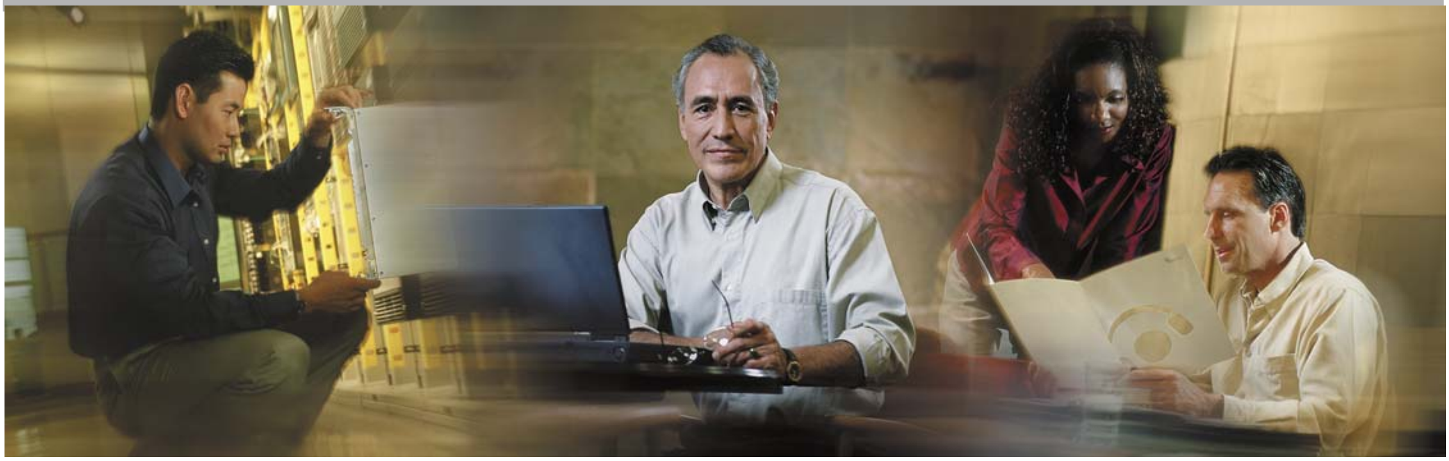


User Guide for the Cisco Multicast Manager 2.3.3

Corporate 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: 408 526-4100

Customer Order Number:
Text Part Number: OL-7348-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

User Guide for the Cisco Multicast Manager 2.3.3

CONTENTS

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Preface

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/

Cisco Marketplace:

http://www.cisco.com/go/marketplace/

Cisco Systems

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output.

Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

CHAPTER 1

Using the Cisco Multicast Manager

This chapter covers:

System Requirements

Operating Systems:

- Solaris 8
- Solaris 9
- Red Hat Enterprise Linux AS Release 3 (Taroon Update 4)

Minimum Recommended Systems:

Sun Fire V100 with:

- Disk Space—300MB
- Memory—1GB
- Up to 150 devices
- Up to 1500 S,Gs

Sun Fire V210 with:

- Disk Space—300MB
- Memory—1GB
- Supports up to 300 devices
- Supports up to 3000 S,Gs

Sun Fire 280R with:

- Disk Space—300MB
- Memory—1GB
- Supports up to 500 devices
- Supports up to 5000 S,Gs

Note If the number of devices/S,Gs exceeds 500/5000, and/or other applications are installed on the system, then the requirements might be greater than shown here.

Intel PIII 1GHz (running RHEL AS 4) (Taroon Update 4) with:

- Disk Space—300MB
- Memory—512MB

Note *Disk space requirements will vary depending on the size of the network, the number of devices being polled for thresholds, and how often log files are rotated. The following log files are generated by CMM 2.3(3):*

```
<INSTALLDIR>/mmtsys/sys/events.log
<INSTALLDIR>/mmtsys/sys/rmspolld.log
<INSTALLDIR>/httpd_perl/logs/error_log
```

Solaris Installation Instructions

To install the CMM for Solaris 2.8 or Solaris 2.9, log in as the root user and follow one of the approaches outlined below.

Note Approximately 300MB of disk space is required for installation.

1. Install the CMM in the following directory:

   ```
   /opt/RMSMMT
   ```

   If there is not enough room in the */opt* directory, create the *RMSMMT* directory on another partition and create a symbolic link to it from */opt*. For example:

   ```
   # mkdir /space/RMSMMT
   # cd /opt
   # ln -s /space/RMSMMT RMSMMT
   # chown -h mmtuser:mmtuser RMSMMT
   ```

If you symbolically link */opt/RMSMMT* to the actual installation directory as shown above, when installation is complete, you **must** cd to the actual installation directory, similar to:

```
# cd /space
```

and issue the following command:

```
# chown -R mmtuser:mmtuser RMSMMT
```

Otherwise, the installation will create the directory and set the ownership for you.

2. If you are installing from the CDROM, enter:

```
# cd /cdrom/cdrom0
# ./setup.sh
```

(Optional) If for some reason vold is not running, you will have to manually mount the cdrom by entering:

```
# mount -rt hsfs /dev/sr0 /cdrom
```

or

```
# mount -rt hsfs /dev/dsk/c0t6d0s2 /cdrom
```

3. If you are installing from the tar file, create a tmp directory and place the tar file in the directory:

```
# cd /tmp
# mkdir rms
# cd rms
# gunzip -c mmt-sol-2.1-X-full.tar.gz | tar xvf -
# ./setup.sh
```

You should then be able to start and stop the server by entering:

```
/opt/RMSMMT/S98mmt
```

and

```
/opt/RMSMMT/K98mmt
```

The default login is admin/rmsmmt.

Note The K98mmt script will stop the apache server and the polling daemon.

The S98mmt script will only start the apache server. You will have to manually start the polling daemon through the application if desired.

During installation, the K98mmt script is installed in the */etc/rc0.d* directory.

This will ensure that the polling daemon shuts down properly upon system reboot.

The server is configured by default to run on port 8080. If you want to change the port, edit the following file:

```
/opt/RMSMMT/httpd_perl/conf/httpd.conf
```

Output from a sample installation:

```
#=====[ Sample Installation ]=====#

root@ganymede/export/home/mike/mmtinstall-> ./setup.sh
Installing Cisco Multicast Manager Version 2.1
Copyright (c) 2003-2004 Cisco Systems, Inc. All Rights Reserved.

The application installs in /opt/RMSMMT. Do you wish to continue? [y/n]: y
Creating mmtuser gid...
Creating mmtuser uid...
Locking mmtuser account...
Installing Apache...
Installing Perl...
Installing MIBS...
Installing support files...
Installing K98mmt to /etc/rc0.d to ensure proper shutdown of application...
Would you like the S98mmt script installed in /etc/rc3.d to start the application upon
system boot? [y/n]: y
Seeding IP Address database with reserved Multicast Addresses...
Modifying httpd.conf file for this system...
Installation Finished.
```

Linux Installation Instructions

To install the CMM for Red Hat Enterprise Linux AS Release 3 (Taroon Update 4), log in as the root user and follow one of the approaches outlined below.

Note Approximately 300MB of disk space is required for installation.

1. Install the CMM in the following directory:

   ```
   /usr/local/netman
   ```

   If there is not enough room in the */usr/local* directory, create the *netman* directory on another partition and create a symbolic link to it from */usr/local*. For example:

   ```
   # mkdir /space/netman
   # cd /usr/local
   # ln -s /space/netman netman
   # chown -h mmtuser:mmtuser netman
   ```

   If you symbolically link */usr/local/netman* to the actual installation directory as shown above, when installation is complete, you **must** cd to the actual installation directory, similar to:

   ```
   # cd /space
   ```

   and issue the following command:

   ```
   # chown -R mmtuser:mmtuser netman
   ```

   Otherwise, the installation will create the directory and set the ownership for you.

2. If you are installing from the CDROM, enter:

   ```
   # cd /mnt/cdrom
   # ./setup.sh
   ```

3. If you are installing from the tar file, create a tmp directory and place the tar file in the directory:

```
# cd /tmp
# mkdir rms
# cd rms
# gunzip -c mmt-linux-2.1-X-full.tar.gz | tar xvf -
# ./setup.sh
```

You should then be able to start and stop the server by entering:

```
/usr/local/netman/S98mmt
```

and

```
/usr/local/netman/K98mmt
```

The default login is admin/rmsmmt.

Note The K98mmt script will stop the apache server and the polling daemon.

The S98mmt script will only start the apache server. You will have to manually start the polling daemon through the application if desired.

During installation, the K98mmt script is installed in the */etc/rc0.d* directory.

This will ensure that the polling daemon shuts down properly upon system reboot.

The server is configured by default to run on port 8080. If you want to change the port, edit the following file:

```
/usr/local/netman/httpd_perl/conf/httpd.conf
```

Output from a sample installation:

```
#=====[ Sample Installation ]=====#

root@ganymede/export/home/mike/mmtinstall-> ./setup.sh
Installing Cisco Multicast Manager Version 2.3
Copyright (c) 2003-2004 Cisco Systems, Inc. All Rights Reserved.

The application installs in /usr/local/netman. Do you wish to continue? [y/n]: y
Creating mmtuser gid...
Creating mmtuser uid...
Locking mmtuser account...
Installing Apache...
Installing Perl...
Installing MIBS...
Installing support files...
Installing K98mmt to /etc/rc0.d to ensure proper shutdown of application...
Would you like the S98mmt script installed in /etc/rc3.d to start the application upon
system boot? [y/n]: y
Seeding IP Address database with reserved Multicast Addresses...
Modifying httpd.conf file for this system...
Installation Finished.
```

Licensing

CMM 2.3.3 requires a license file. The application license is contained in the license.key file. This file should be placed in the following directory:

On Solaris:

```
/opt/RMSMMT/mmtsys/sys
```

On Linux:

```
/usr/local/netman/mmtsys/sys
```

The file should be owned by mmtuser (chown mmtuser:mmtuser license.key) and be set to read-only (chmod 0444 license.key). The license is tied to the IP address of the CMM server.

Starting and Stopping CMM

To start the application:

On Solaris:
From the CMM home directory (by default, */opt/RMSMMT*) run the S98mmt script.

On Linux:
From the CMM home directory (by default, */usr/local/netman*) run the S98mmt script.on Linux.

To stop the application, run the K98mmt script.

The S98mmt script also runs the S98mmtpolld script, which starts the polling daemon. The S98mmtpolld script can also be used as a watchdog script to ensure that the polling daemon is up and running. The root crontab configuration would be:

On Solaris:

```
0,5,10,15,20,25,30,35,40,45,50,55 * * * * /opt/RMSMMT/S98mmtpolld
```

On Linux:

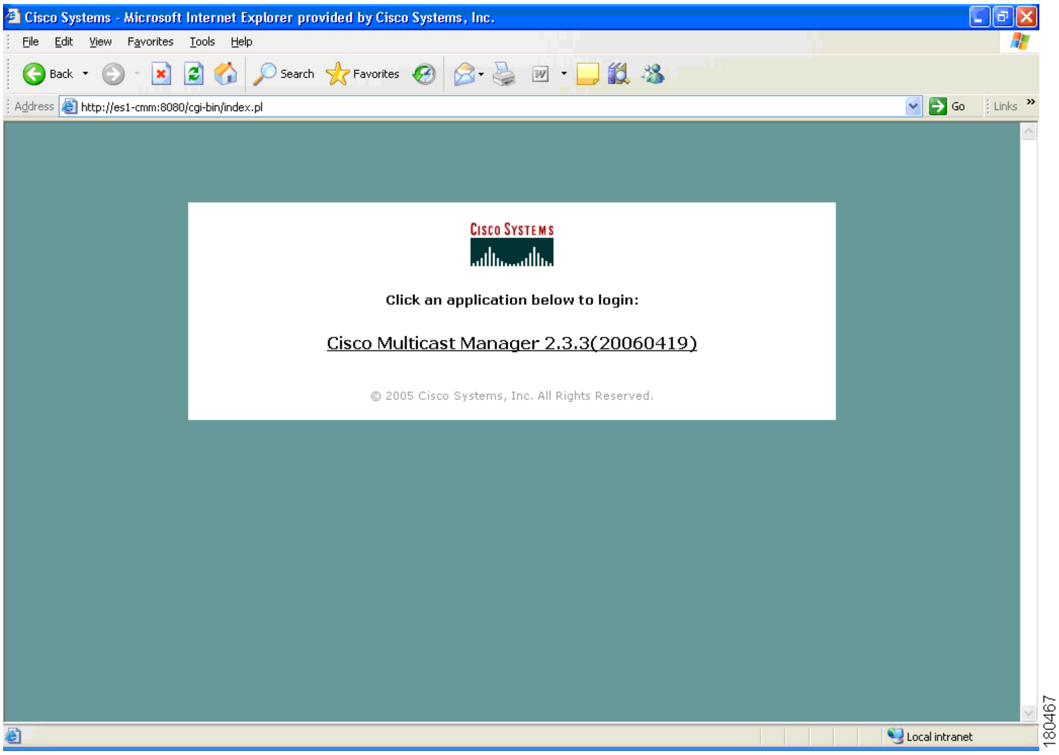
```
*/5 * * * * /usr/local/netman/S98mmtpolld
```

These entries will run the script every 5 minutes.

Logging Into CMM

To access CMM, enter the IP address or the name of the server where the software is installed. For example: http://192.168.1.9:8080. The default port of 8080 can be changed as described in the installation instructions.

Figure 1-1 Login Page for CMM 2.3.3


Cisco Systems - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
http://es1-cmm:8080/cgi-bin/index.pl
Go
Links
Cisco Systems
Local intranet
180467

Click an application below to login:

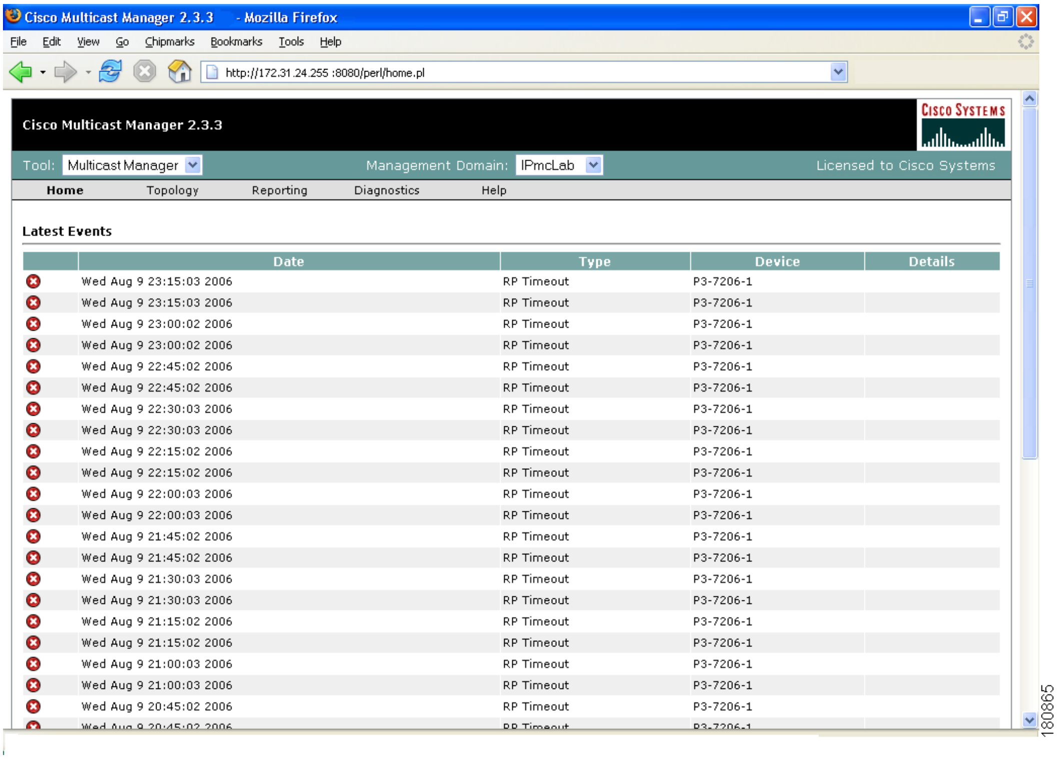
Cisco Multicast Manager 2.3.3(20060419)

© 2005 Cisco Systems, Inc. All Rights Reserved.

To enter CMM, click on Cisco Multicast Manager 2.3.3. You are prompted for a username and a password. The default CMM username is *admin*, and the default CMM password is *rmsmmt*.

The Multicast Manager Home page appears.

Figure 1-2 Multicast Manager Home Page



Cisco Multicast Manager 2.3.3 - Mozilla Firefox
File Edit View Go Chipmarks Bookmarks Tools Help
http://172.31.24.255:8080/perl/home.pl
Cisco Multicast Manager 2.3.3
Cisco Systems
Tool: Multicast Manager
Management Domain: IPmcLab
Licensed to Cisco Systems
Home
Topology
Reporting
Diagnostics
Help
180865

Latest Events

	Date	Type	Device	Details
⊗	Wed Aug 9 23:15:03 2006	RP Timeout	P3-7206-1	
⊗	Wed Aug 9 23:15:03 2006	RP Timeout	P3-7206-1	
⊗	Wed Aug 9 23:00:02 2006	RP Timeout	P3-7206-1	
⊗	Wed Aug 9 23:00:02 2006	RP Timeout	P3-7206-1	
⊗	Wed Aug 9 22:45:02 2006	RP Timeout	P3-7206-1	
⊗	Wed Aug 9 22:45:02 2006	RP Timeout	P3-7206-1	
⊗	Wed Aug 9 22:30:03 2006	RP Timeout	P3-7206-1	
⊗	Wed Aug 9 22:30:03 2006	RP Timeout	P3-7206-1	
⊗	Wed Aug 9 22:15:02 2006	RP Timeout	P3-7206-1	
⊗	Wed Aug 9 22:15:02 2006	RP Timeout	P3-7206-1	
⊗	Wed Aug 9 22:00:03 2006	RP Timeout	P3-7206-1	
⊗	Wed Aug 9 22:00:03 2006	RP Timeout	P3-7206-1	
⊗	Wed Aug 9 21:45:02 2006	RP Timeout	P3-7206-1	
⊗	Wed Aug 9 21:45:02 2006	RP Timeout	P3-7206-1	
⊗	Wed Aug 9 21:30:03 2006	RP Timeout	P3-7206-1	
⊗	Wed Aug 9 21:30:03 2006	RP Timeout	P3-7206-1	
⊗	Wed Aug 9 21:15:02 2006	RP Timeout	P3-7206-1	
⊗	Wed Aug 9 21:15:02 2006	RP Timeout	P3-7206-1	
⊗	Wed Aug 9 21:00:03 2006	RP Timeout	P3-7206-1	
⊗	Wed Aug 9 21:00:03 2006	RP Timeout	P3-7206-1	
⊗	Wed Aug 9 20:45:02 2006	RP Timeout	P3-7206-1	
⊗	Wed Aug 9 20:45:02 2006	RP Timeout	P3-7206-1	

For detailed information on this window, see the "Using the Multicast Manager Tool" section on page 1-43.

CMM 2.3.3 has two main Tools:

- **Administration**—Perform configuration tasks
- **Multicast Manager**—View or monitor data

You can find these Tools listed at the top left of the CMM 2.3.3 Web interface.

Using the Administration Tool

System administrators can configure their network using the CMM Administration Tool, containing these web pages:

- Domain Management, page 1-9
- Discovery, page 1-11
- Admin Utilities, page 1-15
- System Security, page 1-17
- User Management, page 1-18
- Device Configuration, page 1-20
- Global Polling Configuration, page 1-23
- Address Management, page 1-27
- Multicast Manager, page 1-28

Domain Management

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

The first step in using the CMM is to create a domain:

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

Step 2 Click on Domain Management.

Step 3 Click on add a new domain. The System Configuration page appears.

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

The System Configuration page contains:

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 the CMM 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.

Field	Description
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.
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 receiver 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.
Use SG Cache	Some networks contain thousands of S,Gs. 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 1-28). 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 1-61). This button only appears 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 only updated when you click the **Refresh Cache** button.

Discovery

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

- Add Router (not supported)
- Adding Layer 2 Switches to Discovery, page 1-11
- Performing Multicast Discovery, page 1-12
- Adding or Re-discovering a Single Device, page 1-14

The discovery process is multicast-specific and only finds 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 re-discovered 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, the snmp ifindex persist command should be used 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:

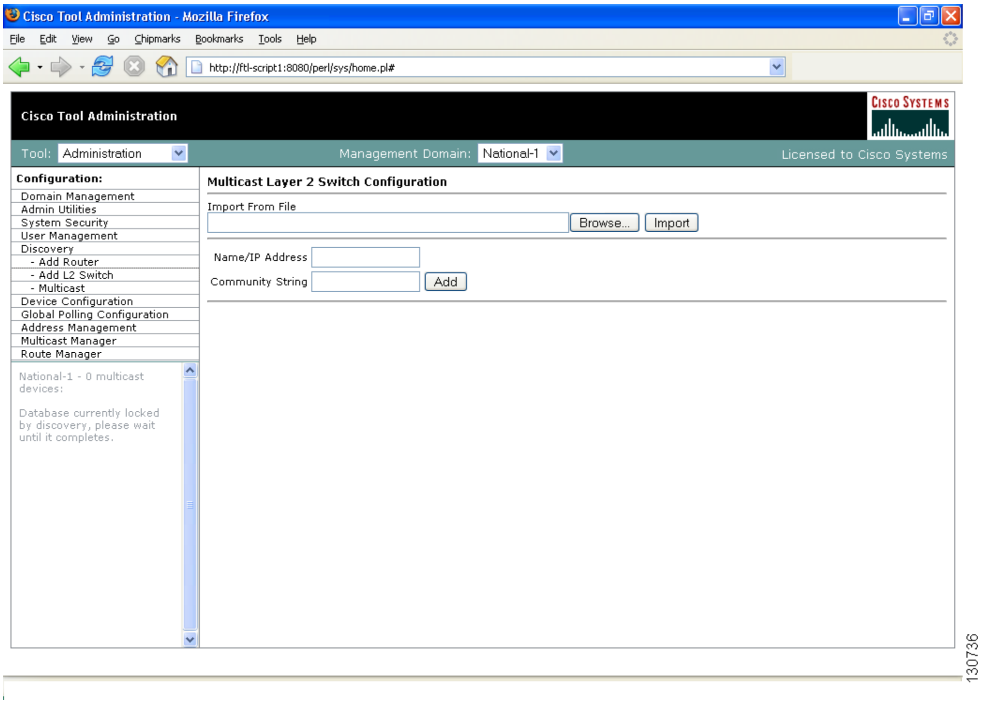
```
#import file format switch IP address or switch name
# this line will be skipped
switchA
192.168.1.1
switchC
10.10.10.1
```

Step 2 Save the file.

Step 3 Within the Administration too, click on **Discovery**.

Step 4 Click **Add L2 Switch**. The Multicast Layer 2 Switch Configuration page appears.

Figure 1-3 Multicast Layer 2 Switch Configuration



Multicast Layer 2 Switch Configuration

Import From File

Name/IP Address

Community String

National-1 - 0 multicast devices:

Database currently locked by discovery, please wait until it completes.

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

Step 6 Click **Import**.

Note Sometimes switches are deployed in a network using different SNMP community strings than those used on the routers. In this case, simply create another domain, with the appropriate SNMP community strings, and add the switches to this domain.

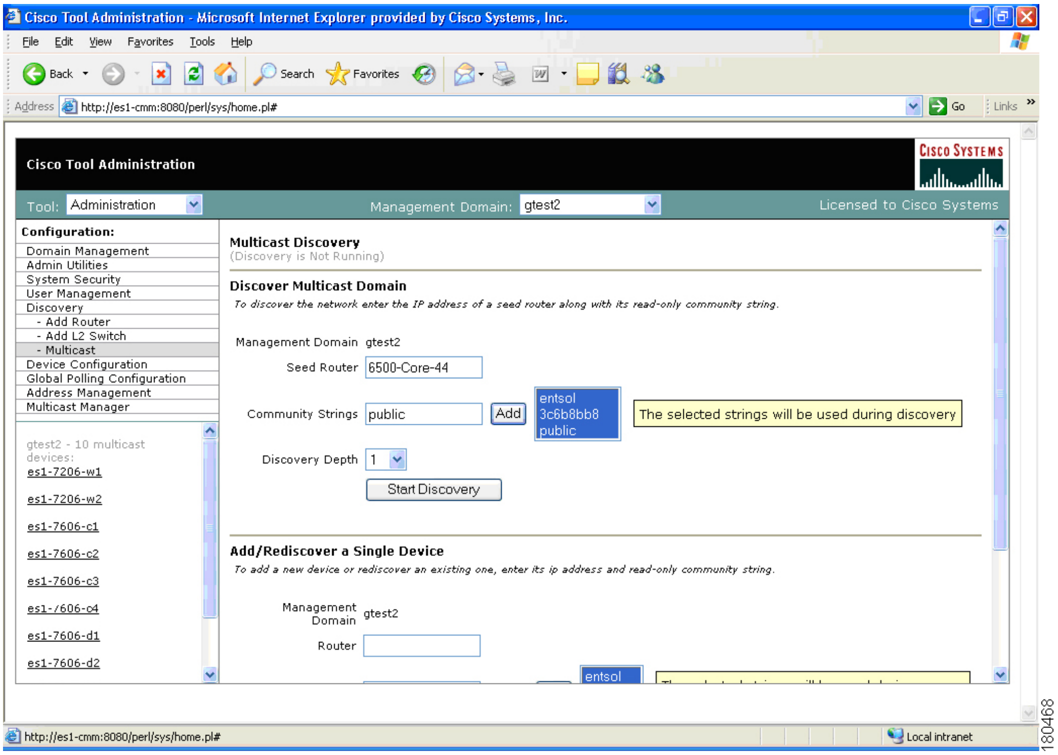
Performing Multicast Discovery

To perform a new multicast discovery:

Step 1 Within the Administration tool, click on **Discovery**.

Step 2 Click **Multicast**. The Multicast Discovery page appears.

Figure 1-4 Multicast Discovery


Cisco Tool Administration - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back Search Favorites
Address http://es1-cmm:8080/perl/sys/home.pl#
Go Links
Cisco Tool Administration
Cisco Systems
Licensed to Cisco Systems
Start Discovery
Add
http://es1-cmm:8080/perl/sys/home.pl#
Local intranet
180468

Tool: Administration
Management Domain: gtest2

Configuration:
- Domain Management
- Admin Utilities
- System Security
- User Management
- Discovery
  - Add Router
  - Add L2 Switch
  - Multicast
- Device Configuration
- Global Polling Configuration
- Address Management
- Multicast Manager

gtest2 - 10 multicast devices:
es1-7206-w1
es1-7206-w2
es1-7606-c1
es1-7606-c2
es1-7606-c3
es1-7606-c4
es1-7606-d1
es1-7606-d2

Multicast Discovery
(Discovery is Not Running)

Discover Multicast Domain
To discover the network enter the IP address of a seed router along with its read-only community string.

Management Domain gtest2
Seed Router 6500-Core-44
Community Strings public [Add] entsol
3c6b8bb8
public The selected strings will be used during discovery
Discovery Depth 1

Add/Rediscover a Single Device
To add a new device or rediscover an existing one, enter its ip address and read-only community string.

Management Domain gtest2
Router
entsol

Step 3 Next to **Management Domain**, select the domain you want to discover (only domains that are created from the System Configuration window appear here). If you select a different domain from the default, you must complete steps 1 and 2 again.

Step 4 Complete the fields in the **Discover Multicast Domain** pane (see field descriptions below) and click **Start Discovery** to continue. As routers are discovered, they appear in the browser window.

Step 5 (Optional) To view discovery progress as it is running, click **Refresh Status**.

Note For details on adding or re-discovering a single device, see the "Adding or Re-discovering a Single Device" section on page 1-14.

The Discover Multicast Domain pane of the Multicast Discovery page contains:

Field	Description
Management Domain	(Read-only) Lists the selected management domain.
Seed Router	Enter the IP address of the seed router to initiate discovery from. 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 the CMM will discover from the seed router (similar to a hop count).

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 amount of 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 has finished, you can view the discovered routers in the lower left pane.

Adding or Re-discovering a Single Device

To add or re-discover a single device:

Step 1 Within the Administration tool, click on **Discovery**.

Step 2 Click **Multicast**. The Multicast Discovery page appears (see Figure 1-4).

Step 3 Within the **Add/Rediscover a Single Device** pane, enter the

Step 4 Next to **Management Domain**, select the domain you want to discover or add to (only domains that are created from the System Configuration window appear here). If you select a different domain from the default, you must complete steps 1 and 2 again.

Step 5 Complete the fields in the **Add/Rediscover a Single Device** pane (see field descriptions below) and click **Add/Rediscover** to continue. As devices are discovered, they appear in the browser window.

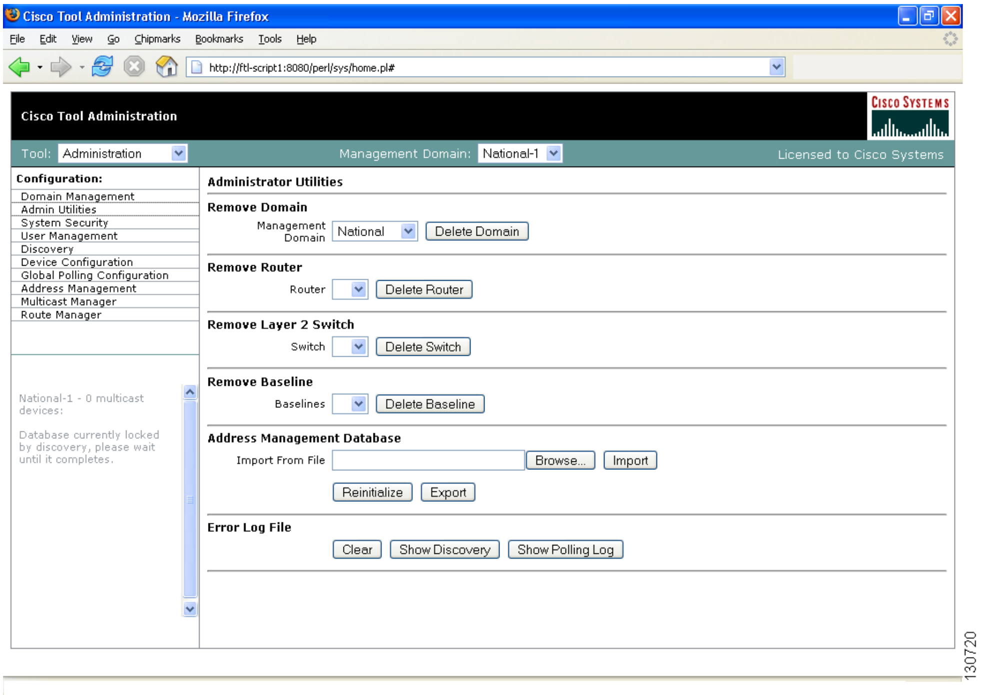
The Add/Rediscover a Single Device pane of the Multicast Discovery page contains:

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.

Admin Utilities

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

Figure 1-5 Administrative Utilities



Cisco Tool Administration - Mozilla Firefox

http://ftl-script1:8080/perl/sys/home.pl#

Cisco Tool Administration

Tool: Administration

Management Domain: National-1

Licensed to Cisco Systems

National-1 - 0 multicast devices:

Database currently locked by discovery, please wait until it completes.

Administrator Utilities

Remove Domain

Management Domain: National

Remove Router

Router

Remove Layer 2 Switch

Switch

Remove Baseline

Baselines

Address Management Database

Import From File

Error Log File

The Administrative Utilities page contains:

Field	Description
Remove Domain	Removes all data associated with a management domain. **Note** Domains cannot be removed while the polling daemon is running.
Remove Router	Removes a specific router from a management domain. However, if the device is being polled, you must remove it from the polling configuration first.
Remove Layer 2 Switch	Removes Layer 2 switches from the management database.
Remove Baseline	Removes a forwarding tree baseline, along with any associated tree change information.

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.

