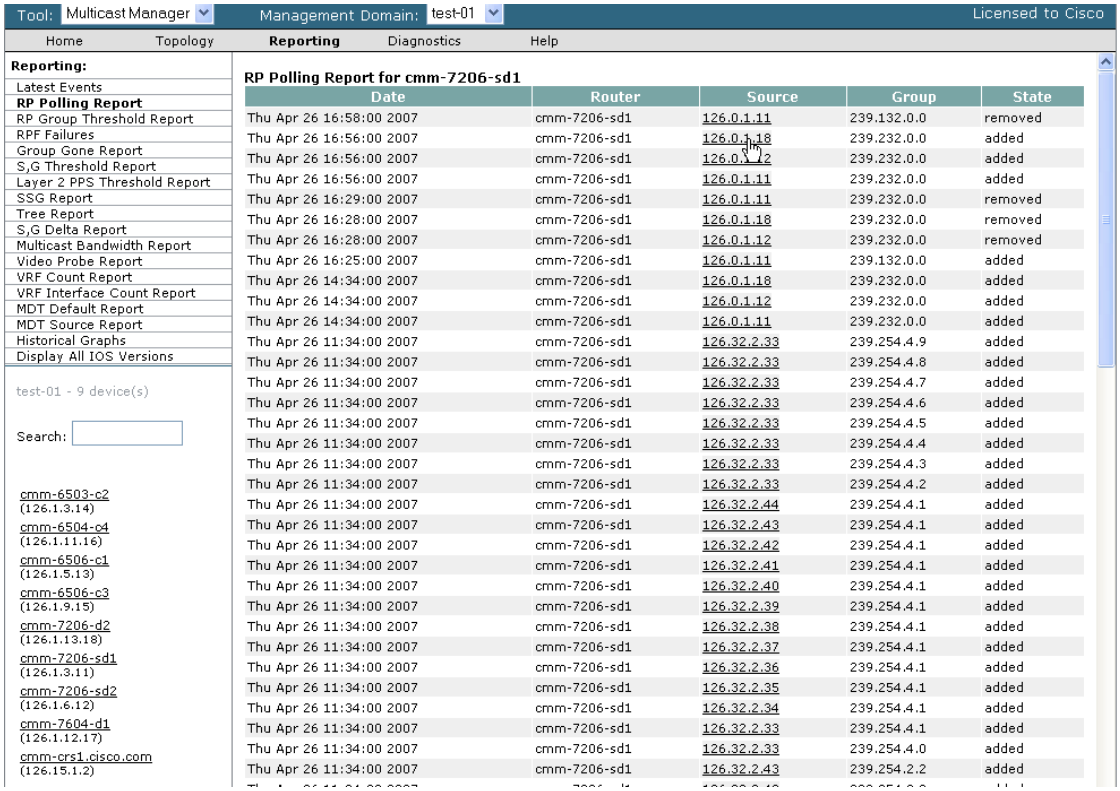
Step 2 On the RP Polling Report page:

- Select an RP from the list.
- Specify the maximum number of events to display.

Step 3 Click **Report**.

An RP Polling Report appears, as shown in Figure 3-6. The report contains any events that have occurred in the last 24 hours.

Figure 3-6 RP Polling Report



Step 4 To see detailed information about a source, click on an IP address in the **Source** column.

RP Group Threshold Report

Using the **RP Group Threshold Report**, you can monitor a list of RPs that have exceeded their active number of groups limit.

To generate an RP Group Threshold report:

Step 1 Select the **Multicast Manager** tool.

Step 2 On the Reporting menu, select **RP Group Threshold Report**.

The RP Group Threshold Report page opens.

Step 3 On the RP Polling Report page:

- Select an RP from the list.
- You can specify the maximum number of events to display.

Step 4 Click **Report**.

An RP Group Threshold Report appears.

Step 5 The report contains any events that have occurred in the last 24 hours.

RPF Failures

Using the **RPF Failures Report**, you can monitor all routers that are experiencing RPF failures above the configured threshold for the configured sources and groups.

To generate an RPF Failures report:

Step 1 Select the **Multicast Manager** tool.

Step 2 On the Reporting menu, select **RPF Failures**.

The RPF Failure Report page opens.

Step 3 On the RPF Failure Report page:

- Select an RP from the list.
- You can specify the maximum number of events to display.

Step 4 Click **Report**.

The report contains any events that have occurred in the last 24 hours.

Group Gone Report

The **Group Gone Report** is currently unsupported. Please refer to the **S,G Polling Report** (see S,G Threshold Report, page 3-10).

S,G Threshold Report

Using the **S,G Threshold Report**, you can monitor every source and group that has exceeded its configured threshold.

To generate an S,G Threshold report:

Step 1 Select a group from the list.

Step 2 You can specify the maximum number of events to display.

Step 3 Click **Report**. The report contains any events that have occurred in the last 24 hours, and shows pps and bps.

Layer 2 PPS Threshold Report

Using the **Layer 2 PPS Threshold Report**, you can monitor all Layer 2 ports that have exceeded their configured thresholds.

To generate a Layer 2 PPS Threshold Report:

Step 1 Select a switch from the list.

Step 2 Select a port from the list.

Step 3 Click **Select**. The report contains any events that have occurred in the last 24 hours.

Note The report is for inbound and outbound traffic on the port.

SSG Report

Using the **SSG Report**, you can display information about groups that have more than one sender.

To generate an SSG Report:

Step 1 Enter the multicast group address.

Step 2 Click **Report**. The report contains any events that have occurred in the last 24 hours. The count indicates the number of sources sending to the group.

Tree Report

Using the **Multicast Tree Report**, you can draw and save multicast trees (called baselines). You can then set up the CMM to draw trees that have been saved in the background, and report any changes. (Only changes to Layer 3 devices are reported.)

Note The drawing and saving of trees is covered in Show All Groups, page 4-2.

If a multicast tree you are monitoring changes, a trap is generated. You can then view the baseline and the changed tree. Changes are highlighted in the text and also in the drawing.

To generate a Multicast Tree Report:

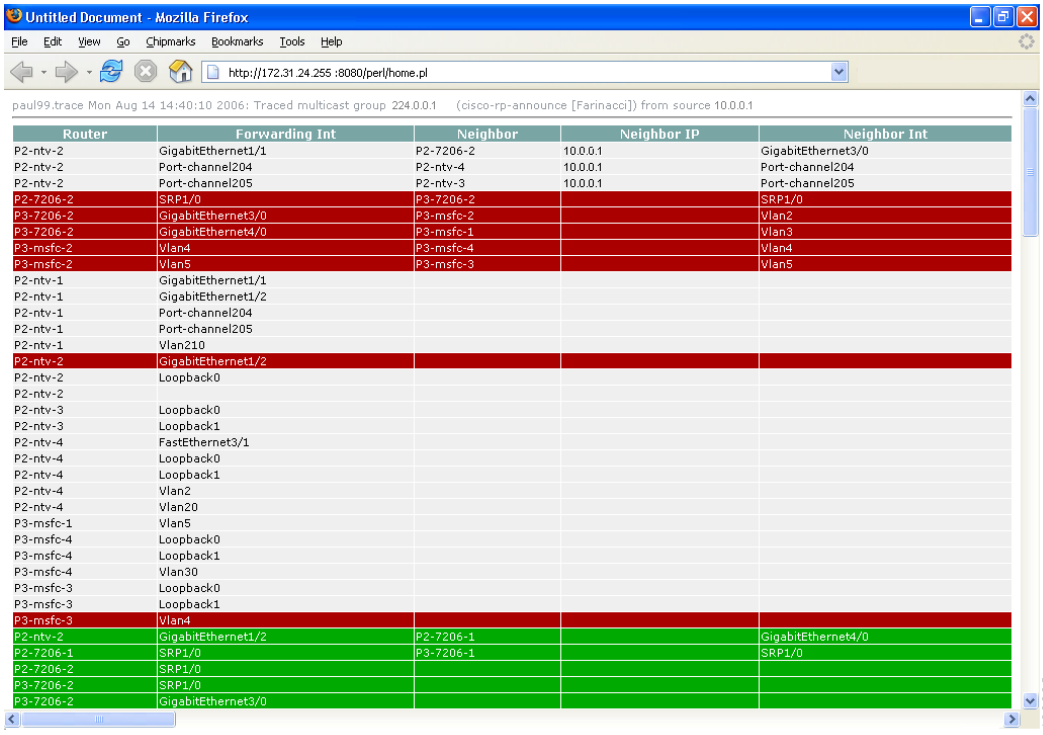
Step 1 Select a baseline (multicast tree) from the list.

Step 2 You can specify the maximum number of events to display.

Step 3 Click **Select**. The report contains any events that have occurred in the last 24 hours.

Selecting "trchanged" in the third column in the report will graphically show the baseline, along with the changed tree. Changes to the tree are highlighted in the table at the top as shown in the figure. The baseline and the current tree are also shown graphically.

Figure 3-7 Tree Report Page with Changed Tree Data



S,G Delta Report

Using the **Multicast S,G Delta Report**, you can view information about PPS rate deviation on multicast trees.

To generate a Multicast S,G Delta Report:

Step 1 Select a baseline (multicast tree) from the list.

Step 2 You can specify the maximum number of events to display.

Step 3 Click **Select**. The report contains any events that have occurred in the last 24 hours.

Multicast Bandwidth Report

To generate a report for a router interface that has exceeded its multicast bandwidth thresholds:

Step 1 Select the device.

Step 2 Select the port.

Step 3 Select the maximum number of events.

Step 4 Click **Report**.

Video Probe Report

Each time CMM interrogates a probe and finds an exception it generates a video probe report and stores it on the hard drive. Using the Video Probe Report, you can view a detailed listing of video probe reports. Each report provides the following information from a video probe:

- **VOS flow MRL high**—The media loss rate (MLR) over the configured threshold
- **VOS delay factor high**—The delay factor (DF) over the configured threshold

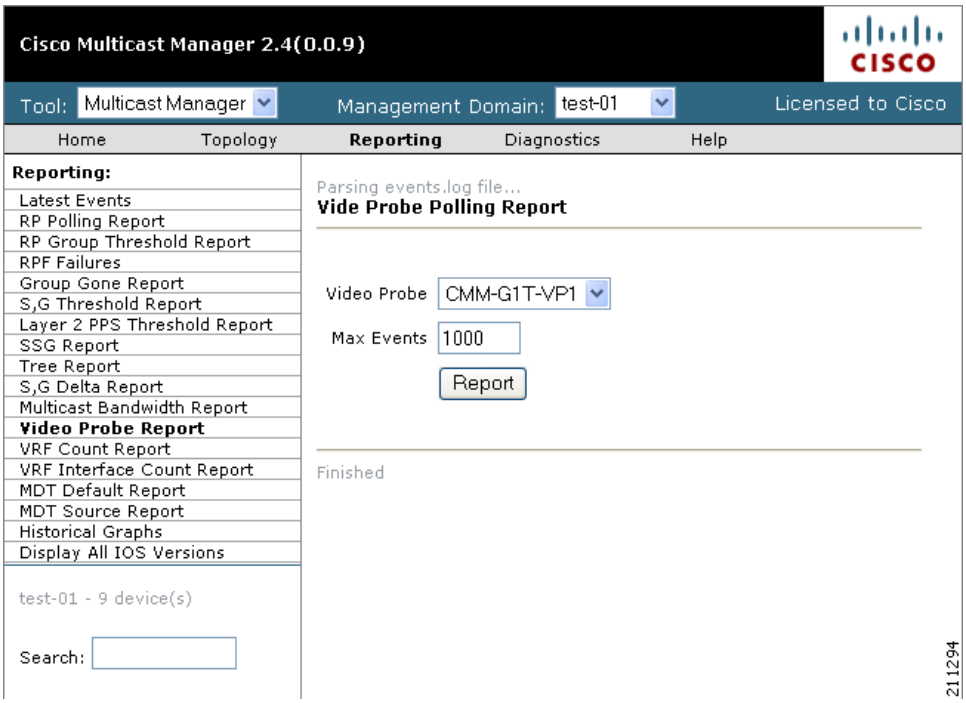
To view video probe reports:

Step 1 Select **Multicast Manager > Reporting**.

Step 2 Click **Video Probe Report**.

The Video Probe Polling Report page appears, as shown in Figure 3-8.

Figure 3-8 Specifying Parameters for the Video Probe Report



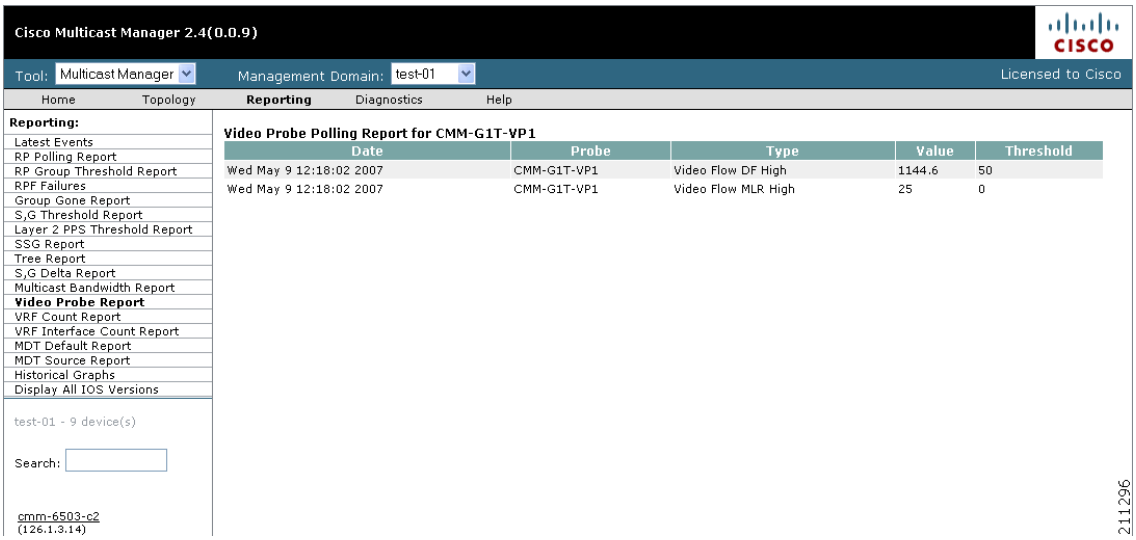
Step 3 From the pull-down list in the **Video Probe** field, select a probe.

Step 4 Enter the number of events you would like to see.

Step 5 Click **Report**.

A report for the specified probe appears. Figure 3-9 shows a sample report.

Figure 3-9 Video Probe Report



VRF Count Report

To generate a VRF Count Report:

Step 1 On the Reporting menu, select **VRF Count Report**.

The VRF Count Report page appears.

Step 2 On the VRF Count Report page, enter the parameters for the report.

A VRF Count Report appears.

VRF Interface Count Report

To generate a VRF Interface Count Report:

Step 1 On the Reporting menu, select **VRF Interface Count Report**.

The VRF Interface Count Report page appears.

Step 2 On the VRF Interface Count Report page, enter the parameters for the report.

