



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.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)

User Guide for the Cisco Multicast Manager 2.3.3 ©2006 Cisco Systems, Inc. All rights reserved.



Preface 5

	Obtaining Documentation 5
	Cisco.com 5
	Documentation DVD 5
	Ordering Documentation 6
	Documentation Feedback 6
	Cisco Product Security Overview 6
	Reporting Security Problems in Cisco Products 7
	Obtaining Technical Assistance 7
	Cisco Technical Support Website 7
	Submitting a Service Request 8
	Definitions of Service Request Severity 8
	Obtaining Additional Publications and Information 9
CHAPTER 1	Using the Cisco Multicast Manager 1-1
	System Requirements 1-1
	Solaris Installation Instructions 1-2
	Linux Installation Instructions 1-4
	Licensing 1-6
	Starting and Stopping CMM 1-6
	Logging Into CMM 1-6
	Using the Administration Tool 1-8
	Domain Management 1-9
	Discovery 1-11
	Admin Utilities 1-15
	System Security 1-17
	User Management 1-18
	Device Configuration 1-20
	Global Polling Configuration 1-23
	Address Management 1-27
	Multicast Manager 1-28
	Using the Multicast Manager Tool 1-43
	Home 1-44
	Topology 1-44 Ciaco Systems Inc. 170 West Teamon Drive San Jaco CA 95134 1706 USA
.սհսհ.	Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA



Reporting 1-48 Diagnostics 1-60 Router Diagnostics 1-77 Help 1-79 Application Maintenance and Troubleshooting 1-80 Configuration Files 1-80 Log Files 1-80 Databases 1-81 Device Configurations 1-81 Historical Data 1-81 Standard Multicast MIBs 1-81 Backups 1-82 L



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/



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

© 2006 Cisco Systems, Inc. All rights reserved.

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



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

10

I



Using the Cisco Multicast Manager

This chapter covers:

- System Requirements, page 1-1
- Solaris Installation Instructions, page 1-2
- Linux Installation Instructions, page 1-4
- Licensing, page 1-6
- Starting and Stopping CMM, page 1-6
- Logging Into CMM, page 1-6
- Using the Administration Tool, page 1-8
- Using the Multicast Manager Tool, page 1-43
- Application Maintenance and Troubleshooting, page 1-80

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



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



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.



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.



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.



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.

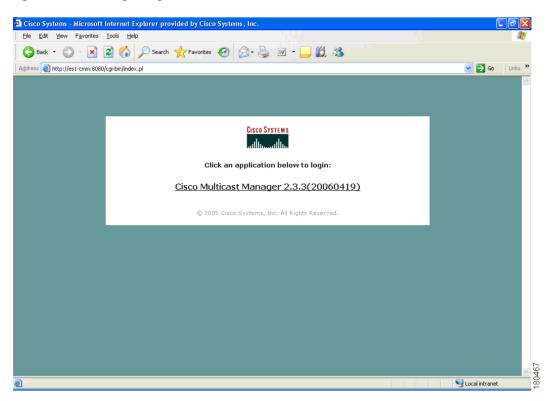


Figure 1-1 Login Page for CMM 2.3.3

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.

¢

Edit	t ⊻iew <u>G</u> o <u>C</u> hipmarks <u>B</u> ook	marks <u>T</u> ools <u>H</u> e	elp			
🛛 🕶 🋶 🥪 🛞 🚷 🗋 http://172.31.24.255 :8080/perl/home.pl			×			
						CISCO SYSTEMS
isco	Multicast Manager 2.3.3					
Tool: Multicast Manager V Management Domain: IPmcLab V			t Domain: IPmcLab 🔽	Licer	nsed to Cisco Systems	
Н	ome Topology	Reporting	Diagnostics	Help		
ates	t Events					
		Date		Туре	Device	Details
8	Wed Aug 9 23:15:03 2006			RP Timeout	P3-7206-1	
8	Wed Aug 9 23:15:03 2006			RP Timeout	P3-7206-1	
8	Wed Aug 9 23:00:02 2006			RP Timeout	P3-7206-1	
3	Wed Aug 9 23:00:02 2006			RP Timeout	P3-7206-1	
8	Wed Aug 9 22:45:02 2006			RP Timeout	P3-7206-1	
8	Wed Aug 9 22:45:02 2006			RP Timeout	P3-7206-1	
8	Wed Aug 9 22:30:03 2006			RP Timeout	P3-7206-1	
8	Wed Aug 9 22:30:03 2006			RP Timeout	P3-7206-1	
8	Wed Aug 9 22:15:02 2006			RP Timeout	P3-7206-1	
8	Wed Aug 9 22:15:02 2006			RP Timeout	P3-7206-1	
8	Wed Aug 9 22:00:03 2006			RP Timeout	P3-7206-1	
8	Wed Aug 9 22:00:03 2006			RP Timeout	P3-7206-1	
8	Wed Aug 9 21:45:02 2006			RP Timeout	P3-7206-1	
8	Wed Aug 9 21:45:02 2006			RP Timeout	P3-7206-1	
8	Wed Aug 9 21:30:03 2006			RP Timeout	P3-7206-1	
8	Wed Aug 9 21:30:03 2006			RP Timeout	P3-7206-1	
8	Wed Aug 9 21:15:02 2006			RP Timeout	P3-7206-1	
8	Wed Aug 9 21:15:02 2006			RP Timeout	P3-7206-1	
8	Wed Aug 9 21:00:03 2006			RP Timeout	P3-7206-1	
8	Wed Aug 9 21:00:03 2006			RP Timeout	P3-7206-1	
0	Wed Aug 9 20:45:02 2006			RP Timeout	P3-7206-1	
õ	Wed Aug 9 20:45:02 2006			PP Timeout	P3-7206-1	

rigure i-z multicast manager nome Pag	Figure 1-2	Multicast Manager Home Page
---------------------------------------	------------	-----------------------------

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.

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 PasswordThe VTY password is required if yo issue show commands from the app Certain features, such as querying I switches, also require this. If TACA used, then a username and password 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.	

The System Configuration page contains:

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.

e <u>E</u> dit ⊻iew <u>G</u> o ⊆hipmarks	Bookmarks Tools Help	
🕨 • 🧼 • 🍠 😣 🟠 [http://ftl-script1:8080/perl/sys/home.pl#	×
Cisco Tool Administration		CISCO SYSTEMS
Tool: Administration 💌	Management Domain: National-1 💌	Licensed to Cisco Systems
Configuration:	Multicast Layer 2 Switch Configuration	
Domain Management	Import From File	
Admin Utilities		
System Security	Browse Import	
Jser Management Discovery		
- Add Router	Name/IP Address	
- Add L2 Switch		
- Multicast	Community String Add	
Device Configuration	·	
Slobal Polling Configuration		
Address Management		
Multicast Manager		
Route Manager		
lational-1 - 0 multicast		
evices:		
Database currently locked		
y discovery, please wait		
ntil it completes.		
~		

Figure 1-3 Multicast Layer 2 Switch Configuration

- 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.

Cisco Tool Administration - Mic	crosoft Internet Explorer provided by Cisco Systems, Inc.	
<u>Eile E</u> dit <u>V</u> iew Favorites <u>T</u> ools	s Help	<u>_</u>
🌀 Back 🔹 🕥 - 💌 🛃 (🏠 🔎 Search 🤺 Favorites 🤣 😥 - 🌉 🕅 - 🛄 🏭 🦓	
Address 🕘 http://es1-cmm:8080/perl/sy	sys/home.pl# 🔍 🎅 🚱	Links 3
		10
Cisco Tool Administration	Cisco Sy Influence Management Domain: gtest2 S Licensed to Cisco Sys	մհո
Configurations		~
Configuration: Domain Management Admin Utilities	Multicast Discovery (Discovery is Not Running)	
System Security User Management Discovery	Discover Multicast Domain To discover the network enter the IP address of a seed router along with its read-only community string.	
- Add Router - Add L2 Switch - Multicast Device Configuration Global Polling Configuration	Management Domain gtest2 Seed Router 6500-Core-44	
Address Management Multicast Manager	Community Strings public Add actic8bb8 public The selected strings will be used during discovery public	5
gtest2 - 10 multicast devices: <u>es1-7206-w1</u>	Discovery Depth 1 Start Discovery	
es1-7206-w2		
es1-7606-c1 es1-7606-c2	Add/Rediscover a Single Device	- []
es1-7606-c3	To add a new device or rediscover an existing one, enter its ip address and read-only community string.	
es1-/606-04	Management Domain	
<u>es1-7606-d1</u>	Router	
es1-7606-d2		· •
		5
http://es1-cmm:8080/perl/sys/home.pl#	# 🧐 Local intrane	t

Figure 1-4 Multicast Discovery

- **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**.



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.

🕹 Cisco Tool Administration - N	ozilla Firefox		
Eile Edit View Go Chipmarks	Bookmarks Tools Help	0	
🍐 • 💩 • 🚭 🔞 🔗 [http://ftl-script1:8080/perl/sys/home.pl#	~	
	Trop://ro-script.com/pen/sys/none.pw	×	
Cisco Tool Administration		CISCO SYSTEMS	
Tool: Administration 💌	Management Domain: National-1 💌	Licensed to Cisco Systems	
Configuration:	Administrator Utilities		
Domain Management			
Admin Utilities	Remove Domain		
System Security User Management	Management National 🔽 Delete Domain		
Discovery	Domain Contraction Contraction		
Device Configuration	Remove Router		
Global Polling Configuration			
Address Management	Router 💙 Delete Router		
Multicast Manager			
Route Manager Remove Layer 2 Switch			
	Switch Velete Switch		
	Remove Baseline		
National-1 - 0 multicast devices:	Baselines V Delete Baseline		
Database currently locked	Address Management Database		
by discovery, please wait			
until it completes.	Import From File Browse Import		
	Reinitialize Export		
	Error Log File		
	Clear Show Discovery Show Polling Log		
	*		
		i i	
		č	

Figure 1-5 Administrative Utilities

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 managemen 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:	
	<pre>#import file format #this line will be skipped 239.1.1.1,test group 192.168.1.1,sourceA</pre>	
	• Reinitialize —Restores all reserved multicast addresses to the IP address database.	
	• Export —Creates a file in <i>/tmp</i> 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	Figure 1-6	System 3	Security
----------------------------	------------	----------	----------

🌍 Back 🝷 💮 🝸 🛃 🛃	🏠 🔎 Search 🤺 Favorites 🚱 🎯 - 嫨 📝 - 📙 饌 🦓	
dress 🗃 http://es1-cmm:8080/perl/s	rs/home.pl#	💌 🄁 Go 🕴 Link
Cisco Tool Administration		CISCO SYSTEMS
Tool: Administration 🌱	Management Domain: gtest2 🛛 💙	Licensed to Cisco Systems
onfiguration: Domain Management	System Security	
Admin Utilities System Security Ser Management	Primary TACACS server info must be configured. Secondary is optional.	
Discovery Device Configuration Global Polling Configuration Address Management	Primary TACACS Server	
Multicast Manager	Primary TACACS Key	
	Primary TACACS Port 49	
gtest2 - 10 multicast devices: es1-7206-w1	Secondary TACACS Key	
es1-7206-w2	Secondary TACACS Port 49	
es1-7606-c1	Enable	
es1-7606-c2 es1-7606-c3	TACACS is now disabled	
es1-7606-c4		
<u>es1-7606-d1</u>		
es1-7606-d2		

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

🐸 Cisco Tool Administration - Mo	zilla Firefox	- F 🗙
<u>File E</u> dit <u>V</u> iew <u>G</u> o ⊆hipmarks §	Bookmarks Iools Help	5.00 5.00
🧇 • 🧼 • 🥩 🙁 🟠 🛽	http://172.31.24.255 :8080/perl/home.pl	O 60 C
Cisco Tool Administration		CISCO SYSTEMS
Tool: Administration 💌	Management Domain: IPmcLab 💌	Licensed to Cisco Systems
Configuration:	User Configuration	
Domain Management Admin Utilities System Security User Management - Manage Users	User ID Description Priv Level Remove admin admin <u>Delete</u>	
- Change Password Discovery	Add User	
Discovery Configuration Global Polling Configuration Address Management Multicast Manager Route Manager IPmcLab - 12 multicast devices:	User ID Description Priv Level Ouser O admin Password Verify	
<u>P2-7206-1</u>	Add	
P2-7206-2		
P2-ntv-1		
P2-ntv-2		
<u>P2-ntv-3</u>		
<u>P2-ntv-4</u>		
<u>P3-7206-1</u>		
P3-7206-2		
P3-msfc-1		
P3-msfc-2		
D2 mefo 2		68808

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).



The admin user account cannot be deleted.

Users can change their password by clicking Change Password.

Figure 1-8 Manage Users—Change Password

<mark>ම Cisco Tool Administration - Mo</mark> Elle Edit <u>Vi</u> ew Go Chipmarks	ozilla Firefox Bookmarks Iools H	eip	▼ ∎_ ○
🤃 🖓 - 🍣 🔇 🕎	http://172.31.24.25	:8080/perl/home.pl	💽 💿 Go 💽
Cisco Tool Administration			CISCO SYSTEMS
Tool: Administration 💌		Management Domain: IPmcLab 💌	Licensed to Cisco Systems
Configuration:	Change Passwo	rd	
Domain Management			
Admin Utilities	User ID		
System Security			
User Management	Old Password		
- Manage Users			
- Change Password Discovery	New Password	Verify	
Discovery Device Configuration	-		
Global Polling Configuration		Change Password	
Address Management			
Multicast Manager			
Route Manager	-		
IPmcLab - 12 multicast			
devices:			
P2-7206-1			
<u>P2-7206-2</u>			
D0 - 1 - 1			
P2-ntv-1			
P2-ntv-2			
1 <u>2 1107 2</u>			
P2-ntv-3			
P2-ntv-4			
<u>P3-7206-1</u>			
<u>P3-7206-2</u>			
P3-msfc-1			
ro-msic-1			
P3-msfc-2			
D2 mefe 2			
			č

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.

.ılı.