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

System Security

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

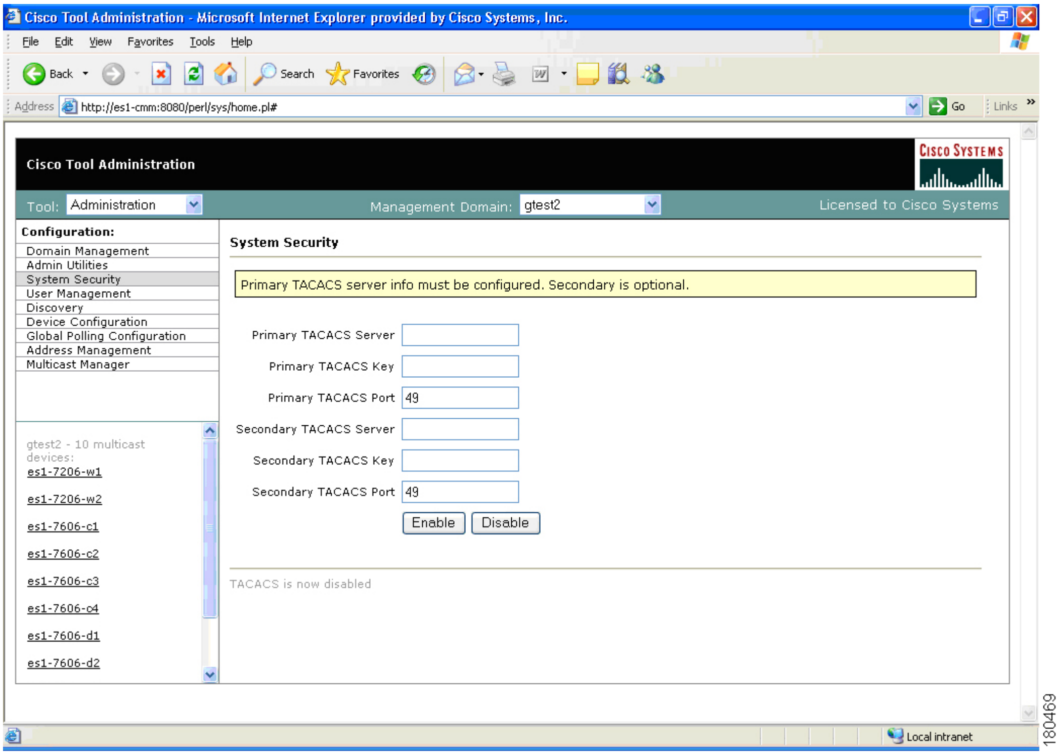
To configure TACACS login, enter the IP address of the TACACS server within the **Primary TACACS Server** field.

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

```
Tacacs_Pri_Key tac_plus_key
  Tacacs_Sec_Key tac_plus_key

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

Figure 1-6 System Security



Cisco Tool Administration - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back
Search
Favorites
Address http://es1-cmm:8080/perl/sys/home.pl#
Go
Links
Cisco Systems
Local intranet
180469

Cisco Tool Administration

Tool: Administration   Management Domain: gtest2   Licensed to Cisco Systems

Configuration:
- Domain Management
- Admin Utilities
- System Security
- User Management
- Discovery
- Device Configuration
- Global Polling Configuration
- Address Management
- Multicast Manager

gtest2 - 10 multicast devices:
- es1-7206-w1
- es1-7206-w2
- es1-7606-c1
- es1-7606-c2
- es1-7606-c3
- es1-7606-c4
- es1-7606-d1
- es1-7606-d2

System Security

Primary TACACS server info must be configured. Secondary is optional.

Primary TACACS Server	
Primary TACACS Key	
Primary TACACS Port	49
Secondary TACACS Server	
Secondary TACACS Key	
Secondary TACACS Port	49

TACACS is now disabled

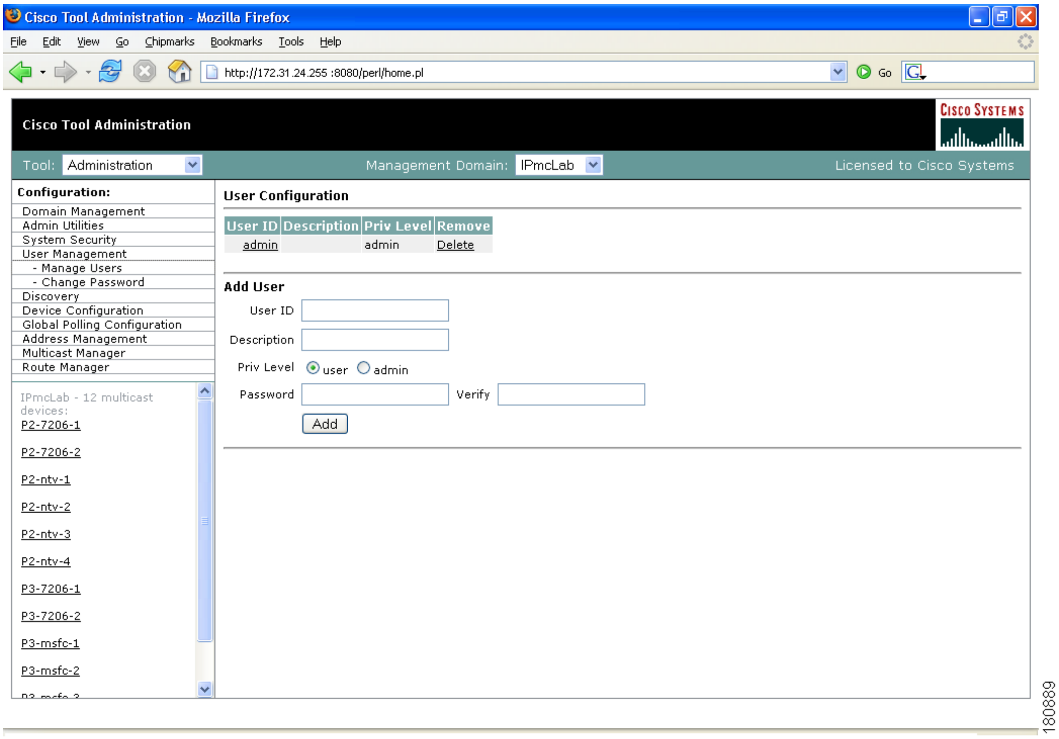
User Management

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

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

- Manage Users
- Change Password

Figure 1-7 Manage Users—User Configuration



User Configuration

User ID	Description	Priv Level	Remove
admin		admin	Delete

Add User

User ID

Description

Priv Level ● user ○ admin

Password Verify

Add

To add a new user:

Step 1 Enter the user ID.

Step 2 (Optional) Enter a description.

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

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

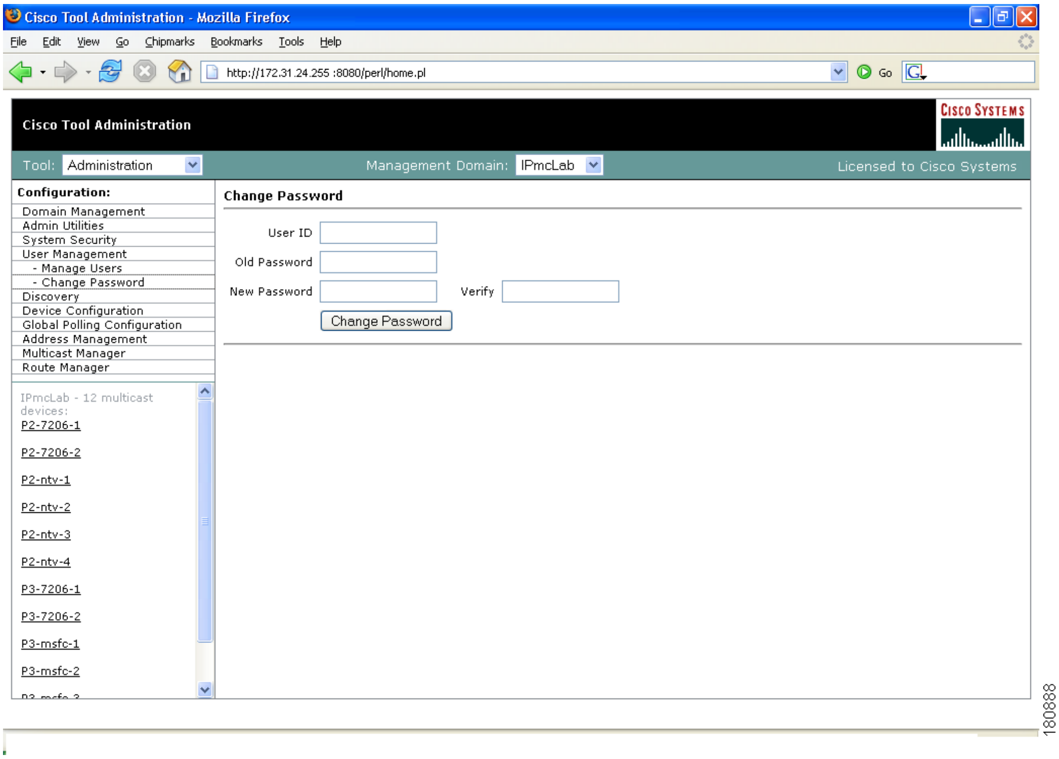
Step 5 Click **Add**.

Clicking on the User ID link in the table allows you to edit the user’s description. Click **Delete** to delete a user (only an administrator can delete users).

Note The admin user account cannot be deleted.

Users can change their password by clicking Change Password.

Figure 1-8 Manage Users—Change Password



To change your password:

Step 1 Enter your user ID.

Step 2 Enter your old password.

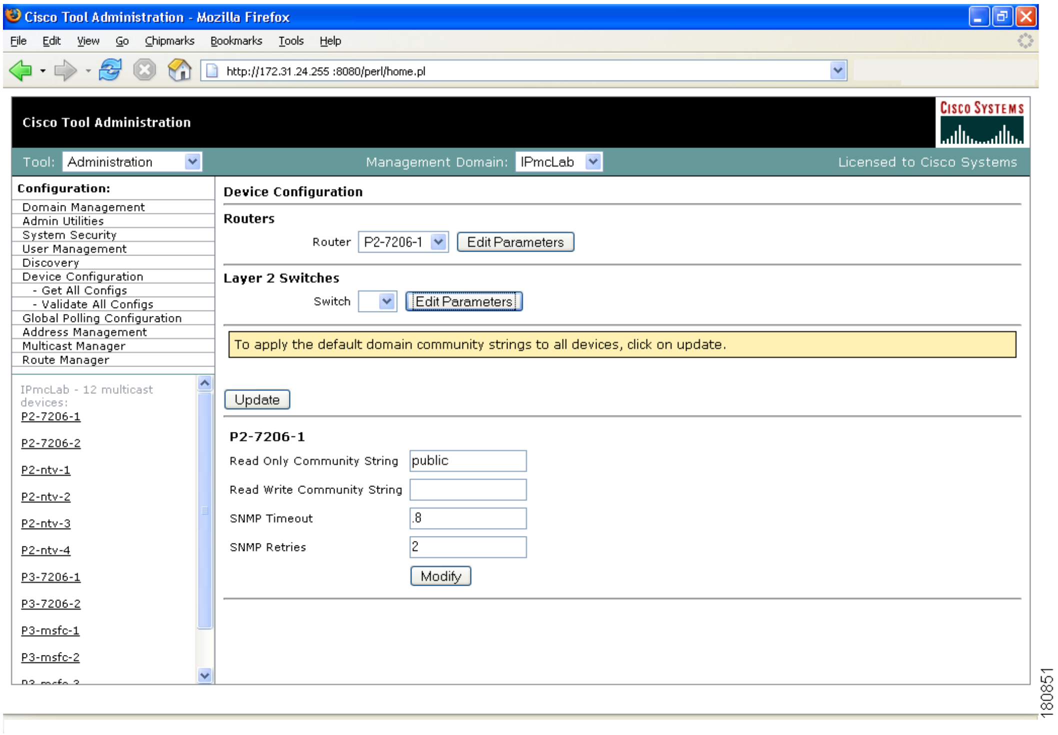
Step 3 Enter your new password in the **Password** and **Verify** boxes.

Step 4 Click **Change Password**.

Device Configuration

Using the Device Configuration page, you can change the SNMP read key of a single device. Select a **Router** or **Switch**, then click **Edit Parameters**.

Figure 1-9 Device Configuration—Edit Parameters



Device Configuration

Routers

Router: P2-7206-1

Layer 2 Switches

Switch:

To apply the default domain community strings to all devices, click on update.

P2-7206-1

Read Only Community String: public

Read Write Community String:

SNMP Timeout: 8

SNMP Retries: 2

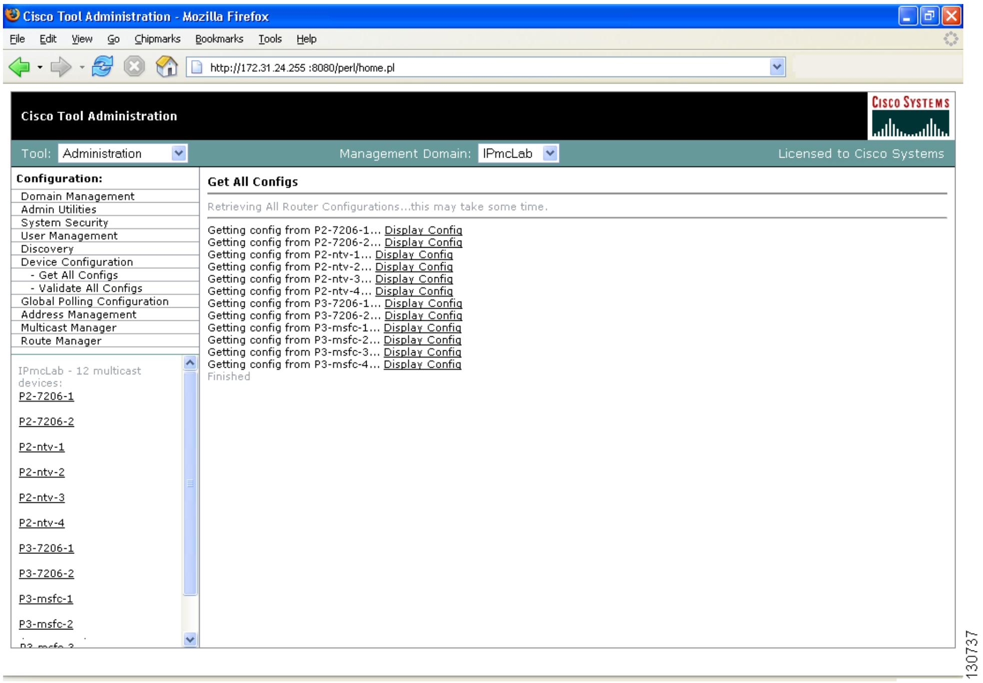
Downloading Router Configurations

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

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

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

Figure 1-10 Get All Configs



Get All Configs

Retrieving All Router Configurations...this may take some time.