The VRF Interface Count report appears.

MDT Default Report

To generate a MDT Default Report:

Step 1 On the Reporting menu, select **MDT Default Report**.

The MDT Default Report page appears.

Step 2 On the MDT Default Report page, enter the parameters for the report.

A MDT Default Report appears.

MDT Source Report

To generate an MDT Source Report:

Step 1 On the Reporting menu, select MDT Source Report.

The MDT Source Report page appears.

Step 2 On the MDT Source Report page, enter the parameters for the report.

An MDT Source Report appears.

Historical Graphs

Using **Historical Graphs**, you can view historical data in a graph format. Historical data is collected when you start to monitor any of the following:

- Source and group activity in a router.
- Multicast packets inbound or outbound of a Layer 2 port.
- Source and group packet deviations on baseline multicast trees.

To view Historical Graphs:

Step 1 Select a **Graph Type** from the list:

- SG Delta PPS
- SG PPS
- SG BPS
- Switch Port PPS

Step 2 Select a **Time Range**:

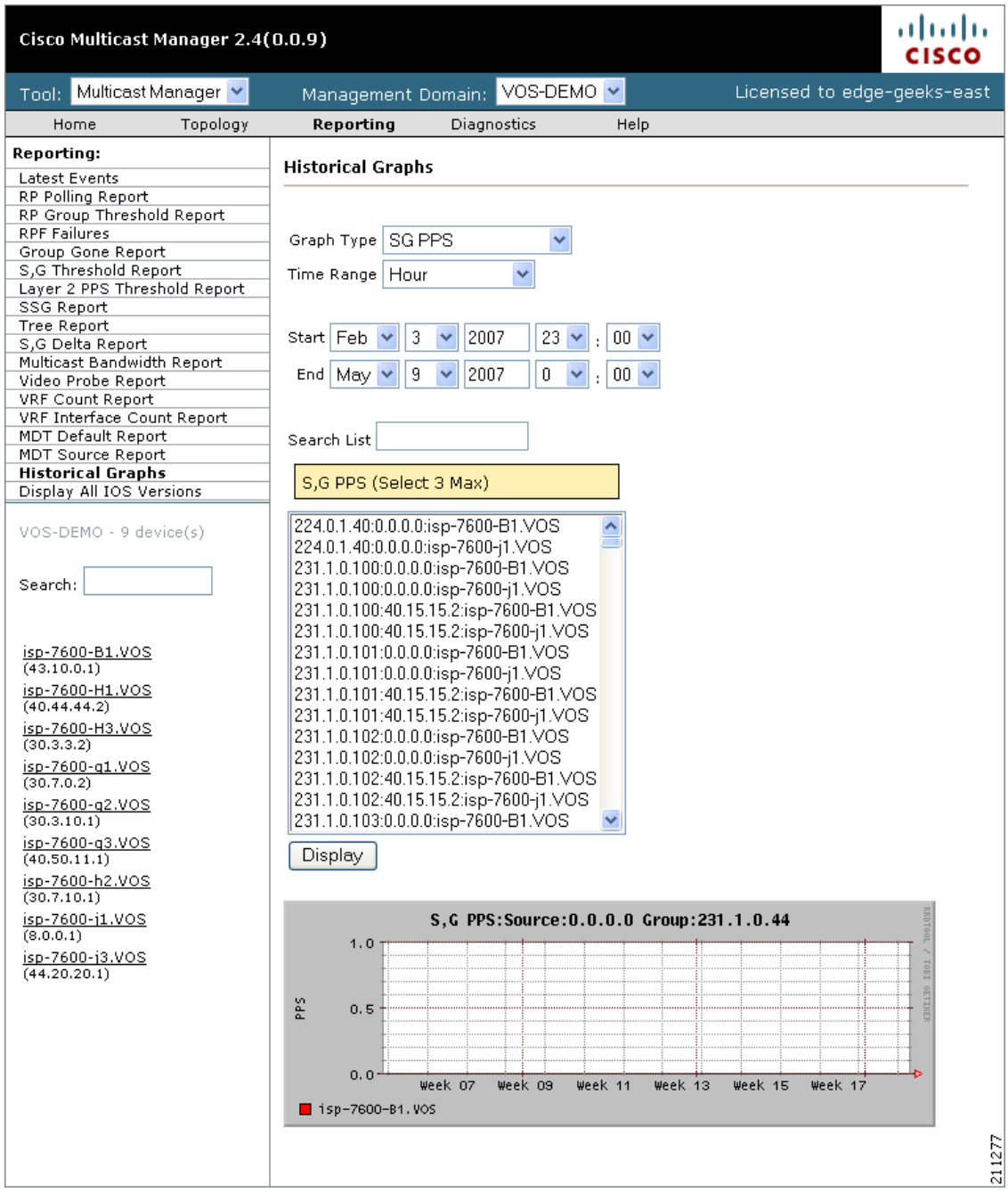
- User Specified
- Hour
- Day
- Week
- Month

Step 3 Select a **Start** and **End** range.

Step 4 A list of available reports appears. Highlight the appropriate report(s) and click **Display**. You can select up to 3 reports to display on the graph. Data stored for trending purposes is kept for up to 18 months.

Note Data must be collected to generate a report. If you have selected the correct Graph Type, and you do not see any entries, ensure that data is being collected (see Top Talkers, page 4-14).

Figure 3-10 Historical Graphs

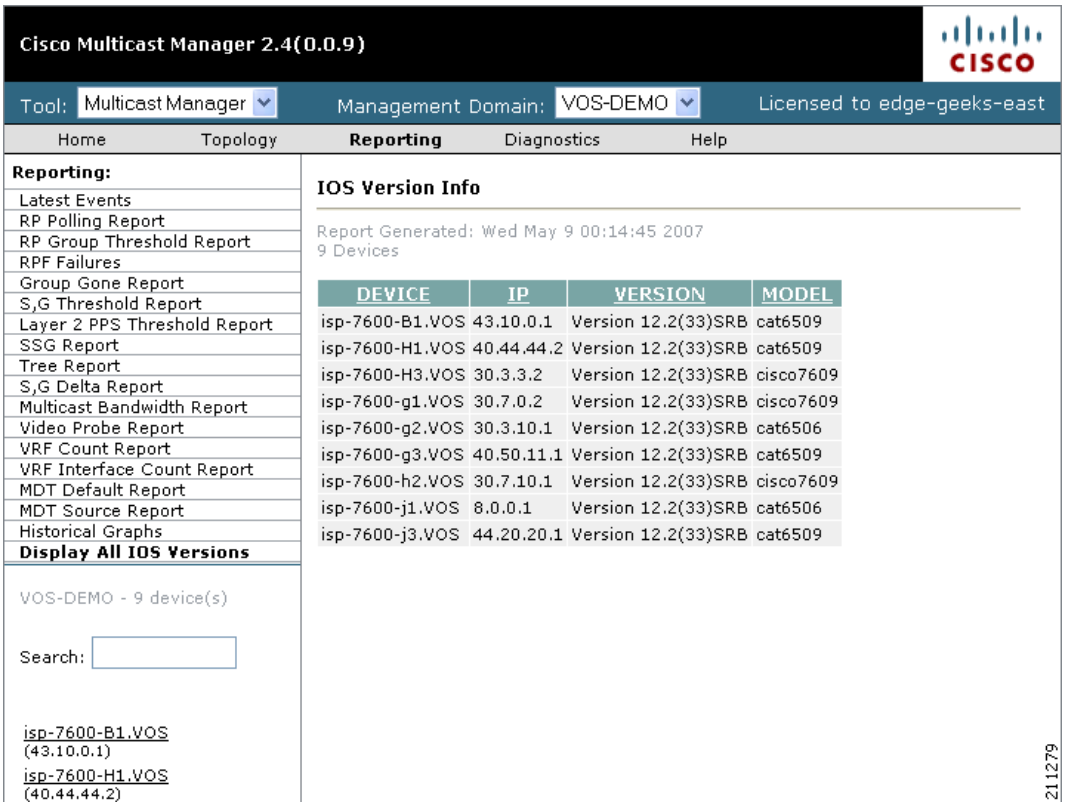


Display All IOS Versions

Using the IOS Version Info page, you can view the IOS version of all discovered routers in the current domain. You can sort the table by device, IP address, IOS version, or model by selecting the corresponding column heading.

Figure 3-11 shows a sample IOS Versions Report.

Figure 3-11 IOS Version Info



CHAPTER 4

Diagnostics and Troubleshooting with the Multicast Manager Tool

This chapter contains the following sections:

Managing Diagnostics

The **Diagnostics** tool gives you a global view and a router-specific view of your network. The following sections describe global diagnostics:

The following section describes router-specific diagnostics:

Show All Groups

With the **Show All Groups** page, you can:

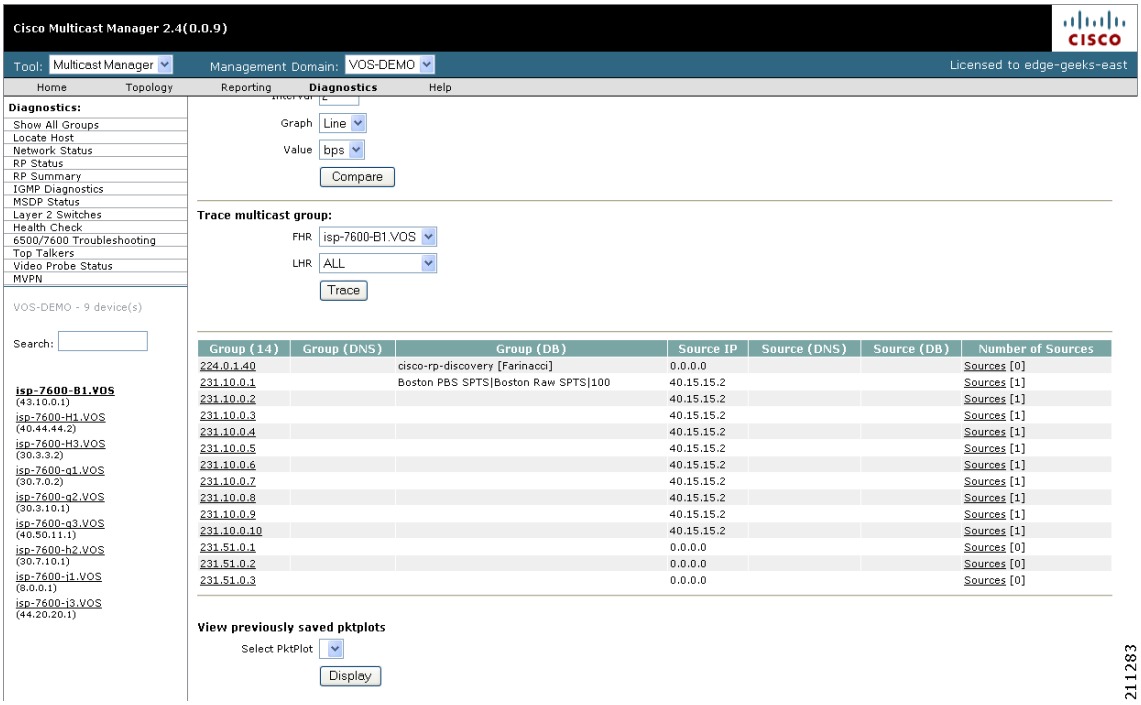
1. View all the active sources and groups in the network in tabular format. Groups are listed in numerical order, and the number of sources for each group appears in the last column. If there is more than one source for a group, select **Sources** to view them all.
2. Draw complete graphical trees by clicking on a group.
3. Draw filtered graphical trees by selecting the **Source**, **Group**, **FHR** and **LHR**.
4. Plot the pps/bps for a particular source and group.

To use the Show All Groups page:

Step 1 On the Diagnostics menu, select **Show All Groups.**

The Multicast Diagnostics page appears, as shown in Figure 4-1.

Figure 4-1 Multicast Diagnostics Page



Step 2 From the drop-down list below the **Source** field in the Set Source and Group to Work On pane, select a source to work on.

Step 3 From the drop-down list below the **Group** field in the Set Source and Group to Work On pane, select a group to work on.

The Multicast Diagnostics page appears with the source and group selected.

Step 4 (Optional) If you are using S,G caching, the cache contents appear. In this case, click **Refresh Cache** to refresh the table of sources and groups.

Step 5 If there are a lot of sources and groups present, you can filter the display to show only those you are interested in:

- **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.

To ensure a source is sending data, you can plot traffic over a period of time:

- **Select Router—**Select the router to take the sample from.
- **Samples—**Enter the number of samples (1-50).

Note If the device is a 6500, you may need to adjust the sampling period in order to generate useful data.

- **Interval—**Enter the interval between samples (1-90s).
- **Graph—**Select the type of graph, line or bar.
- **Value—**Select the value, bps or pps.
- Click **Plot**. This produces a graph for the currently selected S,G on the selected router. You can also save this graph on the server.

Note This option is not meant for long term polling, but rather as an immediate troubleshooting tool. For long term polling of PPS data, the S,G should be configured under S,G Threshold polling

Step 6 To draw a graphical tree between two particular routers:

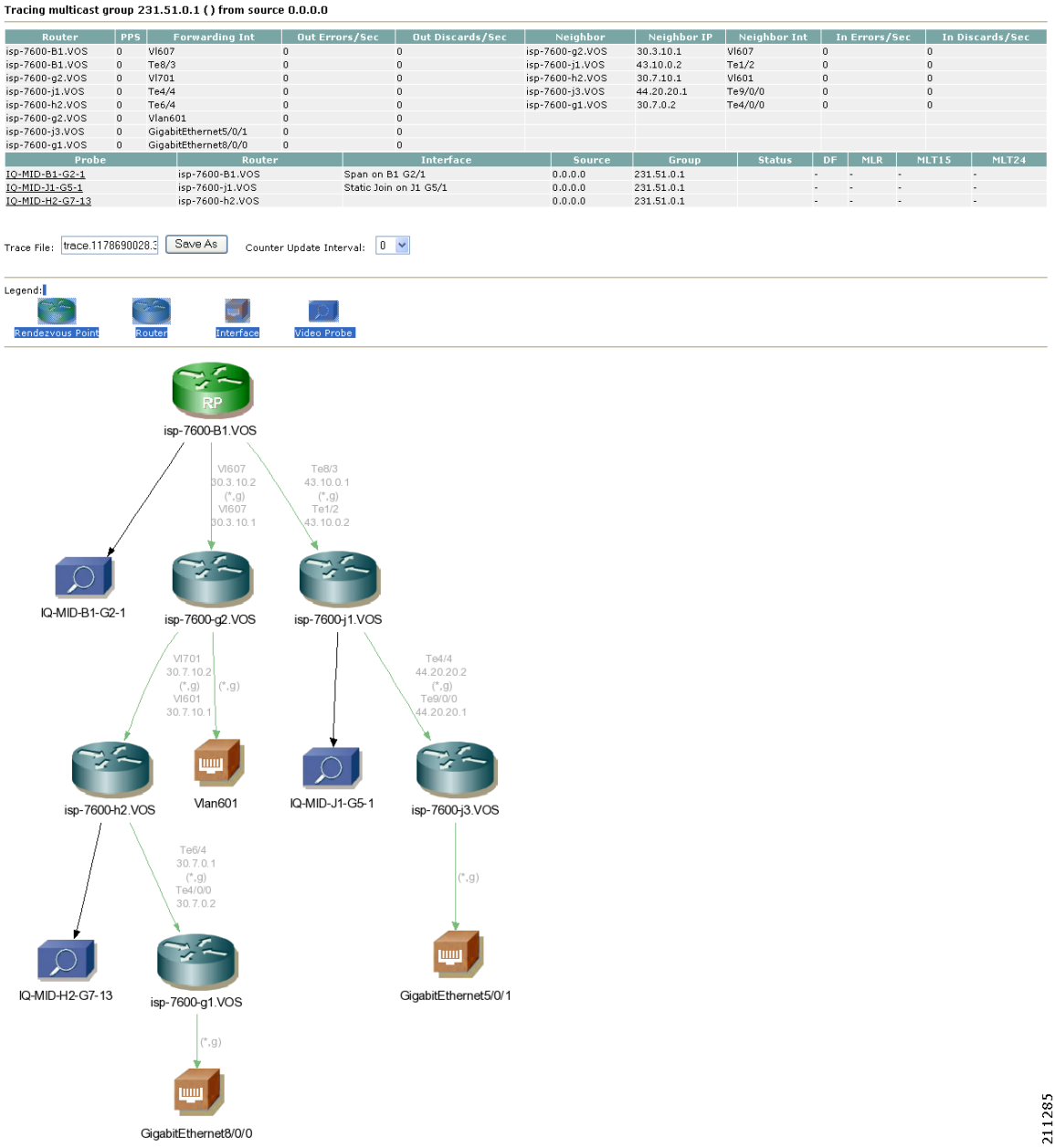
- **FHR—**Select the first hop router that the trace should start under.
- **LHR—**Select the last hop router that the trace should end under.
- Click **Trace**. The CMM draws a tree of the source and group selected from the router in FHR to the router in LHR.