180851

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 🕲 Cisco Tool Administration - Mozilla Firefox Eile Edit Yiew Go Chipmarks Bookmarks Tools Help 🗈 🗸 🛶 🚽 💿 😭 🗋 http://172.31.24.255 :8080/perl/home.pl ~ CISCO SYSTEMS Cisco Tool Administration лh Tool: Administration IPmcLab Configuration: Device Configuration Configuration: Domain Management Admin Utilities System Security User Management Discovery Device Configuration - Get All Configs - Validate All Configs Global Polling Configuration Address Management Multicast Manager Routers Router P2-7206-1 💌 Edit Parameters Layer 2 Switches Switch 🛛 🖌 Edit Parameters To apply the default domain community strings to all devices, click on update ncLab - 12 multicast Update P2-7206-1 P2-7206-1 P2-7206-2 Read Only Community String public <u>P2-ntv-1</u> Read Write Community String <u>P2-ntv-2</u> SNMP Timeout 8 P2-ntv-3 SNMP Retries 2 P2-ntv-4 <u>P3-7206-1</u> Modify <u>P3-7206-2</u> P3-msfc-1 P3-msfc-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.



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.

e Edit ⊻iew <u>G</u> o <u>C</u> hipmarks	; <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp	•
🛯 • 🔶 • 🍠 😢 🏠	http://172.31.24.255 :8060/perl/home.pl	✓
		CISCO SYSTEMS
Cisco Tool Administration		
		անհատոննա
Tool: Administration	Management Domain: IPmcLab 💌	Licensed to Cisco Systems
onfiguration:	Get All Configs	
Domain Management		
Admin Utilities	Retrieving All Router Configurationsthis may take some time.	
System Security	Getting config from P2-7206-1 Display Config	
User Management	Getting config from P2-7206-2 Display Config	
Discovery	Getting config from P2-ntv-1 Display Config	
Device Configuration - Get All Configs	Getting config from P2-ntv-2 Display Config	
- Get All Configs - Validate All Configs	Getting config from P2-ntv-3 <u>Display Config</u>	
- validate All Configuration	Getting config from P2-ntv-4 Display Config	
Address Management	Getting config from P3-7206-1 <u>Display Config</u> Getting config from P3-7206-2 Display Config	
Multicast Manager	Getting config from P3-msfc-1 Display Config	
Route Manager	Getting config from P3-mstc-2 Display Config	
Roate Hanager	Getting config from P3-msfc-3 Display Config	
PmcLab - 12 multicast	Getting config from P3-msfc-4 Display Config	
levices:	Finished	
2-7206-1		
2-7206-2		
2-ntv-1		
-2-IIIW-1		
2-ntv-2		
<u></u>		
2-ntv-3		
2-ntv-4		
<u>23-7206-1</u>		
2 7206 2		
23-7206-2		
23-msfc-1		
0 11010 4		
3-msfc-2		

Figure 1-10 Get All Configs

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

Validating Router Configurations

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

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.
Under the Device Configuration menu, click Validate All Configs . The Configuration Check page opens.
Ensure the correct Management Domain is selected.
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.
Select the template you want to use from the list.
(Optional) Click View to see the contents of each template.
Click Check.

Figure 1-11 Configuration Check

Elle Edit Yiew Go Chipmarks Bookr 	marks Iools Help tp://172.31.24.255 :8080/per//home.pl	0
	tp://172.31.24.255 :8080/perl/home.pl	
Cisco Tool Administration		✓
Tool: Administration	Management Domain: IPmcLab 🗸	CISCO SYSTEMS Intilitional Illin Licensed to Cisco Systems
	onfiguration Check	
System Security User Management Discovery Device Configuration - Get All Configs Sec	pload Configuration Template Upload Elect/View Template For Config Verification cv.config ♥ Check View	
P3-msfc-1		
P3-msfc-2		
D2 meto 2		

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.

e Edit View Go Chipmarks	Bookmarks Tools Help	4
I • 🌳 • 🎯 🙆 😭	http://172.31.24.255 :8080/perl/home.pl	~
		CISCO SYSTEMS
cisco Tool Administration		
		يبالليب بالليب
Tool: Administration 🛛 💌	Management Domain: IPmcLab 💌	Licensed to Cisco Systems
onfiguration:	Configuration Check	
Oomain Management		
Admin Utilities	Upload Configuration Template	
System Security	Browse	
Jser Management	Upload	
)iscovery	Opioad	
evice Configuration		
- Get All Configs	Select/View Template For Config Verification	
- Validate All Configs	rcv.config V Check View	
Slobal Polling Configuration		
ddress Management	Getting config from P2-7206-1	
Iulticast Manager	Checking P2-7206-1's config using template rcv.config	
loute Manager		
ProcLab - 12 multicast	Checking Global Commands	
evices:	hostname is NOT set	
2-7206-1	service timestamps debug datetime msec localtime show-timezone is NOT set	
<u> </u>	service timestamps log datetime msec localtime show-timezone is NOT set	
2-7206-2	service password-encryption is NOT set	
	logging is NOT set	
2-ntv-1	no logging console is NOT set	
	no ip source-route is NOT set	
2-ntv-2	no ip http server is NOT set	
	no cdp run is NOT set	
2-ntv-3	ip subnet-zero is NOT set	
	ip classless is NOT set	
2-ntv-4	snmp-server trap-source is NOT set	
	snmp-server location is NOT set	
3-7206-1	snmp-server contact is NOT set	
	snmp-server host is NOT set	
3-7206-2	banner motd is NOT set	
	line vty 0 4 is NOT set	
3-msfc-1	access-class is NOT set	
2	ntp server is NOT set	
<u>3-msfc-2</u>	end is NOT set	

Figure 1-12 Configuration Check—Output

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.



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

le Edit Yiew Favorites Iools 3 Back • 🕥 - 💌 💋 1	<u>/</u>	Help	- 🛃 🕡 - 🗌	6 8					
dress 🙆 http://es1-cmm:8080/perl/s	evel.							😽 🛃 Go	: Links
a cos antep///est chim.oodo/pen/s	5757	nonic.p#							;
								Cisco Sys	TEMS
Cisco Tool Administration								.l.	.l.
								ա	dilin.
rool: Administration 🏻 🎽		Management Do	omain: gtest2	*		Licer	nsed to	Cisco Syst	ems
onfiguration:									^
Domain Management		The polling daemon must be restarte	ed after making ch	anges on this s	creen.				
Admin Utilities									- 11
System Security Jser Management	1	Polling Intervals and Run Times							
Discovery	1								
Device Configuration									1
Global Polling Configuration			Start Time	Stop Time	Days	Max	Max	Max	
- Domain Trap/Email			Start Hille	Stop Time	Days	Threads	Days	Reports	
Address Management	_	Default Run Times 📃 Use Defaults	00 🔽 - 00 🔽	23 🗙 : 59 🐱	M-F 🗸				
Aulticast Manager	_	Deradic Kan miles 0se Deradits	00 . : 00 .	23 . 133					
		DR Polling Interval 5 Min 🎽	00 💌 : 00 💌	23 🛩 : 59 🛩	M-F 🎽				
		Layer 2 Polling 20 Sec Y							
itest2 - 10 multicast	-	Interval 20 Sec Y	00 💙 : 00 🌱	23 🌱 : 59 🌱	M-F 🌱				
levices:		RP/SG Cache 3 Min 🗸							
es1-7206-w1		Polling Interval 3	00 🚩 : 00 🌱	23 🎽 : 59 🌱	M-F 🖌	10 🚩			
4 7004 0		RP Status Polling 3 Min 🗸							
es1-7206-w2		Interval 3 Min Y	00 💙 : 00 🌱	23 🌱 : 59 🌱	M-F 🖌				
es1-7606-c1		RPF Failure Polling 3 Min 🛩							
		Interval 3 Min	00 🌱 : 00 🌱	23 🌱 : 59 🌱	Everyday 🌱				
es1-7606-c2		Threshold Polling 1 Min 🗸							
es1-7606-c3		Interval 1 Min Y	00 🎽 : 00 🌱	23 🌱 : 59 🌱	M-F 🎽				
351-7606-03		Multiaast Tapalaay							
es1-7606-o4		Multicast Topology Polling Interval 24 Hrs 🍟	04 🌱 : 00 🌱	07 🎽 : 00 🌱	M-F 🎽				
es1-7606-d1		Tree Polling Interval 2 Min Y	00 🜱 : 00 🌱	23 🌱 : 59 🌱	M-F 🎽				
es1-7606-d2		_							
<u></u>		Set							~
	_								

Figure 1-13 Global Polling Configuration

The Global Polling Configuration page contains:



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 <i>rpReachable</i> trap is sent. If the RP does not respond, an <i>rpUnreachable</i> 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 <i>ifIndexes</i> 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.

Cisco Tool Administration - M	
	Bookmarks Iools Help
📮 • 🔿 - 😂 😢 🟠 [http://172.31.24.255 :8080/perl/home.pl
Cisco Tool Administration	Cisco Systems Jatilita
Tool: Administration 💌	Management Domain: IPmcLab 💌 Licensed to Cisco Systems
Configuration:	Trap Receiver/Email Polling Configuration for IPmcLab Domain
Domain Management Admin Utilities	(Polling Daemon is Running since Thu Aug 3 09:38:51 EDT 2006 by watchdog script) Refresh Status
System Security User Management	Start Stop Restart
Discovery Device Configuration Global Polling Configuration	The polling daemon must be restarted after making changes on this screen.
- Domain Trap/Email	Configure Domain Specific SNMP Trap Receivers
Address Management Multicast Manager	Add Trap Receiver Configured Trap Receivers
Route Manager	Add Trap Receiver Remove Trap Receiver
IPmcLab - 12 multicast	These values will override the global defaults.
P2-7206-1	Configure Domain Specific Email Addresses for Event Notification
- <u>P2-7206-2</u>	Add Email Address Configured Email Addresses
. <u>P2-ntv-1</u>	Add Email Address 🛛 🔽 Remove Email Address
. <u>P2-ntv-2</u>	
- <u>P2-ntv-3</u>	These values will override the global defaults.
. <u>P2-ntv-4</u>	The settings on this screen are domain specific. The values specified on this screen will override any trap
- <u>P3-7206-1</u>	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.
. <u>P3-7206-2</u>	
• <u>P3-msfc-1</u>	
P3-msfc-2	

Figure 1-14 Trap Receiver/Email Polling Configuration

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

e <u>E</u> dit ⊻iew <u>G</u> o <u>C</u> hipmarks	Bookmarks <u>T</u> ools <u>H</u> elp)		<
🛯 • 🔿 • 🍠 😣 🟠 [http://172.31.24.255 :8	3080/perl/home.pl		~
				CISCO SYSTEMS
Cisco Tool Administration				
				լուլլին
Tool: Administration 💌		Management Domain: IP	mcLab ≚	Licensed to Cisco Systems
onfiguration:	Address Manager	nent		<u>^</u>
Domain Management Admin Utilities				
Vamin Utilities System Security	IP Address	to		
Jser Management	(from)		Mask Description	
iscovery				
evice Configuration				
lobal Polling Configuration	_	Add Delete	Query Display Database Clear Fields	
ddress Management ulticast Manager				
oute Manager	-	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]	
mcLab - 12 multicast		224.0.0.101	cisco-nhap [Bakke]	
evices:		224.0.0.102	HSRP [Wilson]	
<u>2-7206-1</u>	-			
2-7206-2		224.0.0.103	MDAP [Deleu]	
<u> </u>		224.0.0.104	Nokia MC CH [Kalhour]	
2-ntv-1		224.0.0.105	ff-Ir-address [Glanzer]	
		224.0.0.106-224.0.0.250	Unassigned [JBP]	
<u>2-ntv-2</u>		224.0.0.11	Mobile-Agents [Bill Simpson]	
2-ntv-3		224.0.0.12	DHCP Server / Relay Agent [RFC1884]	
		224.0.0.13	All PIM Routers [Farinacci]	
2-ntv-4		224.0.0.14	RSVP-ENCAPSULATION [Braden]	
3-7206-1		224.0.0.15	all-cbt-routers [Ballardie]	
<u> </u>		224.0.0.16	designated-sbm [Baker]	
3-7206-2		224.0.0.17	all-sbms [Baker]	
3-msfc-1		224.0.0.18	VRRP [Hinden]	
<u>3-11510-1</u>	*	224.0.0.19	IPAIIL1ISs [Przygienda]	
3-msfc-2		224.0.0.2	All Routers on this Subnet [JBP]	
		224.0.0.2	All Routers on this Subnet [JBP]	~

Figure 1-15 Address Management

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



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

Edit ⊻iew Go ⊆hipmarks Bo	iokmarks <u>T</u> ools <u>H</u> e	4p			
ı • 🛶 • 🛃 🔕 🚷 🗈	http://172.31.24.255	:8080/perl/home.pl			~
Cisco Tool Administration					CISCO SYSTEM
rool: Administration 🕑		Managemer	nt Domain:	IPmcLab 💌	Licensed to Cisco Systems
onfiguration:	RP Polling Confi	guration for IPm	cLab Dom	ain	
Domain Management Admin Utilities	(Polling Daemon is	Running since Thu	Aug 3 09:3	8:51 EDT 2006 by watchdog script) Refresh Statu	3
ystem Security Iser Management	Start Stop	Restart			
Discovery Device Configuration	The polling dae	mon must be res	tarted afte	r making changes on this screen.	
ilobal Polling Configuration ddress Management Iulticast Manager	Enable RP Group	Add Delete Tra	ps		
- RP Polling - RPF Polling	🗹 Enable RP Add,	/Delete Traps S∈	it .		
	RP Monitoring				
- L2 Polling - Tree Polling	Select RP 💌	Group Limit -1	M	onitor RP	
- Health Check	RPs Being Monit	ored			
loute Manager	RP Group	Limit Accept-Lis	st Remove		
mcLab - 12 multicast	P3-7206-1 -1	Configure	Delete		
evices:	P2-7206-1 100	Configure	Delete		
2-7206-1	P2-ntv-4 -1	Configure	Delete		
2-7206-2	P3-7206-1 -1	Configure	Delete		
	P3-msfc-1 -1	Configure	Delete		
2-ntv-1	P3-msfc-2 -1	Configure	Delete		
2-ntv-2	P3-msfc-3 -1	Configure	Delete		
	P3-msfc-4 -1	Configure	Delete		
2-ntv-3	P2-ntv-2 50	Configure	Delete		
2-ntv-4	P2-ntv-3 35	Configure	Delete		
3-7206-1	P2-ntv-1 22	Configure	Delete		
	Single S,G Monit				

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.