```
Getting config from P2-7206-1... Display Config
Getting config from P2-7206-2... Display Config
Getting config from P2-ntv-1... Display Config
Getting config from P2-ntv-2... Display Config
Getting config from P2-ntv-3... Display Config
Getting config from P2-ntv-4... Display Config
Getting config from P3-7206-1... Display Config
Getting config from P3-7206-2... Display Config
Getting config from P3-msfc-1... Display Config
Getting config from P3-msfc-2... Display Config
Getting config from P3-msfc-3... Display Config
Getting config from P3-msfc-4... Display Config
Finished
```

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

Validating Router Configurations

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

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

To select a template and initiate validation:

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

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

Step 2 Ensure the correct Management Domain is selected.

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

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

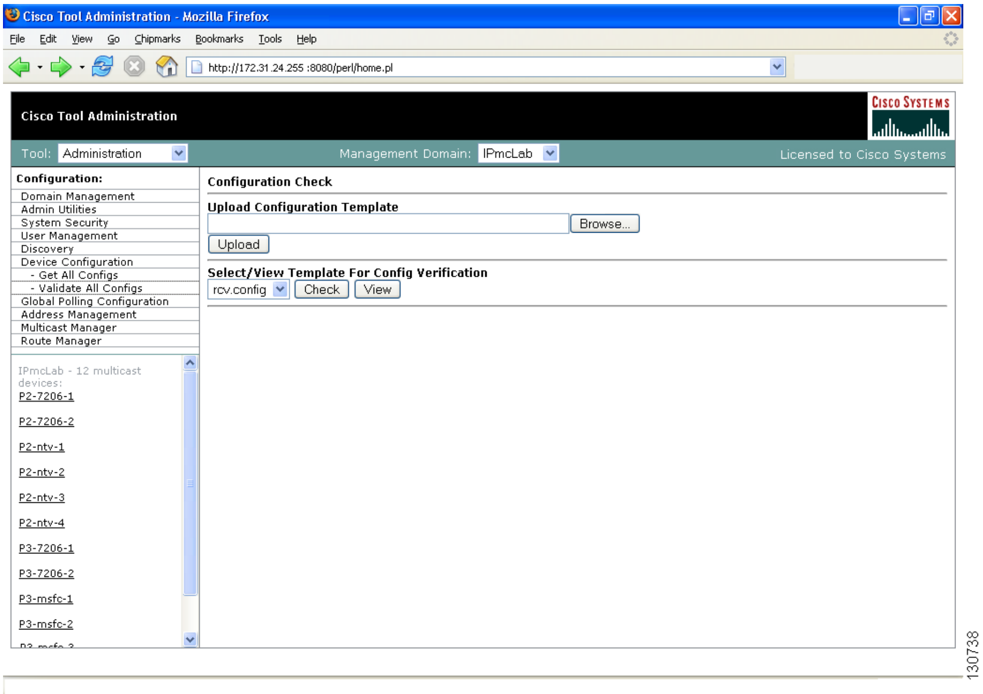
b. Click **Upload**. The user-defined text file appears in the list below.

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

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

Step 6 Click **Check**.

Figure 1-11 Configuration Check



Cisco Tool Administration - Mozilla Firefox

http://172.31.24.255 :8080/perl/home.pl

Cisco Tool Administration

Tool: Administration

Management Domain: IPmcLab

Licensed to Cisco Systems

Configuration Check

Upload Configuration Template

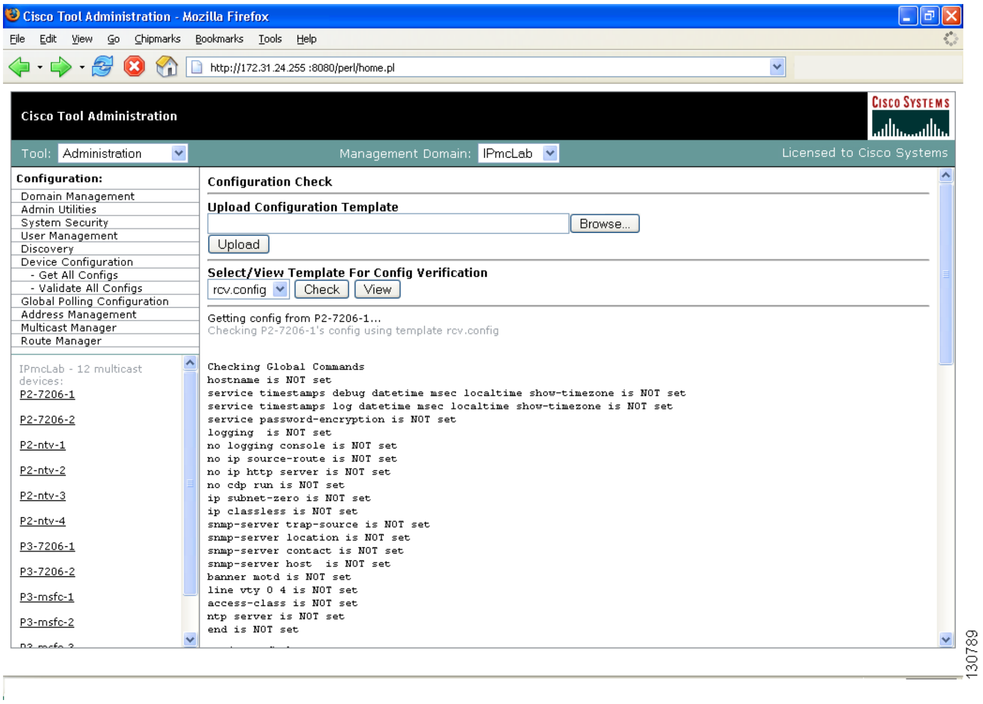
Select/View Template For Config Verification

rcv.config

IPmcLab - 12 multicast devices:

The CMM checks each router in the database for the existence of the commands in the template you specified. Output looks similar to Figure 1-12.

Figure 1-12 Configuration Check—Output



Getting config from P2-7206-1...
Checking P2-7206-1's config using template rcv.config

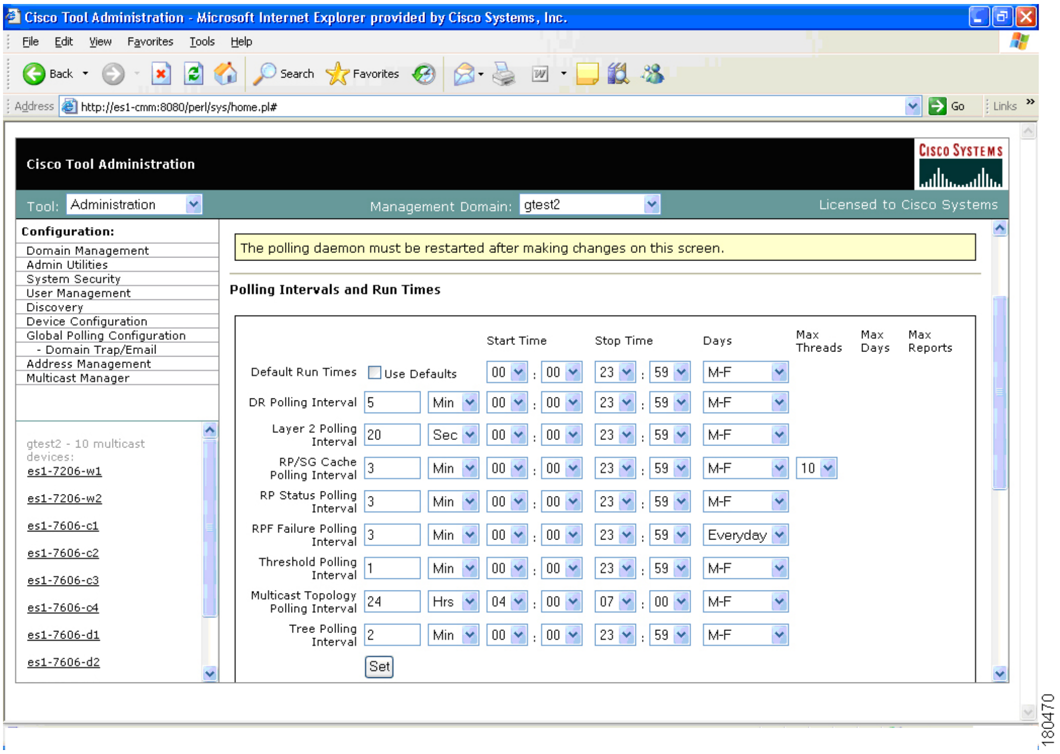
```
Checking Global Commands
hostname is NOT set
service timestamps debug datetime msec localtime show-timezone is NOT set
service timestamps log datetime msec localtime show-timezone is NOT set
service password-encryption is NOT set
logging  is NOT set
no logging console is NOT set
no ip source-route is NOT set
no ip http server is NOT set
no cdp run is NOT set
ip subnet-zero is NOT set
ip classless is NOT set
snmp-server trap-source is NOT set
snmp-server location is NOT set
snmp-server contact is NOT set
snmp-server host  is NOT set
banner motd is NOT set
line vty 0 4 is NOT set
access-class is NOT set
ntp server is NOT set
end is NOT set
```

Global Polling Configuration

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

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

Figure 1-13 Global Polling Configuration


Cisco Tool Administration - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back Search Favorites
Address
Go
Links
Cisco Systems
180470

http://es1-cmm:8080/perl/sys/home.pl#

Cisco Tool Administration

Tool: Administration Management Domain: gtest2 Licensed to Cisco Systems

Configuration:

- Domain Management
- Admin Utilities
- System Security
- User Management
- Discovery
- Device Configuration
- Global Polling Configuration
  - Domain Trap/Email
- Address Management
- Multicast Manager

gtest2 - 10 multicast devices:

- es1-7206-w1
- es1-7206-w2
- es1-7606-c1
- es1-7606-c2
- es1-7606-c3
- es1-7606-c4
- es1-7606-d1
- es1-7606-d2

The polling daemon must be restarted after making changes on this screen.

Polling Intervals and Run Times

			Start Time	Stop Time	Days	Max Threads	Max Days	Max Reports
Default Run Times	☐ Use Defaults		00 : 00	23 : 59	M-F			
DR Polling Interval	5	Min	00 : 00	23 : 59	M-F			
Layer 2 Polling Interval	20	Sec	00 : 00	23 : 59	M-F			
RP/SG Cache Polling Interval	3	Min	00 : 00	23 : 59	M-F	10		
RP Status Polling Interval	3	Min	00 : 00	23 : 59	M-F			
RPF Failure Polling Interval	3	Min	00 : 00	23 : 59	Everyday			
Threshold Polling Interval	1	Min	00 : 00	23 : 59	M-F			
Multicast Topology Polling Interval	24	Hrs	04 : 00	07 : 00	M-F			
Tree Polling Interval	2	Min	00 : 00	23 : 59	M-F			

Set

The Global Polling Configuration page contains:

Note Setting any one of these values to be 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	Amount of time between polling of the Layer 2 ports.

Field or Button	Description
RP/SG Cache Polling Interval	For certain CMM data, such as the data within the Multicast Diagnostics page (see the "Show All Groups" section on page 1-61) the CMM queries each RP, collates a list of active sources, and groups and displays them. There are 2 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 the "Domain Management" section on page 1-9) 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 the "Domain Management" section on page 1-9).
RP Status Polling Interval	RP Status Polling queries the sysUpTime of the RPs configured on the RP Polling Configuration page (see the "RP Polling" section on page 1-28). The purpose of this query is to report availability of the RPs. If the RP responds, an *rpReachable* trap is sent. If the RP does not respond, an *rpUnreachable* trap is sent. Since at least one of these traps is sent at each polling interval, you can also use them to ensure that the polling daemon is up and running.
RPF Failure Polling Interval	Time interval that each router will be polled for each source and group configured to check the number of RPF failures.
Threshold Polling Interval	Time interval that each router will be polled for the existence of each source and group configured, and CMM will ensure that no thresholds are exceeded.

Field or Button	Description
Multicast Topology Polling Interval	Topology polling queries the sysUpTime of each router in the multicast domain to see if it has been reloaded. If it has, the polling daemon launches a Single Router Discovery of that device in the background, to ensure the SNMP *ifIndexes* have not changed.
Tree Polling Interval	Time interval that the monitored trees are drawn and compared with their baselines.
Set	Sets the values you enter.

You can enable or disable the continuous sending of PPS threshold traps using the **Enable Rising/Falling and Normalized Traps for Thresholds** section:

- If the **Rising/Falling** option is not checked (disabled), traps are sent whenever the PPS rate for a monitored S,G exceeds specified thresholds.
- If the **Rising/Falling** option is checked (enabled), a trap is sent only when the PPS rate initially exceeds the high or low threshold. Once the PPS rate returns to the specified range, a normalized threshold trap is sent.
- Since SNMP v1 traps are sent unreliably, you can set the **Trap-Repeat** option to allow the initial and normalized traps to be sent anywhere from 1 to 5 times when an event occurs.

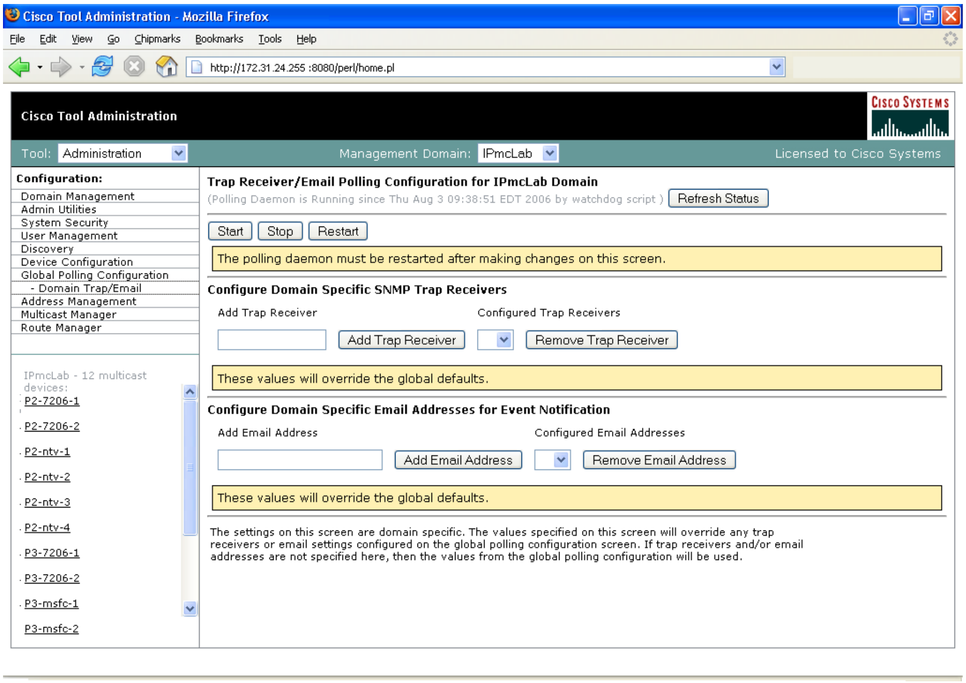
You can add or remove trap receivers using the **Configure Global Default SNMP Trap Receivers** section. The SNMP trap receivers specified here are only used if domain-specific SNMP trap receivers are not specified. Domain-specific trap receivers are specified from the Trap Receiver/Email Polling Configuration page (see the "Configuring Domain-Specific Trap Receivers and Email Addresses" section on page 1-26).

You can add or remove Email addresses using the Configure Global Default Email Addresses for Event Notification section. Email addresses are notified of SSG exceptions and threshold and existence events. The Email addresses specified here are only used if domain-specific Email addresses are not specified. Domain-specific Email addresses are specified from the Trap Receiver/Email Polling Configuration page (see the "Configuring Domain-Specific Trap Receivers and Email Addresses" section on page 1-26).

Configuring Domain-Specific Trap Receivers and Email Addresses

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

Figure 1-14 Trap Receiver/Email Polling Configuration



http://172.31.24.255 :8080/perl/home.pl

Tool: Administration

Management Domain: IPmcLab

Trap Receiver/Email Polling Configuration for IPmcLab Domain

(Polling Daemon is Running since Thu Aug 3 09:38:51 EDT 2006 by watchdog script)

The polling daemon must be restarted after making changes on this screen.

Configure Domain Specific SNMP Trap Receivers

These values will override the global defaults.

Configure Domain Specific Email Addresses for Event Notification

These values will override the global defaults.

The settings on this screen are domain specific. The values specified on this screen will override any trap receivers or email settings configured on the global polling configuration screen. If trap receivers and/or email addresses are not specified here, then the values from the global polling configuration will be used.

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 the "Global Polling Configuration" section on page 1-23).

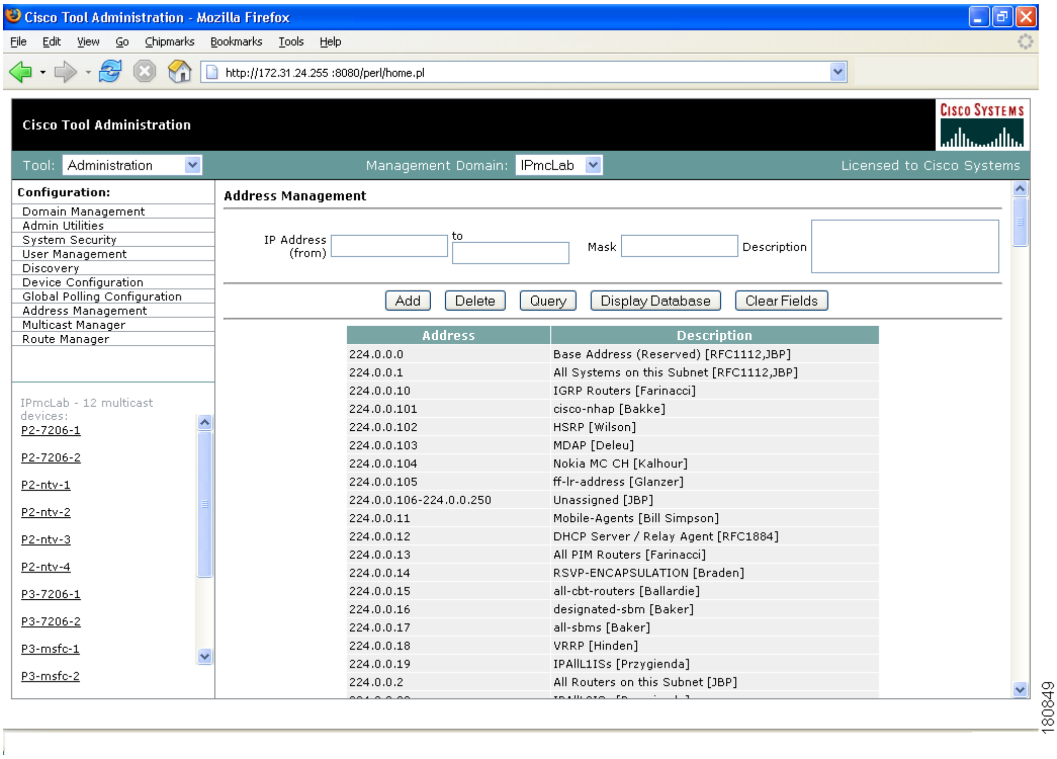
You can add or remove Email addresses using the **Configure Domain Specific Email Addresses for Event Notification** section. Email addresses are notified of SSG exceptions and threshold and existence events. The Email addresses specified here are only used if global Email addresses are not specified. Global Email addresses are specified from the Configure Global Default SNMP Trap Receivers page (see the "Global Polling Configuration" section on page 1-23).

Address Management

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

The database is pre-populated with all of the reserved address space.

Figure 1-15 Address Management



Address	Description
224.0.0.0	Base Address (Reserved) [RFC1112,JBP]
224.0.0.1	All Systems on this Subnet [RFC1112,JBP]
224.0.0.10	IGRP Routers [Farinacci]
224.0.0.101	cisco-nhap [Bakke]
224.0.0.102	HSRP [Wilson]
224.0.0.103	MDAP [Deleu]
224.0.0.104	Nokia MC CH [Kalhour]
224.0.0.105	ff-lr-address [Glanzer]
224.0.0.106-224.0.0.250	Unassigned [JBP]
224.0.0.11	Mobile-Agents [Bill Simpson]
224.0.0.12	DHCP Server / Relay Agent [RFC1884]
224.0.0.13	All PIM Routers [Farinacci]
224.0.0.14	RSVP-ENCAPSULATION [Braden]
224.0.0.15	all-cbt-routers [Ballardie]
224.0.0.16	designated-sbm [Baker]
224.0.0.17	all-sbms [Baker]
224.0.0.18	VRRP [Hinden]
224.0.0.19	IPAllL1ISs [Przygienda]
224.0.0.2	All Routers on this Subnet [JBP]

Multicast Manager

The Multicast Manager contains:

- RP Polling, page 1-28
- RPF Polling, page 1-32
- SG Polling—Main, page 1-33
- SG Polling—by Device, page 1-36
- L2 Polling, page 1-37
- Tree Polling, page 1-38
- Health Check, page 1-41

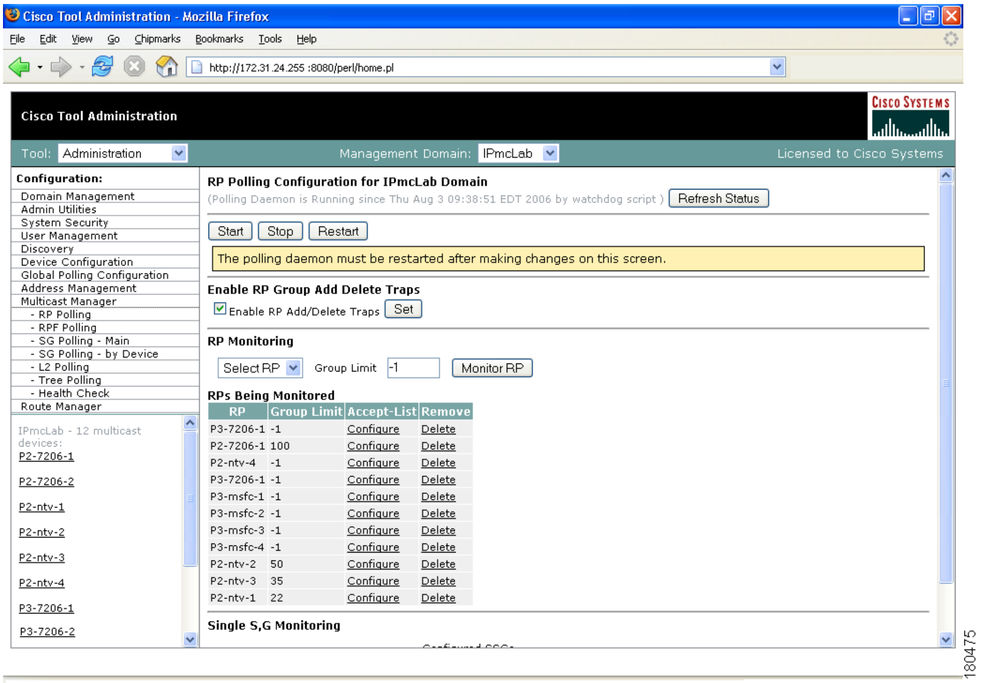
RP Polling

Using the RP Polling Configuration page, you can enable the CMM to:

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

Note RP availability is configured within the Global Polling Configuration page (see the "Global Polling Configuration" section on page 1-23). A trap is sent if an RP becomes unavailable, and a report is generated within the RP Polling Report page (see the "RP Polling Report" section on page 1-49).

Figure 1-16 RP Polling Configuration



RP Polling Configuration for IPmcLab Domain

(Polling Daemon is Running since Thu Aug 3 09:38:51 EDT 2006 by watchdog script) Refresh Status

Start Stop Restart

The polling daemon must be restarted after making changes on this screen.

Enable RP Group Add Delete Traps

☑ Enable RP Add/Delete Traps Set

RP Monitoring

Select RP Group Limit -1 Monitor RP

RPs Being Monitored

RP	Group Limit	Accept-List	Remove
P3-7206-1	-1	Configure	Delete
P2-7206-1	100	Configure	Delete
P2-ntv-4	-1	Configure	Delete
P3-7206-1	-1	Configure	Delete
P3-msfc-1	-1	Configure	Delete
P3-msfc-2	-1	Configure	Delete
P3-msfc-3	-1	Configure	Delete
P3-msfc-4	-1	Configure	Delete
P2-ntv-2	50	Configure	Delete
P2-ntv-3	35	Configure	Delete
P2-ntv-1	22	Configure	Delete

Single S,G Monitoring

The RP Polling Configuration page contains:

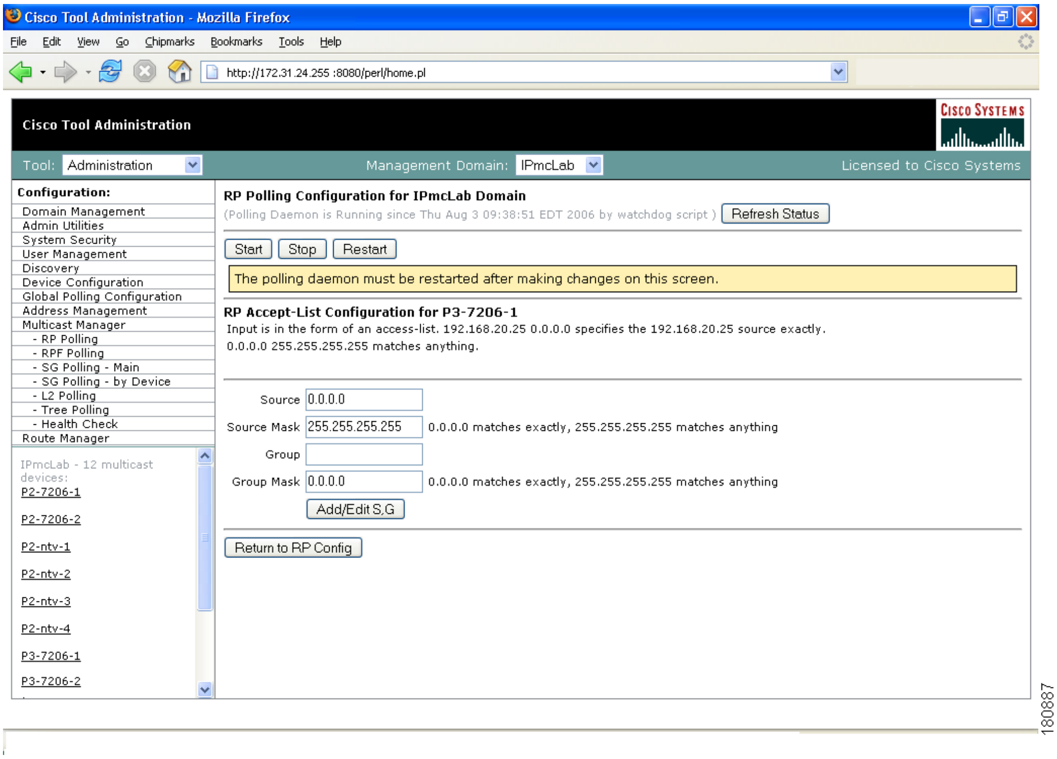
Fields and Buttons	Description
Refresh Status	The status line indicates how long the polling daemon has been running and how it was started. Click **Refresh Status** to update the status information.
Start	Starts the polling daemon globally.
Stop	Stops the polling daemon globally.