Step 7 To list all of the active sources and groups, within the Show All Groups page, simply scroll down to see all entries.

Step 8 To draw a multicast tree, select a **Group** (in the first column of the Source and Group table). A new page appears with the multicast tree in tabular and graphical format. Routers known as RPs to the source router appear green.

Note If there is more than one source for the group, select **Sources** under **Number of Sources** and select the source you want to draw the tree from.

Figure 4-2 Drawing a Multicast Tree (Baseline)



Step 9 To display packet error counters, select a **Counter Update Interval**. These counters are updated each period.

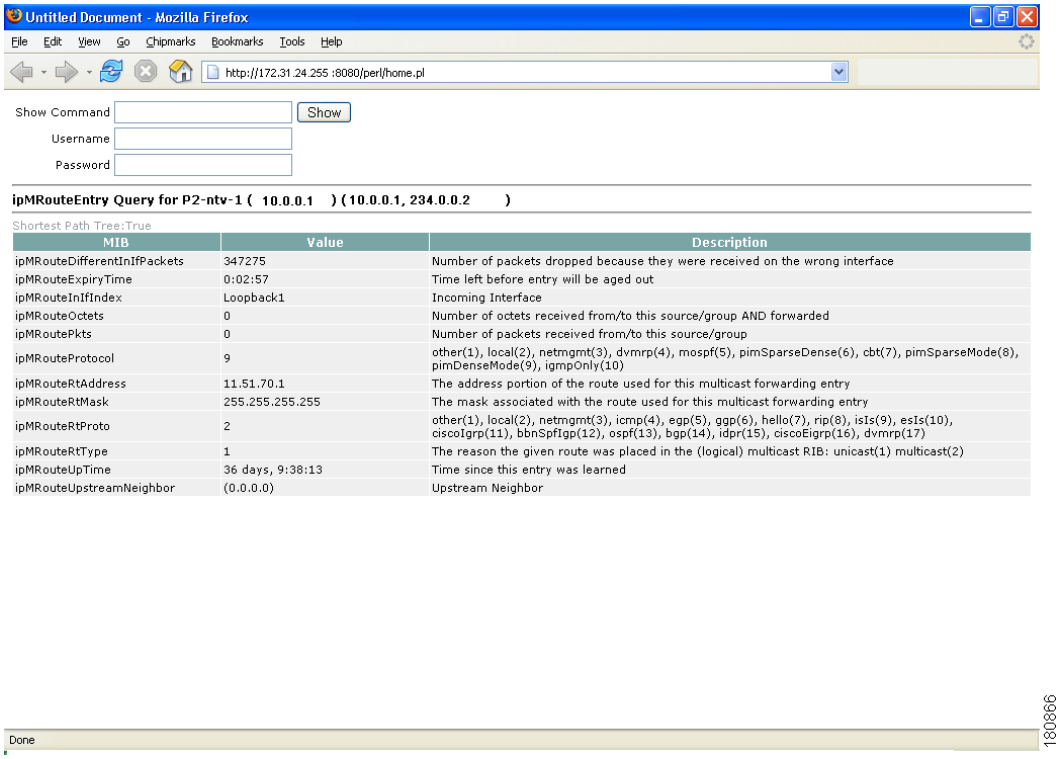
Step 10 To save the multicast tree as a baseline, enter a name within **Trace File**, and click **Save As**. The window closes. You can use the saved baseline for tree polling (see Tree Polling, page 2-39).

Note You can also save the tree as a .jpeg, .bmp, or .png file by right-clicking it.

Step 11 (Optional) To view routing information for a router on a router in the multicast tree click on the router icon.

This opens another page that contains IP multicast routing information for the S,G that has been traced: Figure 4-3 shows sample routing information.

Figure 4-3 Viewing IP Multicast Routing Information



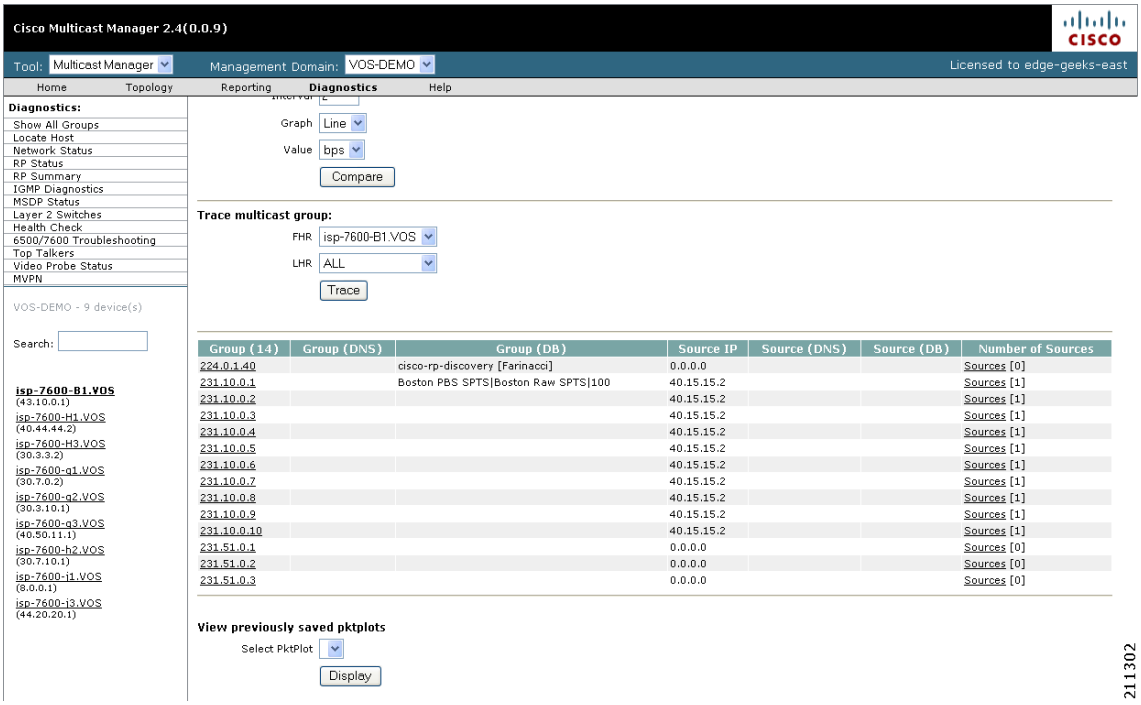
The trace information page contains these fields and selections:

- **Show Command**—Enter any show commands on the router. A new window opens that contains multicast route information for the selected router.
- **Username**—Enter your username.
- **Password**—Enter your password.
- **MIB—**The name of the MIB entry in the MIB to monitor the router.
- **Value—**The value of the MIB entry.
- **Description—**A description of the MIB entry.

Step 12 To display details about a router listed in the lower left pane, click on the router name.

Figure 4-4 shows an example.

Figure 4-4 Multicast Diagnostics



The example in Figure 4-4 shows the following information:

- **Group (DNS)—**Name given to this group in DNS.
- **Group (DB)—**Name given to this group in the address database.
- **Source IP—**IP address of the source.
- **Source (DNS)—**Name given to this source in DNS.

Note The Source (DNS) field is populated only if DNS is configured, and if **Resolve Sources** is selected on the Device Configuration page. It should be noted that resolving thousands of addresses via DNS can be extremely slow.

- **Source (DB)—**Name given to this source in the address database.
- **Number of Sources—**Number of sources in this group.

Step 13 To view previously saved source bps/pps files, select the file, and click **Display**.

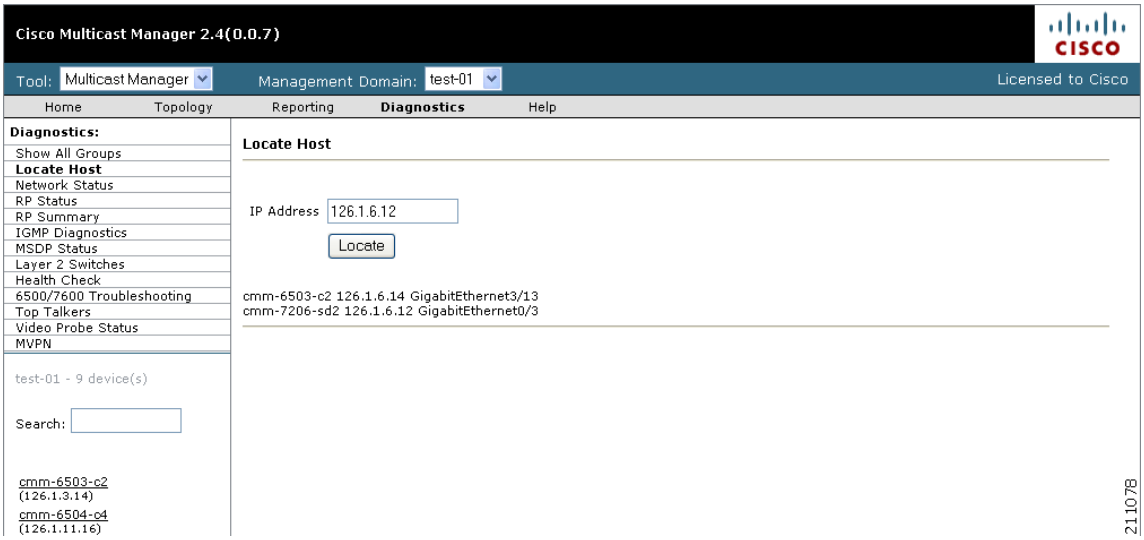
Step 14 To view previously saved traces, select the trace, and click **Display**.

Locate Host

Using the Locate Host page, you can find sources and receivers in the network. Enter the **IP Address** or hostname (if DNS is configured) and click **Locate**.

Figure 4-5 shows the Locate Host page.

Figure 4-5 Locate Host Page

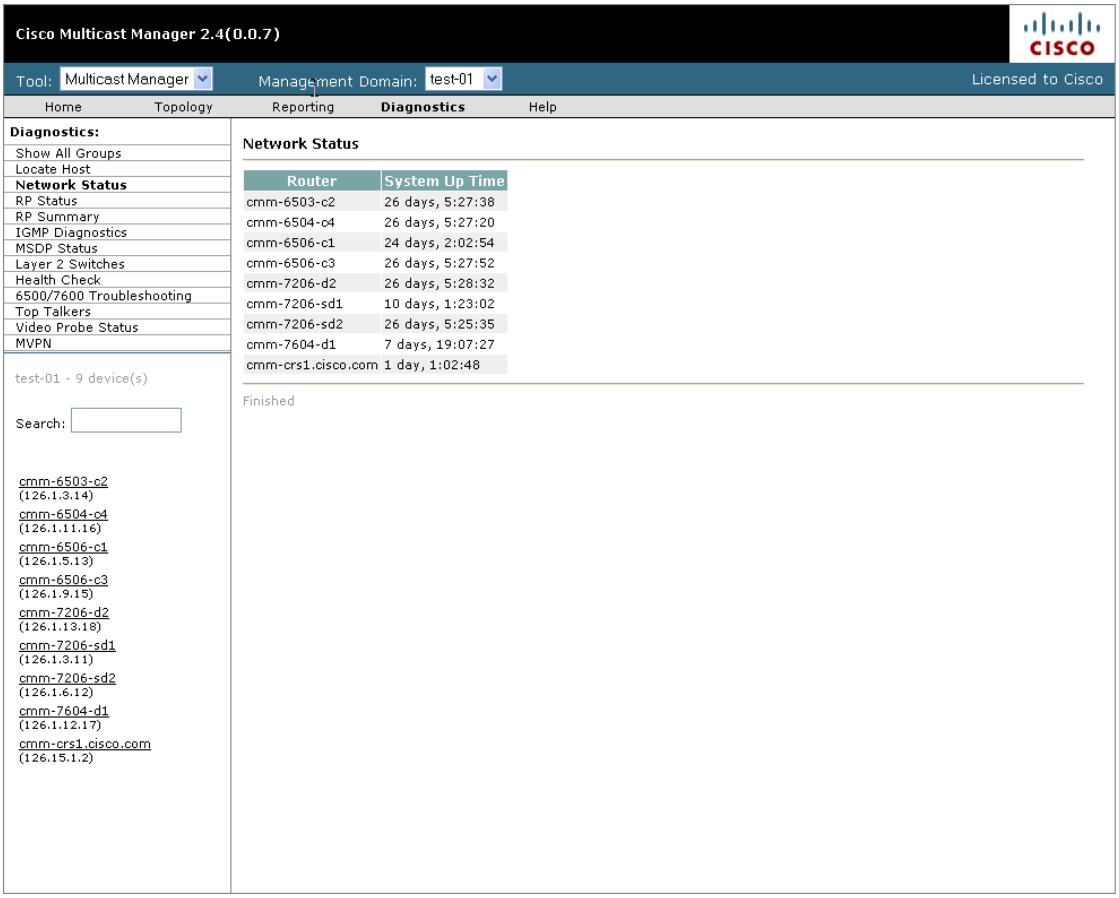


Network Status

Using the Network Status page, you can view the status of all devices in the current multicast domain. The System Up Time appears for all devices that are up. Devices that are down or unreachable appear in red.