Cisco Tool Administration - Mo File Edit View Go Chipmarks (zzilla Firefox
Eile Edit View Go Chipmarks (putrians 1006 gep
Cisco Tool Administration	Cisco Systems and Inner all Inner a
Tool: Administration 💌	Management Domain: IPmcLab 🔽 Licensed to Cisco Systems
Configuration:	RP Polling Configuration for IPmcLab Domain
Domain Management Admin Utilities System Security User Management Discovery Device Configuration	(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.
Global Polling Configuration Address Management Multicast Manager - RP Polling - RPF Polling - SG Polling - Main - SG Polling - by Device	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 matches anything.
- L2 Polling - Tree Polling - Health Check Route Manager	Source 0.0.0.0 Source 455.255.255 0.0.0.0 matches Group 0.0.0.0
IPmcLab - 12 multicast devices: <u>P2-7206-1</u>	Group Mask 0.0.0.0 0.0.0.0 matches exactly, 255.255.255.255 matches anything
<u>P2-7206-2</u>	
<u>P2-ntv-1</u>	Return to RP Config
<u>P2-ntv-2</u>	
P2-ntv-3	
P2-ntv-4	
<u>P3-7206-1</u>	
<u>P3-7206-2</u>	
L. 🖻	

Figure 1-17 RP Accept List Configuration

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.

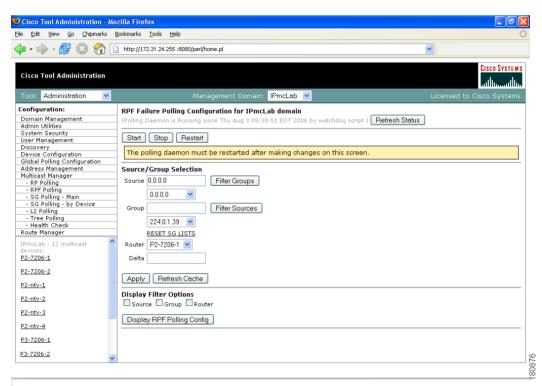
RPF Polling

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



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.

🕲 Cisco Tool Administration - Mo	zilla Firefox	- 7 🛛
Eile Edit View Go Chipmarks B	ookmarks Iools Help	
🤃 🖓 · 🍣 🖉 😭	http://172.31.24.255 :8080/perl/home.pl	•
Cisco Tool Administration		CISCO SYSTEMS
Tool: Administration 💌	Management Domain: IPmcLab 💌	Licensed to Cisco Systems
Configuration:	SG Polling Configuration for IPmcLab domain	~
Domain Management Admin Utilities	(Polling Daemon is Running since Thu Aug 3 09:38:51 EDT 2006 by watchdog script) Refresh Status	
System Security User Management	Start Stop Restart	
Discovery Device Configuration Global Polling Configuration	The polling daemon must be restarted after making changes on this screen.	
Address Management	Source/Group Thresholds	
Multicast Manager		
- RP Polling	Source 0.0.0.0 Filter Groups	
- RPF Polling	0.0.0.0	
- SG Polling - Main		
- SG Polling - by Device - L2 Polling	Group Filter Sources	
- Tree Polling		
- Health Check	224.0.1.39 💌	
Route Manager	RESET SG LISTS	
IPmcLab - 12 multicast devices: <u>P2-7206-1</u> <u>P2-7206-2</u>	Select Routers P2-7206-1 P2-7206-2 P2-ntv-1 P2-ntv-1	
P2-ntv-1	Units 💿 pps 🔘 bps	
P2-ntv-2	High Threshold	
P2-ntv-3	Low Threshold	
<u>P2-ntv-4</u>	Apply Refresh Cache	
<u>P3-7206-1</u>	Display Filter Options	
<u>P3-7206-2</u>	Source Group Router	6/2808

Figure 1-19 SG Polling Configuration

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.

Edit View Go Chipmarks E	<u>a</u> ookmarks <u>T</u> ools	Help							0
• 🔶 • 🛃 😣 🟠 🛯	http://172.31.24	255 :8080/perl/home	e.pl					~	
								Cisco Sys	TEMS
Cisco Tool Administration									միս
Tool: Administration 🛛 💌		Manag	ement Do	main:	IPmo	:Lab	*	Licensed to Cisco Syst	ems
onfiguration:	High Threshol								^
Domain Management	Low Threshol	t							
Admin Utilities									
System Security	(Apply)	efresh Cache							
Jser Management	Apply R	aresh caune							
Discovery	Display Filter	Ontions							_
Device Configuration Slobal Polling Configuration		Group Router							
Address Management	Source	Group 🗆 Router							
Aulticast Manager									
- RP Polling	Display Con	igured SGS							
- RPF Polling			- C						-
- SG Polling - Main		ce/Group Pollin							
- SG Polling - by Device	<u>Source</u>	<u>Group</u>	<u>Router</u>		Low	Units			
- L2 Polling	0.0.0.0	239.0.0.1	P2-ntv-3	100	10	pps	Edit / Delete Time-based Thresholds		
- Tree Polling - Health Check	0.0.0.0	239.0.0.1	P2-ntv-1	100	10	pps	Edit / Delete Time-based Thresholds		
Route Manager	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		
IPmcLab - 12 multicast 🏻 🔗	0.0.0.0	239.0.0.1	P2-ntv-1	1000	10	DDS	Edit / Delete Time-based Thresholds		
devices: P2-7206-1	0.0.0.0	239.0.0.1	P2-ntv-2		10		Edit / Delete Time-based Thresholds		
2 7200-1						pps			
2-7206-2	0.0.0.0	239.0.0.1	P2-ntv-2		2	pps	Edit / Delete Time-based Thresholds		
	0.0.0.0	239.0.0.1	P3-msfc-4		10	pps	Edit / Delete Time-based Thresholds		
P2-ntv-1	0.0.0	239.0.0.1	P2-ntv-4	10000	3	pps	Edit / Delete Time-based Thresholds		
22 - ++ 2	0.0.0	239.0.0.1	P3-msfc-4	100	10	pps	Edit / Delete Time-based Thresholds		
<u>P2-ntv-2</u>	0.0.0.0	239.0.0.1	P3-msfc-3	100	10	pps	Edit / Delete Time-based Thresholds		
P2-ntv-3	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		2	pps	Edit / Delete Time-based Thresholds		
2-ntv-4	0.0.0.0	239.0.0.1	P2-ntv-4		-		Edit / Delete Time-based Thresholds		
2 7206 1	0.0.0.0				-	pps			
<u>P3-7206-1</u>		239.0.0.1	P2-ntv-2		10	pps	Edit / Delete Time-based Thresholds		
	0.0.0.0	239.0.0.1			10	pps	Edit / Delete Time-based Thresholds		
P3-7206-2	0.0.0.0	239.0.0.1	P2-ntv-2			pps	Edit / Delete Time-based Thresholds		×

Figure 1-20 Current Source/Group Polling Configuration

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.

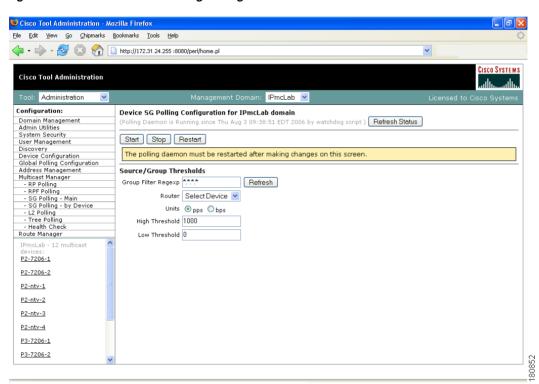


Figure 1-21 Device SG Polling Configuration

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.

🕲 Cisco Tool Administration - Mo	zilla Firefox
File Edit View Go Chipmarks E	lookmarks Tools Help
De fai Jeu Ze Suburge i	international Tests Tests
· 🗇 • 🕪 • 🛃 区 🏠 🛽] http://es1-cmm:8080/perl/sys/home.pl#
	<u>Cisco Systems</u>
Cisco Tool Administration	adhoadho
Tool: Administration 💌	Management Domain: 🛛 🗾 🔽 🚽 🚽 Licensed to Cisco Systems
Configuration:	L2 Polling Configuration for gtulumba domain
Domain Management	(Pollina Deemon is Running since Mon Aug 14 11:06:49 2006) Refresh Status
Admin Utilities	(Poling Daenon's Kunning since Mon Aug 14 11:00:49 2006) Renesin Status
System Security	Start Stop Restart
User Management	Star, Stup Hestar
Discovery Device Configuration	The polling daemon must be restarted after making changes on this screen.
Global Polling Configuration	The pointing deeleft mask be restarted after making dranges on this screen.
Address Management	Layer 2 Switch Monitoring
Multicast Manager	
- RP Polling	Select Switch to Monitor Select Switch 💌
- RPF Polling	
- SG Polling - Main	Direction INBOUND Y
- SG Polling - by Device - L2 Polling	High PPS
- L2 Polling - Interface Polling	
- Tree Polling	Low PPS
- Health Check	
	Select Port to Monitor
Search:	
gtulumba - 10 total device(s)	Add/Edit
es1-7206-w1	· · · · · · · · · · · · · · · · · · ·
<u>C31 7200 W1</u>	Import/Export
es1-7206-w2	Export Filename: Export
an1 7606 a1	Import Filename: Stowse Smerge O Replace Import
<u>es1-7606-c1</u>	
es1-7606-c2	Current Layer 2 Switch Polling Configuration
	Switch Part Direction High Low Modify Time Threshold
es1-7606-c3	s1-3750-a4 Gi1/0/1 INBOUND 100 90 Edit / Delete Time-based Thresholds
es1-7606-c4	est-5750-44 (GL/02 INDOUND 100 90 CLIC/ Delete Inter-based Infestiolos
es1-7606-d1	es1-3750-a4 Gi1/0/2 INBOUND 100 90 <u>Edit / Delete Time-based Thresholds</u> es1-3750-a4 Gi1/0/7 INBOUND 100 90 <u>Edit / Delete Time-based Thresholds</u>
es1-7606-d1	1

Figure 1-22 L2 Polling Configuration

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.

e Edit ⊻iew <u>G</u> o ⊆hipmarks	Bookmarks <u>T</u> ools <u>H</u> elp						<
• 🔶 • 🧬 😣 🚷 [http://172.31.24.255 :8	080/perl/home.pl				~	
Cisco Tool Administration							CISCO SYSTEMS
Tool: Administration 💽		Management Dom	nain: IPmcLab	*		Licensed	to Cisco Systems
tonfiguration: Domain Management Admin Utilities System Security User Management Discovery	(Polling Daemon is N	uration for IPmcLab ot Running) Refresh S Restart					
Device Configuration Global Polling Configuration Address Management	The polling daemo	on must be restarted	after making cha	nges on this scre	en.		
Multicast Manager - RP Polling - RPF Polling - SG Polling - Main - SG Polling - by Device	Saved Trees paul99	l.trace 💌					
- L2 Polling - Tree Polling	Trees to be Polled	0	0	5115	1.1.15	11	Demos
- Health Check	Baseline paul99.trace	Source 10.0.1.1	Group 224.0.1.39	FHR	ALL	Monitor PPS Configure	Remove Delete
Route Manager IPmcLab - 12 multicest devices: P2-7206-1 P2-7206-2 P2-ntv-1 P2-ntv-2 P2-ntv-3 P2-ntv-4 P3-7206-1							

Figure 1-23	Tree	Polling	Configuration
-------------	------	---------	---------------

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

e <u>E</u> dit <u>Vi</u> ew F <u>a</u> vorites <u>T</u> oo	icrosoft Internet Explorer provided by Cisco Systems, Inc.	
ress 🕘 http://172.31.24.255 :808	0/perl/home.pl	💌 🄁 G
🕽 Back 🔹 🕥 🕤 💌 💈	🏠 🔎 Search 🧙 Favorites 🚱 😥 - 🌺 🔟 - 🛄 🎎 🖄	
isco Tool Administration		CISCO SYSTEMS
111111		ավիստովիստ
ool: Administration 🛛 🝸	Management Domain: IPmcLab 🔽 Licensed :	to Cisco Systems
onfiguration:		^
- Iomain Management	Tree Polling Configuration for IPmcLab domain	
dmin Utilities	(Polling Daemon is Running since Tue Aug 15 07;45;57 2006) Refresh Status	
ystem Security	(Foling Decision is Kalining since Fee Reg 15 of Hostor 2000)	
iser Management		
iscovery		
evice Configuration		
lobal Polling Configuration		
ddress Management	Start Stop Restart	
ulticast Management		
- RP Polling		
- RPF Polling - RPF Polling	The polling daemon must be restarted after making changes on this screen.	
- SG Polling - Main		
- SG Polling - Main - SG Polling - by Device		
- L2 Polling	 Select Routers on Tree (1tree.trace) for S,G PPS Monitoring 	
- Tree Polling		
- Health Check	P2-7206-1	
oute Manager	P2-ntv-2	
	▶ P3-7206-1	
PrncLab - 12 multicast	P3-msfc-2	
evices:	P3-msfc-4	
2-7206-1		
2-7206-2	1 Specify Max Delta Between PPS Samples	
<u>'2-ntv-1</u>	Set Return to Main Config Remove	
2 -tu 2	Return to Main Coning Periove	
2-ntv-2		
2 -4. 2		
2-ntv-3		
2-ntv-4	Routers selected here will be monitored for (S,G) PPS when the tree is polled. If the PPS rate on any deviates by MAX Delta from the others, an SNMP trap will be generated.	router
3-7206-1		~

• 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

e ⊑dit ⊻iew <u>G</u> o ⊆hipmarks	Bookmarks Iools Help	4
þ • 🌳 • 🍠 💿 🟠 [http://172.31.24.255 :8080/perl/home.pl	×
Cisco Tool Administration	David also	Cisco Systems authreadhreadhreadhreadhreadhreadhreadhread
Configuration:	Management Domain: IPmcLab Health Check Configuration for IPmcLab domain	Licensed to Cisco Systems
Domain Management		
Admin Utilities		
System Security	Create New Health Check Add	
User Management		
Discovery	Modify Existing Health Check IPmcLAB 💌 🛛 Load Remove	
Device Configuration	1	
Global Polling Configuration		
ddress Management		
Iulticast Manager		
- RP Polling		
- RPF Polling		
- SG Polling - Main		
- SG Polling - by Device		
- L2 Polling		
- Tree Polling		
- Health Check	_	
loute Manager		
IPmcLab - 12 multicast devices: <u>P2-7206-1</u>		
<u>P2-7206-2</u>		
<u>2-ntv-1</u>		
<u>2-ntv-2</u>		
2-ntv-3		
2 <u>-ntv-4</u>		
<u>3-7206-1</u>		
93-7206-2		