Restart	Restarts the polling daemon globally. Each time you change a polling interval, click **Restart**.
Enable RP Group Add Delete Traps	Click the checkbox to monitor all leaves and joins, which are then reported within the RP Polling Report page (see the "RP Polling Report" section on page 1-49).

Fields and Buttons	Description
RP Monitoring	To monitor an RP, select the RP from the box. To monitor a specific number of groups, enter a number in the **Group Limit** box. Click **Monitor RP**. If the group limit is exceeded, a report is generated within the RP Group Threshold Report page (see the "RP Group Threshold Report" section on page 1-50).
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 1-31). • **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 1-17 RP Accept List Configuration



RP Polling Configuration for IPmcLab Domain

(Polling Daemon is Running since Thu Aug 3 09:38:51 EDT 2006 by watchdog script)

The polling daemon must be restarted after making changes on this screen.

RP Accept-List Configuration for P3-7206-1

Input is in the form of an access-list. 192.168.20.25 0.0.0.0 specifies the 192.168.20.25 source exactly.
0.0.0.0 255.255.255.255 matches anything.

Source 0.0.0.0

Source Mask 255.255.255.255 0.0.0.0 matches exactly, 255.255.255.255 matches anything

Group

Group Mask 0.0.0.0 0.0.0.0 matches exactly, 255.255.255.255 matches anything

The RP Accept List Configuration section contains:

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

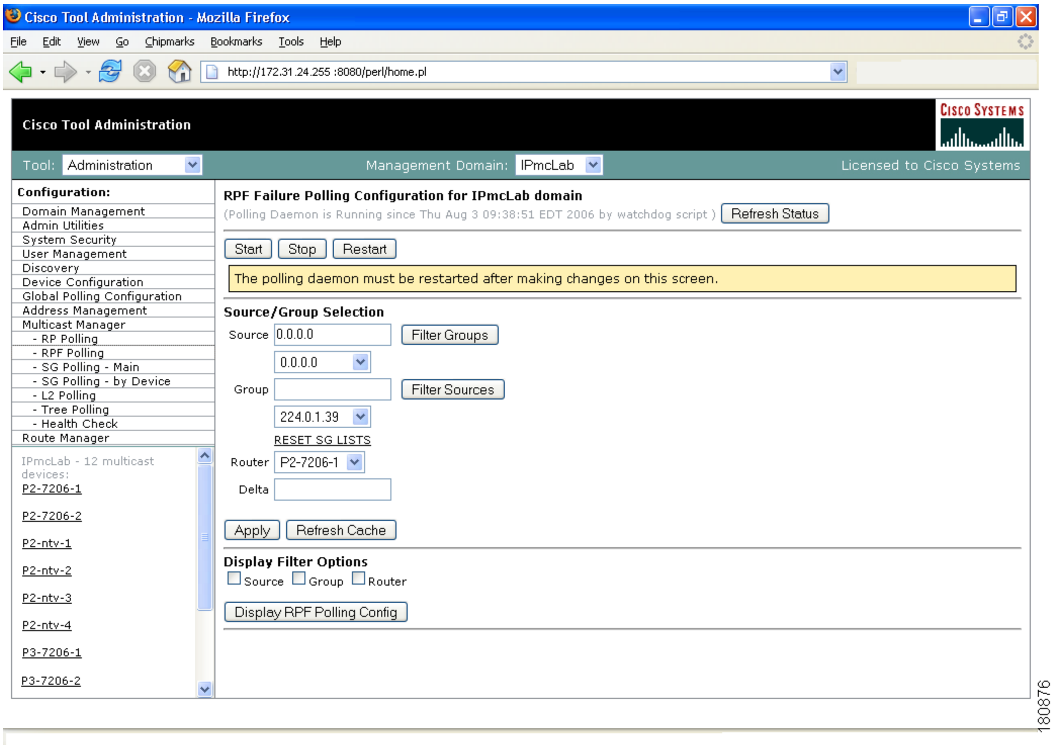
RPF Polling

Using the CMM, you can monitor RPF failures for a particular source and group on any selected router.

If any monitored source and group begins to experience RPF failures that rise above the delta, then SNMP traps can be sent, and a report generated, which you can view under RPF Failures (see the "RPF Failures" section on page 1-51).

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 you are selecting an S,G that actually exists in the network. The filter option displays only the sources for a selected group, or only the groups for a selected source. To reset the lists, click **Reset S,G Lists**.

Figure 1-18 RPF Failure Polling Configuration



RPF Failure Polling Configuration for IPmcLab domain

(Polling Daemon is Running since Thu Aug 3 09:38:51 EDT 2006 by watchdog script)

The polling daemon must be restarted after making changes on this screen.

Source/Group Selection

Source 0.0.0.0

0.0.0.0

Group

224.0.1.39

Router P2-7206-1

Delta

Display Filter Options

□ Source □ Group □ Router

The RP Failure Polling Configuration page contains:

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

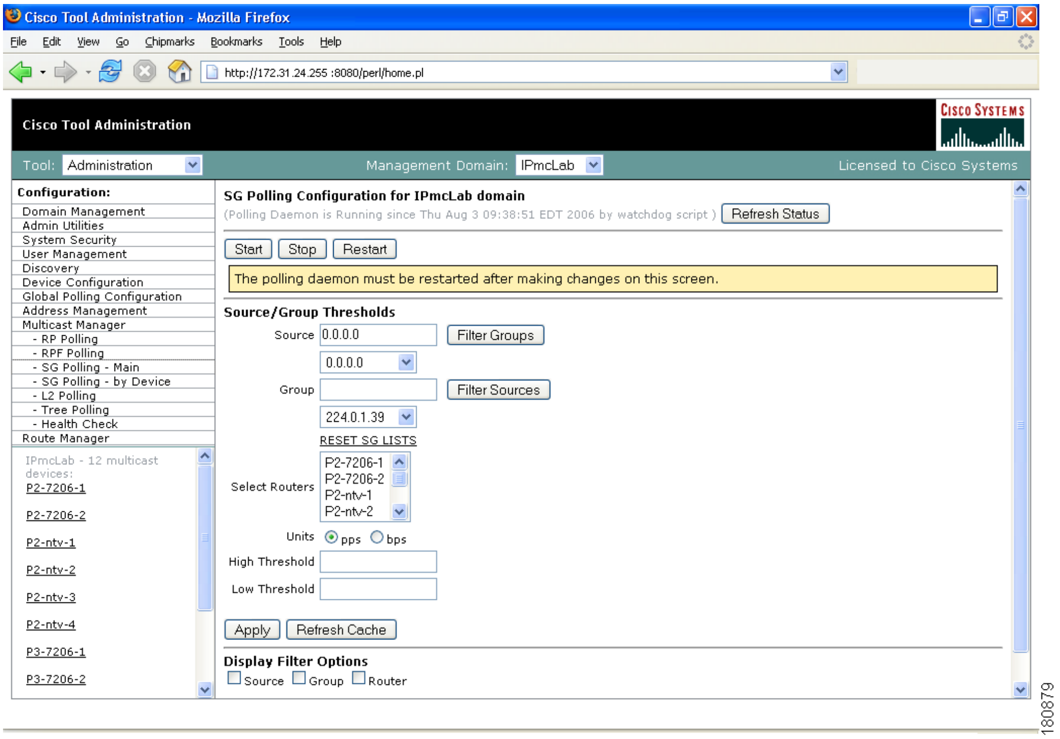
Fields and Buttons	Description
Source	Enter or select the IP address of the source to monitor.
Filter Groups	Filters the output to contain only the relevant groups.
Group	Enter or select the IP address of the group to monitor.
Filter Sources	Filters the output to contain only the relevant sources.
Reset SG Lists	Clears any entries and refreshes the source and group lists.
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.

SG Polling—Main

Using the CMM, you can poll sources and groups with high and low thresholds.

You can select the source and group from the list, or you can enter them manually. If there are a lot of sources and/or groups, you can use the filter option, to ensure 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.

Figure 1-19 SG Polling Configuration



SG Polling Configuration for IPmcLab domain

(Polling Daemon is Running since Thu Aug 3 09:38:51 EDT 2006 by watchdog script)

The polling daemon must be restarted after making changes on this screen.

Source/Group Thresholds

Source: 0.0.0.0

0.0.0.0

Group:

224.0.1.39

Select Routers: P2-7206-1, P2-7206-2, P2-ntv-1, P2-ntv-2

Units ● pps ○ bps

High Threshold

Low Threshold

Display Filter Options

□ Source □ Group □ Router

The SG Polling Configuration page contains:

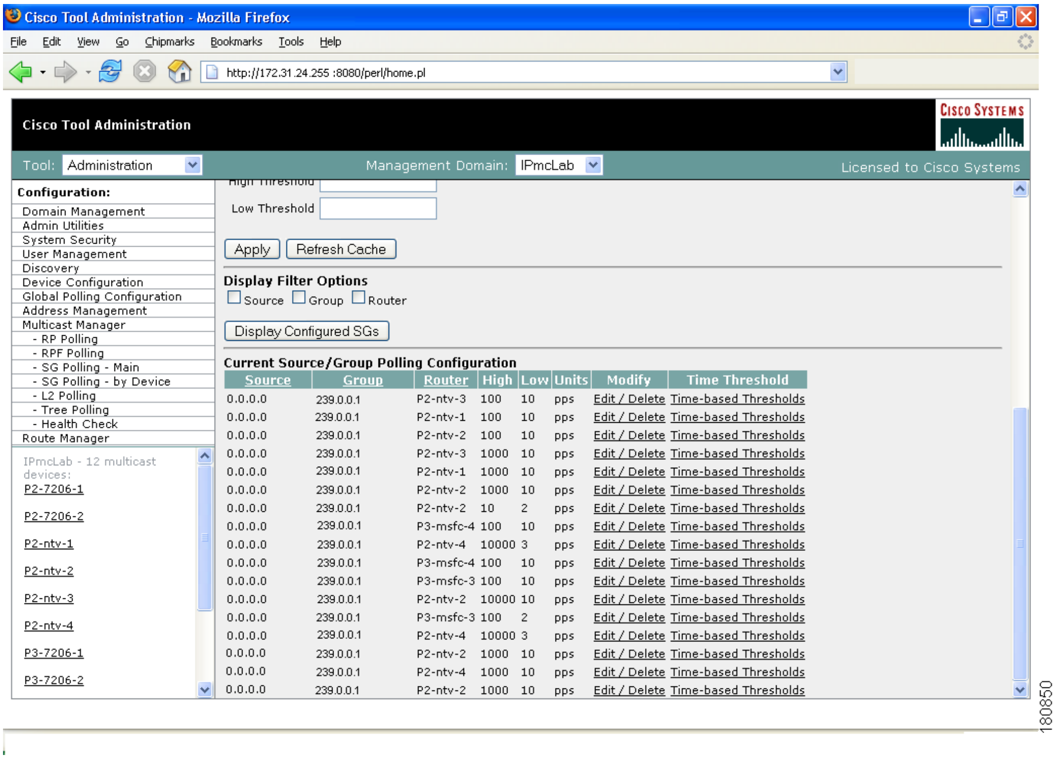
Fields and Buttons	Description
Refresh Status	The status line indicates how long the polling daemon has been running and how it was started. Click **Refresh Status** to update the status information.
Start	Starts the polling daemon globally.
Stop	Stops the polling daemon globally.
Restart	Restarts the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

Fields and Buttons	Description
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 the "Current Source/Group Polling Configuration" section on page 1-35).

Current Source/Group Polling Configuration

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

Figure 1-20 Current Source/Group Polling Configuration



Display Filter Options
□ Source □ Group □ Router

Current Source/Group Polling Configuration

Source	Group	Router	High	Low	Units	Modify	Time Threshold
0.0.0.0	239.0.0.1	P2-ntv-3	100	10	pps	Edit / Delete	Time-based Thresholds
0.0.0.0	239.0.0.1	P2-ntv-1	100	10	pps	Edit / Delete	Time-based Thresholds
0.0.0.0	239.0.0.1	P2-ntv-2	100	10	pps	Edit / Delete	Time-based Thresholds
0.0.0.0	239.0.0.1	P2-ntv-3	1000	10	pps	Edit / Delete	Time-based Thresholds
0.0.0.0	239.0.0.1	P2-ntv-1	1000	10	pps	Edit / Delete	Time-based Thresholds
0.0.0.0	239.0.0.1	P2-ntv-2	1000	10	pps	Edit / Delete	Time-based Thresholds
0.0.0.0	239.0.0.1	P2-ntv-2	10	2	pps	Edit / Delete	Time-based Thresholds
0.0.0.0	239.0.0.1	P3-msfc-4	100	10	pps	Edit / Delete	Time-based Thresholds
0.0.0.0	239.0.0.1	P2-ntv-4	10000	3	pps	Edit / Delete	Time-based Thresholds
0.0.0.0	239.0.0.1	P3-msfc-4	100	10	pps	Edit / Delete	Time-based Thresholds
0.0.0.0	239.0.0.1	P3-msfc-3	100	10	pps	Edit / Delete	Time-based Thresholds
0.0.0.0	239.0.0.1	P2-ntv-2	10000	10	pps	Edit / Delete	Time-based Thresholds
0.0.0.0	239.0.0.1	P3-msfc-3	100	2	pps	Edit / Delete	Time-based Thresholds
0.0.0.0	239.0.0.1	P2-ntv-4	10000	3	pps	Edit / Delete	Time-based Thresholds
0.0.0.0	239.0.0.1	P2-ntv-2	1000	10	pps	Edit / Delete	Time-based Thresholds
0.0.0.0	239.0.0.1	P2-ntv-4	1000	10	pps	Edit / Delete	Time-based Thresholds
0.0.0.0	239.0.0.1	P2-ntv-2	1000	10	pps	Edit / Delete	Time-based Thresholds

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

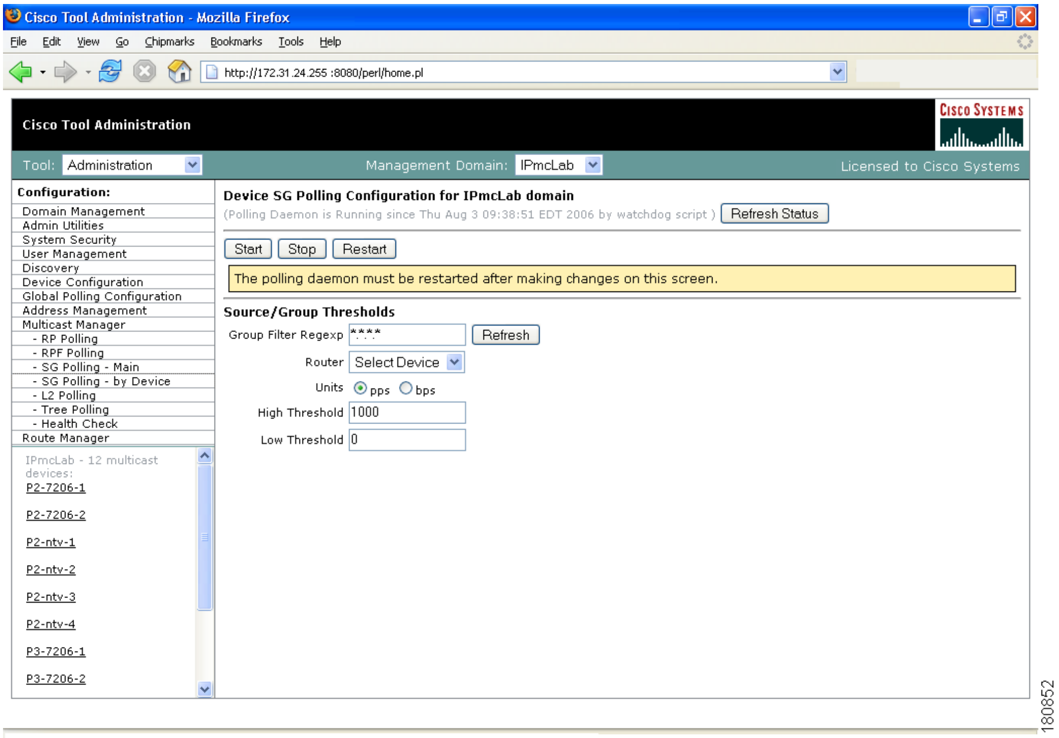
- Under the **Modify** column, you can edit or delete a specific source and group.
- Under the **Time Threshold** column, click on **Time-Based Thresholds** to configure up to 50 different time of day high and low thresholds for each source and group. Click the **Set Thresholds** button to save your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

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

SG Polling—by Device

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

Figure 1-21 Device SG Polling Configuration



Device SG Polling Configuration for IPmcLab domain

(Polling Daemon is Running since Thu Aug 3 09:38:51 EDT 2006 by watchdog script)

The polling daemon must be restarted after making changes on this screen.

Source/Group Thresholds

Group Filter Regexp *.*.*

Router Select Device

Units ● pps ○ bps

High Threshold 1000

Low Threshold 0

The Device SG Polling Configuration page contains:

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.

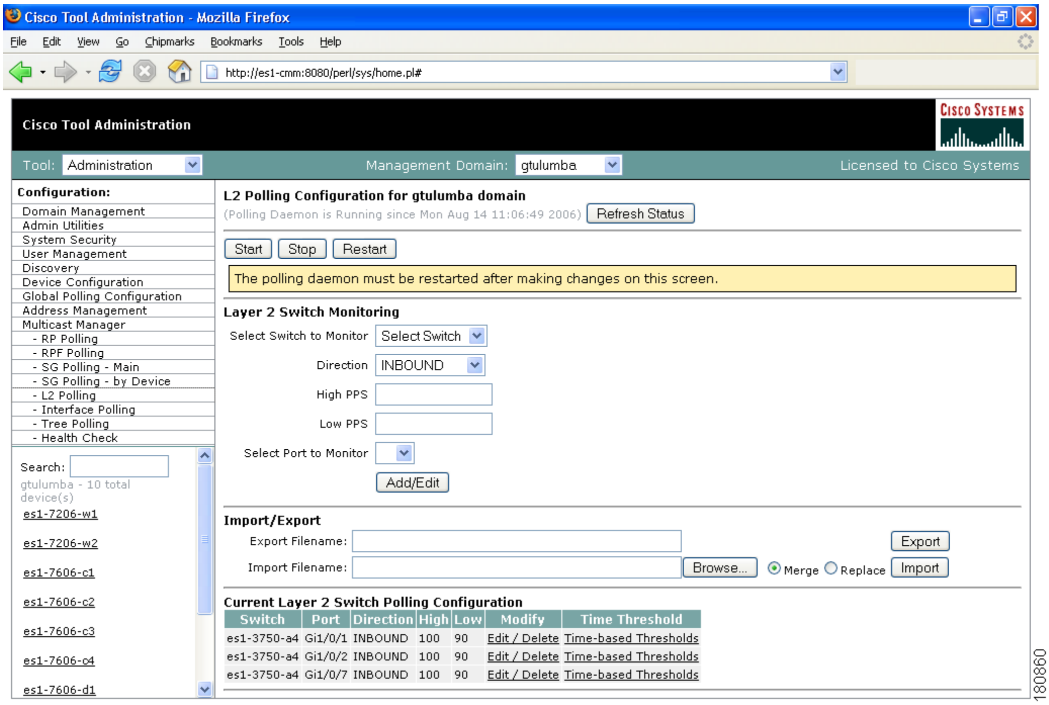
Fields and Buttons	Description
Restart	Restarts the polling daemon globally. Each time you change a polling interval, click **Restart**.
Group Filter Regexp	Enter any part of the multicast address. Only those that match appear.
Refresh	Clears the Group Filter Regexp previously entered.
Router	Select the router name.
Units	Select either packets per sampling period (pps) or bits per sampling period (bps).
High Threshold	Enter the high threshold that, if exceeded, generates a report.
Low Threshold	Enter the low threshold that, if exceeded, generates a report.

L2 Polling

You can add Layer 2 switches to the CMM individually, or you can import a list (see the "Adding Layer 2 Switches to Discovery" section on page 1-11). The CMM can monitor the total number of multicast packets inbound and/or outbound from any Layer 2 port.

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

Figure 1-22 L2 Polling Configuration



L2 Polling Configuration for gtulumba domain

(Polling Daemon is Running since Mon Aug 14 11:06:49 2006)

The polling daemon must be restarted after making changes on this screen.

Layer 2 Switch Monitoring

Select Switch to Monitor: Select Switch

Direction: INBOUND

High PPS:

Low PPS:

Select Port to Monitor:

Import/Export

Export Filename:

Import Filename: ● Merge ○ Replace

Current Layer 2 Switch Polling Configuration

Switch	Port	Direction	High	Low	Modify	Time Threshold
es1-3750-a4	Gi1/0/1	INBOUND	100	90	Edit / Delete	Time-based Thresholds
es1-3750-a4	Gi1/0/2	INBOUND	100	90	Edit / Delete	Time-based Thresholds
es1-3750-a4	Gi1/0/7	INBOUND	100	90	Edit / Delete	Time-based Thresholds

The L2 Polling Configuration page contains:

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.

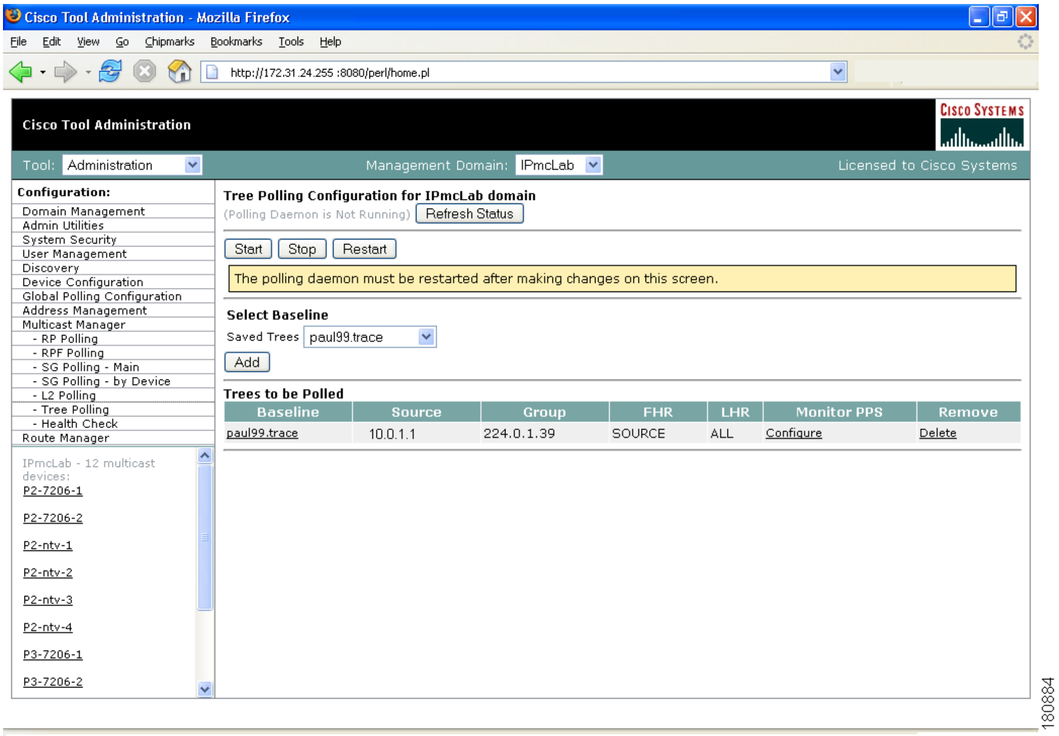
Each time a port exceeds a threshold, a trap is sent and a report is generated.

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 the "Show All Groups" section on page 1-61).

Once saved, the trees appear in the **Saved Trees** list of the Tree Polling Configuration page. To monitor a tree, select the tree name, and click Add. The tree is drawn in the background for every interval that you set up for tree polling (see the Global Polling Configuration, page 1-23). This tree is compared with the tree saved in the database. If it is different, a trap is sent, and a report generated.

Figure 1-23 Tree Polling Configuration



Tree Polling Configuration for IPmcLab domain

(Polling Daemon is Not Running)

The polling daemon must be restarted after making changes on this screen.

Select Baseline

Saved Trees: paul99.trace

Trees to be Polled

Baseline	Source	Group	FHR	LHR	Monitor PPS	Remove
paul99.trace	10.0.1.1	224.0.1.39	SOURCE	ALL	Configure	Delete

The Tree Polling Configuration page contains:

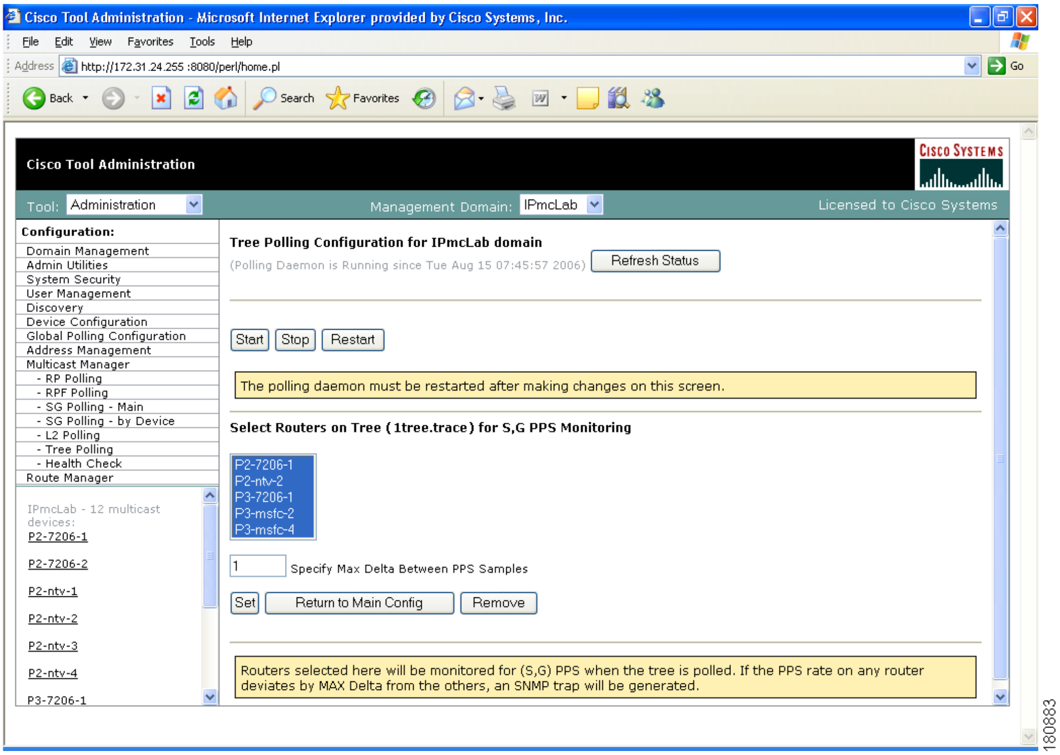
Fields and Buttons	Description
Refresh Status	The status line indicates how long the polling daemon has been running and how it was started. Click **Refresh Status** to update the status information.
Start	Starts the polling daemon globally.
Stop	Stops the polling daemon globally.
Restart	Restarts the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

Trees to be Polled

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

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

Figure 1-24 Tree Polling Configuration—Configure



Cisco Tool Administration - Microsoft Internet Explorer provided by Cisco Systems, Inc.

Address: http://172.31.24.255 :8080/perl/home.pl

Cisco Tool Administration

Tool: Administration — Management Domain: IPmcLab — Licensed to Cisco Systems

Tree Polling Configuration for IPmcLab domain

(Polling Daemon is Running since Tue Aug 15 07:45:57 2006) [Refresh Status]

[Start] [Stop] [Restart]

The polling daemon must be restarted after making changes on this screen.

Select Routers on Tree (1tree.trace) for S,G PPS Monitoring

P2-7206-1
P2-ntv-2
P3-7206-1
P3-msfc-2
P3-msfc-4

1 Specify Max Delta Between PPS Samples

[Set] [Return to Main Config] [Remove]

Routers selected here will be monitored for (S,G) PPS when the tree is polled. If the PPS rate on any router deviates by MAX Delta from the others, an SNMP trap will be generated.

IPmcLab - 12 multicast devices:
P2-7206-1
P2-7206-2
P2-ntv-1
P2-ntv-2
P2-ntv-3
P2-ntv-4
P3-7206-1

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

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

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

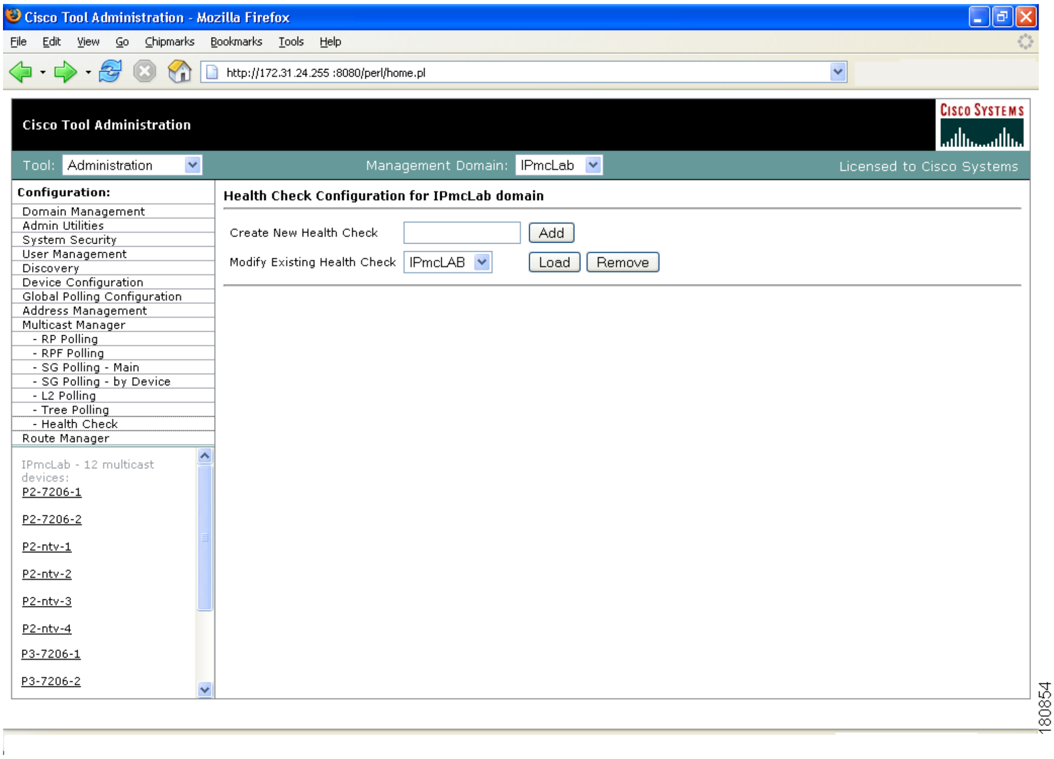
Health Check

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

- Status of selected RPs
- MSDP status
- Existence of S,G entries on selected routers
- Status of multicast forwarding trees

You can create several health checks. Health checks run dynamically, meaning they must be user-initiated.

Figure 1-25 Health Check Configuration



http://172.31.24.255 :8080/perl/home.pl

Cisco Tool Administration

Tool: Administration
Management Domain: IPmcLab
Licensed to Cisco Systems

Health Check Configuration for IPmcLab domain

Create New Health Check