Figure 4-6 shows the Network Status page.

Figure 4-6 Network Status

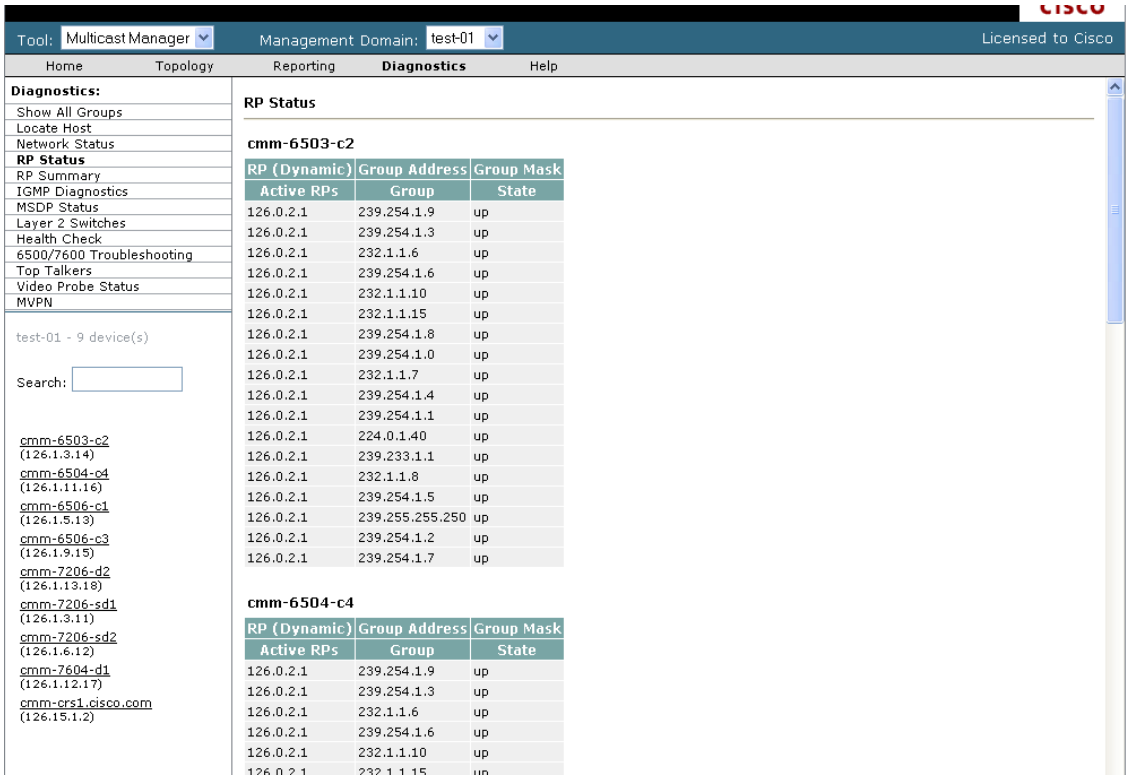


RP Status

Using the RP Status page, you can view all routers in the database, their RPs, and the active groups. In a large network with, many S,Gs, it may take some time for this data to appear, because each router in the multicast domain is queried.

Figure 4-7 shows the RP Status page.

Figure 4-7 RP Status Page



RP Summary

Using the RP Summary, you can view all the RPs that the CMM is aware of, based upon the discovery. For details on clicking on an RP, see Viewing Topology, page 3-2.

IGMP Diagnostics

Note IGMP Diagnostics does not work for IOS 12.0S devices.

Using the IGMP Diagnostics page, you can see the interfaces that have joined onto a particular group:

Step 1 Select the routers you want to query.

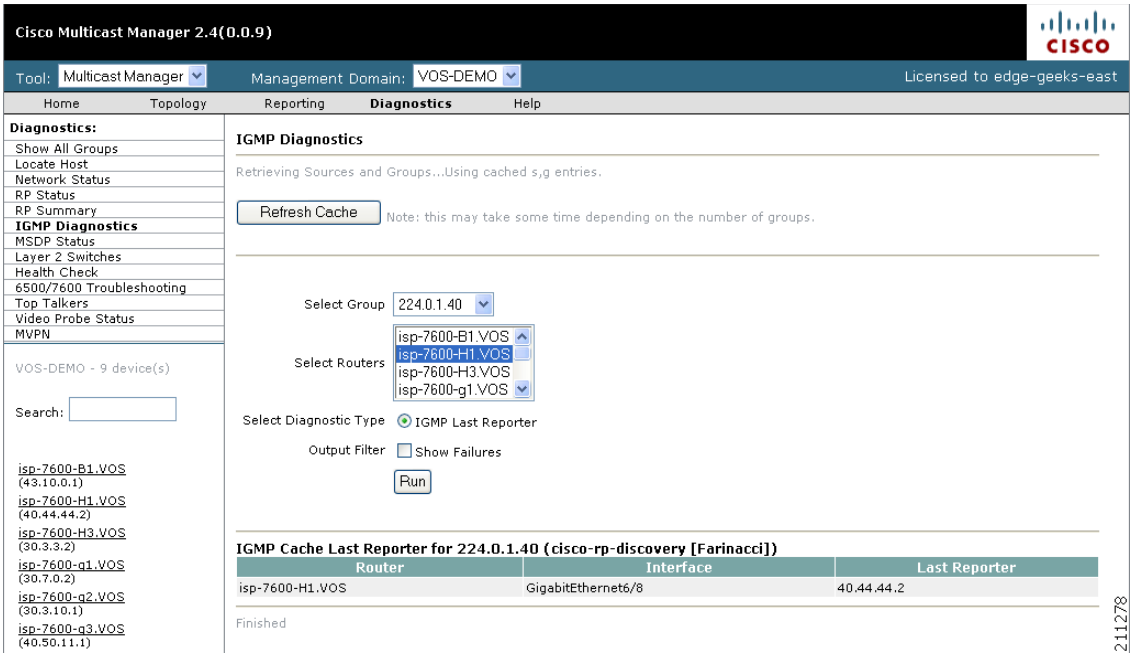
Step 2 **Select Diagnostic Type** is always set to **IGMP Last Reporter**.

Step 3 Select **Show Failures** to display all interfaces on the router.

Step 4 Click **Run**.

Figure 4-8 shows the IGMP Diagnostics page.

Figure 4-8 IGMP Diagnostics Page



MSDP Status

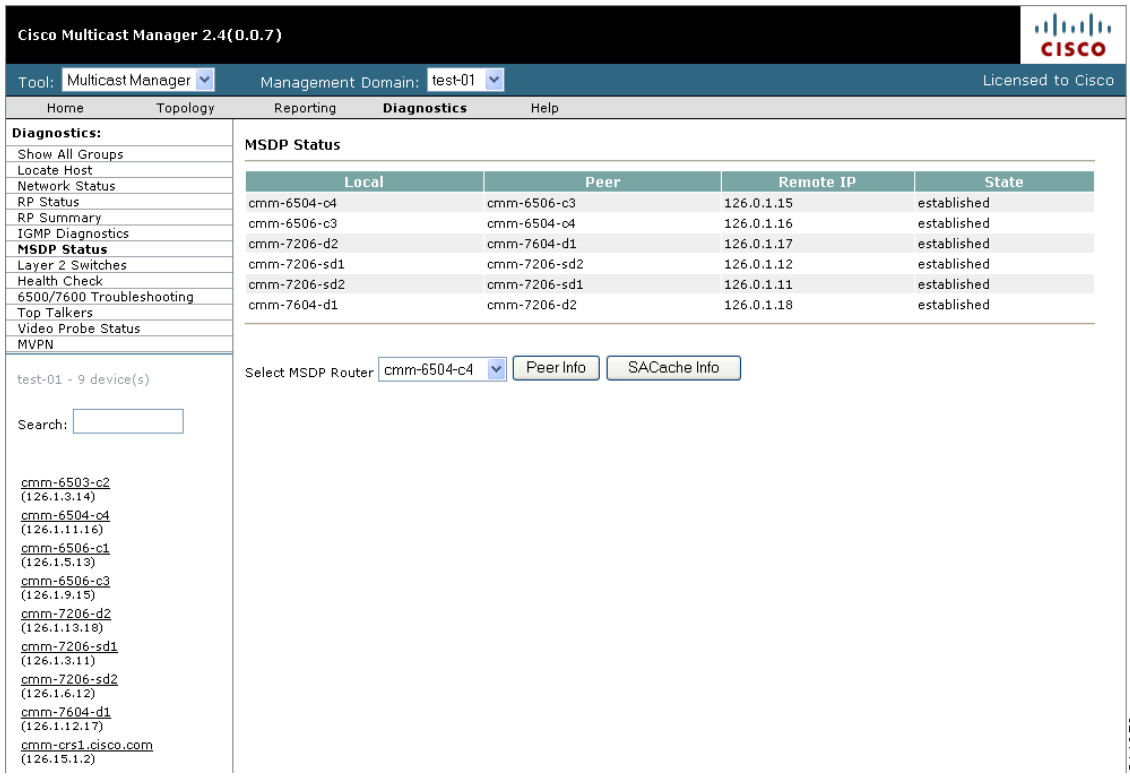
Using the MSPD Status page, you can view all routers running MSDP and their peering connectivity. You can also view details for a specific router, such as peering information and the SA cache.

Note The MSDP MIB is supported only in IOS releases 12.0S, 12.1T (12.2) and 12.3. Version 12.1(x) does not support this MIB. Therefore, any RP running 12.1(x) with MSDP configured does not appear on this table.

To view peer information or SA cache information, select a router from the list and click the corresponding button.

Figure 4-9 shows the MSDP Status page.

Figure 4-9 MSDP Status Page



Layer 2 Switches

Using the Layer 2 Switches pages, you can view:

- Layer 2 Multicast Information.
- Layer 2 Host IPs.

Note These queries require the VTY password, or a TACACS username/password. The table that is generated, shows, from a Layer 2 perspective, which multicast groups are being forwarded out which interfaces.

To view Layer 2 multicast information or host IPs:

Step 1 Enter your username.

Step 2 Enter your password.

Step 3 Select the switch(es) you want to view.

Step 4 Click **Query**.

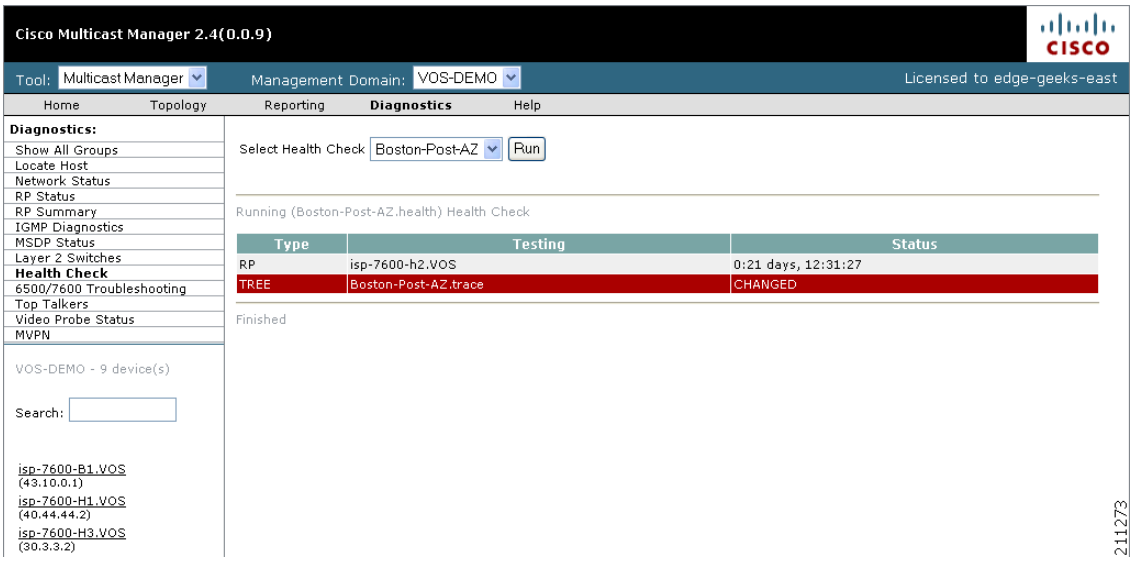
A display of L2 Multicast information appears. The possible IP addresses that can be mapped to the MAC address are also shown.

Health Check

Using the Health Check page, you can run a health check on a domain. To run a health check, select it from the list, and click **Run**.

Figure 4-10 shows a sample health check display.

Figure 4-10 Health Check



The color of the displayed text on the Health Check display indicates the status of the monitored condition:

- Gray = normal
- White = normal
- Red = error condition

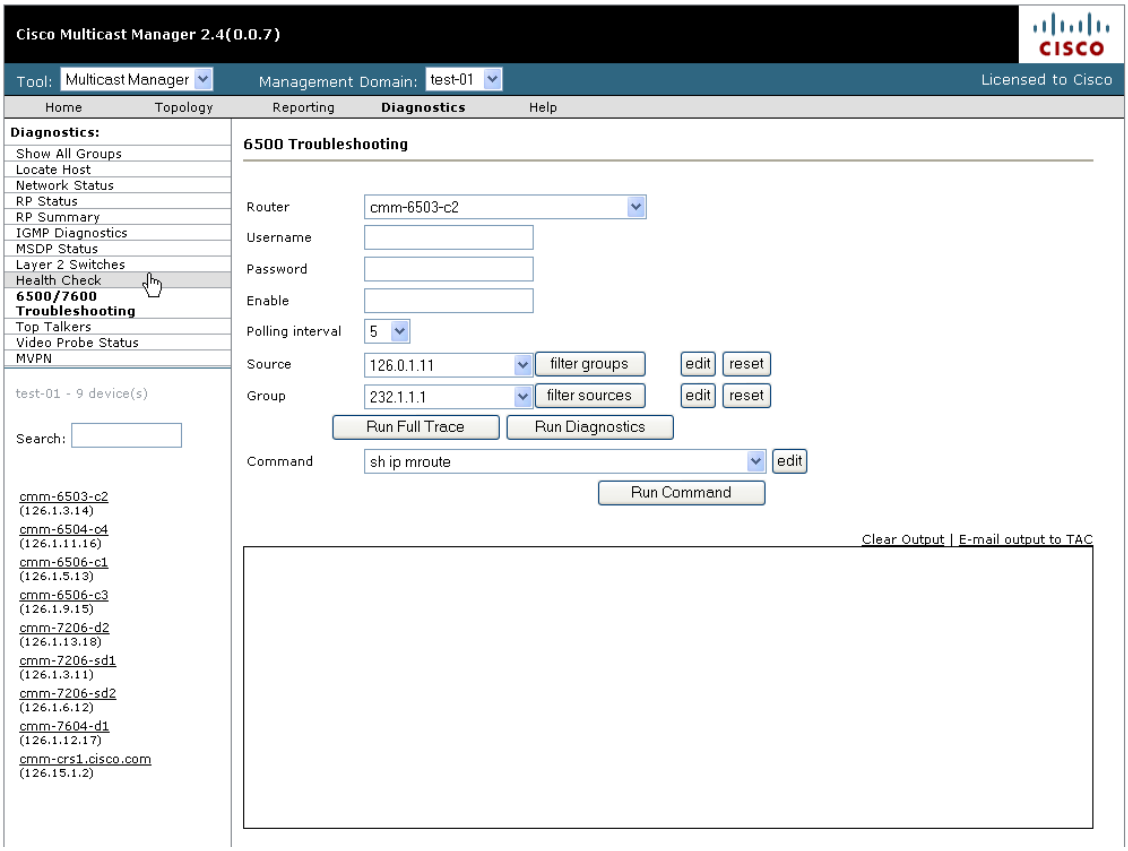
6500/7600 Troubleshooting

Using the 6500/7600 Troubleshooting page, you can enable the CMM to gather accurate packet forwarding statistics and other information in a timely manner. This option initiates a remote login session into the PFC. A persistent Telnet session issues show commands and displays live statistics. These sessions are terminated when the windows are closed.