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 - Mo	zilla Firefox	×
Eile Edit ⊻iew Go ⊆hipmarks E	gookmarks Iools Help	
🔷 • 🌳 · 🍠 😣 🟠 🚺	http://172.31.24.255 :8080/perl/home.pl	
Cisco Tool Administration	Cisco System authoriallin Management Domain: IPmcLab V Licensed to Cisco Systems	
Configuration:	Health Check Configuration for IPmCLab domain	~
Domain Management Admin Utilities System Security User Management Discovery Device Configuration	Create New Health Check Add Modify Existing Health Check IPmcLAB	
Global Polling Configuration Address Management	(IPmcLAB.health) Health Check Configuration for IPmcLab domain	
Multicast Manager - RP Polling - RPF Polling - SG Polling - Main - SG Polling - by Device	Rendezvous Points Select RP to Check P2-7206-1 Y Add	8
- L2 Polling - Tree Polling	RPs Being Checked	
- Health Check Route Manager IPmcLab - 12 multicast devices: P2-7206-1	RP MSDP Remove P2-7206-1 Configure Delete P2-rtv-1 Configure Delete P3-r5206-1 Configure Delete	
<u>P2-7206-2</u>	Source/Group Thresholds	
P2-ntv-1	Source 0.0.0. Filter Groups	
P2-ntv-2	0.0.0 💌	
<u>P2-ntv-3</u>	Group Filter Sources	
P2-ntv-4	224.0.1.39	
<u>P3-7206-1</u>	RESET SG LISTS	55
<u>P3-7206-2</u>	Router P2-7206-1 💌	180855

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

Cisco Tool Administration - Mo		
e Edit View Go Chipmarks	Bookmarks Iools Help	1
🕨 • 🌳 • 🥵 • 🏠 🚺	http://172.31.24.255 :8080/perl/home.pl	
	Cisc	O SYSTEMS
Cisco Tool Administration		տամիս
Tool: Administration 💽	Management Domain: IPmcLab 💌 Licensed to Cisco S	Systems
Configuration:	Health Check Configuration for IPmcLab domain	
Domain Management		
Admin Utilities	Create New Health Check Add	
System Security		
User Management	Modify Existing Health Check IPmcLAB V Load Remove	
Discovery		
Device Configuration		
Global Polling Configuration Address Management	(IPmcLAB.health) P2-7206-1 MSDP Health Check Configuration	
Address Management Multicast Manager	Columba 2005 A Brown to Shark	
- RP Polling	Select P2-7206-1 Peers to Check	
- RPF Polling		
- SG Polling - Main	- :224.1.1.2	
- SG Polling - by Device	P3-7206-1:224.1.1.2	
- L2 Polling		
- Tree Polling		
- Health Check		
Route Manager	Set Return to Main Config Clear Selections	
^		
IPmcLab - 12 multicast		
devices:		
P2-7206-1		
P2-7206-2		
P2-ntv-1		
P2-ntv-2		
P2-ntv-3		
P2-ntv-4		
<u>P3-7206-1</u>		
P3-7206-2		

Figure 1-27 Health Check Configuration—Peers

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

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

	- 🛃 💿 🏠 🗈 he	to://172.31.24.255	:8080/perl/home.pl		*	
. 4		(p.//172.31.24.233	.0000/pen/nome.pr			
sco Mi	ulticast Manager 2.3.3					CISCO SYSTEMS
ol: M	lulticast Manager 💌		Managemer	nt Domain: IPmcLab 💌	Licer	sed to Cisco Systems
Hom	e Topology	Reporting	Diagnostics	Help		
itest E	vents					
		Date		Туре	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	

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.

🌀 Back 🝷 🌍 🗧 🗴	2	🏠 🔎 Search 👷	Favorites 🥳		-	w •	12 - 28					
idress 🕘 http://es1-cmm:8	080/perl/to	po.pl#									💙 ラ Go	; Links
											Cinco Svo	
Cisco Multicast Mana	ger 2.3.3	3									CISCO SYST	
Tool: Multicast Manag	ger 🔽		Managem	ient Doi	main:	gtest2	~		Lic	ensed	to Cisco Syste	
Home Toj	pology	Reporting	Diagnostics		Help							
Fopology: Display All		Network Topology (P	IM Neighbors)	using da	atabase		.db (contains 10 dev 7206-w1	ices)				^
		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)	
atest2 - 10 devices:	^					es1-	7206-w2					
<u>es1-7206-w1</u>		Local Int	Local IP	PIM Mode	IGMP	Neighbor	Neighbor's Int	Neighbor IP	PIM Mode	IGMP	DR	
<u>es1-7206-w2</u>		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	
<u>es1-7606-c1</u>		Serial4/0	172.31.24.255	sparse	2	es1-7206- w1	Serial4/0	172.31.24.255	sparse		N/A (0.0.0.0)	
<u>es1-7606-c2</u>		Serial4/1	172.31.24.255	sparse	2	es1-7206- w1	Serial4/1	172.31.24.255	sparse		N/A (0.0.0.0)	
<u>es1-7606-c3</u>						es1-	7606-c1					
<u>es1-7606-c4</u>		Local Int	Local IP	PIM Mode	IGMP	Neighbor	Neighbor's Int	Neighbor IP	PIM Mode	IGMP	DR	
<u>es1-7606-d1</u>	~	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	~

Figure 1-29 Topology Display All

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.

	Help					
) Back 🔹 🌍 🔹 💌 😰	🏠 🔎 Search 🦻		3- 📐 🗹 -	1 12 - 83		
ss 🖉 http://es1-cmm:8080/perl/1						Go 🕴 Link
						CISCO SYSTEMS
co Multicast Manager 2.3	.3					ահես ահես
ol: Multicast Manager 😪		Management	Domain: gtest2	*	Licensed 1	to Cisco Systems
Home Topology	Reporting	Diagnostics	Help			
ology:			1			~
lay All	Topology Informa	tion for es1-7606-c2 v	when discovered			
	Username					
	Username					
	Password					
	Show Command		Show			
			PI	<u> 1 Neighbors</u>		
atest2 - 10 devices:		Local Int	Neighbo	· Neighb	oor IP Neighbor's Int	
-7206-w1		GigabitEthernet3/42	es1-7606-c3	172.31.24.2	55 GigabitEthernet3/42	
		GigabitEthernet3/40	es1-7606-sd1	172.31.24.2	55 GigabitEthernet3/40	
-7206-w2		GigabitEthernet3/14	es1-7606-c4	172.31.24.2	-	
-7606-c1		GigabitEthernet3/38	es1-7606-c1	172.31.24.2		
		GigabitEthernet3/13	es1-7606-sd2	172.31.24.2		
-7606-c2		GigabitEthernet3/1	es1-7206-w1	172.31.24.2	55 GigabitEthernet0/1	
-7606-c3			РІМ І	nterface Mode		
	1	Local Int	Local IP	PIM Mode	DR	
		GigabitEthernet3/42	172.31.24.255	sparse	es1-7606-c3 172.31.24.255	
-7606-04		2			es1-7606-c2 172.31.24.255	
<u>-7606-c4</u> -7606-d1		.oopback1	172.31.24.255	sparse		

Figure 1-30 Topology for an Individual Router

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.



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**.

Ele Edit Wew Favorites Tools Help Image: Seck + Image: Seck + Image: Sec + Image: S	(STEM S
dress ≧ http://esi-cmm:8080/per/topo.pl# Cisco Multicast Manager 2.3.3 Tool: Multicast Manager V Management Domain: glest2 V Licensed to Cisco Syst Home Topology Reporting Diagnostics Help Topology: Display All esi-7606-ca1 (glgabilEthemet340) (esi-7606-ca)	(STEMS IIIIIII. stems
Cisco Multicast Manager 2.3.3	(STEMS IIIIIII. stems
Cisco Multicast Manager 2.3.3	a ıllı ı. stems
Tool: Multicast Manager V Management Domain: gtest2 V Licensed to Cisco Syst Home Topology: Best-7606-c2 Neighbor Interface Display All es1-7606-sd1 GigabilEthemet340	tems
Topology: Display All es1-7606-c2 Neighbor Interface es1-7606-sd1 GigabilEtheme1340 es1-7606-c3	~
GigabitEthemet3/40	~
es1-7606-sd1 GigabitEthemet3/40	
es1-7606-c3	
est-7206-w1 est-7206-w2 GigabitEthemet3/14 GigabitEthemet3/40 GigabitEthemet3/42	
GigabilEthemet3/14 GigabilEthemet3/14	
<u>es1-7606-c2</u>	
es1-7606-c2	
GigabilEthemet3/1	
es1-7606-d1	
	~

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



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.

Cisco Multicast Manager 2, 3, 3(20060419) - Microsoft Internet Explorer provided by Cisco Systems, Inc C 🗗 🗙 Eile Edit View Favorites Tools Help 🔇 Back 🔹 🕥 📲 📓 🕎 🔎 Search 🤸 Favorites 🤣 🍰 🐷 👻 🖕 🏭 🎎 Address 🗃 http://es1-cmm:8080/perl/report.pl# 🗸 🛃 Go Links » CISCO SYSTEMS Cisco Multicast Manager 2.3.3 մի Tool: Multicast Manager 🜱 Management Domain: SEVT-TEST Home Topology Reporting Diagnostics Help Reporting: Latest Events Latest Events Latest Events RP Polling Report RP Group Threshold Report RPF Failures Group Gone Report SyG Threshold Report Layer 2 PPS Threshold Report SSG Report Three Report SyG Delta Report Historical Graphs Max Events 100 Report Historical Graphs Display All IOS Versions SEVT-TEST - 10 devices: <u>es1-7206-w1</u> <u>es1-7206-w2</u> <u>es1-7606-c1</u> es1-7606-c2 es1-7606-c3 <u>es1-7606-c4</u> <u>es1-7606-d1</u> 180489

Figure 1-32 Latest Events

RP Polling Report

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

- All leaves and joins for the selected RP (if the Enable RP Add/Delete Traps option is selected, see the "RP Polling" section on page 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.

e <u>E</u> dit ⊻iew <u>G</u> o ⊆hipmarks	<u>B</u> ookmarks <u>T</u> ools <u>H</u> elp					4
Þ• 🔶 • 🥰 😣 🟠 🛙	http://172.31.24.255 :80	80/perl/home.pl			~	
Cisco Multicast Manager 2.3.	.3(2)					CISCO SYSTEMS
Tool: Multicast Manager 💌		Management Domain:	IPmcLab 🔽		Licensed	to Cisco Systems
Home Topology	Reporting	Diagnostics Help				
Reporting:	RP Polling Report	or P2-7206-1				
atest Events		Date	Router	Source	Group	State
RP Polling Report	Thu Aug 10 16:15:00	2006	P2-7206-1	10.255.255.255	239.0.0.1	removed
RP Group Threshold Report RPF Failures	Thu Aug 10 16:15:00		P2-7206-1	10.255.255.255	239.0.0.1	removed
RPF Failures Group Gone Report	Thu Aug 10 16:15:00		P2-7206-1	10.255.255.255	239.0.0.1	removed
S,G Threshold Report	Thu Aug 10 16:15:00		P2-7206-1	10.255.255.255	239.0.0.1	removed
Layer 2 PPS Threshold Report	Thu Aug 10 16:15:00		P2-7206-1 P2-7206-1		239.0.0.1	removed
SSG Report	-			10.255.255.255		
Tree Report S.G Delta Report	Thu Aug 10 16:15:00		P2-7206-1	10.255.255.255	239.0.0.1	removed
S,G Deita Report Historical Graphs	Thu Aug 10 16:15:00		P2-7206-1	10.255.255.255	239.0.0.1	removed
Display All IOS Versions	Thu Aug 10 16:00:00		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
IPmcLab - 12 multicast	Thu Aug 10 16:00:00	2006	P2-7206-1	10.255.255.255	239.0.0.1	added
devices:	Thu Aug 10 16:00:00	2006	P2-7206-1	10.255.255.255	239.0.0.1	added
<u>P2-7206-1</u>	Thu Aug 10 16:00:00	2006	P2-7206-1	10.255.255.255	239.0.0.1	added
P2-7206-2	Thu Aug 10 16:00:00	2006	P2-7206-1	10.255.255.255	239.0.0.1	added
<u>F2-7200-2</u>	Thu Aug 10 16:00:00		P2-7206-1	10.255.255.255	239.0.0.1	added
P2-ntv-1					_00.0.0.1	
P2 -t+ 2						
<u>P2-ntv-2</u>						
P2-ntv-3						
P2-ntv-4						
P3-7206-1						
<u>P3-7206-2</u>						
P3-msfc-1						
D2 mefe 2	1					

Figure 1-33 RP Polling Report

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.