Modify Existing Health Check IPmcLAB

The Health Check page contains:

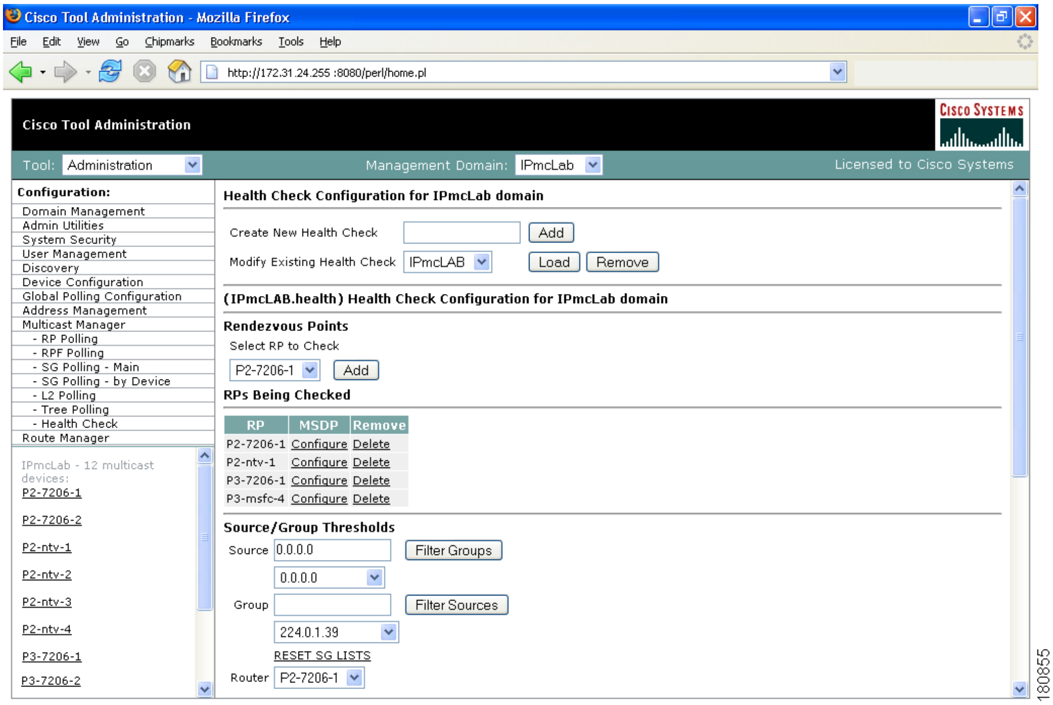
Fields and Buttons	Description
Create New Health Check	Type a name for the health check.
Add	Adds a new named health check.
Modify Existing Health Check	Select the named health check you want to modify.

Fields and Buttons	Description
Load	Loads an existing named health check for modification (see the "Modifying Health Checks" section on page 1-42).
Remove	Deletes the health check selected in the **Modify Existing Health Check** box.

Modifying Health Checks

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

Figure 1-26 Health Check Configuration—Modification


Cisco Tool Administration - Mozilla Firefox
File Edit View Go Chipmarks Bookmarks Tools Help
Cisco Systems
180855

http://172.31.24.255 :8080/perl/home.pl

Cisco Tool Administration

Tool: Administration Management Domain: IPmcLab Licensed to Cisco Systems

Configuration:
- Domain Management
- Admin Utilities
- System Security
- User Management
- Discovery
- Device Configuration
- Global Polling Configuration
- Address Management
- Multicast Manager
  - RP Polling
  - RPF Polling
  - SG Polling - Main
  - SG Polling - by Device
  - L2 Polling
  - Tree Polling
  - Health Check
- Route Manager

IPmcLab - 12 multicast devices:
P2-7206-1
P2-7206-2
P2-ntv-1
P2-ntv-2
P2-ntv-3
P2-ntv-4
P3-7206-1
P3-7206-2

Health Check Configuration for IPmcLab domain

Create New Health Check [ ] Add

Modify Existing Health Check IPmcLAB Load Remove

(IPmcLAB.health) Health Check Configuration for IPmcLab domain

Rendezvous Points

Select RP to Check P2-7206-1 Add

RPs Being Checked

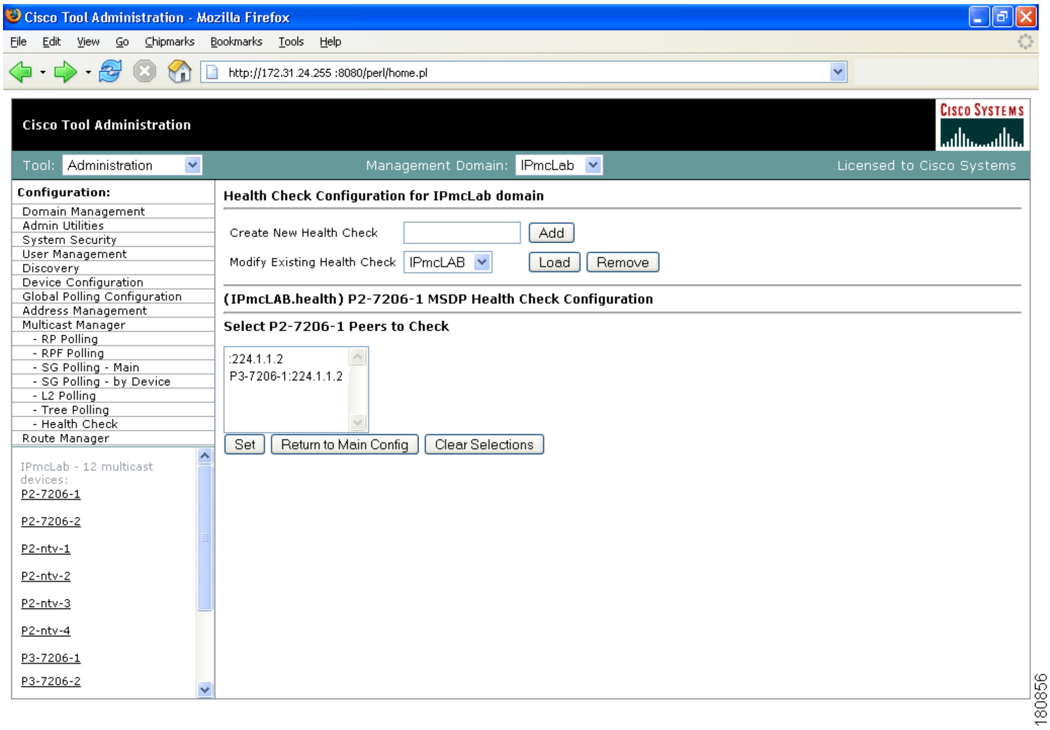
RP	MSDP	Remove
P2-7206-1	Configure	Delete
P2-ntv-1	Configure	Delete
P3-7206-1	Configure	Delete
P3-msfc-4	Configure	Delete

Source/Group Thresholds

Source 0.0.0.0 Filter Groups
0.0.0.0
Group [ ] Filter Sources
224.0.1.39
RESET SG LISTS
Router P2-7206-1

You can also check MSDP peering of the selected router by clicking **Configure** within the **RPs Being Checked** table.

Figure 1-27 Health Check Configuration—Peers



Health Check Configuration for IPmcLab domain

Create New Health Check

Modify Existing Health Check: IPmcLAB

(IPmcLAB.health) P2-7206-1 MSDP Health Check Configuration

Select P2-7206-1 Peers to Check

:224.1.1.2
P3-7206-1:224.1.1.2

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

To run the actual health check, see the "Health Check" section on page 1-73.

Using the Multicast Manager Tool

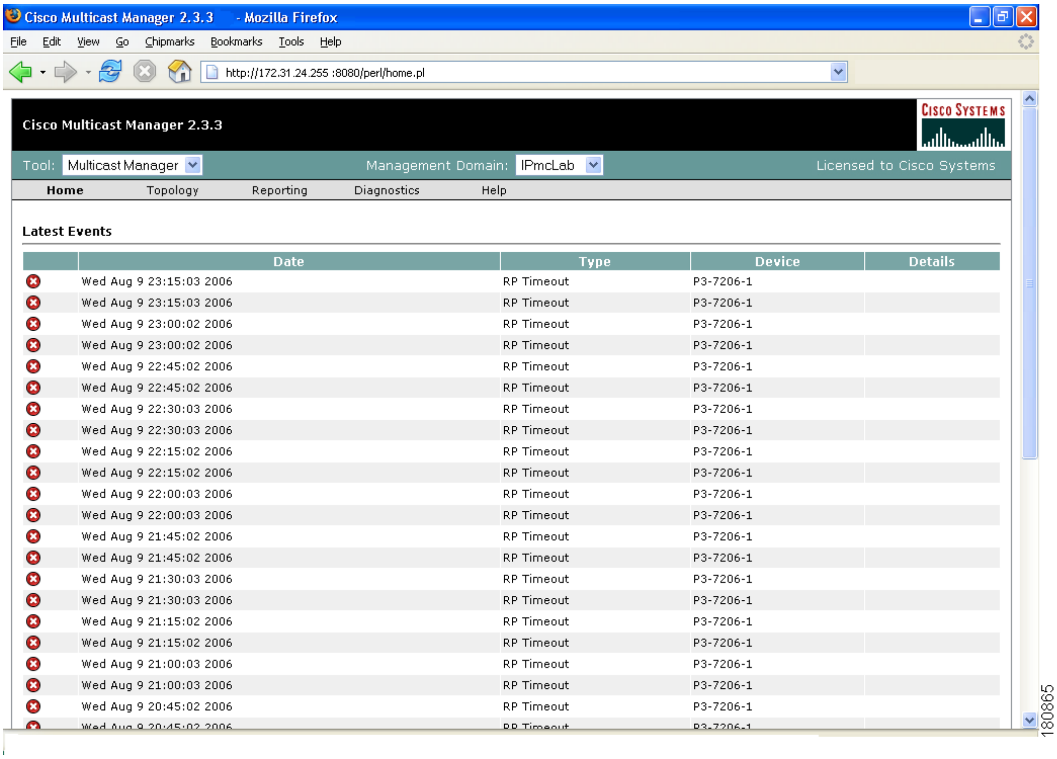
You can view or monitor data using the CMM **Multicast Manager** Tool, containing these web pages:

- Home, page 1-44
- Topology, page 1-44
- Reporting, page 1-48
- Diagnostics, page 1-60
- Help, page 1-79

Home

The **Home** page shows the last 20 events (see the "Latest Events" section on page 1-49).

Figure 1-28 Multicast Manager Home Page


Cisco Multicast Manager 2.3.3 - Mozilla Firefox
File Edit View Go Chipmarks Bookmarks Tools Help
http://172.31.24.255 :8080/perl/home.pl
Cisco Multicast Manager 2.3.3
Cisco Systems
Tool: Multicast Manager
Management Domain: IPmcLab
Licensed to Cisco Systems
Home
Topology
Reporting
Diagnostics
Help
180865

Latest Events

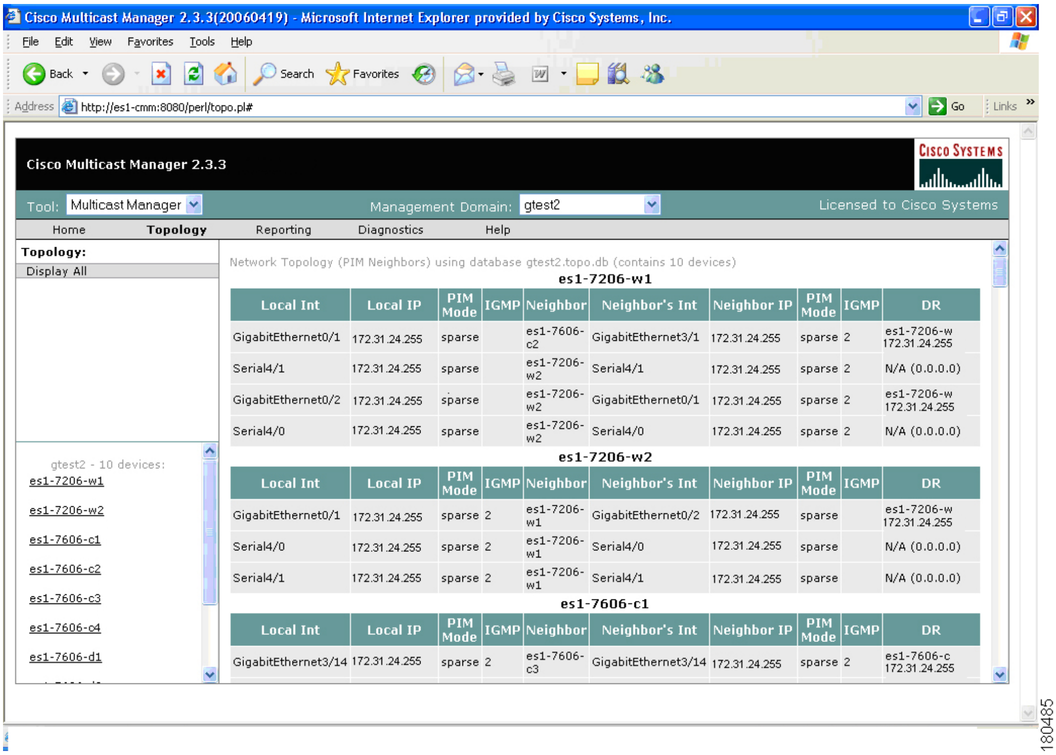
	Date	Type	Device	Details
✖	Wed Aug 9 23:15:03 2006	RP Timeout	P3-7206-1	
✖	Wed Aug 9 23:15:03 2006	RP Timeout	P3-7206-1	
✖	Wed Aug 9 23:00:02 2006	RP Timeout	P3-7206-1	
✖	Wed Aug 9 23:00:02 2006	RP Timeout	P3-7206-1	
✖	Wed Aug 9 22:45:02 2006	RP Timeout	P3-7206-1	
✖	Wed Aug 9 22:45:02 2006	RP Timeout	P3-7206-1	
✖	Wed Aug 9 22:30:03 2006	RP Timeout	P3-7206-1	
✖	Wed Aug 9 22:30:03 2006	RP Timeout	P3-7206-1	
✖	Wed Aug 9 22:15:02 2006	RP Timeout	P3-7206-1	
✖	Wed Aug 9 22:15:02 2006	RP Timeout	P3-7206-1	
✖	Wed Aug 9 22:00:03 2006	RP Timeout	P3-7206-1	
✖	Wed Aug 9 22:00:03 2006	RP Timeout	P3-7206-1	
✖	Wed Aug 9 21:45:02 2006	RP Timeout	P3-7206-1	
✖	Wed Aug 9 21:45:02 2006	RP Timeout	P3-7206-1	
✖	Wed Aug 9 21:30:03 2006	RP Timeout	P3-7206-1	
✖	Wed Aug 9 21:30:03 2006	RP Timeout	P3-7206-1	
✖	Wed Aug 9 21:15:02 2006	RP Timeout	P3-7206-1	
✖	Wed Aug 9 21:15:02 2006	RP Timeout	P3-7206-1	
✖	Wed Aug 9 21:00:03 2006	RP Timeout	P3-7206-1	
✖	Wed Aug 9 21:00:03 2006	RP Timeout	P3-7206-1	
✖	Wed Aug 9 20:45:02 2006	RP Timeout	P3-7206-1	
✖	Wed Aug 9 20:45:02 2006	RP Timeout	P3-7206-1	

Topology

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

To see the complete database, click **Display All**. Router names appear at the top of each table.

Figure 1-29 Topology Display All


Cisco Multicast Manager 2.3.3(20060419) - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back Search Favorites
Address http://es1-cmm:8080/perl/topo.pl#
Go Links
Cisco Multicast Manager 2.3.3
Tool: Multicast Manager
Management Domain: gtest2
Licensed to Cisco Systems
Home Topology Reporting Diagnostics Help
Topology:
Display All
gtest2 - 10 devices:
es1-7206-w1
es1-7206-w2
es1-7606-c1
es1-7606-c2
es1-7606-c3
es1-7606-c4
es1-7606-d1
180485

Network Topology (PIM Neighbors) using database gtest2.topo.db (contains 10 devices)

es1-7206-w1

Local Int	Local IP	PIM Mode	IGMP	Neighbor	Neighbor's Int	Neighbor IP	PIM Mode	IGMP	DR
GigabitEthernet0/1	172.31.24.255	sparse		es1-7606-c2	GigabitEthernet3/1	172.31.24.255	sparse	2	es1-7206-w 172.31.24.255
Serial4/1	172.31.24.255	sparse		es1-7206-w2	Serial4/1	172.31.24.255	sparse	2	N/A (0.0.0.0)
GigabitEthernet0/2	172.31.24.255	sparse		es1-7206-w2	GigabitEthernet0/1	172.31.24.255	sparse	2	es1-7206-w 172.31.24.255
Serial4/0	172.31.24.255	sparse		es1-7206-w2	Serial4/0	172.31.24.255	sparse	2	N/A (0.0.0.0)

es1-7206-w2

Local Int	Local IP	PIM Mode	IGMP	Neighbor	Neighbor's Int	Neighbor IP	PIM Mode	IGMP	DR
GigabitEthernet0/1	172.31.24.255	sparse	2	es1-7206-w1	GigabitEthernet0/2	172.31.24.255	sparse		es1-7206-w 172.31.24.255
Serial4/0	172.31.24.255	sparse	2	es1-7206-w1	Serial4/0	172.31.24.255	sparse		N/A (0.0.0.0)
Serial4/1	172.31.24.255	sparse	2	es1-7206-w1	Serial4/1	172.31.24.255	sparse		N/A (0.0.0.0)

es1-7606-c1

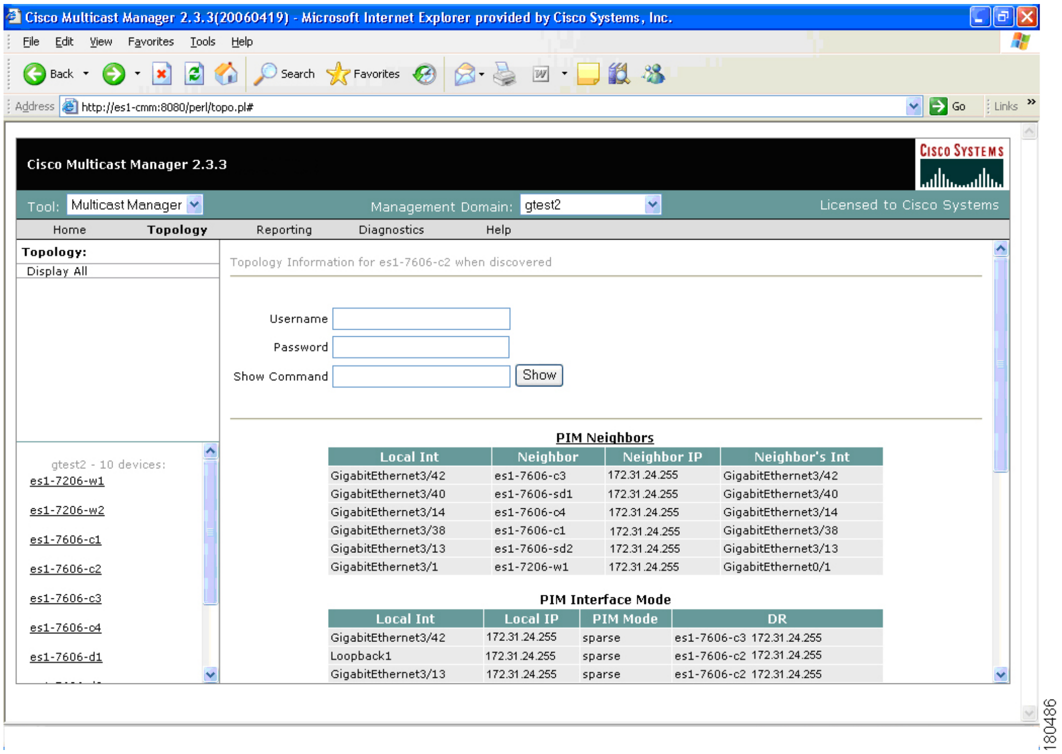
Local Int	Local IP	PIM Mode	IGMP	Neighbor	Neighbor's Int	Neighbor IP	PIM Mode	IGMP	DR
GigabitEthernet3/14	172.31.24.255	sparse	2	es1-7606-c3	GigabitEthernet3/14	172.31.24.255	sparse	2	es1-7606-c 172.31.24.255

The Topology Display All page contains:

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.

To see topology for an individual router, click a router from the list pane at lower left.

Figure 1-30 Topology for an Individual Router


Cisco Multicast Manager 2.3.3(20060419) - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
Go
Links
Cisco Systems
180486

Address: http://es1-cmm:8080/perl/topo.pl#

Cisco Multicast Manager 2.3.3

Tool: Multicast Manager Management Domain: gtest2 Licensed to Cisco Systems

Home | **Topology** | Reporting | Diagnostics | Help

Topology:
Display All

gtest2 - 10 devices:
es1-7206-w1
es1-7206-w2
es1-7606-c1
es1-7606-c2
es1-7606-c3
es1-7606-c4
es1-7606-d1

Topology Information for es1-7606-c2 when discovered

Username
Password
Show Command
Show

PIM Neighbors

Local Int	Neighbor	Neighbor IP	Neighbor's Int
GigabitEthernet3/42	es1-7606-c3	172.31.24.255	GigabitEthernet3/42
GigabitEthernet3/40	es1-7606-sd1	172.31.24.255	GigabitEthernet3/40
GigabitEthernet3/14	es1-7606-c4	172.31.24.255	GigabitEthernet3/14
GigabitEthernet3/38	es1-7606-c1	172.31.24.255	GigabitEthernet3/38
GigabitEthernet3/13	es1-7606-sd2	172.31.24.255	GigabitEthernet3/13
GigabitEthernet3/1	es1-7206-w1	172.31.24.255	GigabitEthernet0/1

PIM Interface Mode

Local Int	Local IP	PIM Mode	DR
GigabitEthernet3/42	172.31.24.255	sparse	es1-7606-c3 172.31.24.255
Loopback1	172.31.24.255	sparse	es1-7606-c2 172.31.24.255
GigabitEthernet3/13	172.31.24.255	sparse	es1-7606-c2 172.31.24.255

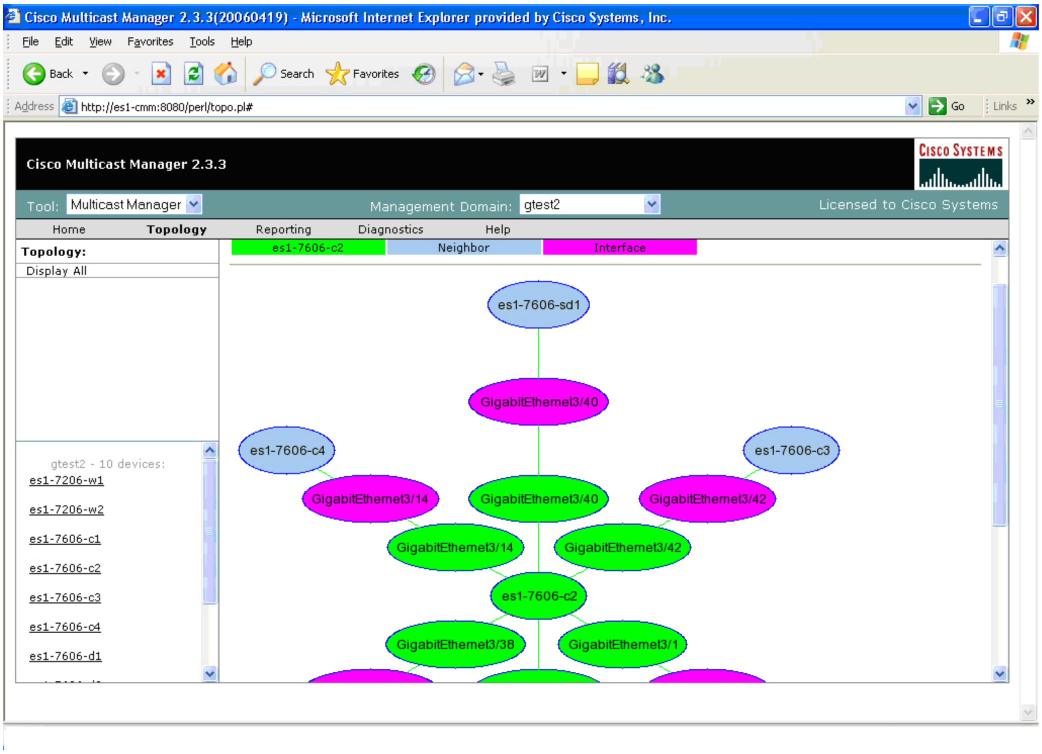
The Topology for an Individual Router page contains:

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 table columns within this window, see the descriptions for the Topology Display All window.

To see a topological display of the routers, click on **PIM Neighbors**.

Figure 1-31 PIM Neighbors



On the PIM Neighbors page:

- Green = Router that was selected and its local interfaces
- Purple = PIM neighbor’s interfaces of this router’s PIM neighbors
- Blue = Names of the PIM neighbors of the selected router

Reporting

With the **Reporting** tool, you can view:

- A record of the latest SNMP traps sent
- Historical graphs or trends
- Routers in the database IOS versions

The following options are available under reporting:

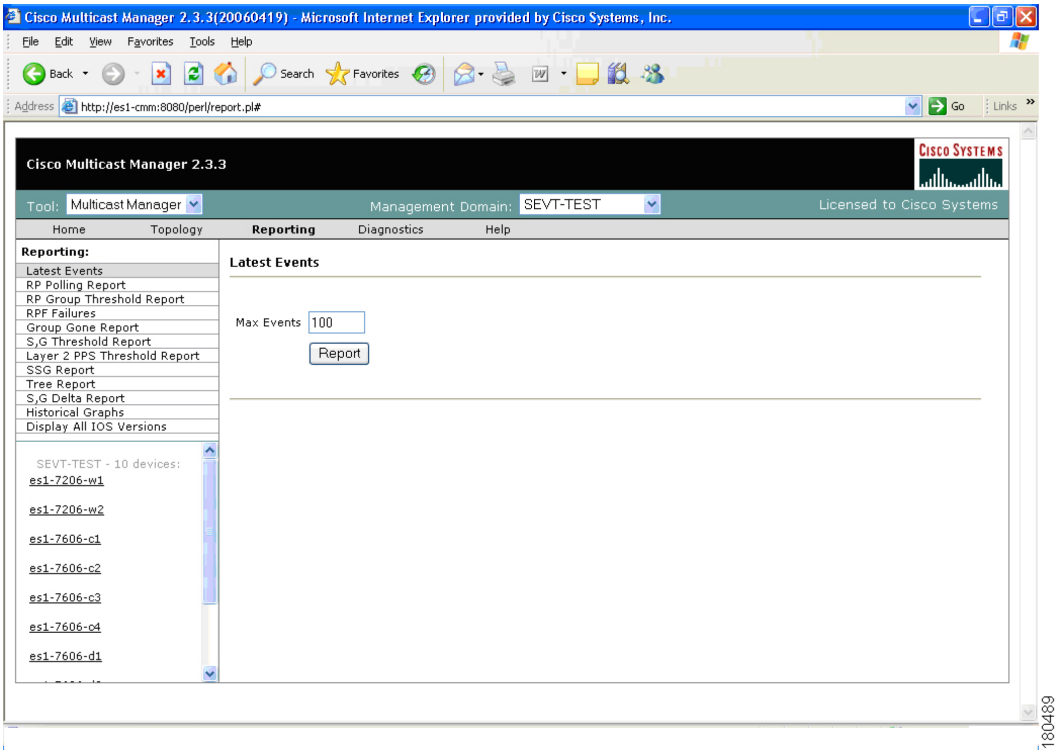
- Latest Events, page 1-49
- RP Polling Report, page 1-49
- RP Group Threshold Report, page 1-50
- RPF Failures, page 1-51
- Group Gone Report, page 1-52
- S,G Threshold Report, page 1-52
- Layer 2 PPS Threshold Report, page 1-53
- SSG Report, page 1-54
- Tree Report, page 1-55
- S,G Delta Report, page 1-57
- Historical Graphs, page 1-58
- Display All IOS Versions, page 1-60

Note The information shown for each type of report, with the exception of Historical Graphs, only spans 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 1-32 Latest Events



Cisco Multicast Manager 2.3.3(20060419) - Microsoft Internet Explorer provided by Cisco Systems, Inc.

Address http://es1-cmm:8080/perl/report.pl#

Cisco Multicast Manager 2.3.3

Tool: Multicast Manager | Management Domain: SEVT-TEST | Licensed to Cisco Systems

Reporting:

Latest Events

Max Events: 100

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 1-28).
- If the selected RP becomes unavailable
- Any rogue source or group that joins the selected RP

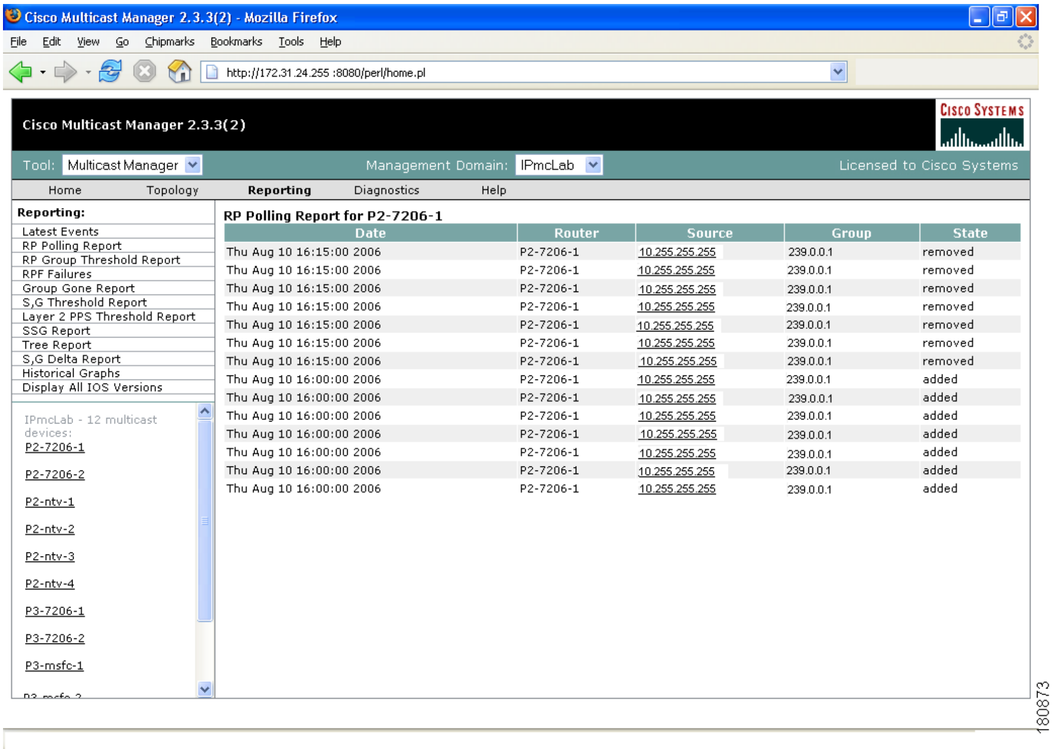
To generate an RP Polling report:

Step 1 Select an RP 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.

Figure 1-33 RP Polling Report



RP Polling Report for P2-7206-1

Date	Router	Source	Group	State
Thu Aug 10 16:15:00 2006	P2-7206-1	10.255.255.255	239.0.0.1	removed
Thu Aug 10 16:15:00 2006	P2-7206-1	10.255.255.255	239.0.0.1	removed
Thu Aug 10 16:15:00 2006	P2-7206-1	10.255.255.255	239.0.0.1	removed
Thu Aug 10 16:15:00 2006	P2-7206-1	10.255.255.255	239.0.0.1	removed
Thu Aug 10 16:15:00 2006	P2-7206-1	10.255.255.255	239.0.0.1	removed
Thu Aug 10 16:15:00 2006	P2-7206-1	10.255.255.255	239.0.0.1	removed
Thu Aug 10 16:15:00 2006	P2-7206-1	10.255.255.255	239.0.0.1	removed
Thu Aug 10 16:00:00 2006	P2-7206-1	10.255.255.255	239.0.0.1	added
Thu Aug 10 16:00:00 2006	P2-7206-1	10.255.255.255	239.0.0.1	added
Thu Aug 10 16:00:00 2006	P2-7206-1	10.255.255.255	239.0.0.1	added
Thu Aug 10 16:00:00 2006	P2-7206-1	10.255.255.255	239.0.0.1	added
Thu Aug 10 16:00:00 2006	P2-7206-1	10.255.255.255	239.0.0.1	added
Thu Aug 10 16:00:00 2006	P2-7206-1	10.255.255.255	239.0.0.1	added
Thu Aug 10 16:00:00 2006	P2-7206-1	10.255.255.255	239.0.0.1	added

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.

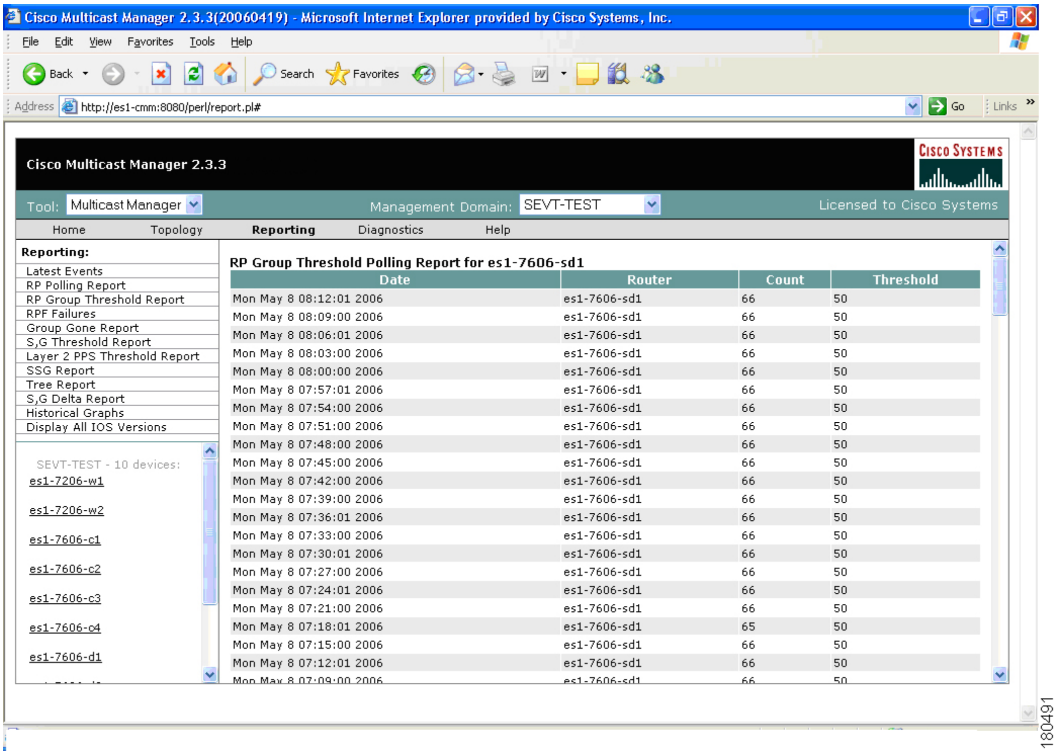
To generate an RP Group Threshold report:

Step 1 Select an RP 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.

Figure 1-34 RP Group Threshold Polling Report



RP Group Threshold Polling Report for es1-7606-sd1

Date	Router	Count	Threshold
Mon May 8 08:12:01 2006	es1-7606-sd1	66	50
Mon May 8 08:09:00 2006	es1-7606-sd1	66	50
Mon May 8 08:06:01 2006	es1-7606-sd1	66	50
Mon May 8 08:03:00 2006	es1-7606-sd1	66	50
Mon May 8 08:00:00 2006	es1-7606-sd1	66	50
Mon May 8 07:57:01 2006	es1-7606-sd1	66	50
Mon May 8 07:54:00 2006	es1-7606-sd1	66	50
Mon May 8 07:51:00 2006	es1-7606-sd1	66	50
Mon May 8 07:48:00 2006	es1-7606-sd1	66	50
Mon May 8 07:45:00 2006	es1-7606-sd1	66	50
Mon May 8 07:42:00 2006	es1-7606-sd1	66	50
Mon May 8 07:39:00 2006	es1-7606-sd1	66	50
Mon May 8 07:36:01 2006	es1-7606-sd1	66	50
Mon May 8 07:33:00 2006	es1-7606-sd1	66	50
Mon May 8 07:30:01 2006	es1-7606-sd1	66	50
Mon May 8 07:27:00 2006	es1-7606-sd1	66	50
Mon May 8 07:24:01 2006	es1-7606-sd1	66	50
Mon May 8 07:21:00 2006	es1-7606-sd1	66	50
Mon May 8 07:18:01 2006	es1-7606-sd1	65	50
Mon May 8 07:15:00 2006	es1-7606-sd1	66	50
Mon May 8 07:12:01 2006	es1-7606-sd1	66	50
Mon May 8 07:09:00 2006	es1-7606-sd1	66	50

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.

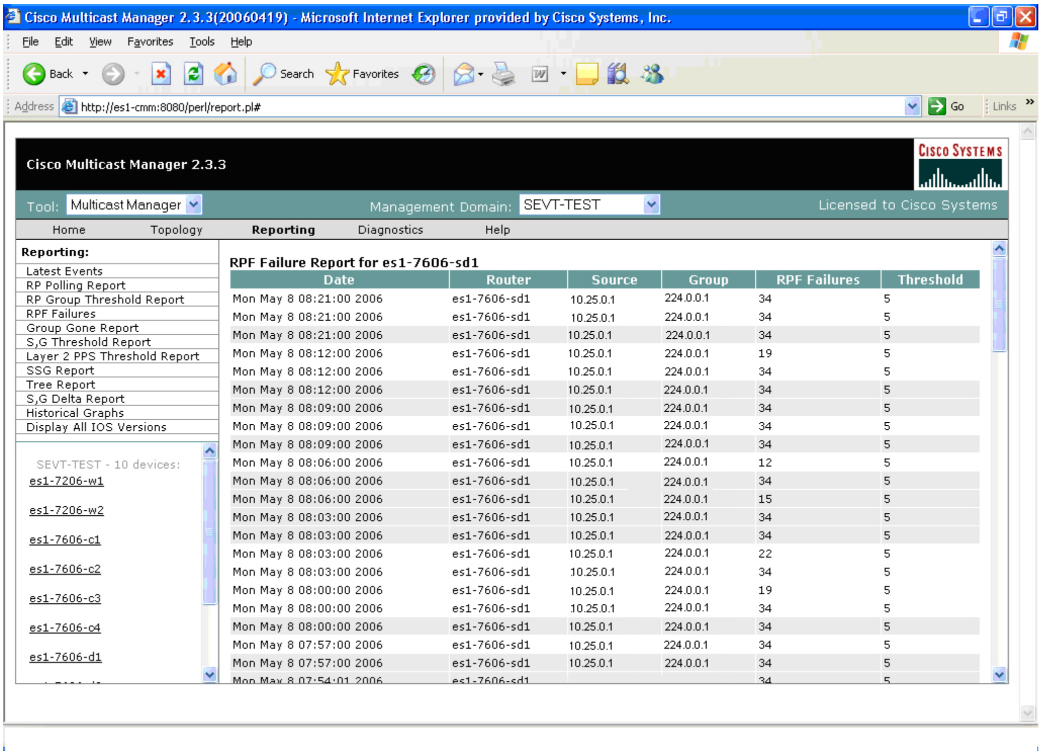
To generate an RPF Failures report:

Step 1 Select an RP 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.