Tip All important sources and groups should be proactively monitored. Use the 6500 Troubleshooting tool to investigate a current problem.

Figure 4-11 shows the 6500/7600 Troubleshooting diagnostics page.

Figure 4-11 6500/7600 Troubleshooting Page



The 6500/7600 Troubleshooting page contains the following fields and buttons:

Fields and Buttons	Description
Router	Select a 6500 or 7600 router.
Username	Enter your username.
Password	Enter the MSFC password.
Enable	Enter the enable password.
Polling Interval	Interval at which the statistics are updated.
Source	IP address of the source.
Group	IP address of the group.
Edit	Lets you manually type in a group or source address.
Reset	Populates the source and group lists again.
Run Full Trace	Starts the tree at the source instead of the selected router. For details, see Show All Groups, page 4-2.

Fields and Buttons	Description
Run Diagnostics	Draws a graphical tree of the source and group selected, starting at the router selected. Live traffic statistics also appear for this source and group at this router. You can click any other router in the picture to see live packets statistics for them (see Show All Groups, page 4-2). Ensure pop-up blockers are disabled.
Command	Provides a list of show commands.
Edit	Add your own command by clicking **Edit**, typing in your command, then click **Run Command**.
Run Command	Runs the selected show command. Output appears in the text box below.
Clear Output	Clears the output.
E-mail output to TAC	Emails the output to the Cisco TAC. **Note** Your server must have email set up.

When troubleshooting a problem, you can keep a record of the command output:

Step 1 Right-click in the output.

Step 2 Choose **Select All**.

Step 3 Copy and paste the content.

Top Talkers

Using the Top Talkers page, you can view the top 20 talkers, sorted by long term. The top 20 talkers are dynamically updated at every polling interval.

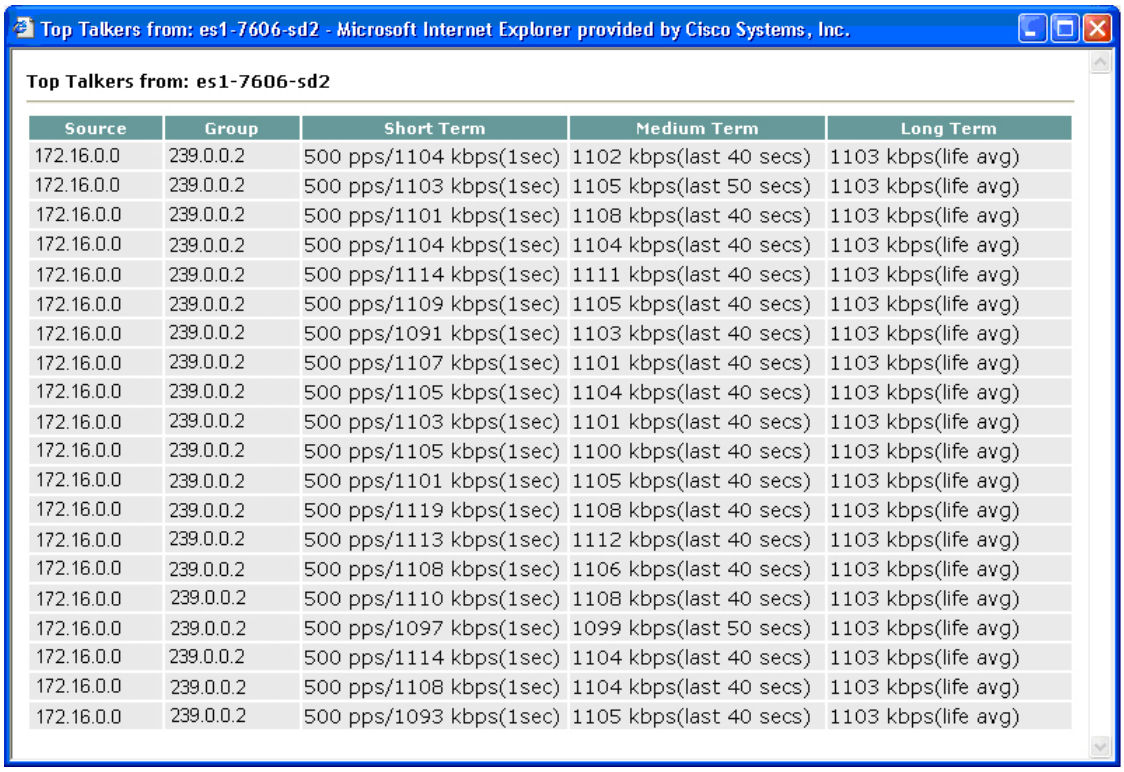
Step 1 Select a router to monitor.

Step 2 Enter your username and password.

Step 3 Select a polling interval, indicating the period (in seconds) for the window to update.

Step 4 Click **Top Talkers**.

Figure 4-12 Top Talkers



Source	Group	Short Term	Medium Term	Long Term
172.16.0.0	239.0.0.2	500 pps/1104 kbps(1sec)	1102 kbps(last 40 secs)	1103 kbps(life avg)
172.16.0.0	239.0.0.2	500 pps/1103 kbps(1sec)	1105 kbps(last 50 secs)	1103 kbps(life avg)
172.16.0.0	239.0.0.2	500 pps/1101 kbps(1sec)	1108 kbps(last 40 secs)	1103 kbps(life avg)
172.16.0.0	239.0.0.2	500 pps/1104 kbps(1sec)	1104 kbps(last 40 secs)	1103 kbps(life avg)
172.16.0.0	239.0.0.2	500 pps/1114 kbps(1sec)	1111 kbps(last 40 secs)	1103 kbps(life avg)
172.16.0.0	239.0.0.2	500 pps/1109 kbps(1sec)	1105 kbps(last 40 secs)	1103 kbps(life avg)
172.16.0.0	239.0.0.2	500 pps/1091 kbps(1sec)	1103 kbps(last 40 secs)	1103 kbps(life avg)
172.16.0.0	239.0.0.2	500 pps/1107 kbps(1sec)	1101 kbps(last 40 secs)	1103 kbps(life avg)
172.16.0.0	239.0.0.2	500 pps/1105 kbps(1sec)	1104 kbps(last 40 secs)	1103 kbps(life avg)
172.16.0.0	239.0.0.2	500 pps/1103 kbps(1sec)	1101 kbps(last 40 secs)	1103 kbps(life avg)
172.16.0.0	239.0.0.2	500 pps/1105 kbps(1sec)	1100 kbps(last 40 secs)	1103 kbps(life avg)
172.16.0.0	239.0.0.2	500 pps/1101 kbps(1sec)	1105 kbps(last 40 secs)	1103 kbps(life avg)
172.16.0.0	239.0.0.2	500 pps/1119 kbps(1sec)	1108 kbps(last 40 secs)	1103 kbps(life avg)
172.16.0.0	239.0.0.2	500 pps/1113 kbps(1sec)	1112 kbps(last 40 secs)	1103 kbps(life avg)
172.16.0.0	239.0.0.2	500 pps/1108 kbps(1sec)	1106 kbps(last 40 secs)	1103 kbps(life avg)
172.16.0.0	239.0.0.2	500 pps/1110 kbps(1sec)	1108 kbps(last 40 secs)	1103 kbps(life avg)
172.16.0.0	239.0.0.2	500 pps/1097 kbps(1sec)	1099 kbps(last 50 secs)	1103 kbps(life avg)
172.16.0.0	239.0.0.2	500 pps/1114 kbps(1sec)	1104 kbps(last 40 secs)	1103 kbps(life avg)
172.16.0.0	239.0.0.2	500 pps/1108 kbps(1sec)	1104 kbps(last 40 secs)	1103 kbps(life avg)
172.16.0.0	239.0.0.2	500 pps/1093 kbps(1sec)	1105 kbps(last 40 secs)	1103 kbps(life avg)

Video Probe Status

You can view diagnostic information about video probes and the flows that they are monitoring from the View Probe Status window.

View probe status shows you:

- The source, group, and channel association that you are troubleshooting.
- A graphical topology tree that clearly shows all of the routers that form the tree, and their input and output interfaces. along with IP addresses and interface descriptions
- The packets per sampling period being received at each point in the tree (sampling periods range from 5 seconds to 30 and are configurable).
- The packet input, output and discard errors being received at each interface.
- A text representation of the tree, which is invaluable when troubleshooting large multicast trees.

In addition, Cisco Multicast Manager draws a topology tree that shows:

- The probes that are positioned along this tree
- The router and interfaces of the probes
- The current status of the flow (Red, Yellow or Green)
- Current and historical flow statistics
- In-depth channel association information

To view video probe status:

Step 1 Select **Multicast Manager > Diagnostics**.

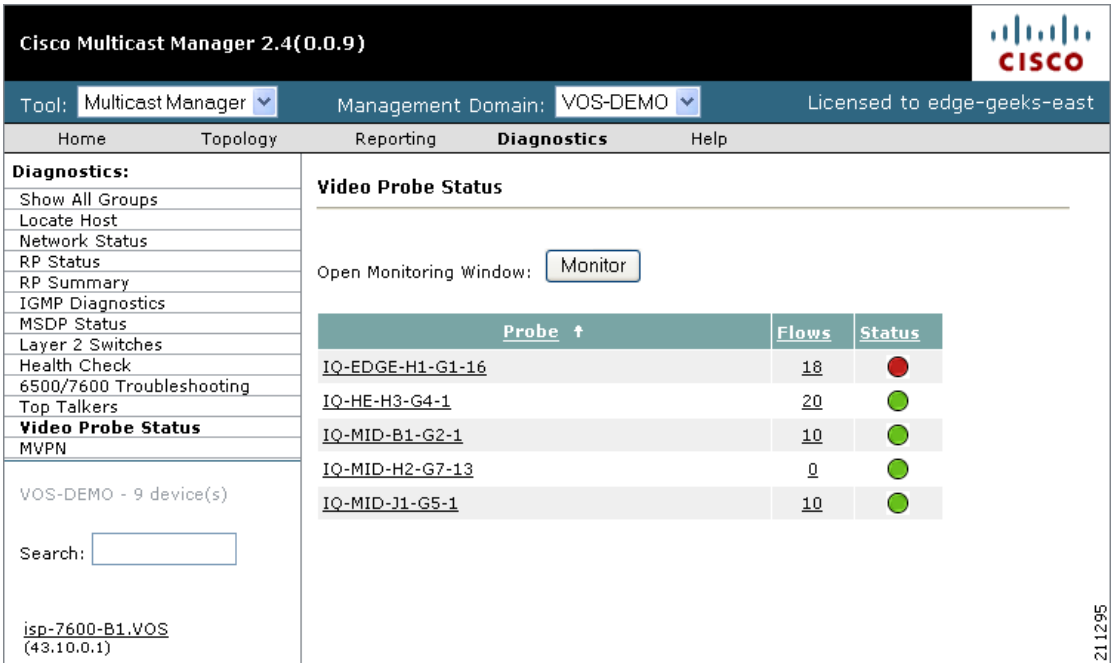
Step 2 Click **Video Probe Status**.

The Video Flow Status window appear, as shown in Figure 4-13. This window shows the probes that are currently configured and running, and indicates how many flows are being monitored and the status of the probe.

The probe status can be:

Green	Good
Yellow	A threshold was exceeded but the status in now normal
Red	Thresholds are currently being exceeded

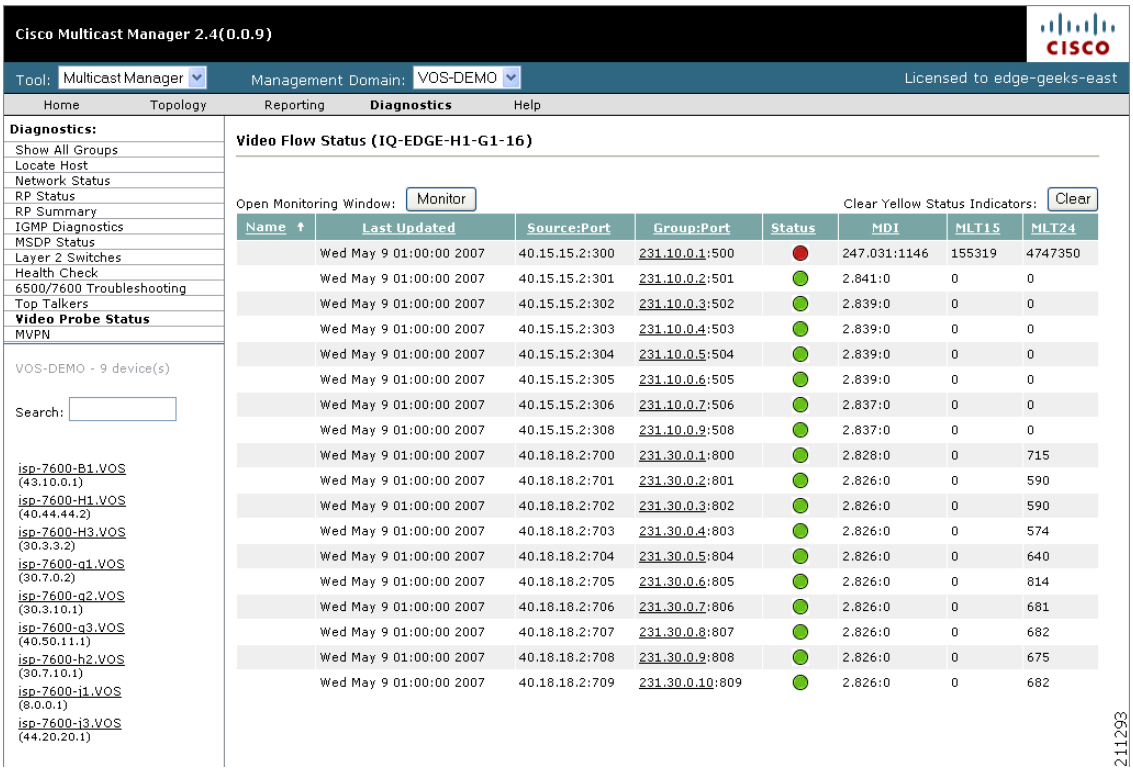
Figure 4-13 Video Flow Status Window



Step 3 To view the current activity on a probe, click on the Probe ID or on the Flows number.