e <u>E</u> dit ⊻iew F <u>a</u> vorites <u>T</u> ools	Help					4
🕽 Back 🔹 🕥 - 💌 😫 🤅	🏠 🔎 Search 🤞	💦 Favorites 🚱 🍰	👿 🛛 🔜 🏭 🚳			
iress 🗃 http://es1-cmm:8080/perl/re	eport.pl#				✓ →	Go Links
					Cisc	O SYSTEMS
isco Multicast Manager 2.3.	3					. di
						haaddiilin
ool: Multicast Manager 🍸		Management Domain:	SEVT-TEST 🎽		Licensed to Cisco 9	Systems
Home Topology	Reporting	Diagnostics Help				
eporting:	DD Cusus Thursh		COC -11			^
atest Events	RP Group Thresh	old Polling Report for es1-7 Date	Router	Count	Threshold	
P Polling Report						
P Group Threshold Report	Mon May 8 08:12:0		es1-7606-sd1	66	50	
PF Failures iroup Gone Report	Mon May 8 08:09:0	00 2006	es1-7606-sd1	66	50	
,G Threshold Report	Mon May 8 08:06:0	01 2006	es1-7606-sd1	66	50	
aver 2 PPS Threshold Report	Mon May 8 08:03:0	0 2006	es1-7606-sd1	66	50	
SG Report	Mon May 8 08:00:0	00 2006	es1-7606-sd1	66	50	
ree Report	Mon May 8 07:57:0	11 2006	es1-7606-sd1	66	50	
,G Delta Report	Mon May 8 07:54:0		es1-7606-sd1	66	50	
listorical Graphs	Mon May 8 07:51:0		es1-7606-sd1	66	50	_
isplay All IOS Versions						
^	Mon May 8 07:48:0		es1-7606-sd1	66	50	
SEVT-TEST - 10 devices:	Mon May 8 07:45:0	00 2006	es1-7606-sd1	66	50	
es1-7206-w1	Mon May 8 07:42:0	00 2006	es1-7606-sd1	66	50	
4 7004 0	Mon May 8 07:39:0	00 2006	es1-7606-sd1	66	50	
<u>s1-7206-w2</u>	Mon May 8 07:36:0	01 2006	es1-7606-sd1	66	50	
es1-7606-c1	Mon May 8 07:33:0	00 2006	es1-7606-sd1	66	50	
<u>191-7808-CI</u>	Mon May 8 07:30:0	01 2006	es1-7606-sd1	66	50	
s1-7606-c2	Mon May 8 07:27:0		es1-7606-sd1	66	50	_
	Mon May 8 07:24:0		es1-7606-sd1	66	50	
<u>s1-7606-c3</u>			es1-7606-sd1	66	50	_
	Mon May 8 07:21:0					_
s1-7606-c4	Mon May 8 07:18:0		es1-7606-sd1	65	50	
-1 7000 41	Mon May 8 07:15:0	00 2006	es1-7606-sd1	66	50	
<u>s1-7606-d1</u>	Mon May 8 07:12:0	01 2006	es1-7606-sd1	66	50	
~	Mon May 8 07:09:0	10.2006	es1-7606-sd1	66	50	×

Figure 1-34 RP Group	Threshold F	Polling Report
----------------------	-------------	----------------

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.

e <u>E</u> dit ⊻iew	Favorites <u>T</u> ools	Help							
Back 🔹 📀) - 💌 😰 (🏠 🔎 Search 🤞	Favorites 🧭	🔊 - 🎍 👿	• 📃 🛍 🕴	8			
ress 😹 http://es	s1-cmm:8080/perl/n	eport.pl#						🐱 🔁 Go	: Links
								CISCO SYST	EMS
isco Multicas	t Manager 2.3.	.3						ւի	
ool: Multicast	t Manager 🔽		Manageme	ent Domain: SEV	T-TEST	<u>~</u>	License	الاستالالليا to Cisco Syste ک	ms
Home	Topology	Reporting	Diagnostics	Help	11201		License	r to cisco byste	115
porting:	ropology		-						~
atest Events		RPF Failure Rep							
P Polling Repor	t	Dá		Router	Source	Group	RPF Failures	Threshold	
P Group Thresh	old Report	Mon May 8 08:21:	00 2006	es1-7606-sd1	10.25.0.1	224.0.0.1	34	5	
PF Failures		Mon May 8 08:21:	00 2006	es1-7606-sd1	10.25.0.1	224.0.0.1	34	5	
roup Gone Rep G Threshold R		Mon May 8 08:21:	00 2006	es1-7606-sd1	10.25.0.1	224.0.0.1	34	5	
yer 2 PPS Thre		Mon May 8 08:12:	00 2006	es1-7606-sd1	10.25.0.1	224.0.0.1	19	5	_
SG Report		Mon May 8 08:12:	0 2006	es1-7606-sd1	10.25.0.1	224.0.0.1	34	5	
ee Report		Mon May 8 08:12:		es1-7606-sd1	10.25.0.1	224.0.0.1	34	5	
G Delta Report		Mon May 8 08:09:		es1-7606-sd1	10.25.0.1	224.0.0.1	34	5	
storical Graphs splaγ All IOS \		Mon May 8 08:09:		es1-7606-sd1	10.25.0.1	224.0.0.1	34	5	
ispiay Mil 103 v	rensions	Mon May 8 08:09:		es1-7606-sd1	10.25.0.1	224.0.0.1	34	5	
	~	Mon May 8 08:06:		es1-7606-sd1	10.25.0.1	224.0.0.1	12	5	
SEVT-TEST - 1	U devices:							5	
<u>s1-7206-w1</u>		Mon May 8 08:06:		es1-7606-sd1	10.25.0.1	224.0.0.1	34		
s1-7206-w2		Mon May 8 08:06:		es1-7606-sd1	10.25.0.1	224.0.0.1	15	5	
		Mon May 8 08:03:		es1-7606-sd1	10.25.0.1	224.0.0.1	34	5	
<u>s1-7606-c1</u>		Mon May 8 08:03:		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	
<u>s1-7606-c2</u>		Mon May 8 08:03:	00 2006	es1-7606-sd1	10.25.0.1	224.0.0.1	34	5	
s1-7606-c3		Mon May 8 08:00:	00 2006	es1-7606-sd1	10.25.0.1	224.0.0.1	19	5	
51 .000 00		Mon May 8 08:00:	00 2006	es1-7606-sd1	10.25.0.1	224.0.0.1	34	5	
<u>s1-7606-c4</u>		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:	0 2006	es1-7606-sd1	10.25.0.1	224.0.0.1	34	5	
<u>s1-7606-d1</u>		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		es1-7606-sd1			34	5	~

Figure 1-35 RPF Failures Report

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.

<u>File Edit View Favorites</u>	Tools	Help						
ddress 🕘 http://172.31.24.2	55 :8080/p	perl/home.pl						
🌀 Back 🔹 🕥 🐇 💌	2	🏠 🔎 Search 🤞	Favorites 🧭	🖉 · 🌺 🗹 ·	- 📕 🗱 🦓			
Cisco Multicast Manag	er 2.3.3	3						Cisc
Tool: Multicast Manage	er 🔽		Managemen	t Domain: IPmcLa	ab 🔽		Lice	الد. ensed to Ci
Home Top	ology	Reporting	Diagnostics	Help				
Reporting:			-					
Latest Events		Group Threshold	Report for 239.0	.0.1				
RP Polling Report								
RP Group Threshold Repo	ort	Hi Lo						
RPF Failures			Date	Router	Source	Group	Value	Thresh
Group Gone Report		Mon Aug 14 13:12	:00 2006	P3-msfc-2			13 pps	900 pps
S,G Threshold Report Layer 2 PPS Threshold Re		Mon Aug 14 13:12		P3-msfc-4			8 pps	900 pps
SSG Report	eport	Mon Aug 14 13:09		P3-msfc-2			8 pps	900 pps
Tree Report		Mon Aug 14 13:09		P3-msfc-4			8 pps	900 pps
S,G Delta Report		Mon Aug 14 13:09		P3-msfc-2				
Historical Graphs							8 pps	900 pps
Display All IOS Versions		Mon Aug 14 13:06		P3-msfc-4			13 pps	900 pps
	~	Mon Aug 14 13:03		P3-msfc-2			8 pps	900 pps
IPmcLab - 12 devices:		Mon Aug 14 13:03	:00 2006	P3-msfc-4			8 pps	900 pps
P2-7206-1		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
<u>P2-7206-2</u>		Mon Aug 14 12:57	:00 2006	P3-msfc-2			8 pps	900 pps
P2-ntv-1	=	Mon Aug 14 12:57	:00 2006	P3-msfc-4			8 pps	900 pps
1211011		Mon Aug 14 12:54	:00 2006	P3-msfc-2			8 pps	900 pps
<u>P2-ntv-2</u>		Mon Aug 14 12:54		P3-msfc-4			13 pps	900 pps
		Mon Aug 14 12:51		P3-msfc-2			8 pps	900 pps
<u>P2-ntv-3</u>		Mon Aug 14 12:51		P3-msfc-4			8 pps	900 pps
P2-ntv-4		Mon Aug 14 12:48		P3-msfc-2			13 pps	900 pps
<u>FZ-1107-4</u>		Mon Aug 14 12:48		P3-msfc-4			8 pps	900 pps
P3-7206-1		Mon Aug 14 12:46 Mon Aug 14 12:45		P3-msfc-2			8 pps	900 pps 900 pps
				P3-mstc-2 P3-msfc-4				
<u>P3-7206-2</u>		Mon Aug 14 12:45					8 pps	900 pps
		Mon Aug 14 12:42	2005	P3-msfc-2			8 pps	900 pps

Figure 1-36 S,G Threshold Report

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.



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

	224		01 F		11 01	e			
Cisco Multicast Mana File Edit View Favo		- Microso	nt internet Ex	cplorer provide	d by Cisco	Systems, In	Β.		
Address 🕘 http://es1-cmn	n:8080/perl/re	eport.pl#							
🚱 Back 🝷 🌍 🐇	🖹 🛃 🤇	🏠 🔎 Search 🛧 F	avorites 🔗	@ • 🎍	w • 🗾	12 🖏			
Cisco Multicast Mar	nager 2.3.4	4							Cisco
Tool: Multicast Man	ager 🔽		Managemei	nt Domain: g	tulumba	~		Lice	nsed to Cisco S
Home	Topology	Reporting	Diagnostics	Help					
Reporting: Latest Events RP Polling Report		Layer 2 Threshold F	Report for sw	vitch es1-375	0-a3 port	10101:Gi1	/0/1		
RP Group Threshold R RPF Failures	eport)ate		Switch	MI	B Port	PPS	Threshold
Group Gone Report					-3750-a3			45680	35000
S,G Threshold Report		Mon Aug 14 09:58:44				Input			
Layer 2 PPS Threshold	d Report	Mon Aug 14 09:58:42			-3750-a3	Input		45689	35000
SSG Report		Mon Aug 14 09:58:40			-3750-a3	Input		45677	35000
Tree Report S.G Delta Report		Mon Aug 14 09:58:38	2006	es1	-3750-a3	Input		45680	35000
Multicast Bandwidth R	eport	Mon Aug 14 09:58:36	2006	es1	-3750-a3	Input	: Gi1/0/1	45718	35000
Historical Graphs		Mon Aug 14 09:58:34	2006	es1	-3750-a3	Input	: Gi1/0/1	45674	35000
Display All IOS Versio	ins	Mon Aug 14 09:58:32	2006	es1	-3750-a3	Input	Gi1/0/1	45682	35000
	<u>^</u>	Mon Aug 14 09:58:30	2006	es1	-3750-a3	Input	Gi1/0/1	45693	35000
Search:		Mon Aug 14 09:58:28	2006	es1	-3750-a3	Input	Gi1/0/1	45681	35000
L	_	Mon Aug 14 09:58:26	2006	es1	-3750-a3	Input	Gi1/0/1	68519	35000
otulumba - 10 total de	evice	Mon Aug 14 09:58:24		es1	-3750-a3	Input		45681	35000
(s)		Mon Aug 14 09:58:22			-3750-a3	Input		45682	35000
<u>es1-7206-w1</u>		Mon Aug 14 09:58:22 Mon Aug 14 09:58:20			-3750-a3	Input		45682	35000
		Mon Aug 14 09:58:20 Mon Aug 14 09:58:18			-3750-a3	Input		45680	35000
<u>es1-7206-w2</u>		-			-3750-a3 -3750-a3			45681	35000
es1-7606-c1		Mon Aug 14 09:58:16				Input			
<u>C31 7000 C1</u>	_	Mon Aug 14 09:58:14			-3750-a3	Input		45690	35000
es1-7606-c2		Mon Aug 14 09:58:12			-3750-a3	Input		45676	35000
		Mon Aug 14 09:58:10			-3750-a3	Input		45685	35000
<u>es1-7606-c3</u>		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
<u>es1-7606-c4</u>	~	Mon Aug 14 09:58:04	2006	es1	-3750-a3	Input	Gi1/0/1	45683	35000

Figure 1-37 Layer 2 PPS Threshold Report

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.

ile <u>E</u> dit <u>V</u> iew F <u>a</u> vorites	<u>⊺</u> ools <u>H</u> elp			
dress 🕘 http://172.31.24.255	:8080/perl/home.pl			
🌏 Back 🔹 🕥 - 💌	🗿 🏠 🔎 Search	📩 Favorites 🚱 🍰	w • 📙 鑬 🦓	
Cisco Multicast Manager	2.3.3			Cisco
ensee Handease Hanager	21010			الس
Tool: Multicast Manager	*	Management Domain:	PmcLab 🔽	
Home Topolo	gy Reporting	Diagnostics Help		
eporting:	SSG Report f	for 220.0.0.1		
Latest Events	33d Report 1	Date	Grou	o Count
RP Polling Report RP Group Threshold Report	Mon Aug 14 13		239.0.0.1	93
RPF Failures	Mon Aug 14 13		239.0.0.1	93
Group Gone Report	-		239.0.0.1	93
S,G Threshold Report	Mon Aug 14 12			
Layer 2 PPS Threshold Repo			239.0.0.1	93
SSG Report	Mon Aug 14 12		239.0.0.1	94
Tree Report S.G Delta Report	Mon Aug 14 12	2:00:02 2006	239.0.0.1	94
Historical Graphs	Mon Aug 14 1:	1:45:03 2006	239.0.0.1	94
Display All IOS Versions	Mon Aug 14 1:	1:15:03 2006	239.0.0.1	94
	Mon Aug 14 1:	1:00:03 2006	239.0.0.1	94
IPmcLab - 12 devices:	Mon Aug 14 10	0:45:02 2006	239.0.0.1	94
P2-7206-1	Mon Aug 14 10	0:30:03 2006	239.0.0.1	94
	Mon Aug 14 10		239.0.0.1	94
<u>P2-7206-2</u>				
P2-ntv-1				
P2-ntv-2				
P2-ntv-3				
<u>12 1107 0</u>				
P2-ntv-4				
<u>P3-7206-1</u>				
P3-7206-2				

Figure 1-38 SSG Report

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).



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.