Figure 1-35 RPF Failures Report



RPF Failure Report for es1-7606-sd1

Date	Router	Source	Group	RPF Failures	Threshold
Mon May 8 08:21:00 2006	es1-7606-sd1	10.25.0.1	224.0.0.1	34	5
Mon May 8 08:21:00 2006	es1-7606-sd1	10.25.0.1	224.0.0.1	34	5
Mon May 8 08:21:00 2006	es1-7606-sd1	10.25.0.1	224.0.0.1	34	5
Mon May 8 08:12:00 2006	es1-7606-sd1	10.25.0.1	224.0.0.1	19	5
Mon May 8 08:12:00 2006	es1-7606-sd1	10.25.0.1	224.0.0.1	34	5
Mon May 8 08:12:00 2006	es1-7606-sd1	10.25.0.1	224.0.0.1	34	5
Mon May 8 08:09:00 2006	es1-7606-sd1	10.25.0.1	224.0.0.1	34	5
Mon May 8 08:09:00 2006	es1-7606-sd1	10.25.0.1	224.0.0.1	34	5
Mon May 8 08:09:00 2006	es1-7606-sd1	10.25.0.1	224.0.0.1	34	5
Mon May 8 08:06:00 2006	es1-7606-sd1	10.25.0.1	224.0.0.1	12	5
Mon May 8 08:06:00 2006	es1-7606-sd1	10.25.0.1	224.0.0.1	34	5
Mon May 8 08:06:00 2006	es1-7606-sd1	10.25.0.1	224.0.0.1	15	5
Mon May 8 08:03:00 2006	es1-7606-sd1	10.25.0.1	224.0.0.1	34	5
Mon May 8 08:03:00 2006	es1-7606-sd1	10.25.0.1	224.0.0.1	34	5
Mon May 8 08:03:00 2006	es1-7606-sd1	10.25.0.1	224.0.0.1	22	5
Mon May 8 08:03:00 2006	es1-7606-sd1	10.25.0.1	224.0.0.1	34	5
Mon May 8 08:00:00 2006	es1-7606-sd1	10.25.0.1	224.0.0.1	19	5
Mon May 8 08:00:00 2006	es1-7606-sd1	10.25.0.1	224.0.0.1	34	5
Mon May 8 08:00:00 2006	es1-7606-sd1	10.25.0.1	224.0.0.1	34	5
Mon May 8 07:57:00 2006	es1-7606-sd1	10.25.0.1	224.0.0.1	34	5
Mon May 8 07:57:00 2006	es1-7606-sd1	10.25.0.1	224.0.0.1	34	5
Mon May 8 07:54:01 2006	es1-7606-sd1			34	5

Group Gone Report

*The **Group Gone Report** is currently unsupported. Functionality in this page has moved to the **S,G Polling Report**.*

S,G Threshold Report

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

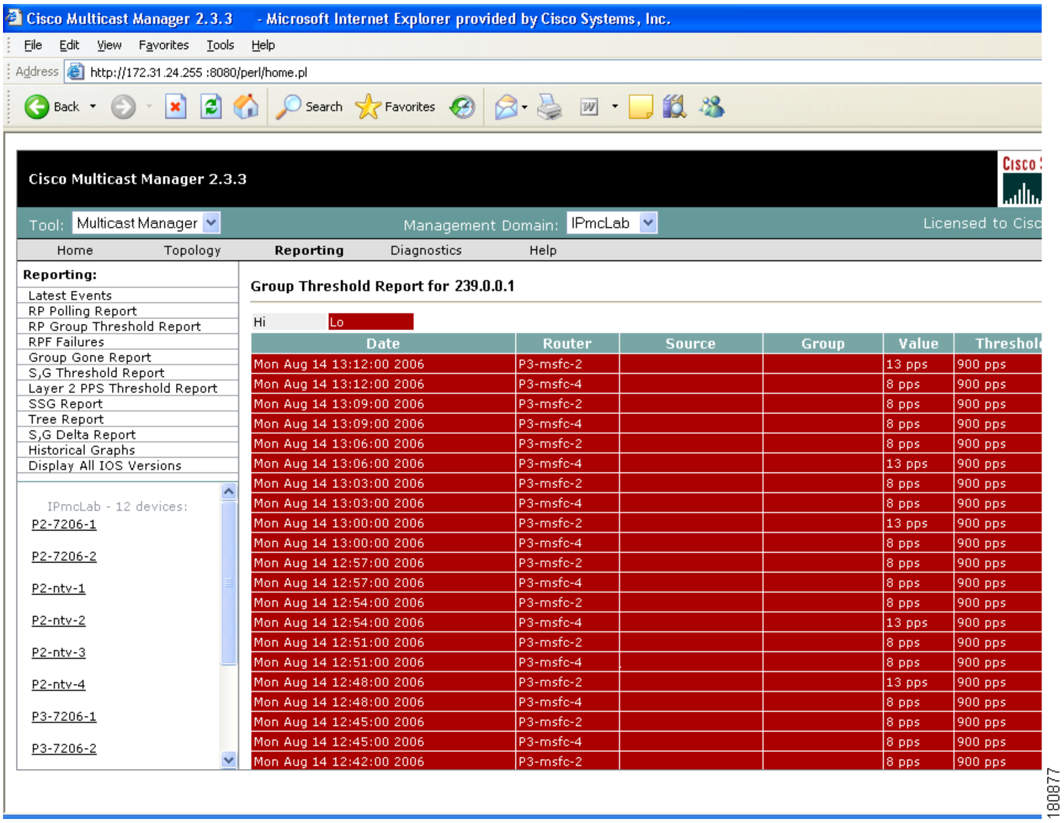
To generate an S,G Threshold report:

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 contains pps and bps.

Figure 1-36 S,G Threshold Report



Group Threshold Report for 239.0.0.1

Hi	Lo

Date	Router	Source	Group	Value	Threshol
Mon Aug 14 13:12:00 2006	P3-msfc-2			13 pps	900 pps
Mon Aug 14 13:12:00 2006	P3-msfc-4			8 pps	900 pps
Mon Aug 14 13:09:00 2006	P3-msfc-2			8 pps	900 pps
Mon Aug 14 13:09:00 2006	P3-msfc-4			8 pps	900 pps
Mon Aug 14 13:06:00 2006	P3-msfc-2			8 pps	900 pps
Mon Aug 14 13:06:00 2006	P3-msfc-4			13 pps	900 pps
Mon Aug 14 13:03:00 2006	P3-msfc-2			8 pps	900 pps
Mon Aug 14 13:03:00 2006	P3-msfc-4			8 pps	900 pps
Mon Aug 14 13:00:00 2006	P3-msfc-2			13 pps	900 pps
Mon Aug 14 13:00:00 2006	P3-msfc-4			8 pps	900 pps
Mon Aug 14 12:57:00 2006	P3-msfc-2			8 pps	900 pps
Mon Aug 14 12:57:00 2006	P3-msfc-4			8 pps	900 pps
Mon Aug 14 12:54:00 2006	P3-msfc-2			8 pps	900 pps
Mon Aug 14 12:54:00 2006	P3-msfc-4			13 pps	900 pps
Mon Aug 14 12:51:00 2006	P3-msfc-2			8 pps	900 pps
Mon Aug 14 12:51:00 2006	P3-msfc-4			8 pps	900 pps
Mon Aug 14 12:48:00 2006	P3-msfc-2			13 pps	900 pps
Mon Aug 14 12:48:00 2006	P3-msfc-4			8 pps	900 pps
Mon Aug 14 12:45:00 2006	P3-msfc-2			8 pps	900 pps
Mon Aug 14 12:45:00 2006	P3-msfc-4			8 pps	900 pps
Mon Aug 14 12:42:00 2006	P3-msfc-2			8 pps	900 pps

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:

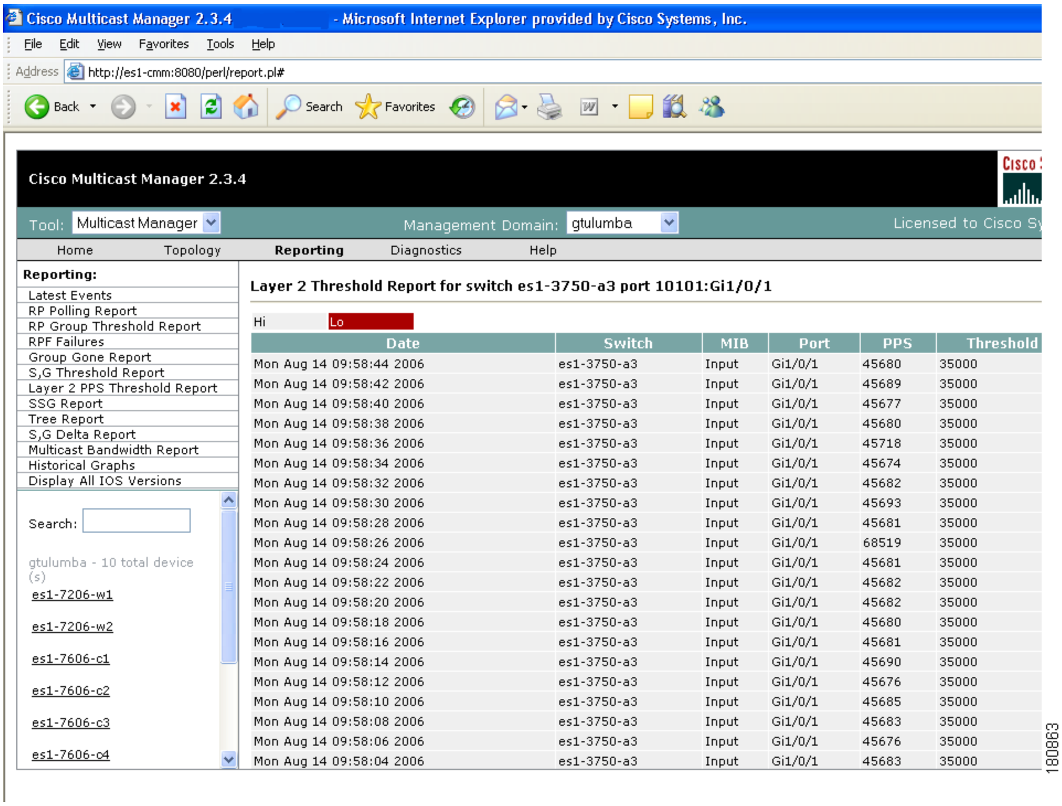
Step 1 Select a switch from the list.

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.

Figure 1-37 Layer 2 PPS Threshold Report



Layer 2 Threshold Report for switch es1-3750-a3 port 10101:Gi1/0/1

Date	Switch	MIB	Port	PPS	Threshold
Mon Aug 14 09:58:44 2006	es1-3750-a3	Input	Gi1/0/1	45680	35000
Mon Aug 14 09:58:42 2006	es1-3750-a3	Input	Gi1/0/1	45689	35000
Mon Aug 14 09:58:40 2006	es1-3750-a3	Input	Gi1/0/1	45677	35000
Mon Aug 14 09:58:38 2006	es1-3750-a3	Input	Gi1/0/1	45680	35000
Mon Aug 14 09:58:36 2006	es1-3750-a3	Input	Gi1/0/1	45718	35000
Mon Aug 14 09:58:34 2006	es1-3750-a3	Input	Gi1/0/1	45674	35000
Mon Aug 14 09:58:32 2006	es1-3750-a3	Input	Gi1/0/1	45682	35000
Mon Aug 14 09:58:30 2006	es1-3750-a3	Input	Gi1/0/1	45693	35000
Mon Aug 14 09:58:28 2006	es1-3750-a3	Input	Gi1/0/1	45681	35000
Mon Aug 14 09:58:26 2006	es1-3750-a3	Input	Gi1/0/1	68519	35000
Mon Aug 14 09:58:24 2006	es1-3750-a3	Input	Gi1/0/1	45681	35000
Mon Aug 14 09:58:22 2006	es1-3750-a3	Input	Gi1/0/1	45682	35000
Mon Aug 14 09:58:20 2006	es1-3750-a3	Input	Gi1/0/1	45682	35000
Mon Aug 14 09:58:18 2006	es1-3750-a3	Input	Gi1/0/1	45680	35000
Mon Aug 14 09:58:16 2006	es1-3750-a3	Input	Gi1/0/1	45681	35000
Mon Aug 14 09:58:14 2006	es1-3750-a3	Input	Gi1/0/1	45690	35000
Mon Aug 14 09:58:12 2006	es1-3750-a3	Input	Gi1/0/1	45676	35000
Mon Aug 14 09:58:10 2006	es1-3750-a3	Input	Gi1/0/1	45685	35000
Mon Aug 14 09:58:08 2006	es1-3750-a3	Input	Gi1/0/1	45683	35000
Mon Aug 14 09:58:06 2006	es1-3750-a3	Input	Gi1/0/1	45676	35000
Mon Aug 14 09:58:04 2006	es1-3750-a3	Input	Gi1/0/1	45683	35000

SSG Report

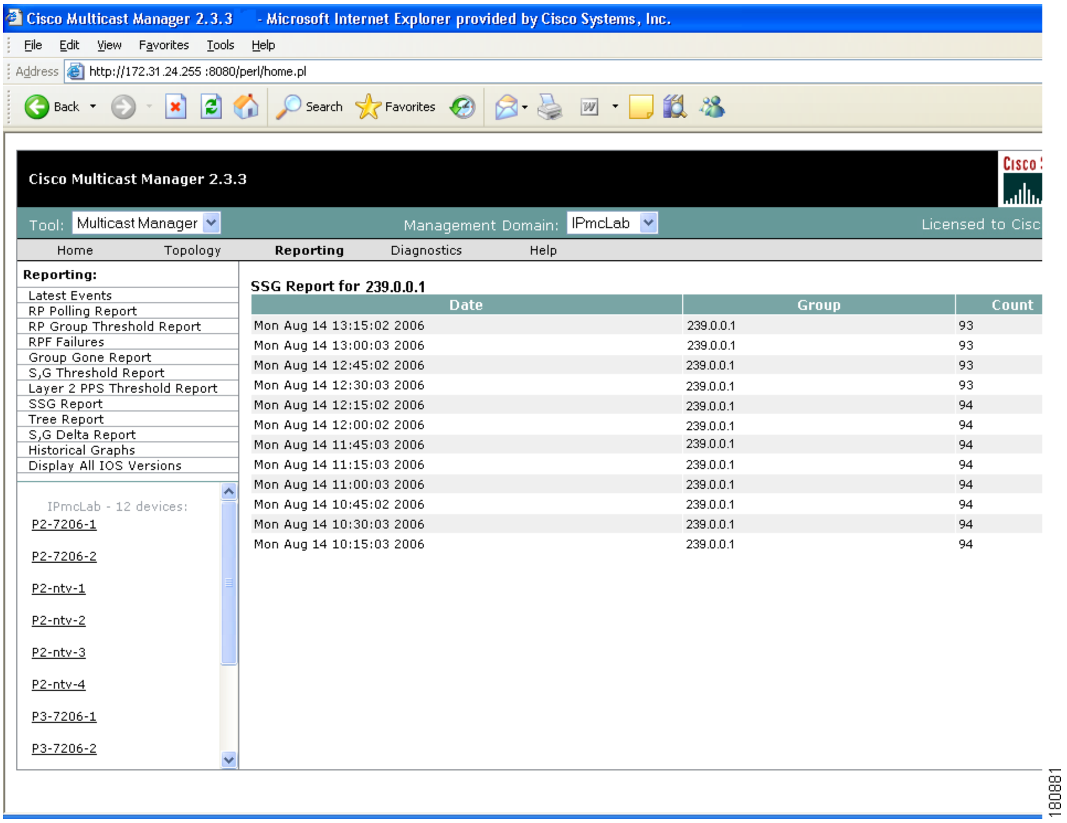
Using the **SSG Report**, you can display information about groups that have more than one sender.

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.

Figure 1-38 SSG Report



SSG Report for 239.0.0.1

Date	Group	Count
Mon Aug 14 13:15:02 2006	239.0.0.1	93
Mon Aug 14 13:00:03 2006	239.0.0.1	93
Mon Aug 14 12:45:02 2006	239.0.0.1	93
Mon Aug 14 12:30:03 2006	239.0.0.1	93
Mon Aug 14 12:15:02 2006	239.0.0.1	94
Mon Aug 14 12:00:02 2006	239.0.0.1	94
Mon Aug 14 11:45:03 2006	239.0.0.1	94
Mon Aug 14 11:15:03 2006	239.0.0.1	94
Mon Aug 14 11:00:03 2006	239.0.0.1	94
Mon Aug 14 10:45:02 2006	239.0.0.1	94
Mon Aug 14 10:30:03 2006	239.0.0.1	94
Mon Aug 14 10:15:03 2006	239.0.0.1	94

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 the "Show All Groups" section on page 1-61.

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.

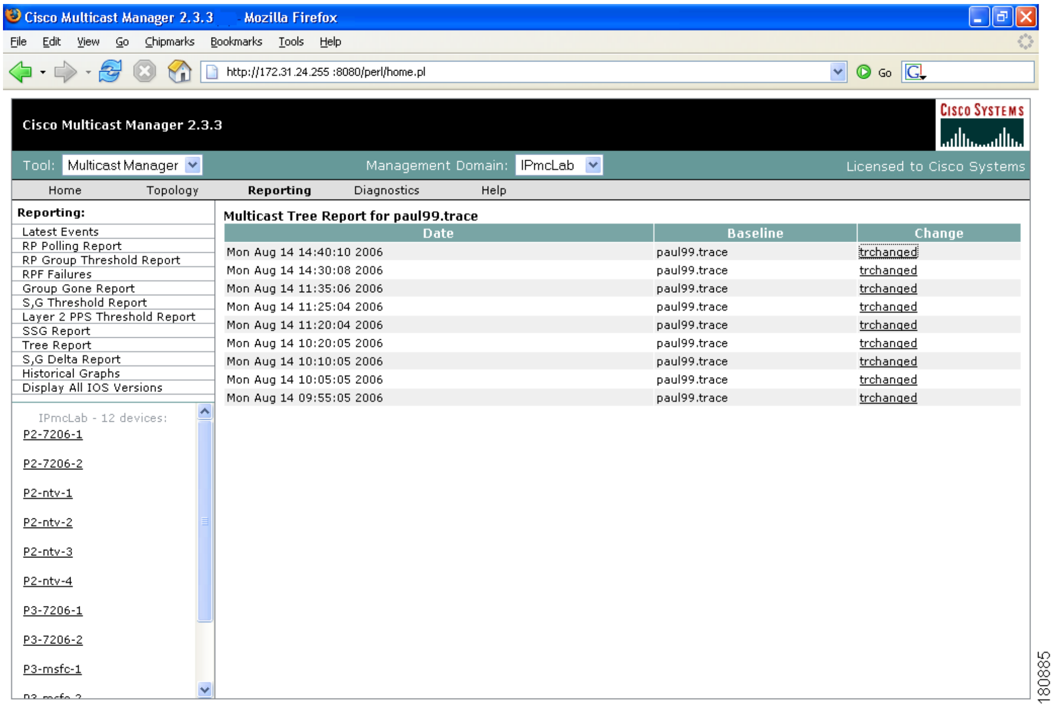
To generate a Multicast Tree Report:

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.

Figure 1-39 Tree Report


Cisco Multicast Manager 2.3.3 Mozilla Firefox
File Edit View Go Chipmarks Bookmarks Tools Help
http://172.31.24.255 :8080/perl/home.pl
Go
Cisco Multicast Manager 2.3.3
Cisco Systems
Tool: Multicast Manager
Management Domain: IPmcLab
Licensed to Cisco Systems
Home
Topology
Reporting
Diagnostics
Help

Reporting:
- Latest Events
- RP Polling Report
- RP Group Threshold Report
- RPF Failures
- Group Gone Report
- S,G Threshold Report
- Layer 2 PPS Threshold Report
- SSG Report
- Tree Report
- S,G Delta Report
- Historical Graphs
- Display All IOS Versions

IPmcLab - 12 devices:
- P2-7206-1
- P2-7206-2
- P2-ntv-1
- P2-ntv-2
- P2-ntv-3
- P2-ntv-4
- P3-7206-1
- P3-7206-2
- P3-msfc-1

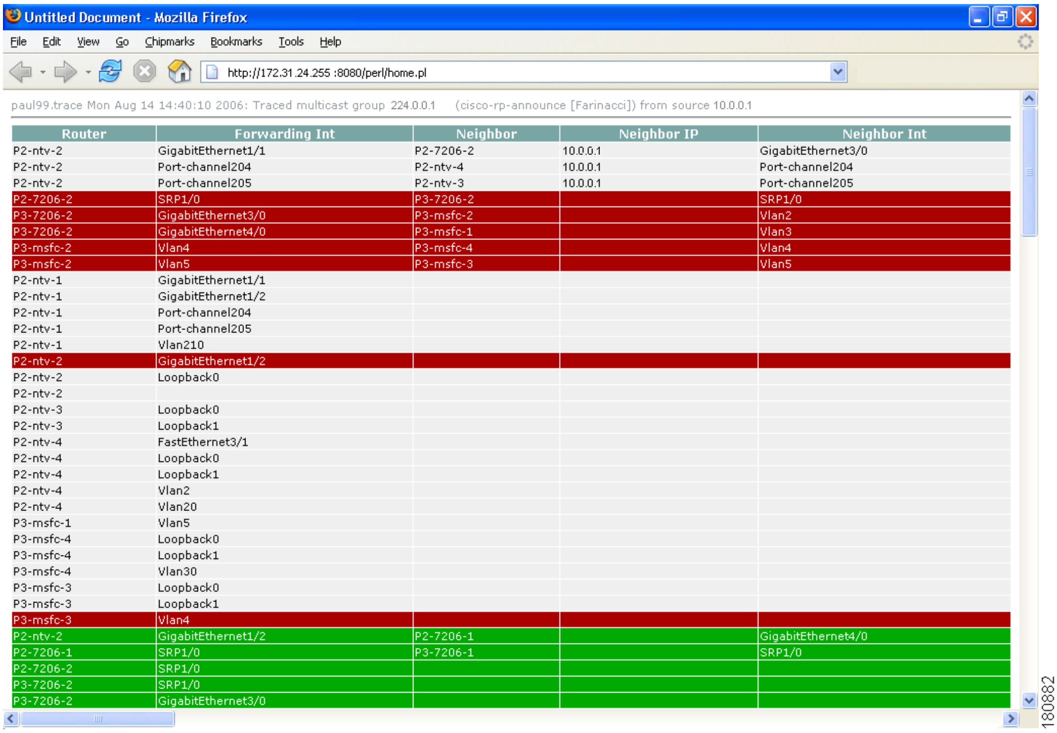
Multicast Tree Report for paul99.trace

Date	Baseline	Change
Mon Aug 14 14:40:10 2006	paul99.trace	trchanged
Mon Aug 14 14:30:08 2006	paul99.trace	trchanged
Mon Aug 14 11:35:06 2006	paul99.trace	trchanged
Mon Aug 14 11:25:04 2006	paul99.trace	trchanged
Mon Aug 14 11:20:04 2006	paul99.trace	trchanged
Mon Aug 14 10:20:05 2006	paul99.trace	trchanged
Mon Aug 14 10:10:05 2006	paul99.trace	trchanged
Mon Aug 14 10:05:05 2006	paul99.trace	trchanged
Mon Aug 14 09:55:05 2006	paul99.trace	trchanged

180885

Clicking “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 1-40 Tree Report Page—Trchanged


Untitled Document - Mozilla Firefox
File Edit View Go Chipmarks Bookmarks Tools Help
http://172.31.24.255 :8080/perl/home.pl
180882

paul99.trace Mon Aug 14 14:40:10 2006: Traced multicast group 224.0.0.1 (cisco-rp-announce [Farinacci]) from source 10.0.0.1

Router	Forwarding Int	Neighbor	Neighbor IP	Neighbor Int
P2-ntv-2	GigabitEthernet1/1	P2-7206-2	10.0.0.1	GigabitEthernet3/0
P2-ntv-2	Port-channel204	P2-ntv-4	10.0.0.1	Port-channel204
P2-ntv-2	Port-channel205	P2-ntv-3	10.0.0.1	Port-channel205
P2-7206-2	SRP1/0	P3-7206-2		SRP1/0
P3-7206-2	GigabitEthernet3/0	P3-msfc-2		Vlan2
P3-7206-2	GigabitEthernet4/0	P3-msfc-1		Vlan3
P3-msfc-2	Vlan4	P3-msfc-4		Vlan4
P3-msfc-2	Vlan5	P3-msfc-3		Vlan5
P2-ntv-1	GigabitEthernet1/1			
P2-ntv-1	GigabitEthernet1/2			
P2-ntv-1	Port-channel204			
P2-ntv-1	Port-channel205			
P2-ntv-1	Vlan210			
P2-ntv-2	GigabitEthernet1/2			
P2-ntv-2	Loopback0			
P2-ntv-2				
P2-ntv-3	Loopback0			
P2-ntv-3	Loopback1			
P2-ntv-4	FastEthernet3/1			
P2-ntv-4	Loopback0			
P2-ntv-4	Loopback1			
P2-ntv-4	Vlan2			
P2-ntv-4	Vlan20			
P3-msfc-1	Vlan5			
P3-msfc-4	Loopback0			
P3-msfc-4	Loopback1			
P3-msfc-4	Vlan30			
P3-msfc-3	Loopback0			
P3-msfc-3	Loopback1			
P3-msfc-3	Vlan4			
P2-ntv-2	GigabitEthernet1/2	P2-7206-1		GigabitEthernet4/0
P2-7206-1	SRP1/0	P3-7206-1		SRP1/0
P2-7206-2	SRP1/0			
P3-7206-2	SRP1/0			
P3-7206-2	GigabitEthernet3/0			

S,G Delta Report

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

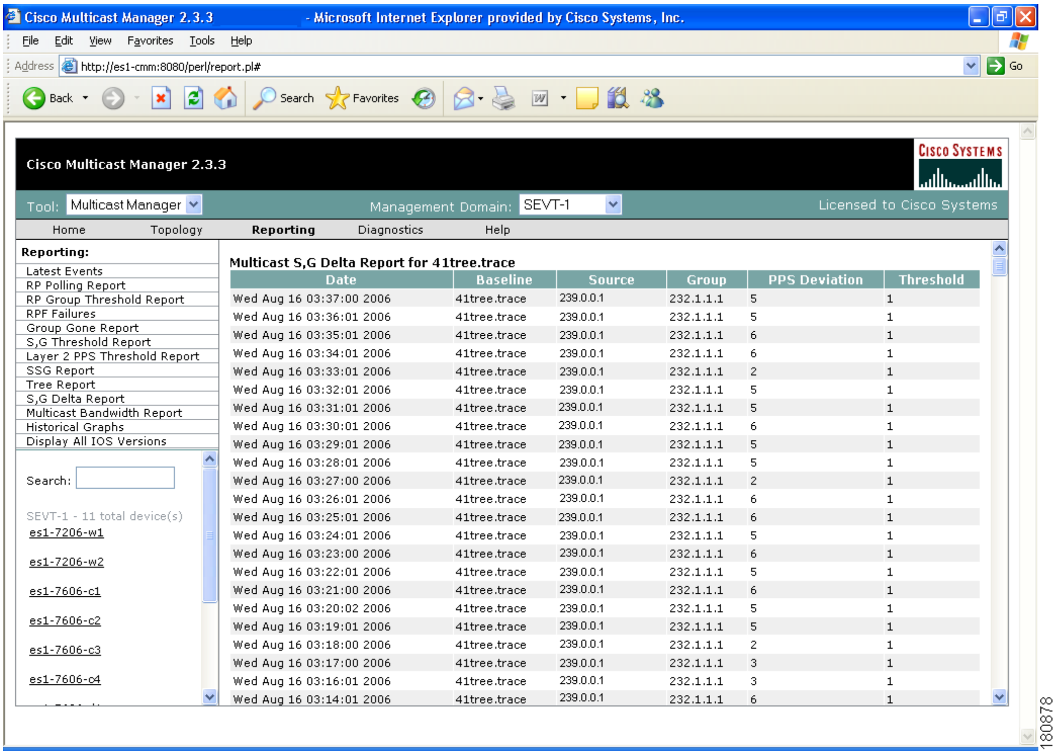
To generate a Multicast S,G Delta Report:

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.

Figure 1-41 Multicast S,G Delta Report



Tool: Multicast Manager

Management Domain: SEVT-1

Multicast S,G Delta Report for 41tree.trace

Date	Baseline	Source	Group	PPS Deviation	Threshold
Wed Aug 16 03:37:00 2006	41tree.trace	239.0.0.1	232.1.1.1	5	1
Wed Aug 16 03:36:01 2006	41tree.trace	239.0.0.1	232.1.1.1	5	1
Wed Aug 16 03:35:01 2006	41tree.trace	239.0.0.1	232.1.1.1	6	1
Wed Aug 16 03:34:01 2006	41tree.trace	239.0.0.1	232.1.1.1	6	1
Wed Aug 16 03:33:01 2006	41tree.trace	239.0.0.1	232.1.1.1	2	1
Wed Aug 16 03:32:01 2006	41tree.trace	239.0.0.1	232.1.1.1	5	1
Wed Aug 16 03:31:01 2006	41tree.trace	239.0.0.1	232.1.1.1	5	1
Wed Aug 16 03:30:01 2006	41tree.trace	239.0.0.1	232.1.1.1	6	1
Wed Aug 16 03:29:01 2006	41tree.trace	239.0.0.1	232.1.1.1	5	1
Wed Aug 16 03:28:01 2006	41tree.trace	239.0.0.1	232.1.1.1	5	1
Wed Aug 16 03:27:00 2006	41tree.trace	239.0.0.1	232.1.1.1	2	1
Wed Aug 16 03:26:01 2006	41tree.trace	239.0.0.1	232.1.1.1	6	1
Wed Aug 16 03:25:01 2006	41tree.trace	239.0.0.1	232.1.1.1	6	1
Wed Aug 16 03:24:01 2006	41tree.trace	239.0.0.1	232.1.1.1	5	1
Wed Aug 16 03:23:00 2006	41tree.trace	239.0.0.1	232.1.1.1	6	1
Wed Aug 16 03:22:01 2006	41tree.trace	239.0.0.1	232.1.1.1	5	1
Wed Aug 16 03:21:00 2006	41tree.trace	239.0.0.1	232.1.1.1	6	1
Wed Aug 16 03:20:02 2006	41tree.trace	239.0.0.1	232.1.1.1	5	1
Wed Aug 16 03:19:01 2006	41tree.trace	239.0.0.1	232.1.1.1	5	1
Wed Aug 16 03:18:00 2006	41tree.trace	239.0.0.1	232.1.1.1	2	1
Wed Aug 16 03:17:00 2006	41tree.trace	239.0.0.1	232.1.1.1	3	1
Wed Aug 16 03:16:01 2006	41tree.trace	239.0.0.1	232.1.1.1	3	1
Wed Aug 16 03:14:01 2006	41tree.trace	239.0.0.1	232.1.1.1	6	1

Historical Graphs

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

- Source and group activity in a router

  or

- multicast packets inbound or outbound of a Layer 2 port

  or

- 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**:

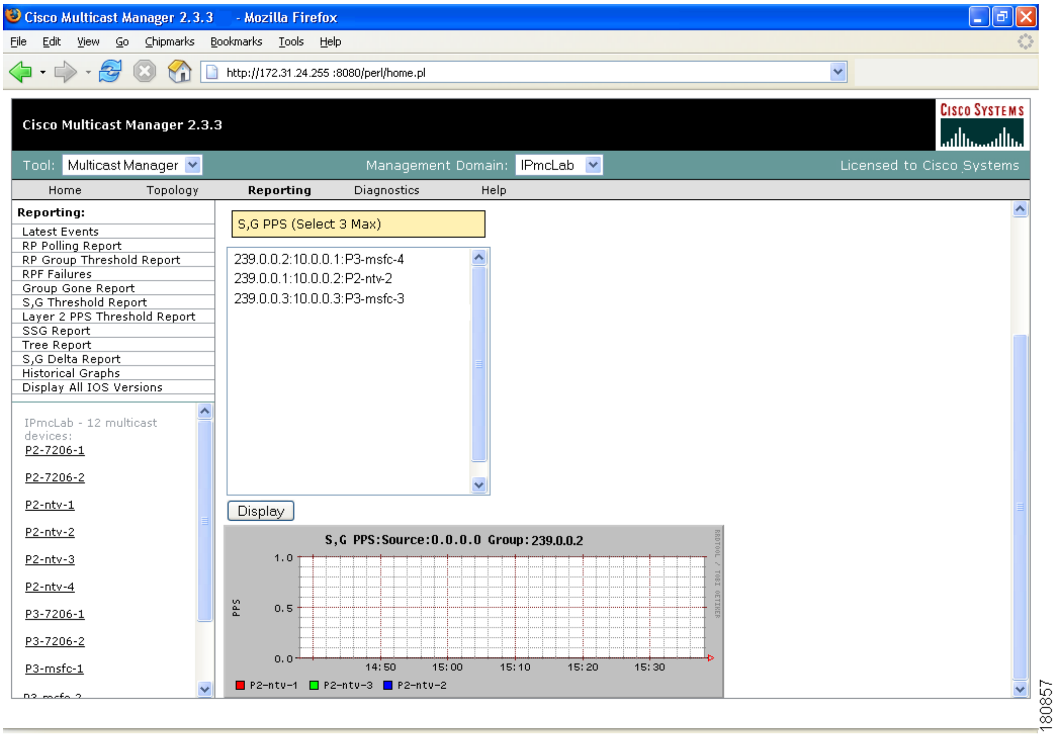
- **User Specified**
- **Hour**
- **Day**
- **Week**
- **Month**

Then select a **Start** and **End** range.

Step 3 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 the "Top Talkers" section on page 1-75).

Figure 1-42 Historical Graphs



Cisco Multicast Manager 2.3.3 - Mozilla Firefox

http://172.31.24.255 :8080/perl/home.pl

Cisco Multicast Manager 2.3.3

Tool: Multicast Manager

Management Domain: IPmcLab

Licensed to Cisco Systems

S,G PPS (Select 3 Max)

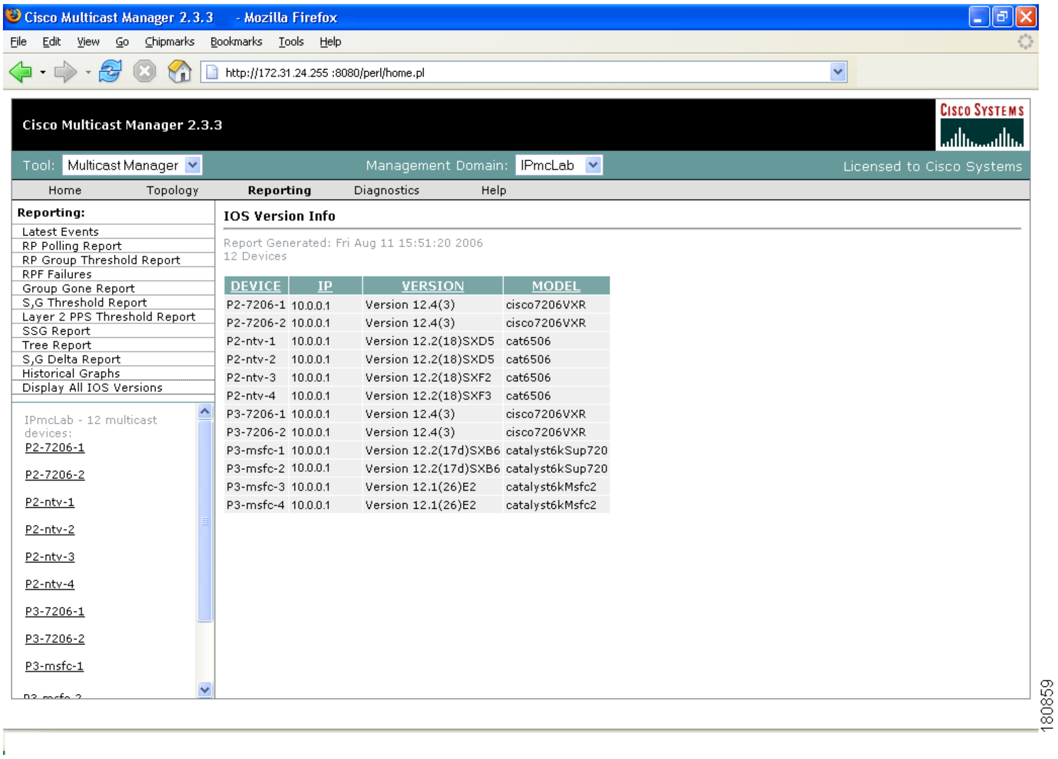
239.0.0.2:10.0.0.1:P3-msfc-4
239.0.0.1:10.0.0.2:P2-ntv-2
239.0.0.3:10.0.0.3:P3-msfc-3

IPmcLab - 12 multicast devices:
P2-7206-1
P2-7206-2
P2-ntv-1
P2-ntv-2
P2-ntv-3
P2-ntv-4
P3-7206-1
P3-7206-2
P3-msfc-1

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 clicking on the corresponding column heading.

Figure 1-43 IOS Version Info


Cisco Multicast Manager 2.3.3 - Mozilla Firefox
File Edit View Go Chipmarks Bookmarks Tools Help
http://172.31.24.255 :8080/perl/home.pl
Cisco Multicast Manager 2.3.3
Cisco Systems
Tool: Multicast Manager
Management Domain: IPmcLab
Licensed to Cisco Systems
Home Topology Reporting Diagnostics Help
Reporting:
Latest Events
RP Polling Report
RP Group Threshold Report
RPF Failures
Group Gone Report
S,G Threshold Report
Layer 2 PPS Threshold Report
SSG Report
Tree Report
S,G Delta Report
Historical Graphs
Display All IOS Versions
IPmcLab - 12 multicast devices:
P2-7206-1
P2-7206-2
P2-ntv-1
P2-ntv-2
P2-ntv-3
P2-ntv-4
P3-7206-1
P3-7206-2
P3-msfc-1
P3-msfc-2
180859

IOS Version Info

Report Generated: Fri Aug 11 15:51:20 2006
12 Devices

DEVICE	IP	VERSION	MODEL
P2-7206-1	10.0.0.1	Version 12.4(3)	cisco7206VXR
P2-7206-2	10.0.0.1	Version 12.4(3)	cisco7206VXR
P2-ntv-1	10.0.0.1	Version 12.2(18)SXD5	cat6506