The Video Flow Status window appears, as shown in Figure 4-14, and indicates the status of the video flows.

Figure 4-14 Viewing Video Flow Status



Step 4 To view a trace showing information about a flow, as well as a topology tree that shows the devices and probes associated with the flow, click on a group name (underlined IP address).

Viewing Detailed Multicast Information and Probe Topology

You can view a detailed trace about a video flow and a topology tree that shows the following:

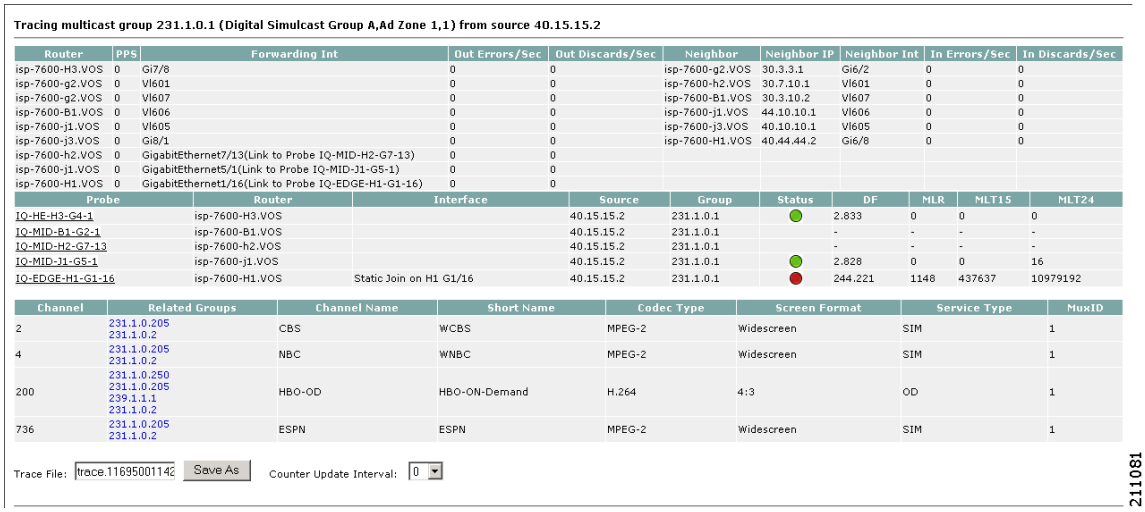
- Rendezvous Points
- Routers
- Interfaces
- Probes

To view a detailed flow trace and topology tree:

Step 1 On the video flow status window, click a group name (underlined IP address).

A message indicating the group and source that is being traced appears. The trace window includes a window with tables that show detailed information about the flow, as shown in Figure 4-15; and, Cisco Multicast Manager draws a topology tree for the flow, as shown in Figure 4-16.

Figure 4-15 Detailed Trace Table



Tracing multicast group 231.1.0.1 (Digital Simulcast Group A,Ad Zone 1,1) from source 40.15.15.2

Router	PPS	Forwarding Int	Out Errors/Sec	Out Discards/Sec	Neighbor	Neighbor IP	Neighbor Int	In Errors/Sec	In Discards/Sec
isp-7600-H3.VOS	0	Gi7/8	0	0	isp-7600-g2.VOS	30.3.3.1	Gi6/2	0	0
isp-7600-g2.VOS	0	Vl601	0	0	isp-7600-h2.VOS	30.7.10.1	Vl601	0	0
isp-7600-g2.VOS	0	Vl607	0	0	isp-7600-B1.VOS	30.3.10.2	Vl607	0	0
isp-7600-B1.VOS	0	Vl606	0	0	isp-7600-j1.VOS	44.10.10.1	Vl606	0	0
isp-7600-j1.VOS	0	Vl605	0	0	isp-7600-j3.VOS	40.10.10.1	Vl605	0	0
isp-7600-j3.VOS	0	Gi8/1	0	0	isp-7600-H1.VOS	40.44.44.2	Gi6/8	0	0
isp-7600-h2.VOS	0	GigabitEthernet7/13(Link to Probe IQ-MID-H2-G7-13)	0	0					
isp-7600-j1.VOS	0	GigabitEthernet5/1(Link to Probe IQ-MID-J1-G5-1)	0	0					
isp-7600-H1.VOS	0	GigabitEthernet1/16(Link to Probe IQ-EDGE-H1-G1-16)	0	0					

Probe	Router	Interface	Source	Group	Status	DF	MLR	MLT15	MLT24
IQ-HE-H3-G4-1	isp-7600-H3.VOS		40.15.15.2	231.1.0.1		2.833	0	0	0
IQ-MID-B1-G2-1	isp-7600-B1.VOS		40.15.15.2	231.1.0.1		-	-	-	-
IQ-MID-H2-G7-13	isp-7600-h2.VOS		40.15.15.2	231.1.0.1		-	-	-	-
IQ-MID-J1-G5-1	isp-7600-j1.VOS		40.15.15.2	231.1.0.1		2.828	0	0	16
IQ-EDGE-H1-G1-16	isp-7600-H1.VOS	Static Join on H1 G1/16	40.15.15.2	231.1.0.1		244.221	1148	437637	10979192

Channel	Related Groups	Channel Name	Short Name	Codec Type	Screen Format	Service Type	MuxID
2	231.1.0.205 231.1.0.2	CBS	WCBS	MPEG-2	Widescreen	SIM	1
4	231.1.0.205 231.1.0.2	NBC	WNBC	MPEG-2	Widescreen	SIM	1
200	231.1.0.250 231.1.0.205 239.1.1.1 231.1.0.2	HBO-OD	HBO-ON-Demand	H.264	4:3	OD	1
736	231.1.0.205 231.1.0.2	ESPN	ESPN	MPEG-2	Widescreen	SIM	1

Trace File: trace.11695001142 Save As Counter Update Interval: 0

211081

The detailed flow trace table shows the following information:

Column	Information Shown
Router	The router that is being monitored.
PPS	Packets per second transmitted.
Forwarding Int	Interface that is forwarding the packets.
Out Errors/Sec	Output errors per second.
Out Discards/Sec	Output packets discarded, per second.
Neighbor	Hostname of the neighbor router in the network.
Neighbor IP	IP address of the neighbor router in the network.
Neighbor Int	The interface of the neighbor router in the network.
In Errors/Sec	Input errors per second.
In Discards/Sec	Input packets discarded, per second.

The probe status table shows the following information:

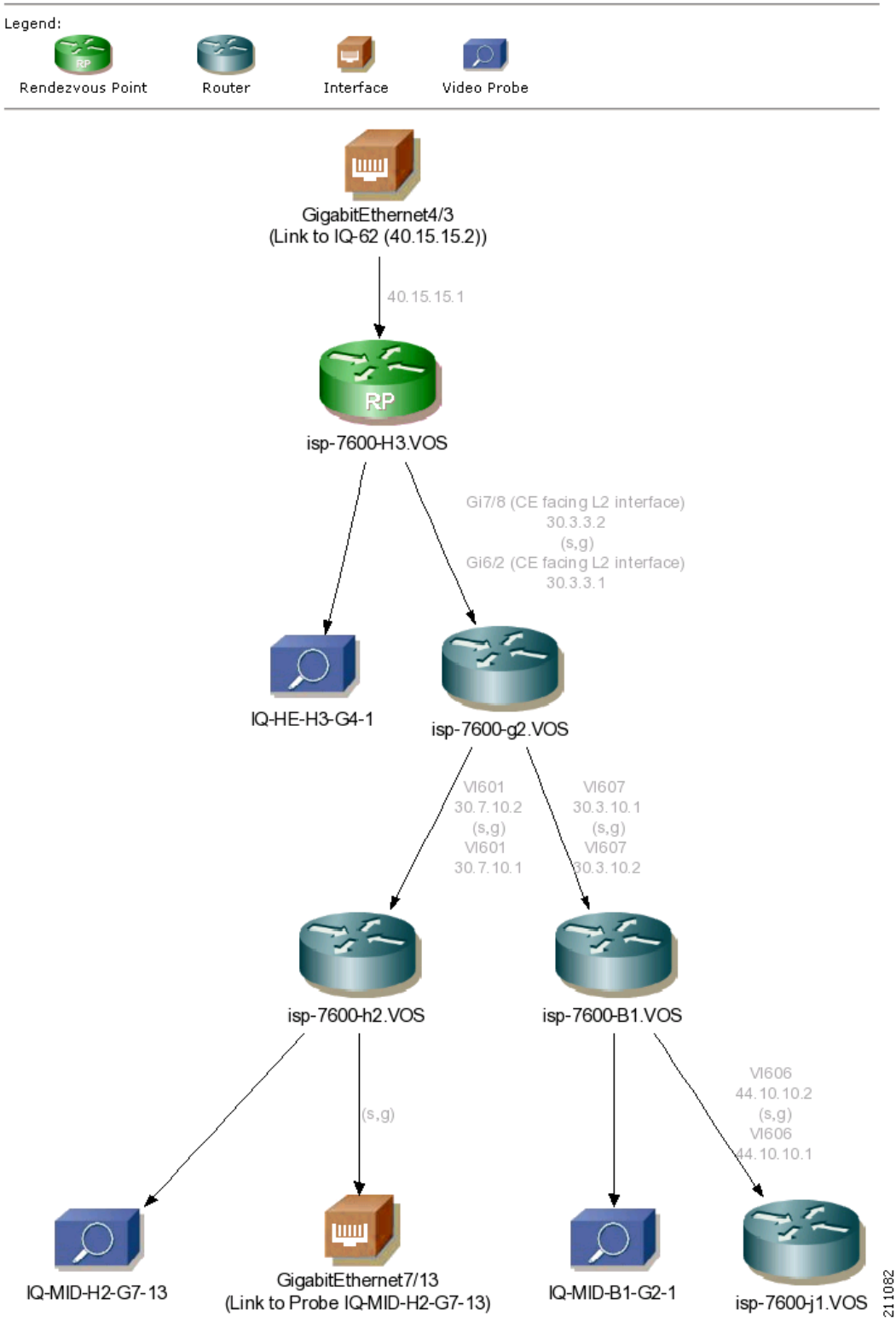
Column	Information Shown
Probe	Name of the probe.
Router	Router that the probe is monitoring.
Interface	The router interface to which the probe is connected.
Source	The source router that is multicasting the video data.
Group	The Group name of the source router.
Status	The status of the probe.
DF	The delay factor of the packets, in milliseconds.
MLR	The media loss rate (MLR) for the video stream.
MLT15	Total media packets lost in the last 15 minutes.
MLT24	Total media packets lost in the last 24 hours.

The channel information table shows information about each channel used to transmit the flow:

Column	Information Shown
Channel	The channels used to transmit the video.
Related Groups	The multicast group addresses of the multicast groups used to transmit the video data for this channel.
Channel Name	The name assigned to the channel.
Short Name	Short version of the channel name.
Codec Type	The type of CODEC used with this channel.
Screen Format	Screen format for this channel,
MuxID	A number representing the ID of the multiplexer.

Figure 4-16 shows a sample topology tree for the data that is shown in Figure 4-15.

Figure 4-16 Probe Topology Tree



The topology tree shows a network diagram starting with the router that is linked to the interface that is multicasting the video stream. This is indicated by an interface icon.

Each router in the topology is shown by a router icon, each interface by an interface icon, and each probe by a probe icon.

Step 2 To view a route query report for a router in the topology tree, click on the router icon for the router that you want to query.

Cisco Multicast Manager displays the results of a route query for the router. See Figure 4-3 for a sample report.

Step 3 To view a Video Flow Status report for a probe shown in the topology tree, click on a probe icon.

Step 4 Figure 4-17 shows a sample Video Flow Status report.

Figure 4-17 Viewing Video Flow Status

Video Flow Status (IQ-HE-H3-G4-1)

Monitor Flows: Monitor Clear Yellow Status Indicators: Clear

Name	Last Updated	Source:Port	Group:Port	Status	MDI	MLT15	MLT24
Video 1	Mon Jan 22 17:55:04 2007	40.15.15.2:2000	231.1.0.1:1000		2.833:0	0	0
Video 2	Mon Jan 22 17:55:03 2007	40.15.15.2:2001	231.1.0.2:1001		2.833:0	0	0
Video 3	Mon Jan 22 17:55:03 2007	40.15.15.2:2002	231.1.0.3:1002		2.833:0	0	0
Video 4	Mon Jan 22 17:55:02 2007	40.15.15.2:2003	231.1.0.4:1003		2.833:0	0	0
Video 5	Mon Jan 22 17:55:03 2007	40.15.15.2:2004	231.1.0.5:1004		2.833:0	0	0
Video 6	Mon Jan 22 17:55:01 2007	40.15.15.2:2005	231.1.0.6:1005		2.833:0	0	0
	Mon Jan 22 17:55:03 2007	40.15.15.2:2006	40.17.17.2:1006		2.835:0	0	0
	Mon Jan 22 17:55:01 2007	40.15.15.2:2007	40.17.17.2:1007		2.833:0	0	0
	Mon Jan 22 17:55:03 2007	40.15.15.2:2008	40.17.17.2:1008		2.833:0	0	0
	Mon Jan 22 17:55:03 2007	40.15.15.2:2009	40.17.17.2:1009		2.833:0	0	0
	Mon Jan 22 17:55:04 2007	40.15.15.2:2010	40.17.17.2:1010		2.833:0	0	0
	Mon Jan 22 17:55:01 2007	40.15.15.2:2011	40.17.17.2:1011		2.833:0	0	0
	Mon Jan 22 17:55:02 2007	40.15.15.2:2012	40.17.17.2:1012		2.833:0	0	0
	Mon Jan 22 17:55:02 2007	40.15.15.2:2013	40.17.17.2:1013		2.833:0	0	0
	Mon Jan 22 17:55:02 2007	40.15.15.2:2014	40.17.17.2:1014		2.833:0	0	0
	Mon Jan 22 17:55:02 2007	40.15.15.2:2015	40.17.17.2:1015		2.833:0	0	0
	Mon Jan 22 17:55:03 2007	40.15.15.2:2016	40.17.17.2:1016		2.833:0	0	0
	Mon Jan 22 17:55:02 2007	40.15.15.2:2017	40.17.17.2:1017		2.833:0	0	0
	Mon Jan 22 17:55:03 2007	40.15.15.2:2018	40.17.17.2:1018		2.833:0	0	0
	Mon Jan 22 17:55:02 2007	40.15.15.2:2019	40.17.17.2:1019		2.833:0	0	0
	Mon Jan 22 17:55:03 2007	40.15.15.2:2020	40.17.17.2:1020		2.833:0	0	0
	Mon Jan 22 17:55:01 2007	40.15.15.2:2021	40.17.17.2:1021		2.833:0	0	0
	Mon Jan 22 17:55:02 2007	40.15.15.2:2022	40.17.17.2:1022		2.833:0	0	0
	Mon Jan 22 17:55:03 2007	40.15.15.2:2023	40.17.17.2:1023		2.833:0	0	0
	Mon Jan 22 17:55:01 2007	40.15.15.2:2024	40.17.17.2:1024		2.833:0	0	0
	Mon Jan 22 17:55:01 2007	40.15.15.2:2025	40.17.17.2:1025		2.833:0	0	0