🕲 Cisco Multicast Manas		Mozilla Firefo				
	9					
Eile Edit View Go Ch	nipmarks E	jookmarks <u>T</u> ools <u>H</u> e	lp			Q
🔶 • 🔶 • 🛃 🙁	<u> </u>	http://172.31.24.255	:8080/perl/home.pl			O 60 C
Cisco Multicast Mana	ager 2.3.	3				Cisco Systems
Tool: Multicast Mana	iger 🔽			omain: IPmcLab 💌		Licensed to Cisco Systems
Home To	opology	Reporting	Diagnostics	Help		
Reporting:		Multicast Tree R	eport for paul99.tra	ce		
Latest Events			Date		Baseline	Change
RP Polling Report		Mon Aug 14 14:40			paul99.trace	trchanged
RP Group Threshold Re	port					
RPF Failures		Mon Aug 14 14:30			paul99.trace	trchanged
Group Gone Report		Mon Aug 14 11:35	:06 2006		paul99.trace	trchanged
S,G Threshold Report		Mon Aug 14 11:25	:04 2006		paul99.trace	trchanged
Layer 2 PPS Threshold SSG Report	Report	Mon Aug 14 11:20	:04 2006		paul99.trace	trchanged
Tree Report		Mon Aug 14 10:20			paul99.trace	trchanged
S,G Delta Report		Mon Aug 14 10:10			paul99.trace	trchanged
Historical Graphs						
Display All IOS Version	IS	Mon Aug 14 10:05			paul99.trace	trchanged
. ,		Mon Aug 14 09:55	:05 2006		paul99.trace	trchanged
IPmcLab - 12 device P2-7206-1	is) 📤					
<u>P2-7206-2</u>						
P2-ntv-1						
<u>P2-ntv-2</u>						
P2-ntv-3						
P2-ntv-4						
<u>P3-7206-1</u>						
<u>P3-7206-2</u>						ي ي
P3-msfc-1	~					180885
D2 mefe 2						~

Figure 1-39 Tree Report

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.

Untitled Docun	nent - Mozilla Firefox				
le <u>E</u> dit ⊻iew	<u>G</u> o ⊆hipmarks <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp				<
þ • 🖒 • 🔁	🕴 💿 🏠 🗋 http://172.31.24.255 :8080/p	erl/home.pl		~	
aul99.trace Mon	Aug 14 14:40:10 2006: Traced multicast gro	up 224.0.0.1 (cisco-rp-anno	unce [Farinacci]) from source 10	.0.0.1	
Router	Forwarding Int	Neighbor	Neighbor IP	Neighbor Int	
2-ntv-2	GigabitEthernet1/1	P2-7206-2	10.0.0.1	GigabitEthernet3/0	
2-ntv-2	Port-channel204	P2-ntv-4	10.0.0.1	Port-channel204	
2-ntv-2	Port-channel205	P2-ntv-3	10.0.0.1	Port-channel205	
2-7206-2	SRP1/0	P3-7206-2		SRP1/0	
3-7206-2	GigabitEthernet3/0	P3-msfc-2		Vlan2	
3-7206-2	GigabitEthernet4/0	P3-msfc-1		Vlan3	
3-msfc-2	Vlan4	P3-msfc-4		Vlan4	
3-msfc-2	Vlan5	P3-msfc-3		Vlan5	
2-ntv-1	GigabitEthernet1/1				
2-ntv-1	GigabitEthernet1/2				
2-ntv-1	Port-channel204				
2-ntv-1	Port-channel205				
2-ntv-1	Vlan210				
2-ntv-2	GigabitEthernet1/2				
2-ntv-2	Loopback0				
2-ntv-2					
2-ntv-3	Loopback0				
2-ntv-3	Loopback1				
2-ntv-4	FastEthernet3/1				
2-ntv-4	Loopback0				
2-ntv-4	Loopback1				
2-ntv-4	Vlan2				
2-ntv-4	Vlan20				
3-msfc-1	Vlan5				
3-msfc-4	Loopback0				
3-msfc-4	Loopback1				
3-msfc-4	Vlan30				
3-msfc-3	Loopback0				
3-msfc-3	Loopback1				
3-msfc-3	Vlan4				
2-ntv-2	GigabitEthernet1/2	P2-7206-1		GigabitEthernet4/0	
2-7206-1	SRP1/0	P3-7206-1		SRP1/0	
2-7206-2	SRP1/0				
3-7206-2	SRP1/0				
3-7206-2	GigabitEthernet3/0				

Figure 1-40 Tree Repor	t Page – Trchanged
------------------------	--------------------

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.

jle Edit ⊻jew Favorites <u>T</u> oo	ls <u>H</u> elp							
idress 🍓 http://es1-cmm:8080/perl	/report.pl#						✓	>
🌏 Back 🝷 🛞 🚪 🛃	🏠 🔎 Search 🚽	7 Favorites	Ø• 🎍 🗷	• 📙 🏭 🖇	8			
								_
Cisco Multicast Manager 2.3	3.3						CISCO SYSTEN	M S
Tool: Multicast Manager 💌		Manageme	ent Domain: SEV	/T-1 🔽		Licensed	to Cisco System	15
Home Topology	Reporting	Diagnostics	Help					
Reporting:	Multicast S,G Del		111100 11200					^
Latest Events	Multicast S,G Del		Baseline	Source	Group	PPS Deviation	Threshold	
RP Polling Report				239.0.0.1				
RP Group Threshold Report RPF Failures	Wed Aug 16 03:37		41tree.trace		232.1.1.1	5	1	
Group Gone Report	Wed Aug 16 03:36		41tree.trace	239.0.0.1	232.1.1.1	5	1	
S,G Threshold Report	Wed Aug 16 03:35		41tree.trace	239.0.0.1	232.1.1.1	6	1	
Layer 2 PPS Threshold Report	Wed Aug 16 03:34	:01 2006	41tree.trace	239.0.0.1	232.1.1.1	6	1	
SSG Report	Wed Aug 16 03:33	:01 2006	41tree.trace	239.0.0.1	232.1.1.1	2	1	
Tree Report	Wed Aug 16 03:32	:01 2006	41tree.trace	239.0.0.1	232.1.1.1	5	1	
S,G Delta Report Multicast Bandwidth Report	Wed Aug 16 03:31	:01 2006	41tree.trace	239.0.0.1	232.1.1.1	5	1	
Historical Graphs	Wed Aug 16 03:30	:01 2006	41tree.trace	239.0.0.1	232.1.1.1	6	1	
Display All IOS Versions	Wed Aug 16 03:29		41tree.trace	239.0.0.1	232.1.1.1	5	1	
	Wed Aug 16 03:28		41tree.trace	239.0.0.1	232.1.1.1	5	1	
Search:	Wed Aug 16 03:27		41tree.trace	239.0.0.1	232.1.1.1	2	1	
Startin	Wed Aug 16 03:26		41tree.trace	239.0.0.1	232.1.1.1	6	1	
SEVT-1 - 11 total device(s)	Wed Aug 16 03:26 Wed Aug 16 03:25		41tree.trace	239.0.0.1	232.1.1.1	6	1	
es1-7206-w1						5	-	
<u></u>	Wed Aug 16 03:24		41tree.trace	239.0.0.1	232.1.1.1		1	
es1-7206-w2	Wed Aug 16 03:23		41tree.trace	239.0.0.1	232.1.1.1	6	1	
	Wed Aug 16 03:22		41tree.trace	239.0.0.1	232.1.1.1	5	1	
es1-7606-c1	Wed Aug 16 03:21		41tree.trace	239.0.0.1	232.1.1.1	6	1	
es1-7606-c2	Wed Aug 16 03:20		41tree.trace	239.0.0.1	232.1.1.1	5	1	
<u>851-7606-02</u>	Wed Aug 16 03:19	:01 2006	41tree.trace	239.0.0.1	232.1.1.1	5	1	
es1-7606-c3	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	
es1-7606-c4	Med Wild TO 02:TO							

Figure 1-41	Multicast S,G Delta Report
-------------	----------------------------

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.



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

- - 🔁	I 😢 🏠 🗈	http://172.31.24.255	:8080/perl/home.pl				*	
								CISCO SYSTEMS
Cisco Multicast	Manager 2.3.	3						ահուսդիր
Tool: Multicast	Manager 🔽			t Domain:	IPmcLab 🔽			Cisco Systems
Home	Topology	Reporting	Diagnostics	Help				
eporting:		S,G PPS (Selec	t O Maul					<u>~</u>
atest Events		S,G PPS (Selec	(3 Max)					
P Polling Report				i and				
RP Group Thresh	old Report	239.0.0.2:10.0.0		^				
PF Failures		239.0.0.1:10.0.0	.2:P2-ntv-2					
Group Gone Repo GG Threshold Re	ort	239.0.0.3:10.0.0	3·P3-msfc-3					
ayer 2 PPS Thre		200.0.0.0.10.0.0	.0.1 0 11010 0					
SG Report	istiola Report							
ree Report								
S,G Delta Report								
istorical Graphs								
Display All IOS V								
IPmcLab - 12 mu devices: P2-7206-1	ulticast							
P2-7206-2				~				
<u>P2-ntv-1</u>		Display						
P2-ntv-2		5	,G PPS:Source:O.	0.0.0 Grou	p:239.0.0.2	REDTO		
P2-ntv-3		1.0						
P2-ntv-4						OBI OEI		
P3-7206-1		۵.5 0.5				TREP		
P3-7206-2		0.0						
P3-msfc-1		0.0	14:50 15	:00 15:	10 15:20	15:30		
	~	P2-ntu_4 D P	2-ntv-3 📕 P2-ntv-:					

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

🔁 • 🔷 • 🛃 (2 🟠 🛄) http://172.31	×			
Cisco Multicast Ma		3				CISCO SYSTEMS attilitionatilitie
Tool: Multicast Ma				Management Domai		Licensed to Cisco Systems
Home	Topology	Report	ing	Diagnostics He	lp	
Reporting:		IOS Versio	on Info			
Latest Events RP Polling Report RP Group Threshold	Report	Report Gene 12 Devices	erated: F	ri Aug 11 15:51:20 2006		
RPF Failures Group Gone Report		DEVICE	IP	VERSION	MODEL	
S,G Threshold Report		P2-7206-1	-	Version 12.4(3)	cisco7206VXR	
Layer 2 PPS Thresho		P2-7206-2		Version 12.4(3)	cisco7206VXR	
SSG Report						
Tree Report		P2-ntv-1			cat6506	
S,G Delta Report		P2-ntv-2		Version 12.2(18)SXD5		
Historical Graphs Display All IOS Vers	ione	P2-ntv-3	10.0.0.1	Version 12.2(18)SXF2	cat6506	
Display Mil 103 Vers		P2-ntv-4	10.0.0.1	Version 12.2(18)SXF3	cat6506	
IPmcl ab - 12 multic		P3-7206-1	10.0.0.1	Version 12.4(3)	cisco7206VXR	
devices:	ast 📄	P3-7206-2	10.0.0.1	Version 12.4(3)	cisco7206VXR	
P2-7206-1		P3-msfc-1	10.0.0.1	Version 12.2(17d)SXB6	catalyst6kSup720	
		P3-msfc-2		Version 12.2(17d)SXB6		
P2-7206-2		P3-msfc-2 P3-msfc-3		Version 12.1(26)E2	catalyst6kMsfc2	
P2-ntv-1						
<u>12 mm 1</u>		P3-msfc-4	10.0.0.1	Version 12.1(26)E2	catalyst6kMsfc2	
P2-ntv-2						
P2-ntv-3						
P2-ntv-4						
<u>P3-7206-1</u>						
<u>P3-7206-2</u>						

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

🛯 • 🖒 • 🛃 .	🗵 🏠 🚺	http://172.31.24.255 :8	3080/perl/home.pl			v
Cisco Multicast M		3				Cisco System authorithm
	lanager 💌			nt Domain: IPmcLab	×	Licensed to Cisco Systems
Home	Topology	Reporting	Diagnostics	Help		
iagnostics:		Grap	oh Line 💌			1
Show All Groups						
ocate Host		Valu	ue bps 🚩			
letwork Status						
IP Status IP Summary			Plot			
GMP Diagnostics						
ISDP Status		Trace selected so	urce and group	between the routers	below:	
ayer 2 Switches			IR SOURCE			
lealth Check		ГГ	IN SUURCE			
500 Troubleshoot	ing	16	IR ALL			
Fop Talkers						
			Trace			
			11000			
PrncLab - 12 multi levices:	icast 😑		(- ()		
2-7206-1		Group (4) Grou		Group (DB)		Source (DB) Number of Sources
272001		<u>224.0.0.1</u>		rp-announce [Farinacci]	10.0.0.1	Sources [3]
2-7206-2		224.0.0.1	cisco-	p-discovery [Farinacci]	10.0.0.1	Sources [6]
		224.0.0.1			10.0.0.1	Sources [0]
<u>2-ntv-1</u>		224.0.0.1			10.0.0.1	Sources [0]
2-ntv-2						
2-1107-2		View previously s	aved source br	s/pps files		
2-ntv-3		Select Fi				
2-ntv-4			Display			
<u>93-7206-1</u>			- Bropidy			
93-7206-2	_	View previously s				
		Select Tra	ce paul99.trace	*		
23-msfc-1						

(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).

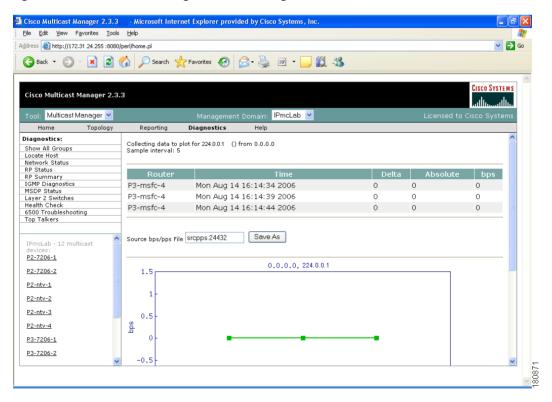
Note If the device is a 6500, you may need to adjust the sampling period in order to generate useful data.

- 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



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.



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.