P2-ntv-2	10.0.0.1	Version 12.2(18)SXD5	cat6506
P2-ntv-3	10.0.0.1	Version 12.2(18)SXF2	cat6506
P2-ntv-4	10.0.0.1	Version 12.2(18)SXF3	cat6506
P3-7206-1	10.0.0.1	Version 12.4(3)	cisco7206VXR
P3-7206-2	10.0.0.1	Version 12.4(3)	cisco7206VXR
P3-msfc-1	10.0.0.1	Version 12.2(17d)SXB6	catalyst6kSup720
P3-msfc-2	10.0.0.1	Version 12.2(17d)SXB6	catalyst6kSup720
P3-msfc-3	10.0.0.1	Version 12.1(26)E2	catalyst6kMsfc2
P3-msfc-4	10.0.0.1	Version 12.1(26)E2	catalyst6kMsfc2

Diagnostics

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

- Show All Groups, page 1-61
- Locate Host, page 1-66
- Network Status, page 1-67
- RP Status, page 1-68
- RP Summary, page 1-69
- IGMP Diagnostics, page 1-69
- MSDP Status, page 1-70
- Layer 2 Switches, page 1-71

- Health Check, page 1-73
- 6500 Troubleshooting, page 1-73
- Top Talkers, page 1-75

The following section describes router-specific diagnostics:

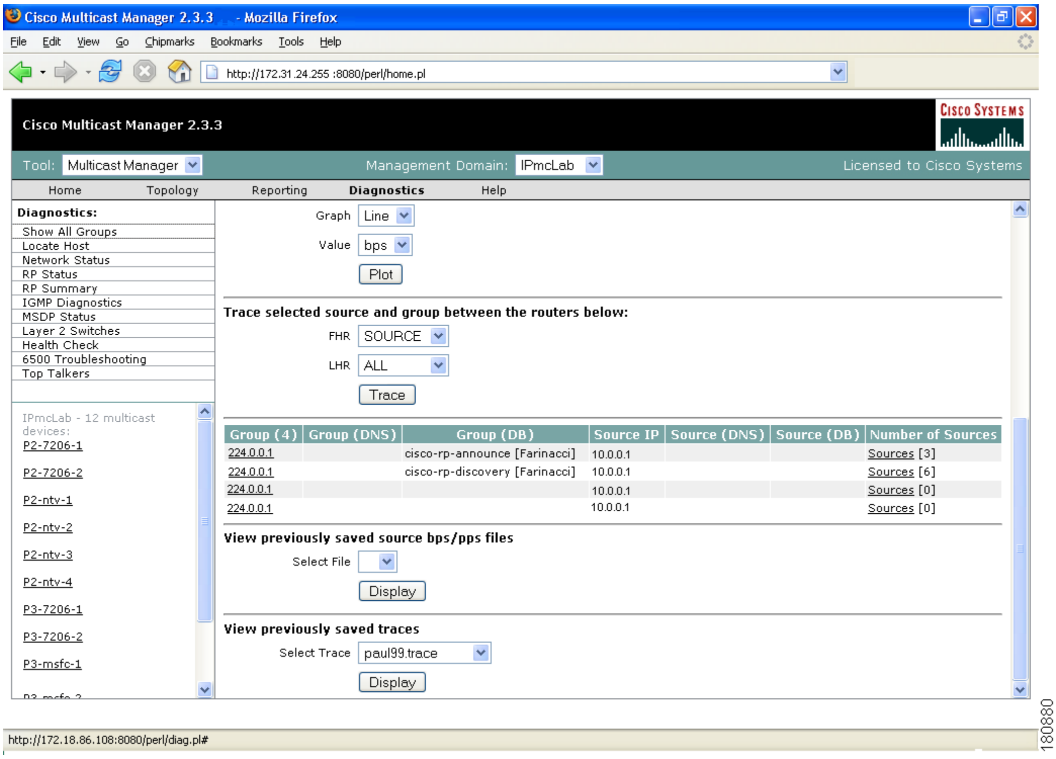
- Router Diagnostics, page 1-77

Show All Groups

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

1. View all of 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, click **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.

Figure 1-44 Multicast Diagnostics



Tool: Multicast Manager   Management Domain: IPmcLab   Licensed to Cisco Systems

Graph: Line
Value: bps

Trace selected source and group between the routers below:

FHR: SOURCE
LHR: ALL

Group (4)	Group (DNS)	Group (DB)	Source IP	Source (DNS)	Source (DB)	Number of Sources
224.0.0.1		cisco-rp-announce [Farinacci]	10.0.0.1			Sources [3]
224.0.0.1		cisco-rp-discovery [Farinacci]	10.0.0.1			Sources [6]
224.0.0.1			10.0.0.1			Sources [0]
224.0.0.1			10.0.0.1			Sources [0]

View previously saved source bps/pps files

Select File:

View previously saved traces

Select Trace: paul99.trace

(Optional) If you are using S,G caching, the cache contents appear. Click **Refresh Cache** to refresh the table of sources and groups.

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:

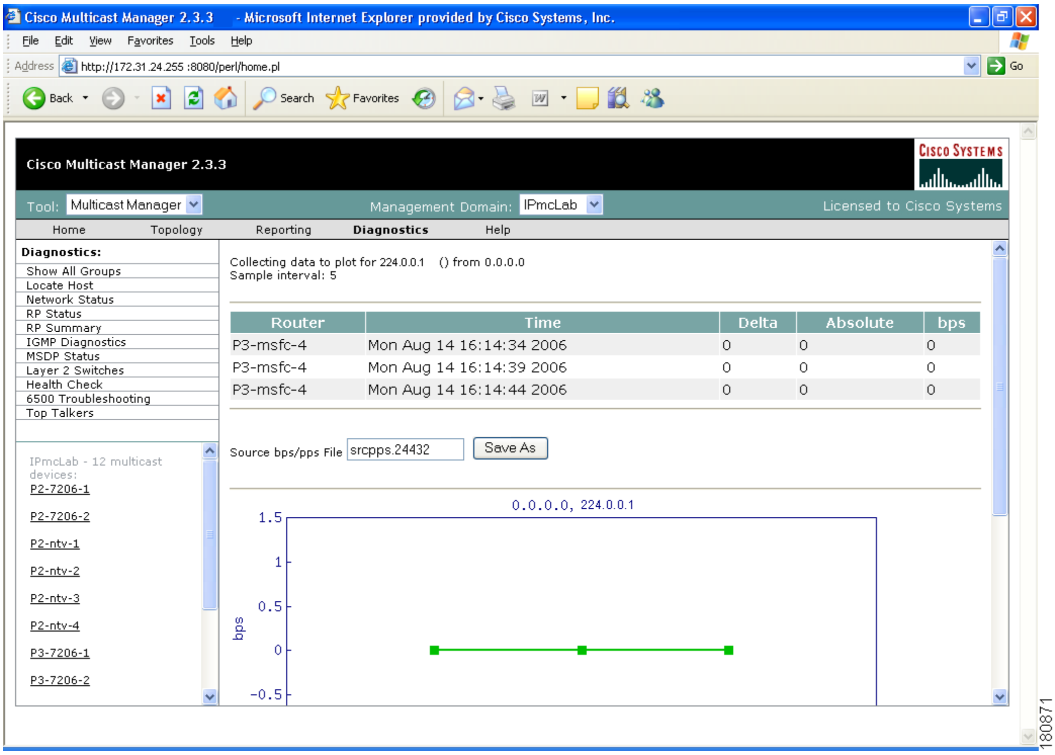
- **Select Router—**Select the router to take the sample from.
- **Samples—**Enter the number of samples (1-50).

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.

Figure 1-45 Multicast Diagnostics—Plotting Traffic



Tool: Multicast Manager Management Domain: IPmcLab Licensed to Cisco Systems

Collecting data to plot for 224.0.0.1 () from 0.0.0.0
Sample interval: 5

Router	Time	Delta	Absolute	bps
P3-msfc-4	Mon Aug 14 16:14:34 2006	0	0	0
P3-msfc-4	Mon Aug 14 16:14:39 2006	0	0	0
P3-msfc-4	Mon Aug 14 16:14:44 2006	0	0	0

Source bps/pps File srcpps.24432

To draw a graphical tree between two particular routers:

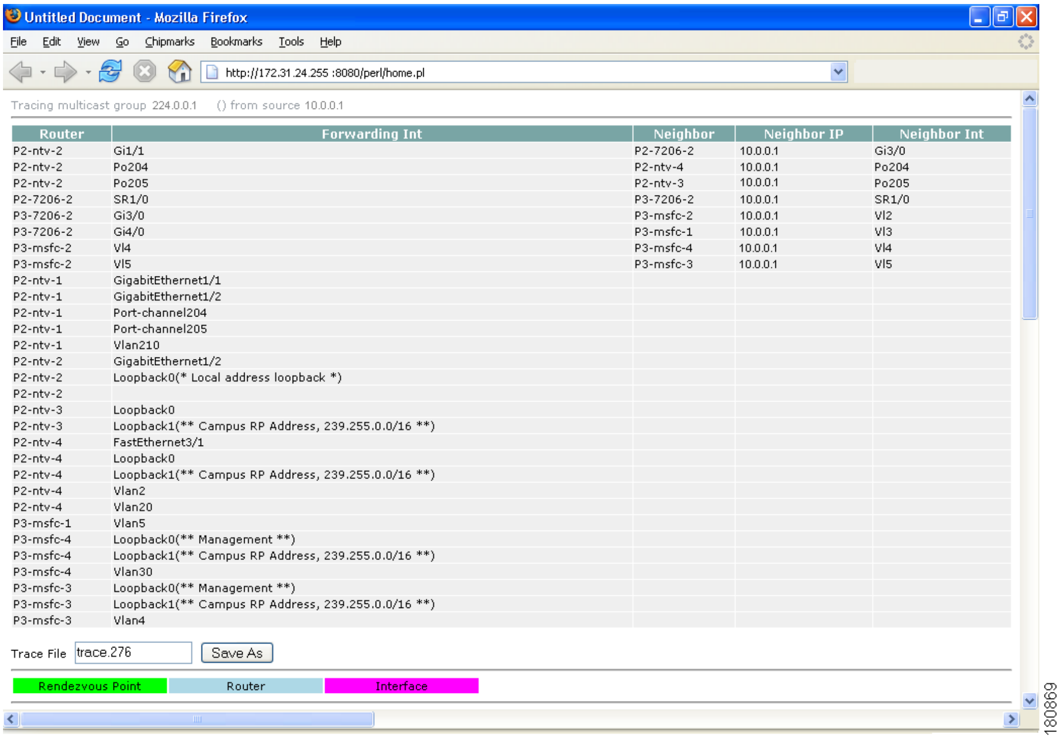
- **FHR—**Select the first hop router that the trace should start under.
- **LHR—**Select the last hop router that the trace should end under.
- Click **Trace**. The CMM draws a tree of the source and group selected from the router in FHR to the router in LHR.

View the list of active sources and groups:

- **Group—**Lists all active groups. To draw a multicast tree, click on a group. 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, click on **Sources** under **Number of Sources** and select the source you want to draw the tree from.

Figure 1-46 Drawing a Multicast Tree (Baseline)


Untitled Document - Mozilla Firefox
File Edit View Go Chipmarks Bookmarks Tools Help
http://172.31.24.255 :8080/perl/home.pl
180869

Tracing multicast group 224.0.0.1 () from source 10.0.0.1

Router	Forwarding Int	Neighbor	Neighbor IP	Neighbor Int
P2-ntv-2	Gi1/1	P2-7206-2	10.0.0.1	Gi3/0
P2-ntv-2	Po204	P2-ntv-4	10.0.0.1	Po204
P2-ntv-2	Po205	P2-ntv-3	10.0.0.1	Po205
P2-7206-2	SR1/0	P3-7206-2	10.0.0.1	SR1/0
P3-7206-2	Gi3/0	P3-msfc-2	10.0.0.1	Vl2
P3-7206-2	Gi4/0	P3-msfc-1	10.0.0.1	Vl3
P3-msfc-2	Vl4	P3-msfc-4	10.0.0.1	Vl4
P3-msfc-2	Vl5	P3-msfc-3	10.0.0.1	Vl5
P2-ntv-1	GigabitEthernet1/1			
P2-ntv-1	GigabitEthernet1/2			
P2-ntv-1	Port-channel204			
P2-ntv-1	Port-channel205			
P2-ntv-1	Vlan210			
P2-ntv-2	GigabitEthernet1/2			
P2-ntv-2	Loopback0(* Local address loopback *)			
P2-ntv-2				
P2-ntv-3	Loopback0			
P2-ntv-3	Loopback1(** Campus RP Address, 239.255.0.0/16 **)			
P2-ntv-4	FastEthernet3/1			
P2-ntv-4	Loopback0			
P2-ntv-4	Loopback1(** Campus RP Address, 239.255.0.0/16 **)			
P2-ntv-4	Vlan2			
P2-ntv-4	Vlan20			
P3-msfc-1	Vlan5			
P3-msfc-4	Loopback0(** Management **)			
P3-msfc-4	Loopback1(** Campus RP Address, 239.255.0.0/16 **)			
P3-msfc-4	Vlan30			
P3-msfc-3	Loopback0(** Management **)			
P3-msfc-3	Loopback1(** Campus RP Address, 239.255.0.0/16 **)			
P3-msfc-3	Vlan4			

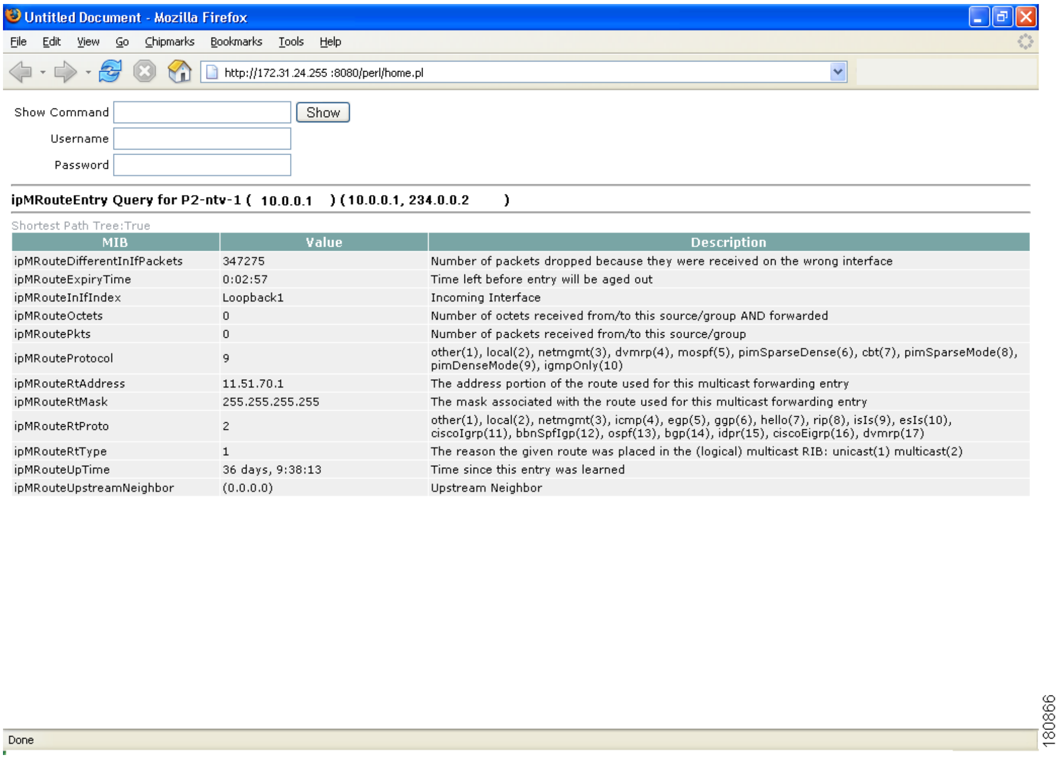
Trace File trace.276 Save As

Rendezvous Point Router Interface

- 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 the "Tree Polling" section on page 1-38).

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

Figure 1-47 Viewing IP Multicast Routing Information


Untitled Document - Mozilla Firefox
File Edit View Go Chipmarks Bookmarks Tools Help
http://172.31.24.255 :8080/perl/home.pl
Show Command
Show
Username
Password
Done
180866

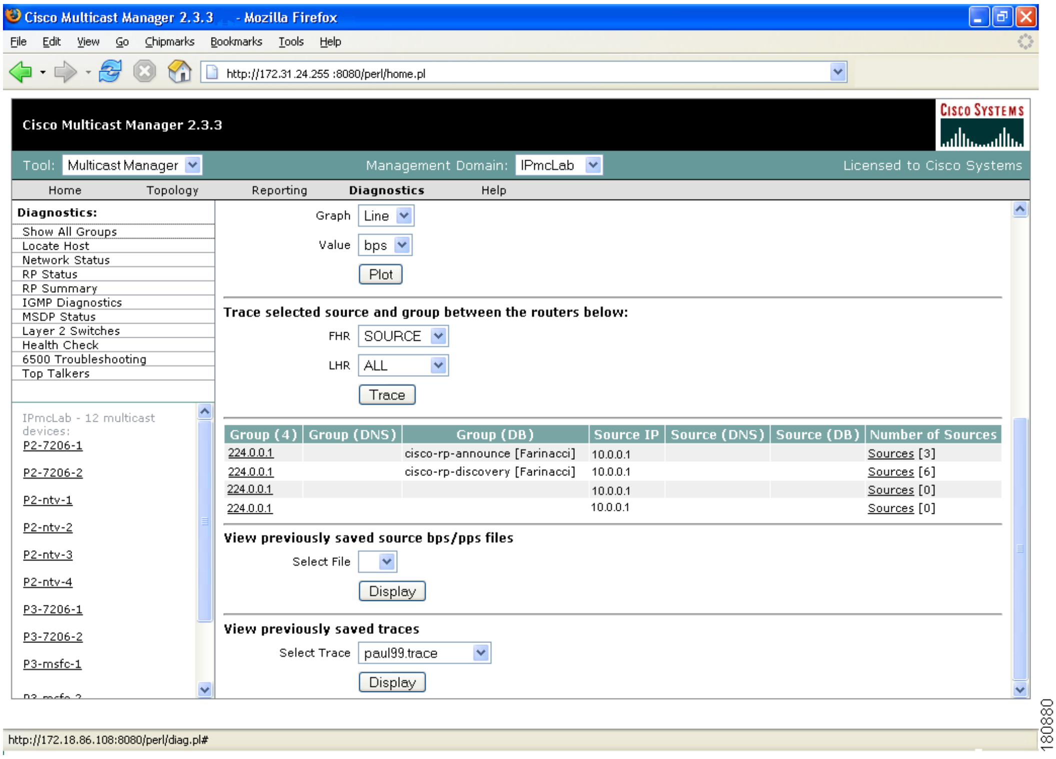
ipMRouteEntry Query for P2-ntv-1 (10.0.0.1) (10.0.0.1, 234.0.0.2)

Shortest Path Tree:True

MIB	Value	Description
ipMRouteDifferentInIfPackets	347275	Number of packets dropped because they were received on the wrong interface
ipMRouteExpiryTime	0:02:57	Time left before entry will be aged out
ipMRouteInIfIndex	Loopback1	Incoming Interface
ipMRouteOctets	0	Number of octets received from/to this source/group AND forwarded
ipMRoutePkts	0	Number of packets received from/to this source/group
ipMRouteProtocol	9	other(1), local(2), netmgmt(3), dvmrp(4), mospf(5), pimSparseDense(6), cbt(7), pimSparseMode(8), pimDenseMode(9), igmpOnly(10)
ipMRouteRtAddress	11.51.70.1	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	36 days, 9:38:13	Time since this entry was learned
ipMRouteUpstreamNeighbor	(0.0.0.0)	Upstream Neighbor

- (Optional) Clicking on a router in the multicast tree opens another page that contains IP multicast routing information for the S,G that has been traced:
  - **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**
  - **Value**
  - **Description**

Figure 1-48 Multicast Diagnostics


Cisco Multicast Manager 2.3.3 - Mozilla Firefox
File Edit View Go Chipmarks Bookmarks Tools Help
http://172.31.24.255 :8080/perl/home.pl
Cisco Multicast Manager 2.3.3
Cisco Systems
Licensed to Cisco Systems
Home Topology Reporting Diagnostics Help
Diagnostics:
Show All Groups
Locate Host
Network Status
RP Status
RP Summary
IGMP Diagnostics
MSDP Status
Layer 2 Switches
Health Check
6500 Troubleshooting
Top Talkers
IPmcLab - 12 multicast devices:
P2-7206-1
P2-7206-2
P2-ntv-1
P2-ntv-2
P2-ntv-3
P2-ntv-4
P3-7206-1
P3-7206-2
P3-msfc-1
Plot
Trace
Display
Display
http://172.18.86.108:8080/perl/diag.pl#
180880

Tool: Multicast Manager

Management Domain: IPmcLab

Graph: Line

Value: bps

Trace selected source and group between the routers below:

FHR: SOURCE

LHR: ALL

Group (4)	Group (DNS)	Group (DB)	Source IP	Source (DNS)	Source (DB)	Number of Sources
224.0.0.1		cisco-rp-announce [Farinacci]	10.0.0.1			Sources [3]
224.0.0.1		cisco-rp-discovery [Farinacci]	10.0.0.1			Sources [6]
224.0.0.1			10.0.0.1			Sources [0]
224.0.0.1			10.0.0.1			Sources [0]

View previously saved source bps/pps files

Select File:

View previously saved traces

Select Trace: paul99.trace

- **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.

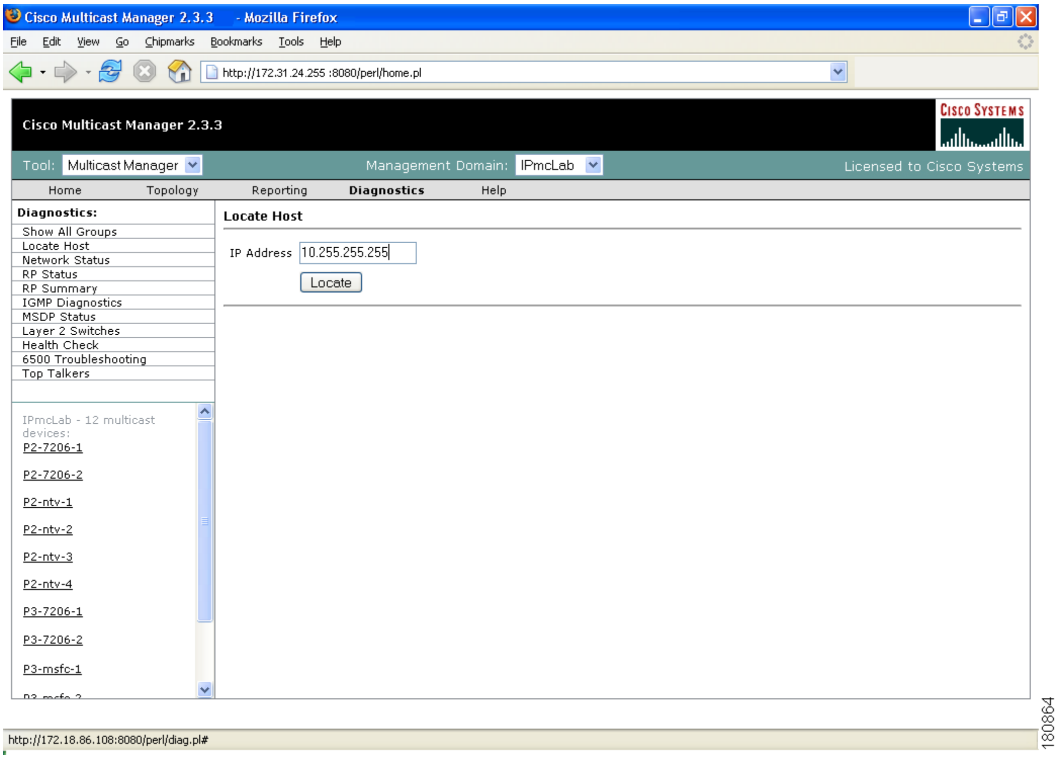
Note The Source (DNS) field is populated only if DNS is configured, and if **Resolve Sources** is selected on the Device Configuration page. It should be noted that resolving thousands of addresses via DNS can be extremely slow.

- **Source (DB)—**Name given to this source in the address database.
- **Number of Sources—**Number of sources in this group.
- To view previously saved source bps/pps files, select the file, and click **Display**.
- To view previously saved traces, select the trace, and click **Display**.t5rrrrrrrrrrrrrrru7

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 1-49 Locate Host



Tool: Multicast Manager
Management Domain: IPmcLab
Licensed to Cisco Systems

Diagnostics:

IPmcLab - 12 multicast devices:

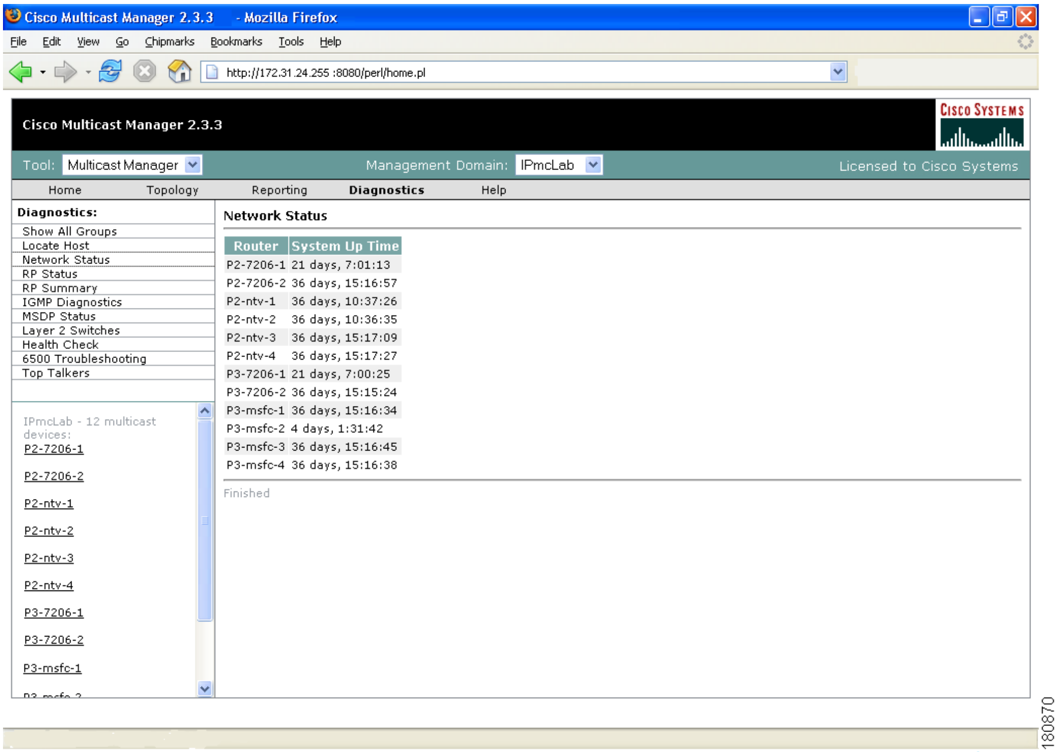
Locate Host

IP Address 10.255.255.255

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 1-50 Network Status


Cisco Multicast Manager 2.3.3 - Mozilla Firefox
File Edit View Go Chipmarks Bookmarks Tools Help
http://172.31.24.255 :8080/perl/home.pl
Cisco Multicast Manager 2.3.3
Cisco Systems
Tool: Multicast Manager
Management Domain: IPmcLab
Licensed to Cisco Systems
Home Topology Reporting Diagnostics Help
Diagnostics:
Show All Groups
Locate Host
Network Status
RP Status
RP Summary
IGMP Diagnostics
MSDP Status
Layer 2 Switches
Health Check
6500 Troubleshooting
Top Talkers
IPmcLab - 12 multicast devices:
P2-7206-1
P2-7206-2
P2-ntv-1
P2-ntv-2
P2-ntv-3
P2-ntv-4
P3-7206-1
P3-7206-2
P3-msfc-1
P3-msfc-2
180870

Network Status

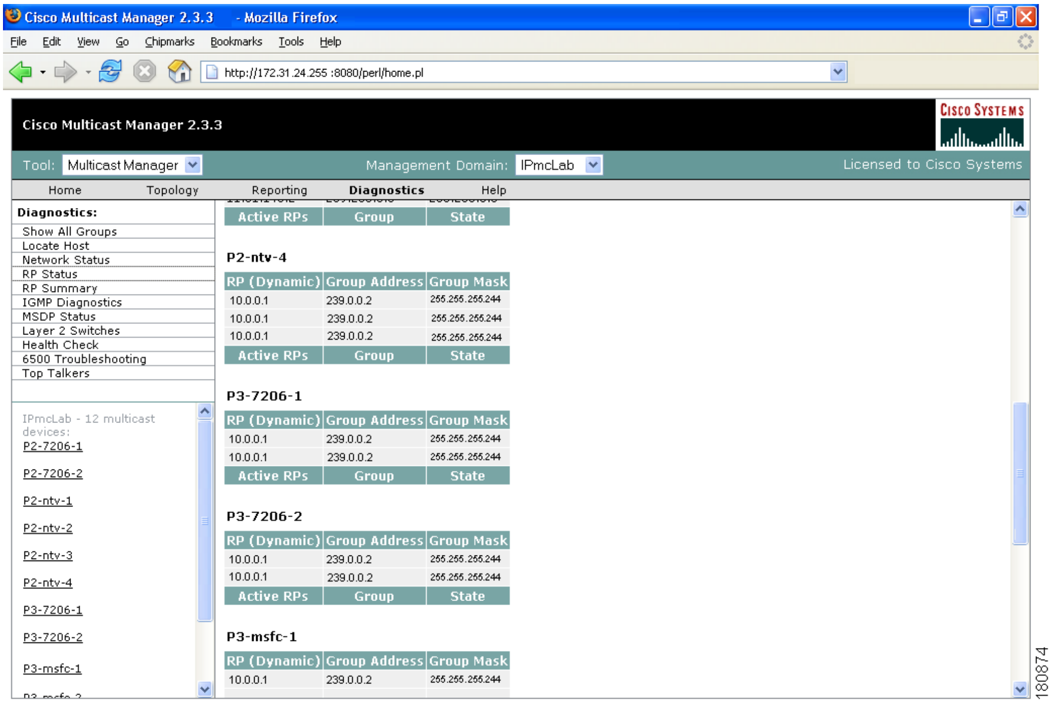
Router	System Up Time
P2-7206-1	21 days, 7:01:13
P2-7206-2	36 days, 15:16:57
P2-ntv-1	36 days, 10:37:26
P2-ntv-2	36 days, 10:36:35
P2-ntv-3	36 days, 15:17:09
P2-ntv-4	36 days, 15:17:27
P3-7206-1	21 days, 7:00:25
P3-7206-2	36 days, 15:15:24
P3-msfc-1	36 days, 15:16:34
P3-msfc-2	4 days, 1:31:42
P3-msfc-3	36 days, 15:16:45
P3-msfc-4	36 days, 15:16:38

Finished

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, since each router in the multicast domain is queried.

Figure 1-51 RP Status



Active RPs	Group	State

P2-ntv-4

RP (Dynamic)	Group Address	Group Mask
10.0.0.1	239.0.0.2	255.255.255.244
10.0.0.1	239.0.0.2	255.255.255.244
10.0.0.1	239.0.0.2	255.255.255.244

Active RPs	Group	State

P3-7206-1

RP (Dynamic)	Group Address	Group Mask
10.0.0.1	239.0.0.2	255.255.255.244
10.0.0.1	239.0.0.2	255.255.255.244

Active RPs	Group	State

P3-7206-2

RP (Dynamic)	Group Address	Group Mask
10.0.0.1	239.0.0.2	255.255.255.244
10.0.0.1	239.0.0.2	255.255.255.244

Active RPs	Group	State

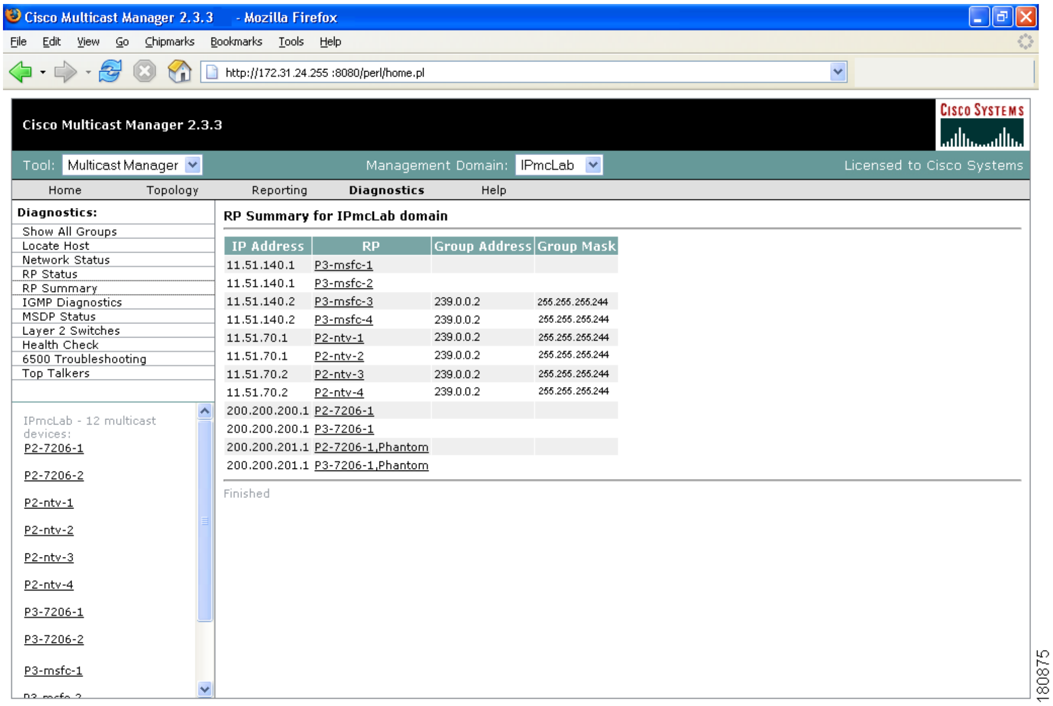
P3-msfc-1

RP (Dynamic)	Group Address	Group Mask
10.0.0.1	239.0.0.2	255.255.255.244

RP Summary

Using the RP Summary, you can view all the RPs that the CMM is aware of, based upon the discovery.

Figure 1-52 RP Summary


Cisco Multicast Manager 2.3.3 - Mozilla Firefox
File Edit View Go Chipmarks Bookmarks Tools Help
http://172.31.24.255 :8080/perl/home.pl
Cisco Multicast Manager 2.3.3
Cisco Systems
Tool: Multicast Manager
Management Domain: IPmcLab
Licensed to Cisco Systems
Home Topology Reporting Diagnostics Help
Diagnostics:
Show All Groups
Locate Host
Network Status
RP Status
RP Summary
IGMP Diagnostics
MSDP Status
Layer 2 Switches
Health Check
6500 Troubleshooting
Top Talkers
IPmcLab - 12 multicast devices:
P2-7206-1
P2-7206-2
P2-ntv-1
P2-ntv-2
P2-ntv-3
P2-ntv-4
P3-7206-1
P3-7206-2
P3-msfc-1
P3-msfc-2
180875

RP Summary for IPmcLab domain

IP Address	RP	Group Address	Group Mask
11.51.140.1	P3-msfc-1		
11.51.140.1	P3-msfc-2		
11.51.140.2	P3-msfc-3	239.0.0.2	255.255.255.244
11.51.140.2	P3-msfc-4	239.0.0.2	255.255.255.244
11.51.70.1	P2-ntv-1	239.0.0.2	255.255.255.244
11.51.70.1	P2-ntv-2	239.0.0.2	255.255.255.244
11.51.70.2	P2-ntv-3	239.0.0.2	255.255.255.244
11.51.70.2	P2-ntv-4	239.0.0.2	255.255.255.244
200.200.200.1	P2-7206-1		
200.200.200.1	P3-7206-1		
200.200.201.1	P2-7206-1,Phantom		
200.200.201.1	P3-7206-1,Phantom		

Finished

For details on clicking on an RP, see the "Topology" section on page 1-44.

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:

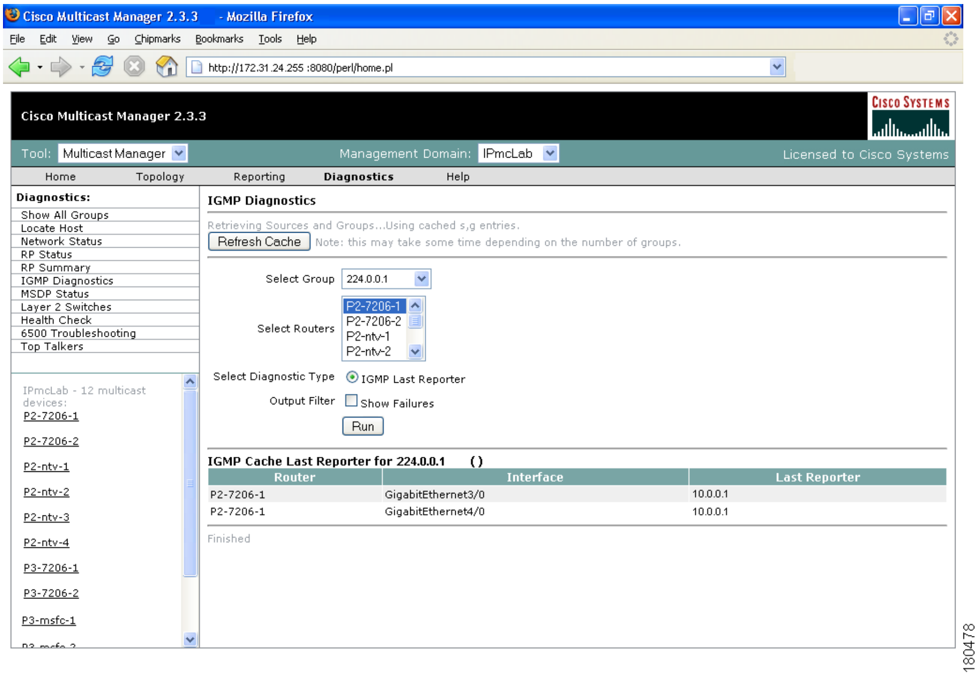
Step 1 Select the router(s) you want to query.

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

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

Step 4 Click **Run**.

Figure 1-53 IGMP Diagnostics


Cisco Multicast Manager 2.3.3 - Mozilla Firefox
File Edit View Go Chipmarks Bookmarks Tools Help
http://172.31.24.255 :8080/perl/home.pl
Cisco Multicast Manager 2.3.3
Cisco Systems
Tool: Multicast Manager
Management Domain: IPmcLab
Licensed to Cisco Systems
Home Topology Reporting Diagnostics Help
Diagnostics:
Show All Groups
Locate Host
Network Status
RP Status
RP Summary
IGMP Diagnostics
MSDP Status
Layer 2 Switches
Health Check
6500 Troubleshooting
Top Talkers
IPmcLab - 12 multicast devices:
P2-7206-1
P2-7206-2
P2-ntv-1
P2-ntv-2
P2-ntv-3
P2-ntv-4
P3-7206-1
P3-7206-2
P3-msfc-1
IGMP Diagnostics
Refresh Cache
Select Group 224.0.0.1
Select Routers P2-7206-1 P2-7206-2 P2-ntv-1 P2-ntv-2
Select Diagnostic Type ● IGMP Last Reporter
Output Filter □ Show Failures
Run
180478

Retrieving Sources and Groups...Using cached s,g entries.

Note: this may take some time depending on the number of groups.

IGMP Cache Last Reporter for 224.0.0.1 ( )

Router	Interface	Last Reporter
P2-7206-1	GigabitEthernet3/0	10.0.0.1
P2-7206-1	GigabitEthernet4/0	10.0.0.1

Finished

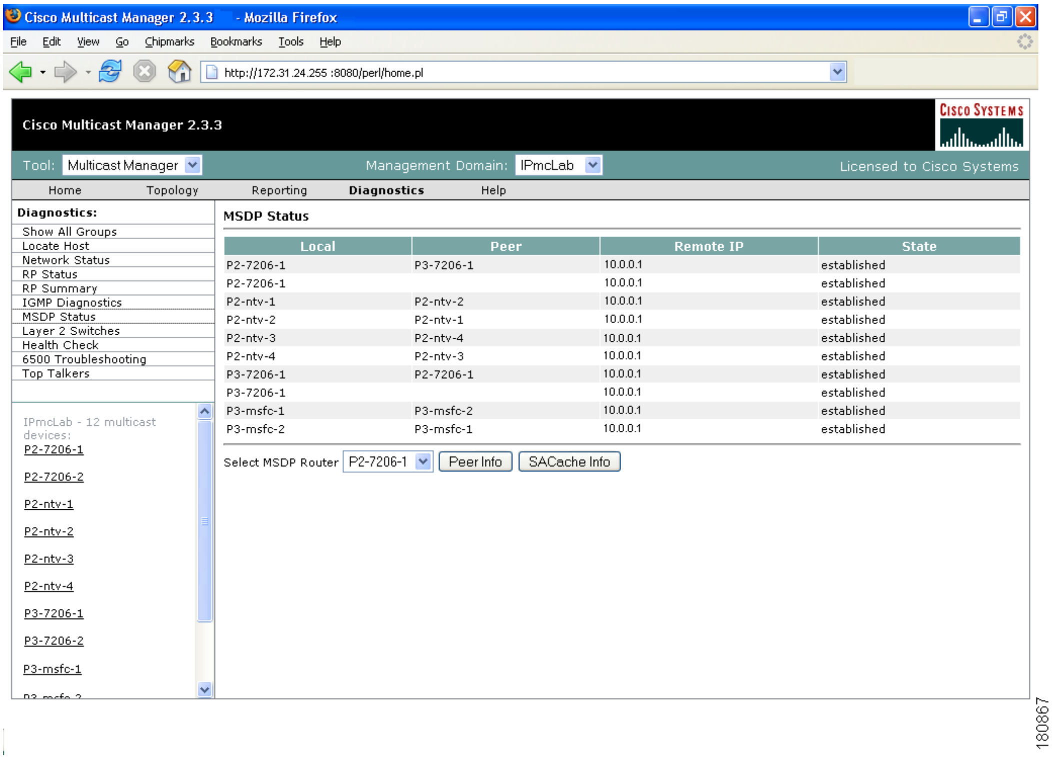
MSDP Status

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 only supported 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 1-54 MSDP Status



MSDP Status

Local	Peer	Remote IP	State
P2-7206-1	P3-7206-1	10.0.0.1	established
P2-7206-1		10.0.0.1	established
P2-ntv-1	P2-ntv-2	10.0.0.1	established
P2-ntv-2	P2-ntv-1	10.0.0.1	established
P2-ntv-3	P2-ntv-4	10.0.0.1	established
P2-ntv-4	P2-ntv-3	10.0.0.1	established
P3-7206-1	P2-7206-1	10.0.0.1	established
P3-7206-1		10.0.0.1	established
P3-msfc-1	P3-msfc-2	10.0.0.1	established
P3-msfc-2	P3-msfc-1	10.0.0.1	established

Select MSDP Router: P2-7206-1

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.

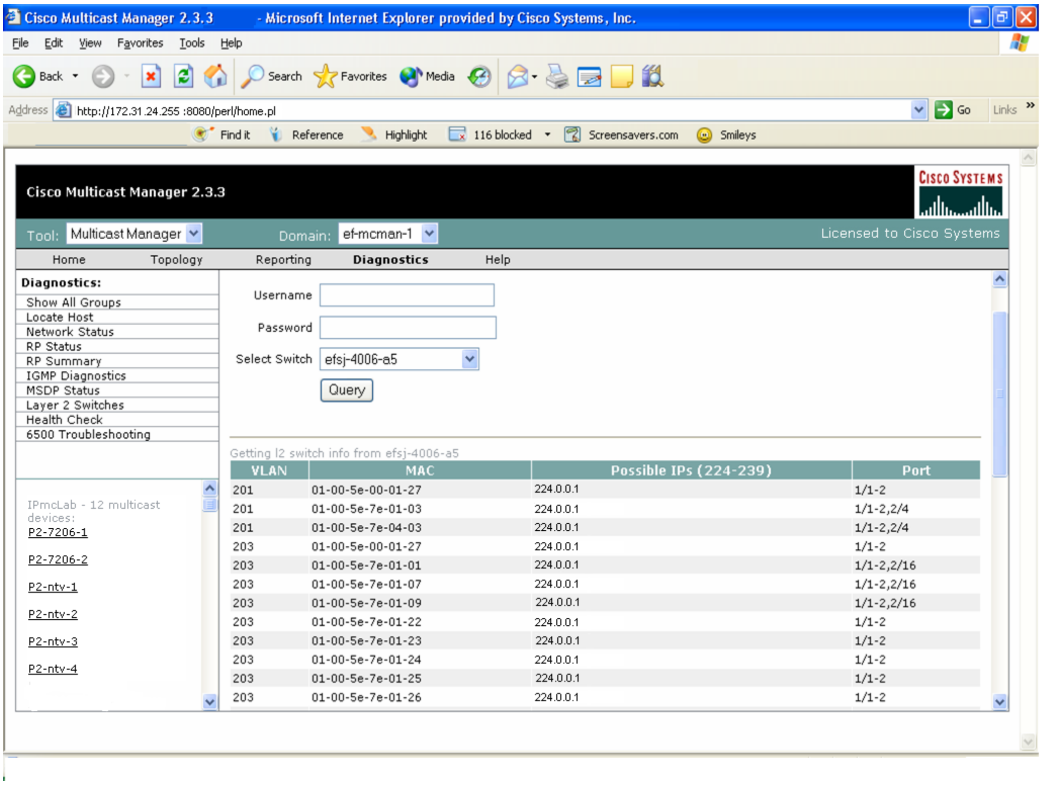
Step 2 Enter your password.

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

Step 4 Click **Query**.

The possible IP addresses which can be mapped to the MAC address are also shown.

Figure 1-55   Layer 2 Multicast Information


Cisco Multicast Manager 2.3.3 - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://172.31.24.255 :8080/perl/home.pl
Go Links
Find it Reference Highlight 116 blocked Screensavers.com Smileys
Cisco Multicast Manager 2.3.3
Cisco Systems
Tool: Multicast Manager
Domain: ef-mcman-1
Licensed to Cisco Systems
Home Topology Reporting Diagnostics Help
Diagnostics:
Show All Groups
Locate Host
Network Status
RP Status
RP Summary
IGMP Diagnostics
MSDP Status
Layer 2 Switches
Health Check
6500 Troubleshooting
IPmcLab - 12 multicast devices:
P2-7206-1
P2-7206-2
P2-ntv-1
P2-ntv-2
P2-ntv-3
P2-ntv-4
Query
180861

Username

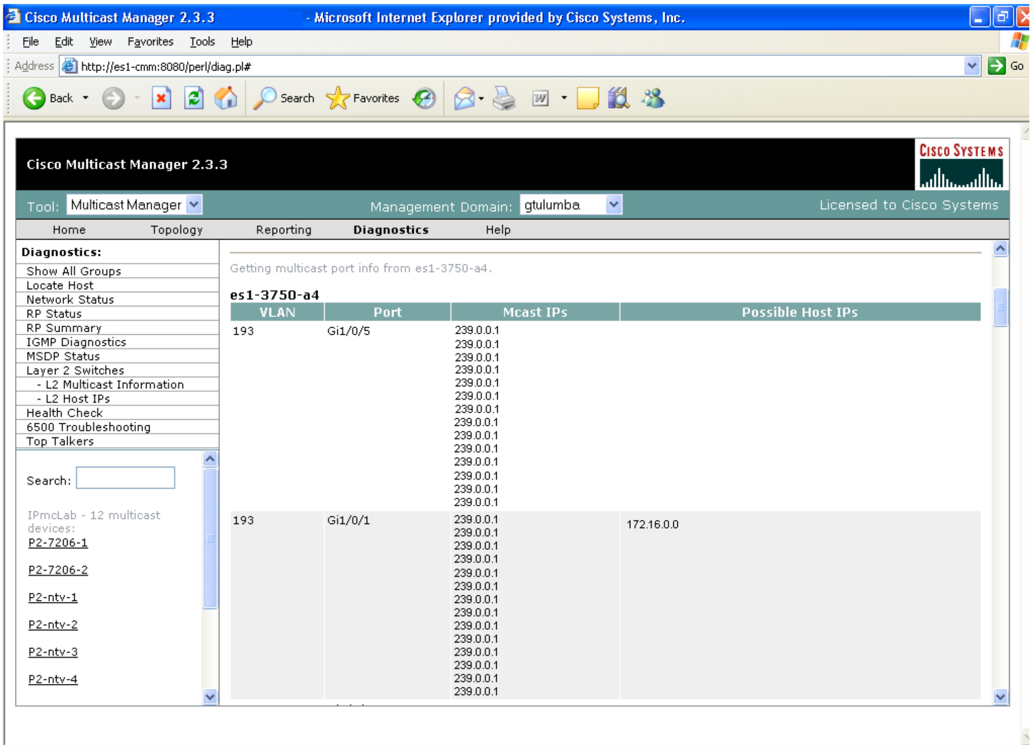
Password

Select Switch efsj-4006-a5

Getting l2 switch info from efsj-4006-a5

VLAN	MAC	Possible IPs (224-239)	Port
201	01-00-5e-00-01-27	224.0.0.1	1/1-2
201	01-00-5e-7e-01-03	224.0.0.1	1/1-2,2/4
201	01-00-5e-7e-04-03	224.0.0.1	1/1-2,2/4
203	01-00-5e-00-01-27	224.0.0.1	1/1-2
203	01-00-5e-7e-01-01	224.0.0.1	1/1-2,2/16
203	01-00-5e-7e-01-07	224.0.0.1	1/1-2,2/16
203	01-00-5e-7e-01-09	224.0.0.1	1/1-2,2/16
203	01-00-5e-7e-01-22	224.0.0.1	1/1-2
203	01-00-5e-7e-01-23	224.0.0.1	1/1-2
203	01-00-5e-7e-01-24	224.0.0.1	1/1-2
203	01-00-5e-7e-01-25	224.0.0.1	1/1-2
203	01-00-5e-7e-01-26	224.0.0.1	1/1-2

Figure 1-56   Layer 2 Host IPs


Cisco Multicast Manager 2.3.3 - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Address http://es1-cmm:8080/perl/diag.pl#
Go
Back Search Favorites
Cisco Multicast Manager 2.3.3
Cisco Systems
Tool: Multicast Manager
Management Domain: gtulumba
Licensed to Cisco Systems
Home Topology Reporting Diagnostics Help
Diagnostics:
Show All Groups
Locate Host
Network Status
RP Status
RP Summary
IGMP Diagnostics
MSDP Status
Layer 2 Switches
- L2 Multicast Information
- L2 Host IPs
Health Check
6500 Troubleshooting
Top Talkers
Search:
IPmcLab - 12 multicast devices:
P2-7206-1
P2-7206-2
P2-ntv-1
P2-ntv-2
P2-ntv-3
P2-ntv-4
180862

Getting multicast port info from es1-3750-a4.

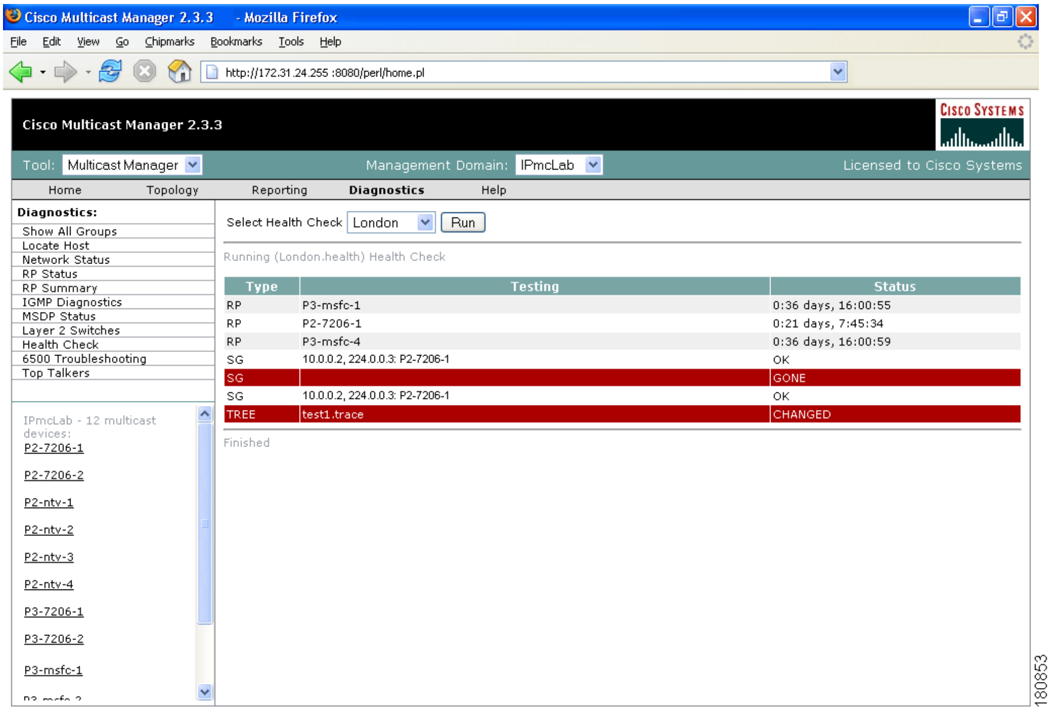
es1-3750-a4

VLAN	Port	Mcast IPs	Possible Host IPs
193	Gi1/0/5	239.0.0.1 239.0.0.1 239.0.0.1 239.0.0.1 239.0.0.1 239.0.0.1 239.0.0.1 239.0.0.1 239.0.0.1 239.0.0.1 239.0.0.1 239.0.0.1 239.0.0.1 239.0.0.1	
193	Gi1/0/1	239.0.0.1 239.0.0.1 239.0.0.1 239.0.0.1 239.0.0.1 239.0.0.1 239.0.0.1 239.0.0.1 239.0.0.1 239.0.0.1 239.0.0.1 239.0.0.1 239.0.0.1 239.0.0.1	172.16.0.0

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 drop-down box, and click **Run**.

Figure 1-57 Health Check



Select Health Check London

Running (London.health) Health Check

Type	Testing	Status
RP	P3-msfc-1	0:36 days, 16:00:55
RP	P2-7206-1	0:21 days, 7:45:34
RP	P3-msfc-4	0:36 days, 16:00:59
SG	10.0.0.2, 224.0.0.3: P2-7206-1	OK
SG		GONE
SG	10.0.0.2, 224.0.0.3: P2-7206-1	OK
TREE	test1.trace	CHANGED

Finished

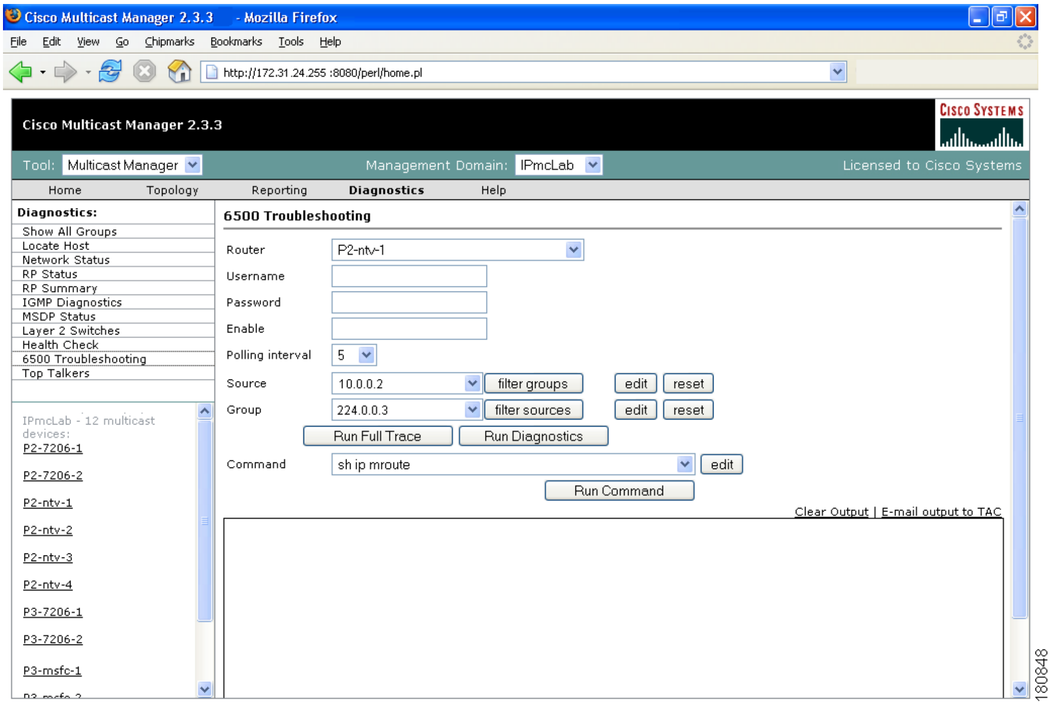
- Gray = normal
- White = normal
- Red = error condition

6500 Troubleshooting

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

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

Figure 1-58 6500 Troubleshooting



Cisco Multicast Manager 2.3.3 - Mozilla Firefox

http://172.31.24.255 :8080/perl/home.pl

Cisco Multicast Manager 2.3.3

Tool: Multicast Manager

Management Domain: IPmcLab

Licensed to Cisco Systems

6500 Troubleshooting

Router: P2-ntv-1

Username:

Password:

Enable:

Polling interval: 5

Source: 10.0.0.2

Group: 224.0.0.3

Command: sh ip mroute

IPmcLab - 12 multicast devices:

The 6500 Troubleshooting page contains:

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	Re-populates the source and group lists.
Run Full Trace	Starts the tree at the source instead of the selected router. For details, see the "Show All Groups" section on page 1-61.

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 on any other router in the picture to see live packets statistics for them (see the "Show All Groups" section on page 1-61). Ensure pop-up blockers are disabled.
Command	Provides a drop-down list of show commands.
Edit	Add your own command by clicking on **Edit**, typing in your command, and 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 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.

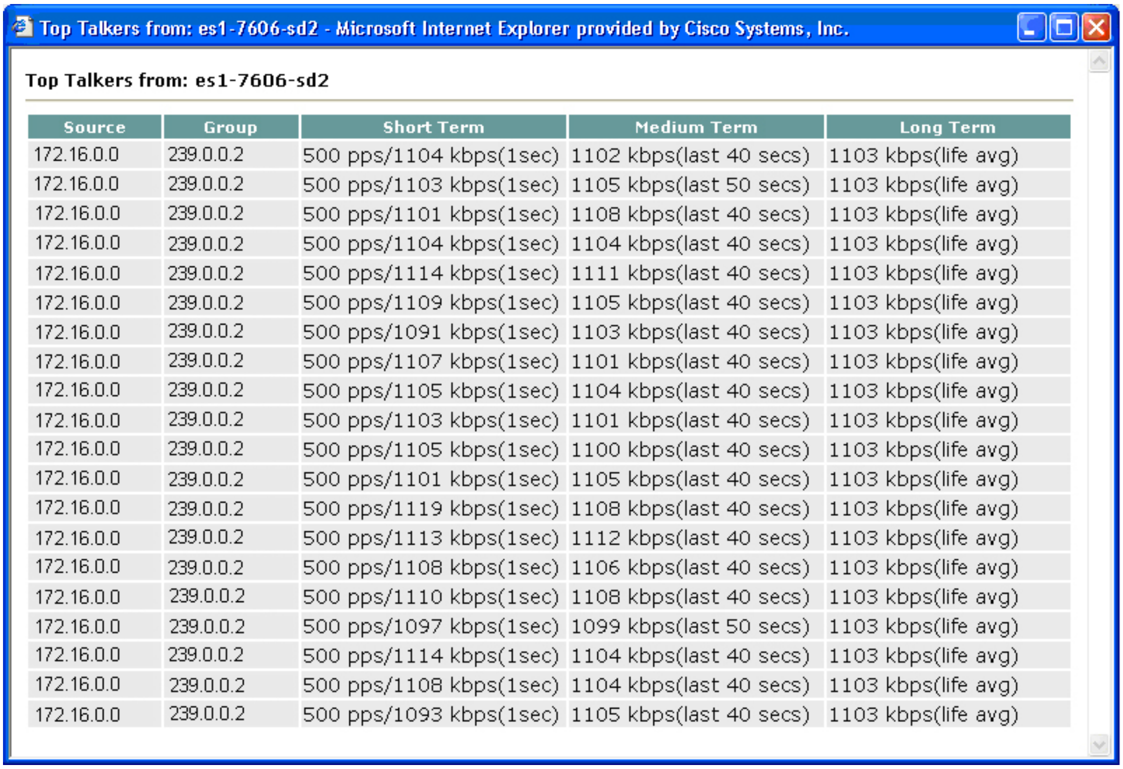
Step 1 Select a router to monitor.

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 1-59 Top Talkers


Top Talkers from: es1-7606-sd2 - Microsoft Internet Explorer provided by Cisco Systems, Inc.

Top Talkers from: es1-7606-sd2

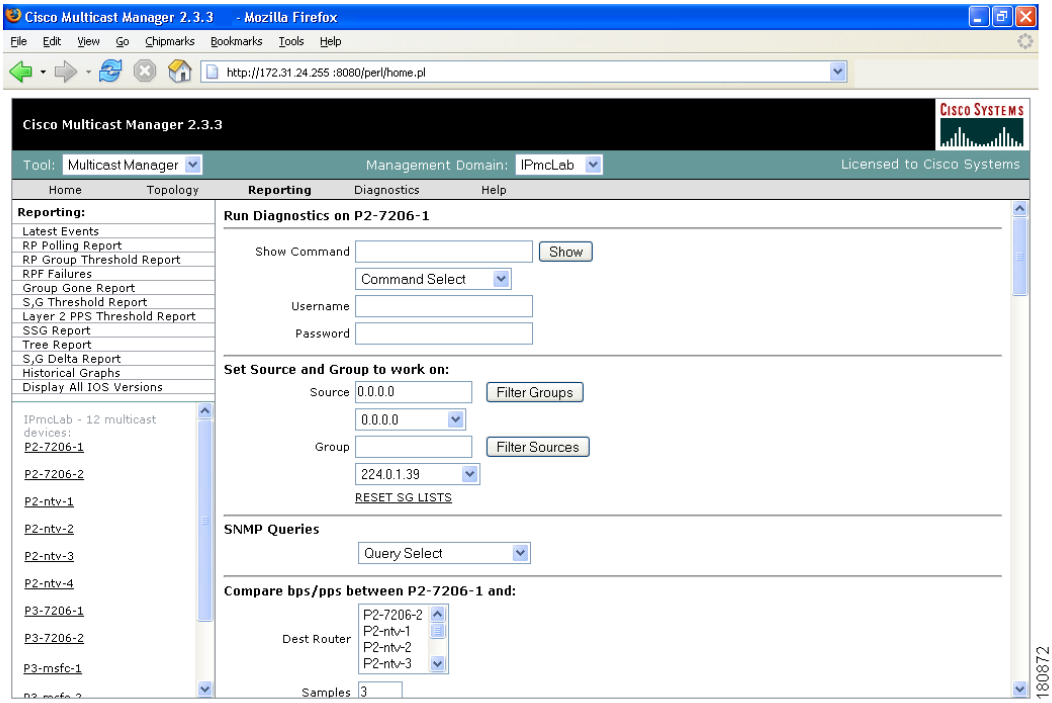
Source	Group	Short Term	Medium Term	Long Term
172.16.0.0	239.0.0.2	500 pps/1104 kbps(1sec)	1102 kbps(last 40 secs)	1103 kbps(life avg)
172.16.0.0	239.0.0.2	500 pps/1103 kbps(1sec)	1105 kbps(last 50 secs)	1103 kbps(life avg)
172.16.0.0	239.0.0.2	500 pps/1101 kbps(1sec)	1108 kbps(last 40 secs)	1103 kbps(life 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)

180484

Router Diagnostics

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

Figure 1-60 Router Diagnostics



Cisco Multicast Manager 2.3.3 - Mozilla Firefox
File Edit View Go Chipmarks Bookmarks Tools Help
http://172.31.24.255 :8080/perl/home.pl
Cisco Multicast Manager 2.3.3
Cisco Systems
Home Topology Reporting Diagnostics Help
Show
Filter Groups
Filter Sources
RESET SG LISTS
180872

Tool: Multicast Manager

Management Domain: IPmcLab

Licensed to Cisco Systems

Reporting:

- Latest Events
- RP Polling Report
- RP Group Threshold Report
- RPF Failures
- Group Gone Report
- S,G Threshold Report
- Layer 2 PPS Threshold Report
- SSG Report
- Tree Report
- S,G Delta Report
- Historical Graphs
- Display All IOS Versions

IPmcLab - 12 multicast devices:

- P2-7206-1
- P2-7206-2
- P2-ntv-1
- P2-ntv-2
- P2-ntv-3
- P2-ntv-4
- P3-7206-1
- P3-7206-2
- P3-msfc-1
- P3-msfc-2

Run Diagnostics on P2-7206-1

Show Command

Command Select

Username

Password

Set Source and Group to work on:

Source 0.0.0.0

0.0.0.0

Group

224.0.1.39

SNMP Queries

Query Select

Compare bps/pps between P2-7206-1 and:

Dest Router P2-7206-2
P2-ntv-1
P2-ntv-2
P2-ntv-3

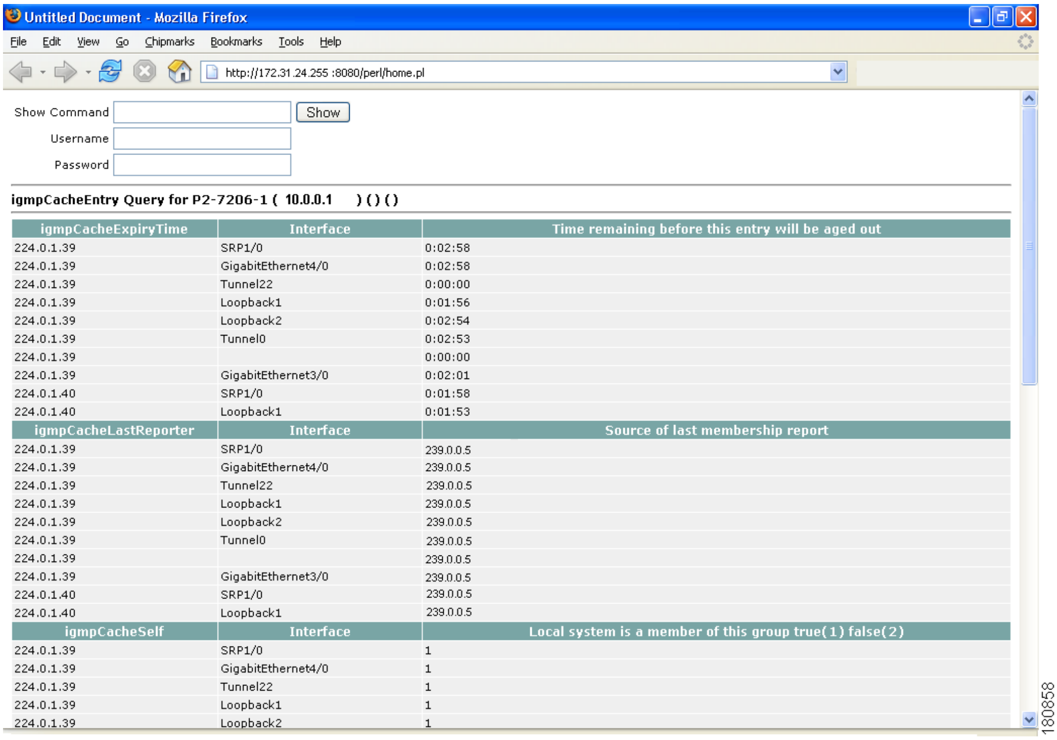
Samples 3

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

The following functions are not found on the Multicast Diagnostics page:

- 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 1-61 IGMP Cache Entries

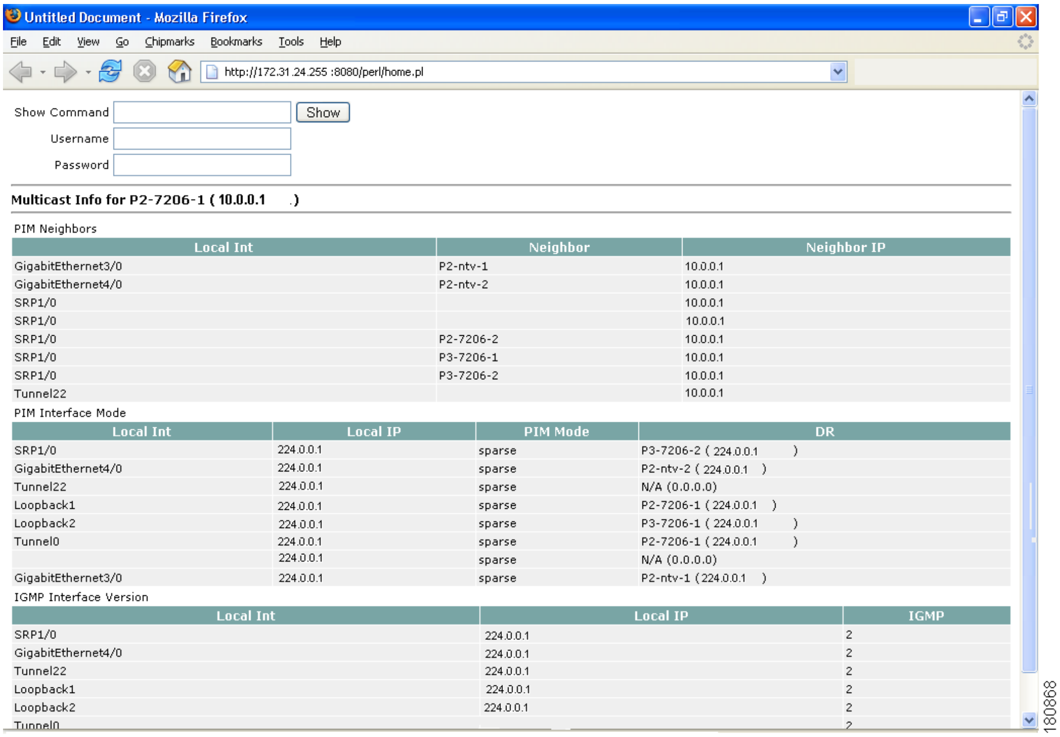

Untitled Document - Mozilla Firefox
File Edit View Go Chipmarks Bookmarks Tools Help
http://172.31.24.255 :8080/perl/home.pl
Show Command
Show
Username
Password
180858

igmpCacheEntry Query for P2-7206-1 (10.0.0.1) () ()

igmpCacheExpiryTime	Interface	Time remaining before this entry will be aged out
224.0.1.39	SRP1/0	0:02:58
224.0.1.39	GigabitEthernet4/0	0:02:58
224.0.1.39	Tunnel22	0:00:00
224.0.1.39	Loopback1	0:01:56
224.0.1.39	Loopback2	0:02:54
224.0.1.39	Tunnel0	0:02:53
224.0.1.39		0:00:00
224.0.1.39	GigabitEthernet3/0	0:02:01
224.0.1.40	SRP1/0	0:01:58
224.0.1.40	Loopback1	0:01:53
igmpCacheLastReporter	**Interface**	**Source of last membership report**
224.0.1.39	SRP1/0	239.0.0.5
224.0.1.39	GigabitEthernet4/0	239.0.0.5
224.0.1.39	Tunnel22	239.0.0.5
224.0.1.39	Loopback1	239.0.0.5
224.0.1.39	Loopback2	239.0.0.5
224.0.1.39	Tunnel0	239.0.0.5
224.0.1.39		239.0.0.5
224.0.1.39	GigabitEthernet3/0	239.0.0.5
224.0.1.40	SRP1/0	239.0.0.5
224.0.1.40	Loopback1	239.0.0.5
igmpCacheSelf	**Interface**	**Local system is a member of this group true(1) false(2)**
224.0.1.39	SRP1/0	1
224.0.1.39	GigabitEthernet4/0	1
224.0.1.39	Tunnel22	1
224.0.1.39	Loopback1	1
224.0.1.39	Loopback2	1

- **Multicast Information**—Shows multicast topology information.

Figure 1-62 Multicast Information


Untitled Document - Mozilla Firefox
File Edit View Go Chipmarks Bookmarks Tools Help
http://172.31.24.255 :8080/perl/home.pl
Show Command
Show
Username
Password
180868

Multicast Info for P2-7206-1 (10.0.0.1)

PIM Neighbors

Local Int	Neighbor	Neighbor IP
GigabitEthernet3/0	P2-ntv-1	10.0.0.1
GigabitEthernet4/0	P2-ntv-2	10.0.0.1
SRP1/0		10.0.0.1
SRP1/0		10.0.0.1
SRP1/0	P2-7206-2	10.0.0.1
SRP1/0	P3-7206-1	10.0.0.1
SRP1/0	P3-7206-2	10.0.0.1
Tunnel22		10.0.0.1

PIM Interface Mode

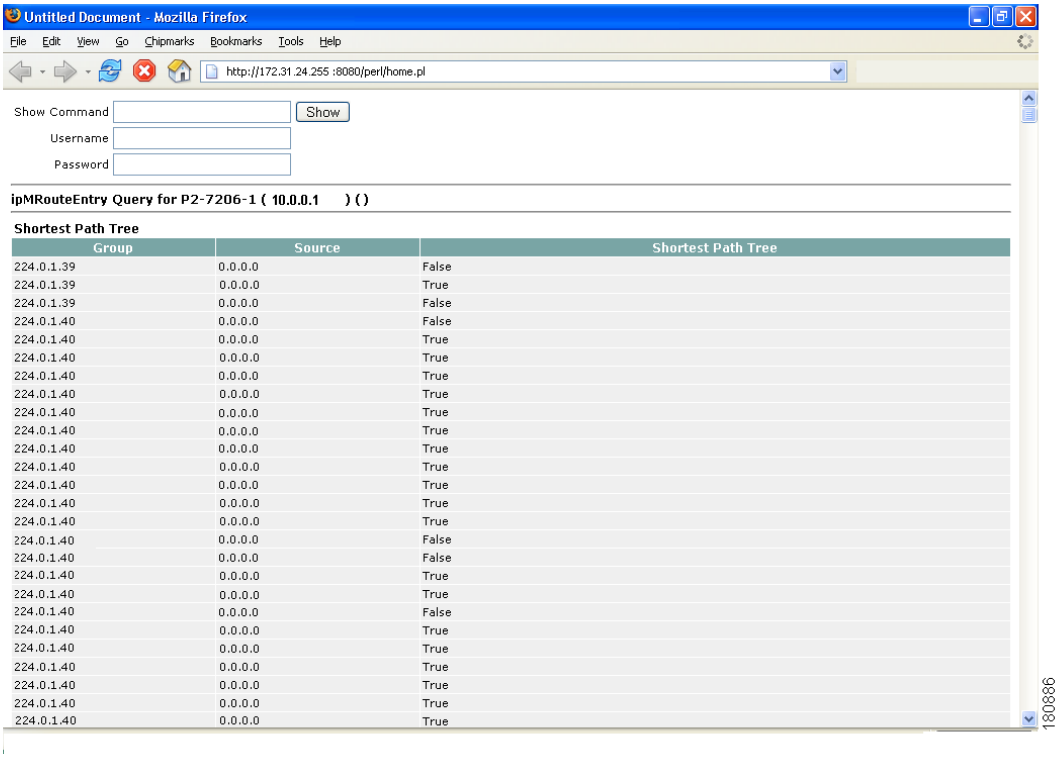
Local Int	Local IP	PIM Mode	DR
SRP1/0	224.0.0.1	sparse	P3-7206-2 (224.0.0.1)
GigabitEthernet4/0	224.0.0.1	sparse	P2-ntv-2 (224.0.0.1)
Tunnel22	224.0.0.1	sparse	N/A (0.0.0.0)
Loopback1	224.0.0.1	sparse	P2-7206-1 (224.0.0.1)
Loopback2	224.0.0.1	sparse	P3-7206-1 (224.0.0.1)
Tunnel0	224.0.0.1	sparse	P2-7206-1 (224.0.0.1)
	224.0.0.1	sparse	N/A (0.0.0.0)
GigabitEthernet3/0	224.0.0.1	sparse	P2-ntv-1 (224.0.0.1)

IGMP Interface Version

Local Int	Local IP	IGMP
SRP1/0	224.0.0.1	2
GigabitEthernet4/0	224.0.0.1	2
Tunnel22	224.0.0.1	2
Loopback1	224.0.0.1	2
Loopback2	224.0.0.1	2
Tunnel0		2

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

Figure 1-63 Multicast Routing Table



ipMRouteEntry Query for P2-7206-1 (10.0.0.1) ()

Shortest Path Tree

Group	Source	Shortest Path Tree
224.0.1.39	0.0.0.0	False
224.0.1.39	0.0.0.0	True
224.0.1.39	0.0.0.0	False
224.0.1.40	0.0.0.0	False
224.0.1.40	0.0.0.0	True
224.0.1.40	0.0.0.0	True
224.0.1.40	0.0.0.0	True
224.0.1.40	0.0.0.0	True
224.0.1.40	0.0.0.0	True
224.0.1.40	0.0.0.0	True
224.0.1.40	0.0.0.0	True
224.0.1.40	0.0.0.0	True
224.0.1.40	0.0.0.0	True
224.0.1.40	0.0.0.0	True
224.0.1.40	0.0.0.0	True
224.0.1.40	0.0.0.0	False
224.0.1.40	0.0.0.0	False
224.0.1.40	0.0.0.0	True
224.0.1.40	0.0.0.0	True
224.0.1.40	0.0.0.0	False
224.0.1.40	0.0.0.0	True
224.0.1.40	0.0.0.0	True
224.0.1.40	0.0.0.0	True
224.0.1.40	0.0.0.0	True
224.0.1.40	0.0.0.0	True
224.0.1.40	0.0.0.0	True

Help

You can view the Cisco Multicast Manager 2.3.3 User Guide PDF by clicking on **Help**.

Application Maintenance and Troubleshooting

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

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 only be modified through the browser interface. The only time these files should be modified manually is with the assistance of RMS tech support.

Log Files

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

events.log

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.

rmspolld.log

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
```

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 will generate a large amount of data and should only be used for short periods in conjunction with working RMS tech support.

Databases

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 db 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.

Device Configurations

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.

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.

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*
```

Backups

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 will stop 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