211084

MPVN Status

Using the Diagnostics tool, you can view detailed information about the status of Multicast VPNs, including:

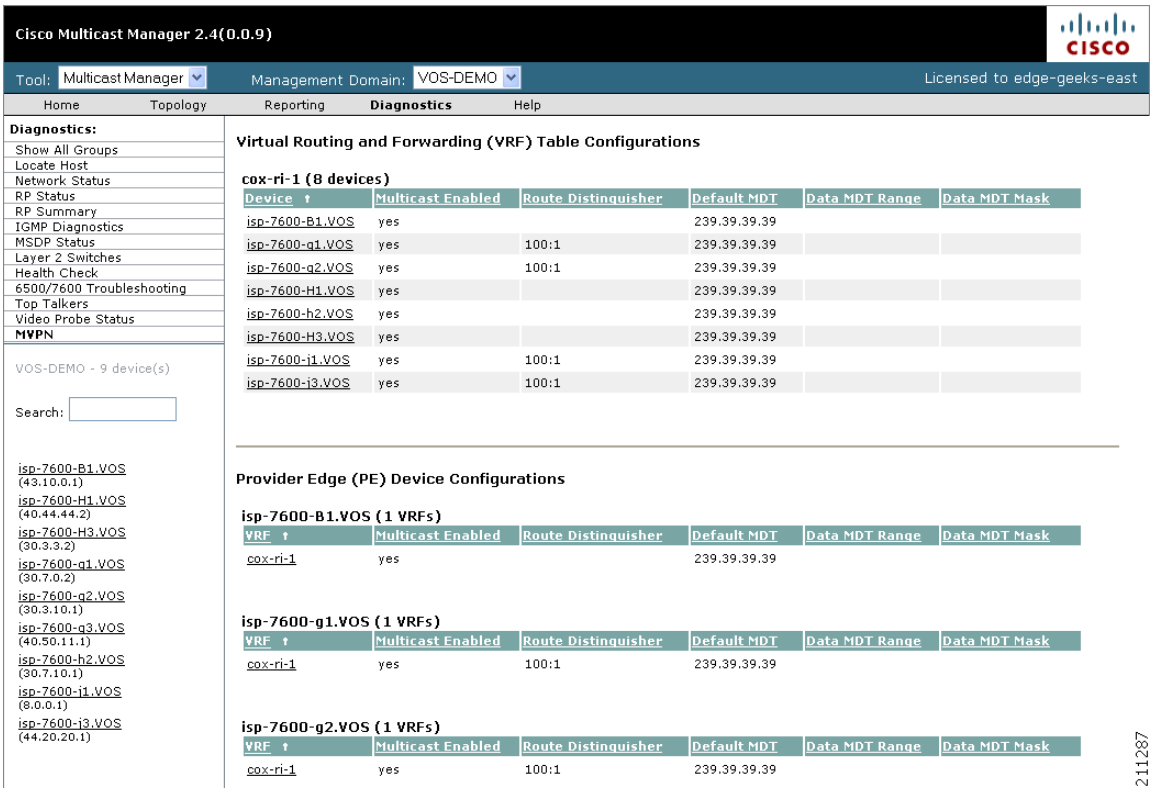
- Virtual Routing and Forwarding (VRF) Table Configurations
- Provider Edge (PE) Device Configurations
- The current status of a specified VRF

To view MVPN status:

Step 1 On the Diagnostics menu, select **MVPN.**

The MVPN Diagnostics page appears, as shown in Figure 4-18.

Figure 4-18 MVPN Diagnostics Page



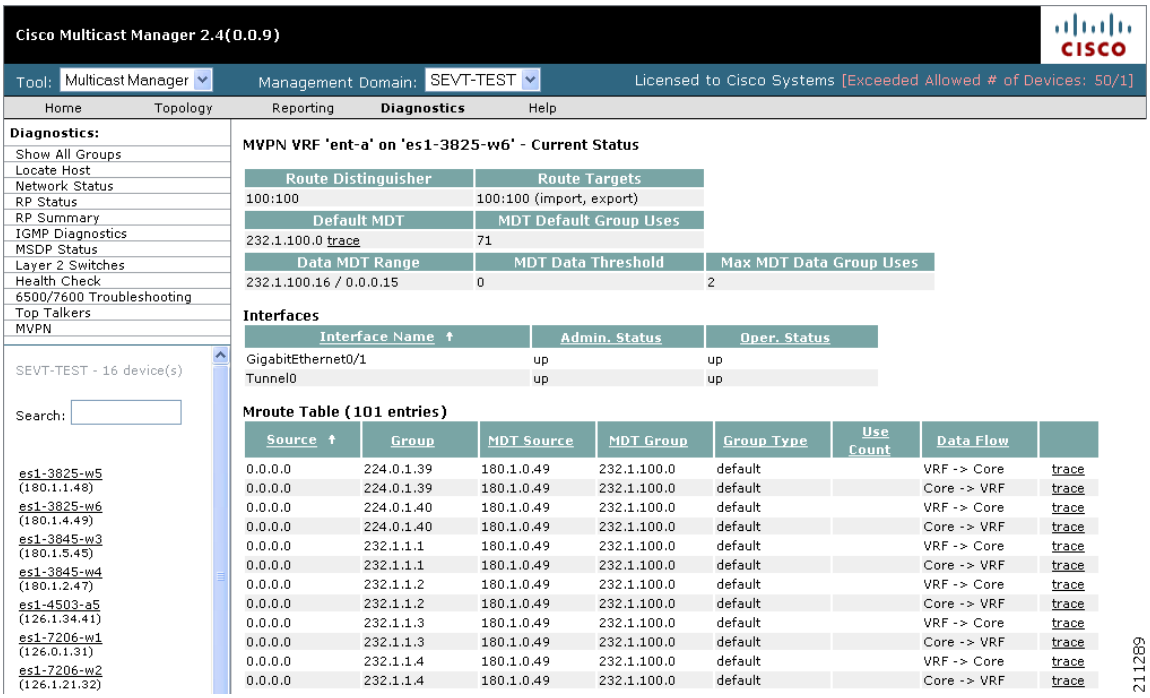
The MPVN Diagnostics page shows:

- Virtual Routing and Forwarding (VRF) Table Configurations
- Provider Edge (PE) Device Configurations

Step 2 To view detailed information about the status a VRF, click on the device name in one of the VRF tables

Cisco Multicast Manager displays the status of the VRF, as shown in Figure 4-19.

Figure 4-19 Viewing VRF Status



The VRF status page indicates:

- **Route Distinguisher**—The route distinguisher for the VRF.
- **Route Targets** —The route targets for the VRF.
- **Default MDT** —The default MDT or the VRF.
- **MDT Default Group Uses** —(please provide description)
- **Data MDT Range**—Default MDT range.
- **MDT Data Threshold Max MDT**—please provide description)
- **Data Group Uses** —please provide description)

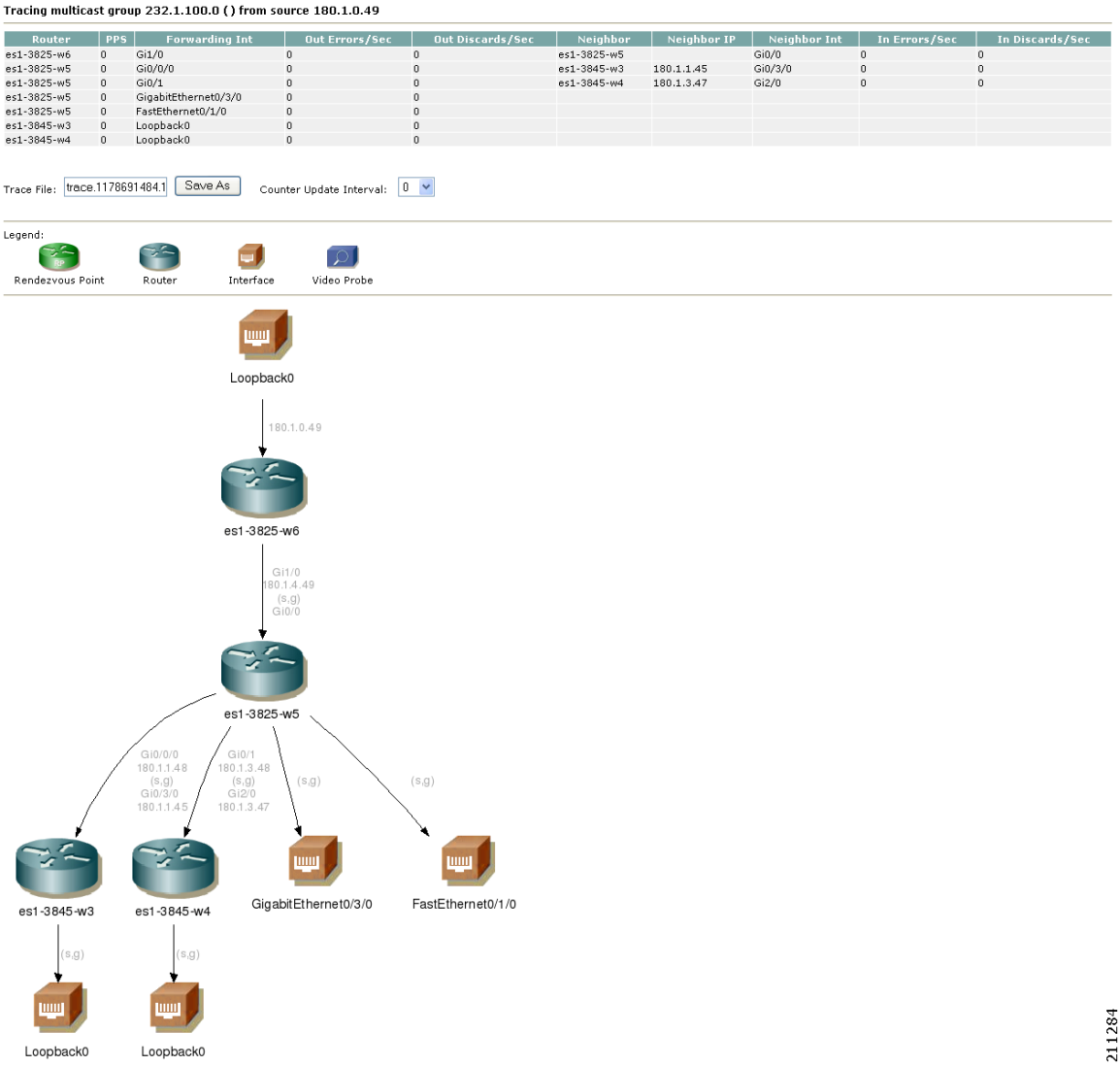
For each interface in the VRF, the VRF status page indicates the interface name, administrative status, and operation status of the interface.

The bottom portion of the display shows an Mroute table for the VRF.

Step 3 To display the current status of a specified multicast group, click on **trace**, next to the IP address in the Default MDT column of the table.

A detailed trace and a topology diagram of the multicast group appear, as shown in Figure 4-20.

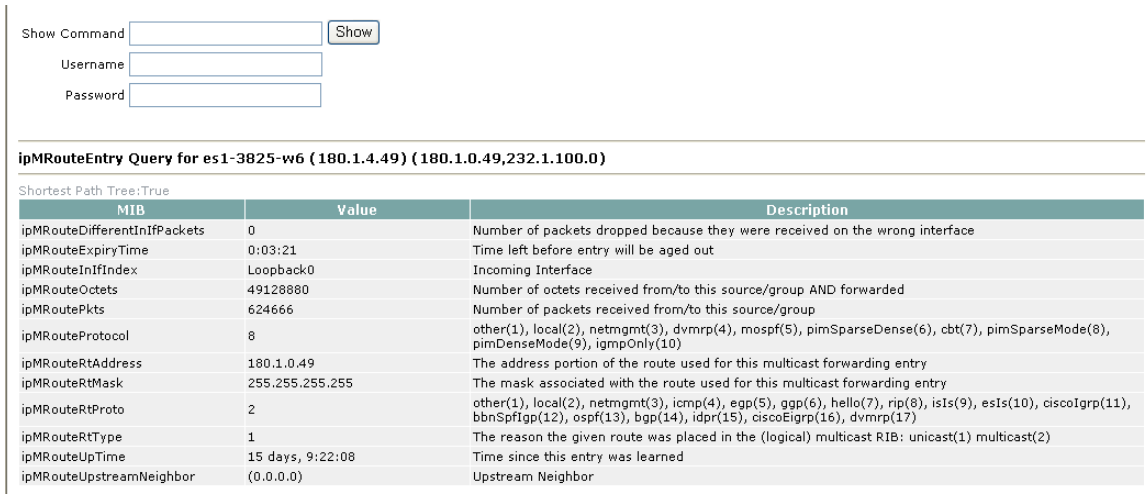
Figure 4-20 Viewing a Multicast Group Trace



Step 4 To run a route entry query for a router, click on a router icon.

Figure 4-21 shows a sample route entry query display.

Figure 4-21 Route Entry Query for a Router in a Multicast Group



MIB	Value	Description
ipMRouteDifferentInIfPackets	0	Number of packets dropped because they were received on the wrong interface
ipMRouteExpiryTime	0:03:21	Time left before entry will be aged out
ipMRouteInIfIndex	Loopback0	Incoming Interface
ipMRouteOctets	49128880	Number of octets received from/to this source/group AND forwarded
ipMRoutePkts	624666	Number of packets received from/to this source/group
ipMRouteProtocol	8	other(1), local(2), netmgmt(3), dvmrp(4), mospf(5), pimSparseDense(6), cbt(7), pimSparseMode(8), pimDenseMode(9), igmpOnly(10)
ipMRouteRtAddress	180.1.0.49	The address portion of the route used for this multicast forwarding entry
ipMRouteRtMask	255.255.255.255	The mask associated with the route used for this multicast forwarding entry
ipMRouteRtProto	2	other(1), local(2), netmgmt(3), icmp(4), egp(5), ggp(6), hello(7), rip(8), isIs(9), esIs(10), ciscoIgrp(11), bbnSpfIgp(12), ospf(13), bgp(14), idpr(15), ciscoEigrp(16), dvmrp(17)
ipMRouteRtType	1	The reason the given route was placed in the (logical) multicast RIB: unicast(1) multicast(2)
ipMRouteUpTime	15 days, 9:22:08	Time since this entry was learned
ipMRouteUpstreamNeighbor	(0.0.0.0)	Upstream Neighbor

Managing Router Diagnostics

You can view specific multicast diagnostics on a router by clicking the router in the lower left pane.

The Router Diagnostics page is similar to the Multicast Diagnostics page (under Show All Groups), except data is for the selected router only.

- From the **Show Command** field, you can issue a show, ping, trace, or mtrace command. Scroll down to see all the sources and groups active on this router.
- From the SNMP Queries pane, for a selected router, you can view:
  - **IGMP Cache Entries—**Shows IGMP cache information.