Image: Provide and Provided And Pr	1 N					
Router Forwarding Int Neighbor Neighbor IP Neighbor Int 22-nty-2 Gi/1 P2-7205-2 100.01 Gi3/0 22-nty-2 Pa204 P2-nty-4 100.01 Pa204 22-nty-2 Pa205 P2-nty-4 100.01 Pa204 22-rty-2 SRJ/0 P3-7206-2 100.01 SRJ/0 22-rty-2 Gi3/0 P3-7306-2 100.01 VI2 23-7206-2 Gi3/0 P3-msfc-2 100.01 VI2 23-7206-2 Gi3/0 P3-msfc-2 100.01 VI3 23-7206-2 Gi3/0 P3-msfc-3 100.01 VI3 23-msfc-2 VI4 P3-msfc-4 100.01 VI5 22-nty-1 GigabitEthernet1/2 P3-msfc-3 100.01 VI5 22-nty-1 GigabitEthernet1/2 P3-msfc-4 100.01 VI5 22-nty-1 GigabitEthernet1/2 P3-msfc-4 100.01 VI5 22-nty-2 Loopback0(* Local address loopback *) P3-msfc-4 100.01 VI6 </th <th></th> <th>Altp://172.31.24.255 :8080/perl/home.pl</th> <th></th> <th>*</th> <th></th> <th></th>		Altp://172.31.24.255 :8080/perl/home.pl		*		
22-ntv-2 Gil/1 P2-7206-2 10.0.1 Gi3/0 22-ntv-2 P0204 P2-ntv-4 10.0.0.1 P0204 22-ntv-2 P0205 P2-ntv-4 10.0.0.1 P0205 22-7206-2 SR1/0 P3-7206-2 10.0.0.1 SR1/0 37206-2 Gi3/0 P3-msfc-2 10.0.0.1 VI2 33-msfc-2 Gi4/0 P3-msfc-1 10.0.0.1 VI3 33-msfc-2 VI4 P3-msfc-3 10.0.0.1 VI4 33-msfc-2 VI5 P3-msfc-4 10.0.0.1 VI4 3-msfc-2 VI5 P3-msfc-3 10.0.0.1 VI5 2-ntv-1 GigabitEthernet1/2 P3-msfc-4 10.0.0.1 VI5 2-ntv-1 Port-channel204 P3-msfc-3 10.0.0.1 VI5 2-ntv-1 Port-channel205 P3-msfc-3 10.0.1 VI5 2-ntv-1 Vanto Vanto P3-msfc-3 10.0.1 VI4 2-ntv-2 GigabitEthernet1/2 P3-msfc-3 10.0.1 VI4 10.0.1 VI4 2-ntv-4 Vanto Vanto Vant	racing multica	ast group 224.0.0.1 () from source 10.0.0.1				_
P2-ntv-2 P204 P001 P004 P2-ntv-2 P0205 P2-ntv-3 100.01 P0205 P2-7206-2 SR1/0 P3-7206-2 100.01 VR1/0 P3-7206-2 Gi3/0 P3-m6-2 100.01 VI2 P3-7206-2 Gi3/0 P3-m6-2 100.01 VI3 P3-7206-2 Gi3/0 P3-m6-2 100.01 VI3 P3-m6-2 VI4 P3-m6-3 100.01 VI4 P3-m6-2 VI5 P3-m6-3 100.01 VI5 P3-m5-2 VI5 P3-m6-3 100.01 VI5 P3-m5-2 VI5 P3-m5-3 100.01 VI5 P2-ntv1 GigabitEthernet1/1 P1-channel204 P1-channel205 P1-channel205 P2-ntv1 VIa200 P1-channel205 P1-channel205 P1-channel205 P1-channel205 P2-ntv2 Lopback(1** Campus RP Address Lopback *) P1-channel205 P1-channel205 P1-channel205 P2-ntv4 Lopback(1** Campus RP Address, 239.255.0.0/16 **) P1-channel205 P1-channel205 P1-channel205 P2-ntv4 Lopback(1** Camp	Router	Forwarding Int	Neighbor	Neighbor IP	Neighbor Int	
P2:nty-2 P2:05 P2:nty-3 100.01 P0:05 P2:7206-2 SR1/0 P3:7206-2 100.01 SR1/0 P3:7206-2 Gi/0 P3:nsfo-2 100.01 V12 P3:7206-2 Gi/0 P3:nsfo-4 100.01 V12 P3:rsfo-2 VI4 P3:nsfo-4 100.01 V14 P3:rsfo-2 VI5 P3:nsfo-4 100.01 V15 P2:ntv1 GigabitEthernet1/2 P3:nsfo-3 100.01 V15 P2:ntv1 GigabitEthernet1/2 P3:nsfo-3 100.01 V15 P2:ntv1 Port-channel204 P3:nsfo-3 100.01 V16 P2:ntv1 V1a10 P1:nstineereereereereereereereereereereereereer	2-ntv-2	Gi1/1	P2-7206-2	10.0.0.1	Gi3/0	
22-7206-2 SR1/0 P3-7206-2 10.0.1 SR1/0 33-7206-2 Gi/0 P3-msfc-2 10.0.1 V12 33-7206-2 Gi/0 P3-msfc-2 10.0.1 V12 33-7206-2 Gi/0 P3-msfc-2 10.0.1 V13 33-msfc-2 V4 P3-msfc-4 10.0.1 V14 33-msfc-2 V15 P3-msfc-4 10.0.1 V14 23-msfc-2 Sigabilithernet1/1 P3-msfc-3 10.0.1 V15 22-ntv-1 Gigabilithernet1/2 P3-msfc-4 10.0.1 V16 22-ntv-1 Port-channel204 P3-msfc-3 10.0.1 P3-msfc-2 22-ntv-1 Port-channel204 P3-msfc-3 P3-msfc-4 P3-msfc-3 22-ntv-2 Gigabilithernet1/2 P3-msfc-3 P3-msfc-3 P3-msfc-3 22-ntv-2 Gipabak0(* Local address loopback *) P3-msfc-4 P3-msfc-4 P3-msfc-4 22-ntv-4 Loopback0(** Campus RP Address, 239.255.0.0/16 **) P3-msfc-3 P3-msfc-1 P3-msfc-4 22-ntv-4 Loopback0(** Campus RP Address, 239.255.0.0/16 **) P3-msfc-4 P3-msfc-4 P3-msfc-4 22-ntv-4 Loopback0(** Management **) P3-msfc-4 P3-msfc-4 P3-msfc-4 23-msfc-4 Loo	2-ntv-2	Po204	P2-ntv-4	10.0.0.1	Po204	
93-7206-2 Gi3/0 P3-msfc-2 10.0.0.1 VI2 93-7206-2 Gi4/0 P3-msfc-4 10.0.0.1 VI3 93-7206-2 VI4 P3-msfc-4 10.0.0.1 VI4 93-msfc-2 VI5 P3-msfc-3 10.0.1 VI5 93-msfc-2 Gigabitthernett/1 P3-msfc-3 10.0.1 VI5 92-ntv-1 Gigabitthernett/2 P3-msfc-3 10.0.1 VI5 92-ntv-1 Gigabitthernet1/2 P3-msfc-3 10.0.1 VI5 92-ntv-1 Gigabitthernet1/2 P3-msfc-3 10.0.1 P3-msfc-3 92-ntv-1 Port-channel205 P3-msfc-3 P3-msfc-3 P3-msfc-3 92-ntv-2 Loopback0(* Local address loopback *) P3-msfc-3 P3-msfc-3 P3-msfc-3 92-ntv-3 Loopback1(** Campus RP Address, 239.255.0.0/16 **) P3-msfc-3 P3-msfc-3 P3-msfc-3 92-ntv-4 Loopback1(** Campus RP Address, 239.255.0.0/16 **) P3-msfc-3 P3-msfc-4 P3-msfc-3 93-msfc-4 Loopback0(** Management **) P3-msfc-4 P3-msfc-4 P3-msfc-4 93-msfc-4 Loopback0(** Management **) P3-msfc-3 P3-msfc-4 P3-msfc-3 93-msfc-3 Loopback0(** Management **) P3-msfc-3 P3-msfc-3 P3	2-ntv-2	Po205	P2-ntv-3	10.0.0.1	Po205	
93-7206-2 Gi4/0 P3-msfc-1 10.0.1 VI3 93-msfc-2 VI4 P3-msfc-3 10.0.1 VI4 93-msfc-2 VI5 P3-msfc-3 10.0.1 VI5 93-msfc-2 VI5 10.0.1 VI5 93-msfc-2 VI5 10.0.1 VI5 93-msfc-3 10.0.1 VI5 92-ntv-1 GigabitThernet1/2 1 1 92-ntv-1 Port-channel205 1 1 1 92-ntv-2 GigabitThernet1/2 1 1 1 92-ntv-1 Port-channel205 1 1 1 92-ntv-2 GigabitThernet1/2 1 1 1 92-ntv-2 GigabitThernet1/2 1 1 1 92-ntv-2 GigabitThernet1/2 1 1 1 92-ntv-3 Loopback0(* Local address loopback *) 1 1 1 92-ntv-4 Loopback0 1 1 1 1 92-ntv-4 Loopback1(** Campus RP Address, 239,255.0.0/16 **) 1 1 1 92-ntv-4 Loopback0(** Maagement **) 1 1 1 93-msfc-4 Loopback0(** Maagement **) 1 1 1 93-msfc	2-7206-2	SR1/0	P3-7206-2	10.0.0.1	SR1/0	
33-msfc-2 VI P3-msfc-4 10.0.1 VI4 93-msfc-2 VI5 P3-msfc-3 10.0.1 VI5 92-ntv-1 GigabitEthernet1/2 Pat-channel204 P3 P3 92-ntv-1 VIan210 P3 P3 P3 P3 92-ntv-2 Loopback(0** Local address loopback *) P3 P3 P3 P3 92-ntv-3 Loopback(1** Campus RP Address, 239.255.0.0/16 **) P3 P3 P3 P3 92-ntv-4 FastEthernet3/1 P3 P3 P3 P3 P3 92-ntv-4 Loopback(1** Campus RP Address, 239.255.0.0/16 **) P3 P3 P3 P3 92-ntv-4 Loopback(1** Campus RP Address, 239.255.0.0/16 **) P3 P3 P3 P3 92-ntv-4 Loopback(1** Campus RP Address, 239.255.0.0/16 **) P3 P3 P3 P3 92-ntv-4 VIan20 P3 P3 P3 P3 P3 93-msfc-3 Loopback(1** Campus RP Address, 239.255.0.0/16 **) P3 P3 <td>93-7206-2</td> <td>Gi3/0</td> <td>P3-msfc-2</td> <td>10.0.0.1</td> <td>VI2</td> <td></td>	93-7206-2	Gi3/0	P3-msfc-2	10.0.0.1	VI2	
P3-msfo-2 VIS P3-msfo-3 10.0.1 VIS P2-ntv-1 GigabitEthernet1/2 Image: Constraint of the	93-7206-2	Gi4/0	P3-msfc-1	10.0.0.1	VI3	
22-rtv-1 GigabitEthernet1/1 22-rtv-1 GigabitEthernet1/2 22-rtv-1 Port-channel204 22-rtv-1 Port-channel205 22-rtv-1 Port-channel205 22-rtv-2 GigabitEthernet1/2 22-rtv-2 GigabitEthernet1/2 22-rtv-2 GigabitEthernet1/2 22-rtv-2 Loopback(1* Local address loopback *) 22-rtv-3 Loopback(1** Campus RP Address, 239.255.0.0/16 **) 22-rtv-4 Loopback(1** Campus RP Address, 239.255.0.0/16 **) 22-rtv-4 Loopback0 22-rtv-4 Loopback0 22-rtv-4 Loopback0 22-rtv-4 Loopback0 22-rtv-4 Loopback0 22-rtv-4 Loopback0 22-rtv-4 Vlan20 23-rmsfc-1 Vlan5 23-rmsfc-4 Loopback(1** Campus RP Address, 239.255.0.0/16 **) 23-rmsfc-4 Loopback(1** Campus RP Address, 239.255.0.0/16 **) 23-rmsfc-4 Loopback(1** Campus RP Address, 239.255.0.0/16 **) 23-rmsfc-3 Loopback(1** Campus RP Address, 239.255.0.0/16 **) 23-rmsfc-3 Loopback(1** Campus RP Address, 239.255.0.0/16 **)	93-msfc-2	Vl4	P3-msfc-4	10.0.0.1	VI4	
GigabitEthernet1/2 2r.htv-1 Port-channel204 2r.htv-1 Port-channel205 2r.htv-1 Vlan210 2r.htv-1 Vilan210 2r.htv-1 Vilan210 2r.htv-1 Vilan210 2r.htv-2 Loopback0(* Local address loopback *) 2r.htv-3 Loopback1(** Campus RP Address, 239.255.0.0/16 **) 2r.htv-4 Vlan20 3r.mtfo-1 Vlan5 3r.mtfo-4 Loopback1(** Campus RP Address, 239.255.0.0/16 **) 3r.mtfo-4 Loopback1(** Management **) 3r.mtfo-3 Loopback1(** Campus RP Address, 239.255.0.0/16 **) 3r.mtfo-3 Loopb	3-msfc-2	VI5	P3-msfc-3	10.0.0.1	VI5	
Port-channel204 Port-channel205 Port-channel3/1 Port-channel3/1 Port-channel3/1 Port-channel3/1 Port-chanet**) Poopback1(** Cam	2-ntv-1	GigabitEthernet1/1				
22.ntv-1 Port-channel205 22.ntv-1 Vla210 22.ntv-2 GigabitEthernet1/2 22.ntv-2 Loopback(0** Local address loopback *) 22.ntv-3 Loopback(1** Campus RP Address, 239.255.0.0/16 **) 22.ntv-4 FastEthernet3/1 22.ntv-4 Loopback(1** Campus RP Address, 239.255.0.0/16 **) 22.ntv-4 Vlan2 23.nts/c-1 Vlan5 23.nts/c-4 Loopback(1** Campus RP Address, 239.255.0.0/16 **) 23.nts/c-5 Loopback(1** Campus RP Address, 239.255.0.0/16 **) 24.ntv-6 Loopback(1** Campus RP Address, 239.255.0.0	2-ntv-1	GigabitEthernet1/2				
22-rtv-1 Vlan210 22-rtv-2 GigabitEthernet1/2 1 Loopback(0'coal address loopback *) 22-rtv-2 Ioopback(0' 22-rtv-3 Loopback(0' 22-rtv-3 Loopback(1** Campus RP Address, 239.255.0.0/16 **) 22-rtv-4 FastEthernet3/1 22-rtv-4 Loopback(1** Campus RP Address, 239.255.0.0/16 **) 22-rtv-4 Loopback(1** Campus RP Address, 239.255.0.0/16 **) 22-rtv-4 Loopback(1** Campus RP Address, 239.255.0.0/16 **) 22-rtv-4 Vlan2 22-rtv-4 Vlan2 22-rtv-4 Loopback(0** Management **) 33-msfc-4 Loopback(1** Campus RP Address, 239.255.0.0/16 **) 23-msfc-4 Loopback(1** Management **) 23-msfc-3 Loopback(1** Campus RP Address, 239.255.0.0/16 **) 23-msfc-3 Vlan2 <td< td=""><td>2-ntv-1</td><td>Port-channel204</td><td></td><td></td><td></td><td></td></td<>	2-ntv-1	Port-channel204				
22.ntv-2 Gigabilithemett/2 22.ntv-2 Loopback(* Local address loopback *) 22.ntv-3 Loopback(** Campus RP Address, 239.255.0.0/16 **) 22.ntv-4 FastEthermet3/1 22.ntv-4 Loopback(** Campus RP Address, 239.255.0.0/16 **) 22.ntv-4 Loopback(** Campus RP Address, 239.255.0.0/16 **) 22.ntv-4 Loopback(** Campus RP Address, 239.255.0.0/16 **) 22.ntv-4 Vlan2 22.ntv-4 Vlan2 23.ntv-4 Vlan2 23.ntv-4 Loopback(** Campus RP Address, 239.255.0.0/16 **) 23.ntv-4 Vlan30 23.ntv-4 Loopback(** Campus RP Address, 239.255.0.0/16 **) 23.ntv-4 Vlan30 23.ntv-4 Loopback(** Campus RP Address, 239.255.0.0/16 **) 23.ntv-4 Vlan30 23.ntv-4 Vlan30 23.ntv-4 Vlan30 23.ntv-53 Loopback(** Campus RP Address, 239.255.0.0/16 **) 23.ntv-63 Loopback(** Campus RP Address, 239.255.0.0/16 **) 24.ntv-6 Save As	2-ntv-1	Port-channel205				
12-nty-2 Loopback(0* Local address loopback *) 2-nty-3 Loopback(1** Campus RP Address, 239.255.0.0/16 **) 2-nty-4 Vlan20 3-msfc-4 Loopback(1** Campus RP Address, 239.255.0.0/16 **) 3-msfc-3 Loopback(1** Campus RP Address, 239.255.0.0/16 **) 3-msfc-3 Loopback(1** Campus RP Address, 239.255.0.0/16 **) 3-msfc-3 Loopback(1** Campus RP Address, 239.255.0.0/16 **) 3-msfc-4 Loopback(1** Campus RP Address, 239.255.0.0/16 **) 3-msfc-3 Loopback(1** Campus RP Address, 239.255.0.0/16 **) 3-msfc-3 Loopback(1** Campus RP Address, 239.255.0.0/16 **) 3-msfc-4 Loopback(1** Campus RP Address, 239.255.0.0/16 **)	2-ntv-1	Vlan210				
22-nty-2 Loopback0 22-nty-3 Loopback1(** Campus RP Address, 239.255.0.0/16 **) 22-nty-4 FastEthernet3/1 22-nty-4 Loopback0 22-nty-4 Loopback1(** Campus RP Address, 239.255.0.0/16 **) 22-nty-4 Loopback1(** Campus RP Address, 239.255.0.0/16 **) 22-nty-4 Vlan2 22-nty-4 Vlan2 22-nty-4 Vlan2 23-msfc-1 Vlan5 33-msfc-4 Loopback1(** Management **) 23-msfc-4 Loopback0(** Management **) 23-msfc-3 Loopback0(** Management **) 23-msfc-3 Loopback0(** Campus RP Address, 239.255.0.0/16 **) 23-msfc-4 Vlan30 23-msfc-3 Loopback1(** Campus RP Address, 239.255.0.0/16 **) 23-msfc-3 Vlan4	2-ntv-2	GigabitEthernet1/2				
22-ntv-3 Loopback1(** Campus RP Address, 239.255.0.0/16 **) 22-ntv-4 Loopback1(** Campus RP Address, 239.255.0.0/16 **) 22-ntv-4 Loopback1(** Campus RP Address, 239.255.0.0/16 **) 22-ntv-4 Vlan2 27-ntv-4 Loopback0(** Management **) 28-nmfc-3 Loopback1(** Campus RP Address, 239.255.0.0/16 **) 29-nmfc-3 Loopback1(** Campus RP Address, 239.255.0.0/16 **) 29-nmfc-3 Loopback1(** Campus RP Address, 239.255.0.0/16 **) 29-nmfc-3 Vlan4 29-nmfc-3 Vlan4	2-ntv-2	Loopback0(* Local address loopback *)				
22-ntv-3 Loopback1(** Campus RP Address, 239.255.0.0/16 **) 22-ntv-4 FastEthernet3/1 22-ntv-4 Loopback1(** Campus RP Address, 239.255.0.0/16 **) 22-ntv-4 Loopback1(** Campus RP Address, 239.255.0.0/16 **) 22-ntv-4 Vlan20 23-msfc-1 Vlan5 37-msfc-4 Loopback0(** Management **) 37-msfc-4 Loopback0(** Management **) 37-msfc-4 Loopback0(** Management **) 37-msfc-3 Loopback0(** Management **) 37-msfc-3 Loopback0(** Campus RP Address, 239.255.0.0/16 **) 37-msfc-4 Vlan20 37-msfc-4 Vlan20 37-msfc-4 Loopback1(** Campus RP Address, 239.255.0.0/16 **) 37-msfc-3 Loopback1(** Campus RP Address, 239.255.0.0/16 **)	2-ntv-2					
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 Vlan2 P3-msfc-1 Vlan5 P3-msfc-4 Loopback1(** Campus RP Address, 239.255.0.0/16 **) P3-msfc-4 Loopback1(** Campus RP Address, 239.255.0.0/16 **) P3-msfc-3 Loopback1(** Campus RP Address, 239.255.0.0/16 **)	2-ntv-3	Loopback0				
22-ntv-4 Loopback1(** Campus RP Address, 239.255.0.0/16 **) 22-ntv-4 Vlan20 23-msfc-1 Vlan2 33-msfc-4 Loopback1(** Campus RP Address, 239.255.0.0/16 **) 33-msfc-3 Loopback1(** Campus RP Address, 239.255.0.0/16 **) 33-msfc-3 Loopback1(** Campus RP Address, 239.255.0.0/16 **) 33-msfc-4 Loopback1(** Campus RP Address, 239.255.0.0/16 **) 33-msfc-3 Loopback1(** Campus RP Address, 239.255.0.0/16 **) 33-msfc-4 Loopback1(** Campus RP Address, 239.255.0.0/16 **) 33-msfc-3 Loopback1(** Campus RP Address, 239.255.0.0/16 **) 33-msfc-4 Loopback1(** Campus RP Address, 239.255.0.0/16 **) 34-msfc-3 Vlan4	2-ntv-3	Loopback1(** Campus RP Address, 239.255.0.0/16 **)				
22-nty-4 Loopback1(** Campus RP Address, 239.255.0.0/16 **) 22-nty-4 Vlan2 22-nty-4 Vlan2 23-msfc-1 Vlan5 33-msfc-4 Loopback0(** Management **) 23-msfc-4 Loopback1(** Campus RP Address, 239.255.0.0/16 **) 23-msfc-4 Loopback0(** Management **) 23-msfc-4 Loopback0(** Management **) 23-msfc-3 Loopback0(** Campus RP Address, 239.255.0.0/16 **) 23-msfc-3 Loopback1(** Campus RP Address, 239.255.0.0/16 **) 23-msfc-3 Loopback1(** Campus RP Address, 239.255.0.0/16 **) 23-msfc-3 Vlan4	2-ntv-4	FastEthernet3/1				
V2-ntv-4 Vlan2 V2-ntv-4 Vlan20 3rmsfc-1 Vlan50 3rmsfc-4 Loopback0(** Management **) 3rmsfc-4 Vlan30 3rmsfc-4 Vlan30 3rmsfc-3 Loopback0(** Management **) 3rmsfc-3 Loopback0(** Management **) 3rmsfc-3 Loopback0(** Campus RP Address, 239.255.0.0/16 **) 3rmsfc-3 Loopback0(** Campus RP Address, 239.255.0.0/16 **) 3rmsfc-3 Vlan4	2-ntv-4	Loopback0				
V2-ntv-4 Vlan2 V2-ntv-4 Vlan20 3rmsfc-1 Vlan50 3rmsfc-4 Loopback0(** Management **) 3rmsfc-4 Vlan30 3rmsfc-4 Vlan30 3rmsfc-3 Loopback0(** Management **) 3rmsfc-3 Loopback0(** Management **) 3rmsfc-3 Loopback0(** Campus RP Address, 239.255.0.0/16 **) 3rmsfc-3 Loopback0(** Campus RP Address, 239.255.0.0/16 **) 3rmsfc-3 Vlan4	2-ntv-4	Loopback1(** Campus RP Address, 239.255.0.0/16 **)				
13-msfc-1 Vlan5 3-msfc-4 Loopback0(** Management **) 3-msfc-4 Loopback1(** Campus RP Address, 239,255.0.0/16 **) 3-msfc-4 Vlan30 3-msfc-3 Loopback1(** Campus RP Address, 239,255.0.0/16 **) 3-msfc-3 Loopback1(** Campus RP Address, 239,255.0.0/16 **) 3-msfc-3 Loopback1(** Campus RP Address, 239,255.0.0/16 **) 3-msfc-3 Vlan4						
93-msfc-1 Vlan5 93-msfc-4 Loopback0(** Management **) 93-msfc-4 Loopback1(** Campus RP Address, 239.255.0.0/16 **) 93-msfc-4 Vlan30 93-msfc-3 Loopback1(** Campus RP Address, 239.255.0.0/16 **) 93-msfc-3 Loopback1(** Campus RP Address, 239.255.0.0/16 **) 93-msfc-3 Loopback1(** Campus RP Address, 239.255.0.0/16 **) 93-msfc-3 Vlan4						
37-msfc-4 Loopback1(** Campus RP Address, 239.255.0.0/16 **) 29-msfc-4 Vlan30 37-msfc-4 Loopback1(** Management **) 37-msfc-3 Loopback1(** Campus RP Address, 239.255.0.0/16 **) 39-msfc-3 Loopback1(** Campus RP Address, 239.255.0.0/16 **) 39-msfc-3 Vlan4 7-race File Save As	- 93-msfc-1	Vlan5				
37-msfc-4 Loopback1(** Campus RP Address, 239.255.0.0/16 **) 29-msfc-4 Vlan30 37-msfc-4 Loopback1(** Management **) 37-msfc-3 Loopback1(** Campus RP Address, 239.255.0.0/16 **) 39-msfc-3 Loopback1(** Campus RP Address, 239.255.0.0/16 **) 39-msfc-3 Vlan4 7-race File Save As						
V3amsfc-4 Vlan 30 V3amsfc-3 Loopback0(** Management **) y3amsfc-3 Loopback1(** Campus RP Address, 239.255.0.0/16 **) v3amsfc-3 Vlan4						
P3-msfc-3 Loopback1(** Campus RP Address, 239,255.0.0/16 **) P3-msfc-3 Vlan4 race File trace.276						
P3-msfc-3 Loopback1(** Campus RP Address, 239,255.0.0/16 **) P3-msfc-3 Vlan4 race File trace.276	93-msfc-3	Loopback0(** Management **)				
P3-msfc-3 Vlan4						
rrace File trace.276 Save As	3-msfc-3					
	race File trac	ce.276 Save As				
Rendezvous Point Router Interface						_
	Rendezvo	us Point Router Interface				
						_