Figure 4-22 IGMP Cache Entries

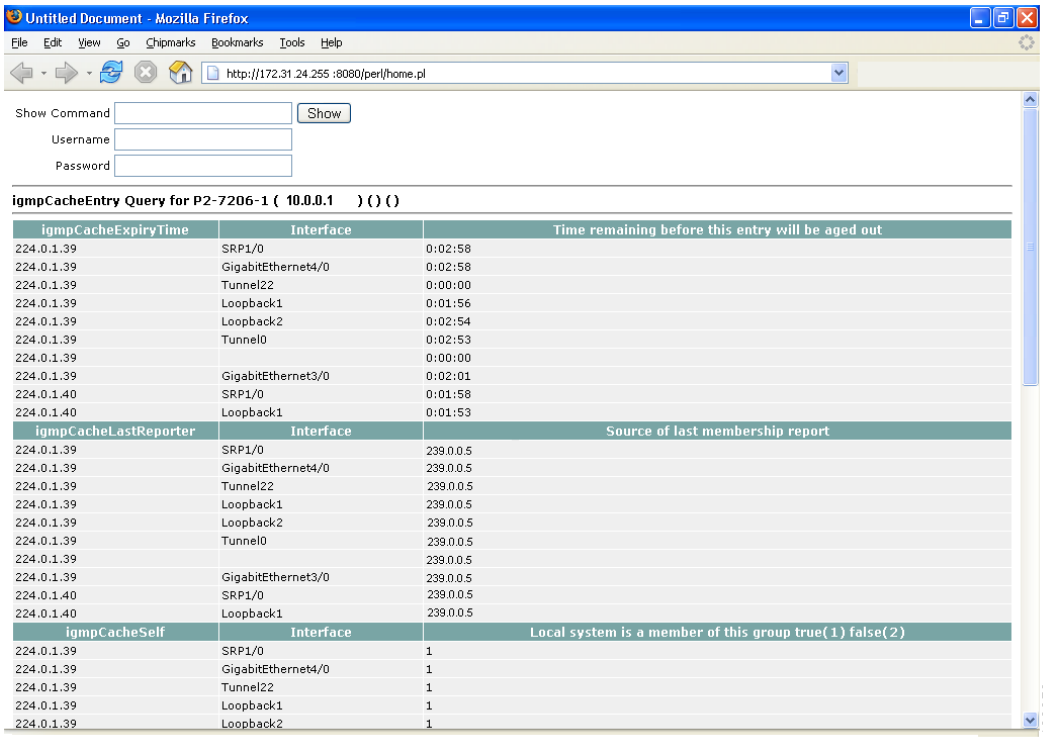
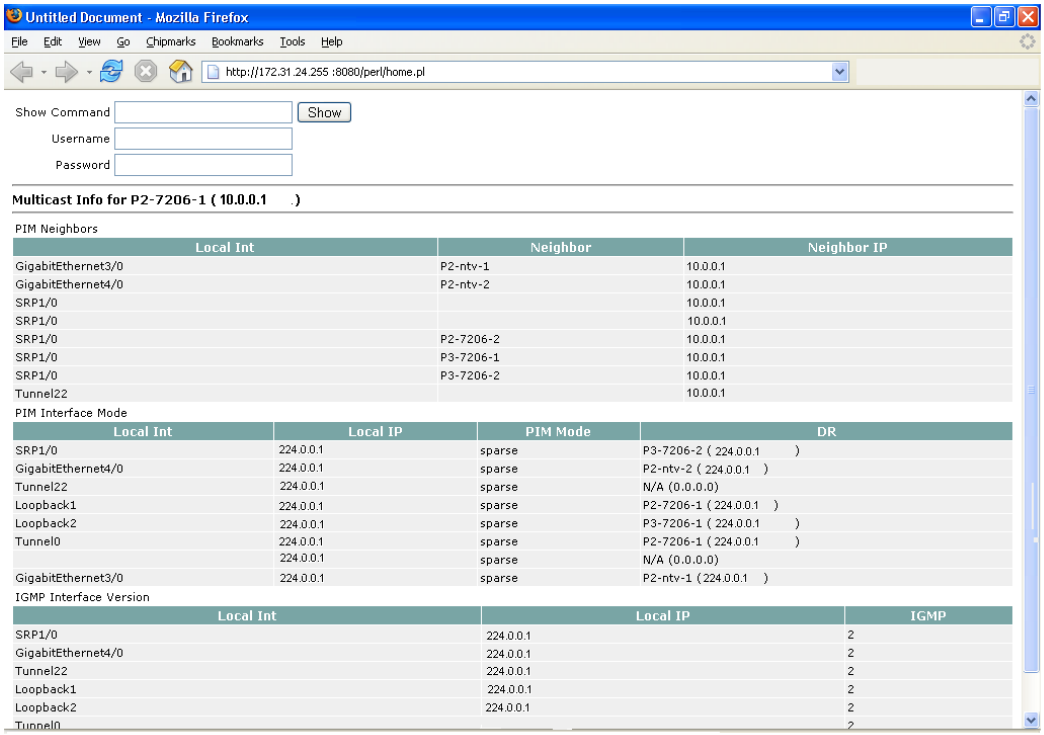
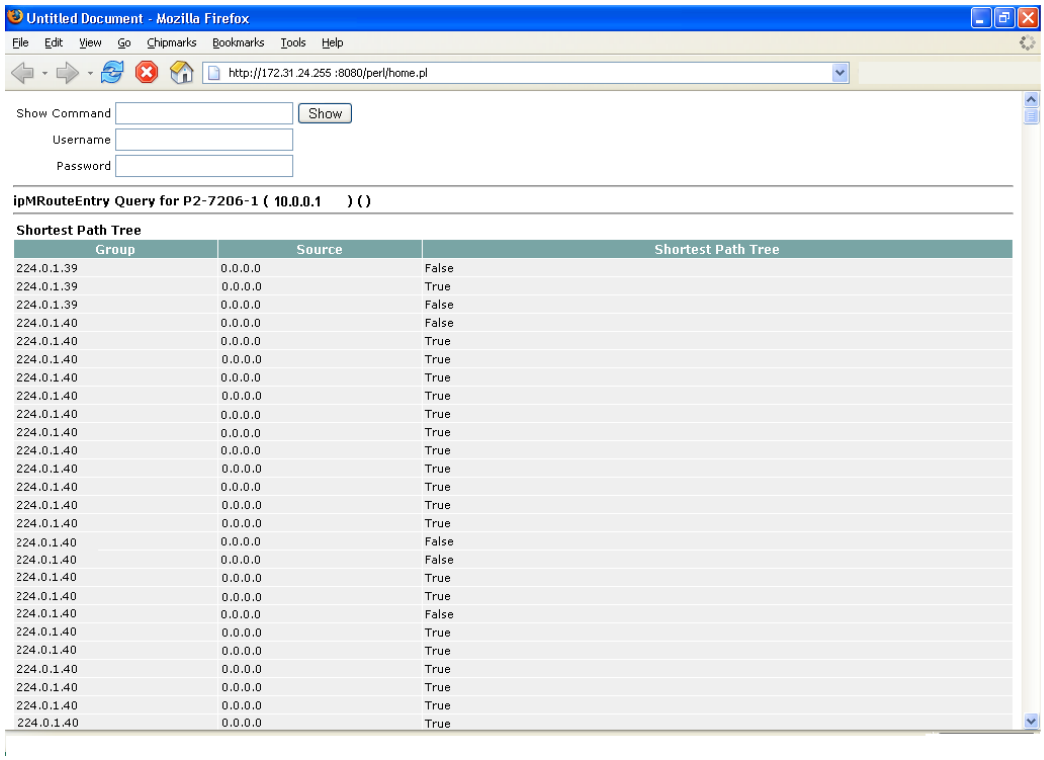


Figure 4-23 Multicast Information



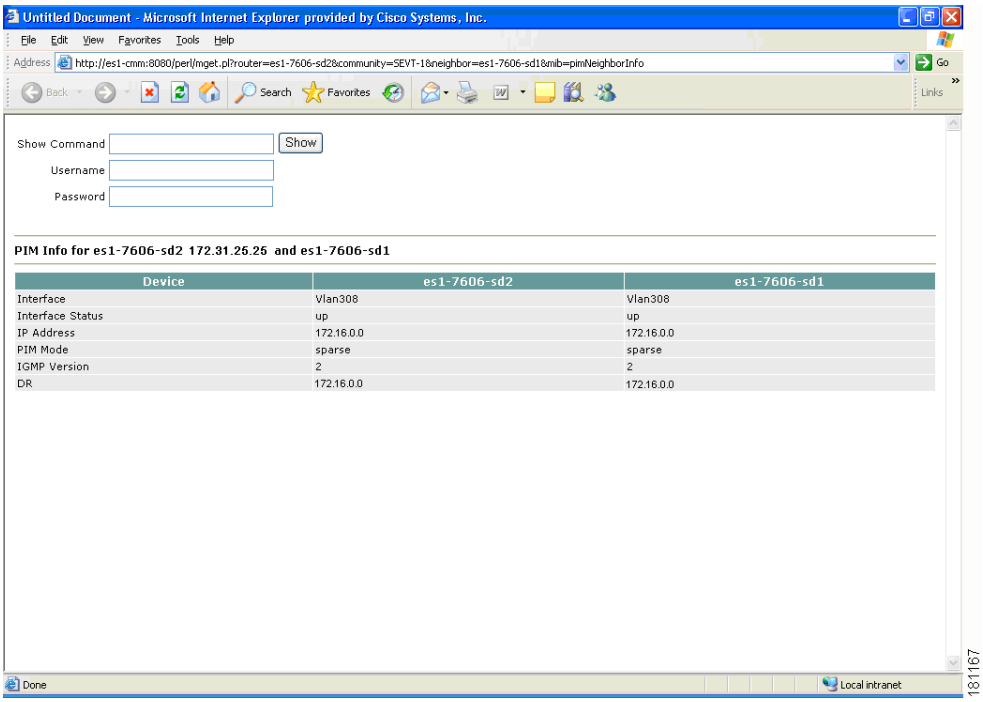
- **Multicast Routing Table**—Shows the multicast routing table.
- **Multicast Information**—Shows multicast topology information.

Figure 4-24 Multicast Routing Table



- **PIM Neighbor Information**—Check that a PIM neighbor exists and compare a router's PIM neighbor information. Select the PIM neighbor you want to query.

Figure 4-25 PIM Neighbor Information



Viewing User Guide Help

To view a PDF version of the *User Guide for Cisco Multicast Manager, 2.4,* select **Help**.

CHAPTER 5

Maintaining and Managing the CMM

This section contains information concerning the underlying operation of CMM and will be of most interest to the System Administrator that supports the application.

This chapter covers:

Viewing Configuration Files

Assuming the application is installed on Solaris, the directory location will be */opt/RMSMMT* (on Linux it would be */usr/local/netman*). Multicast domain configuration files are kept in */opt/RMSMMT/mmtsys/sys* and named <*domain*>*.mm.conf*, where <*domain*> is the name of the multicast domain. The file is in the format of option=value. This file should not be edited manually. The polling daemon configuration files are also kept in this directory. The global polling configuration file is *rmspoll.conf*, and the domain specific files are *rmspoll.*<*domain*>*.conf*. Like the domain configuration files, these files should be modified only through the browser interface. The only time these files should be modified manually is with the assistance of RMS tech support.

Viewing Log Files

The */opt/RMSMMT/mmtsys/sys* directory also contains two log files: *events.log* and *rmspolld.log*.

Viewing the events.log File

The `events.log` file contains syslog type messages, shown below, that correspond to the SNMP traps sent by the polling daemon.

monlo:1082550198:172.16.1.9:1.3.6.1.2.1.31.1.1.1.2.10:0:10:631643:0:50

gone:1082550198:192.168.201.254:239.1.1.1:192.168.1.25:0:0:0:0

hi:1082550198:172.16.1.9:239.1.1.1:192.168.1.25:4116:92785:137:100

This file provides the information for the text-based reports provided by CMM. Depending on the polling interval, and number of objects being polled, this file may grow very quickly. It should be rotated along with all other syslog files on the server.

Viewing the rmspolld.log File

The rmspolld.log file contains log messages pertaining to the polling daemon.

```
04/23/2004 09:40:54 RMS Polling Agent v2.1(1) started successfully.
04/23/2004 09:55:49 Exiting on SIGTERM
```

Viewing Apache Log Files

The Apache log files are located in */opt/RMSMMT/httpd_perl/logs*. When troubleshooting the application, tailing the error_log file (**tail –f error_log**) will provide useful information. Additional application information can be logged to the error_log file by adding the line **debug=1** to the <*domain*>*.mm.conf* file mentioned above.

Note Turning on this debug option generates a large amount of data and should be used only for short periods in conjunction with working RMS tech support.

Viewing Database Files

The database files used by CMM are located in */opt/RMSMMT/mmtsys/db*. The topology database created by running discovery is <*domain*>*.topo.db*. The S,G cache, also created during discovery, is <*domain*>*.sg.db*. The cache file is recreated when the polling daemon is running and polling the RPs. The lock files associated with each database file should never be manually removed. Removing these files could corrupt the databases.

Each domain also has a */opt/RMSMMT/mmtsys/db/*<*domain*> directory associated with it. This directory contains the IOS versions (*iosver.db*) for the domain. Multicast forwarding tree baselines are also saved in this directory.

The IP address database (*ipaddr.db*) is also located in *opt/RMSMMT/mmtsys/db*.

Viewing Device Configuration Files

If TFTP is enabled on the server, and the SNMP read-write community string is supplied, then the application can download router configurations. The configurations are initially stored in the */tftpboot* directory. If a configuration is saved from the “Display Router Config” screen, then a directory will be created (*/opt/RMSMMT/configs/*<*device*>) to hold the saved configurations.

Viewing Historical Data

PPS data collected by the polling daemon for S,G threshold polling and Layer 2 switch port polling, are stored in RRD files in */opt/RMSMMT/mmtsys/data*.

Viewing Standard Multicast MIBs

Certain versions of IOS now support the standard based IPMROUTE and IGMP MIBs. The STDMIBS file in the */opt/RMSMMT/mmtsys/db* controls which IOS versions the standard MIBs will be used for. The file currently contains the following entries:

```
# This file contains versions of IOS that use the standard multicast MIBs.

12.3.*.*
12.2.*.T*
12.2.*.BC*
```

Including Backup Directories

To backup application specific data, the following directories should be included in any system backups:

```
/opt/RMSMMT/mmtsys/data
/opt/RMSMMT/mmtsys/db
/opt/RMSMMT/mmtsys/sys
/opt/RMSMMT/configs
```

Prior to performing backups, the */opt/RMSMMT/K98mmt* script should be run to ensure that files are being changed while the backup is being performed.

Note Running the K98mmt script stops the Apache server along with the polling daemon. The S98mmt script will only start the Apache server. The polling daemon has to be started from the browser at this time.

INDEX

E

F

G

H

I

L

M

N

P

R

S

T

U

V