Figure 1-46 Drawing a Multicast Tree (Baseline)

• 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).



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

Untitled Document - Mozilla	Firefox	
jile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> hipmarks	<u>B</u> ookmarks <u>T</u> ools <u>H</u> elp	
🖕 • 🍌 • 🎜 🙁 🚷	http://172.31.24.255 :8080/perl/ho	ome.pl
Show Command Username Password	Show	
pMRouteEntry Query for P2 Shortest Path Tree:True	-ntv-1 (10.0.0.1) (10.0.0.1	1, 234.0.0.2)
MIB	Value	Description
ipMRouteDifferentInIfPackets	347275	Number of packets dropped because they were received on the wrong interface
pMRouteExpiryTime	0:02:57	Time left before entry will be aged out
pMRouteInIfInde×	Loopback1	Incoming Interface
pMRouteOctets	0	Number of octets received from/to this source/group AND forwarded
pMRouteOctets pMRoutePkts	0	
pMRoutePkts		Number of octets received from/to this source/group AND forwarded
, pMRoutePkts pMRouteProtocol	0	Number of octets received from/to this source/group AND forwarded Number of packets received from/to this source/group other(1), local(2), netumm(13), dwnrp(4), mospf(5), pimSparseDense(6), cbt(7), pimSparseMode(8),
, pMRoutePkts pMRouteProtocol pMRouteRtAddress	0 9	Number of octets received from/to this source/group AND forwarded Number of packets received from/to this source/group other(1), local(2), netmgmt(3), dvmrp(4), mospf(5), pimSparseDense(6), cbt(7), pimSparseMode(8), pimDenseMode(9), jempOnly(10)
pMRoutePkts pMRouteProtocol pMRouteRtAddress pMRouteRtMask	0 9 11.51.70.1	Number of octets received from/to this source/group AND forwarded Number of packets received from/to this source/group other(1), local(2), netmomt(3), dvmp(4), mospf(5), pimSparseDense(6), cbt(7), pimSparseMode(8), pimDenseMode(9), ipmpOn(y(10) The address portion of the route used for this multicast forwarding entry
pMRoutePkts pMRouteProtocol pMRouteRtAddress pMRouteRtMask pMRouteRtProto	0 9 11.51.70.1 255.255.255.255	Number of octets received from/to this source/group AND forwarded Number of packets received from/to this source/group other(1), local(2), netmgmt(3), dvmrp(4), mospf(5), pimSparseDense(6), cbt(7), pimSparseMode(8), pimDenseMode(9), jompOnly(10) The address portion of the route used for this multicast forwarding entry The mask associated with the route used for this multicast forwarding entry other(1), local(2), netmgmt(3), icmp(4), egp(5), ggp(6), hello(7), rip(8), is1s(9), es1s(10),
·	0 9 11.51.70.1 255.255.255 2	Number of octets received from/to this source/group AND forwarded Number of packets received from/to this source/group other(1), local(2), netmamt(3), dvmrp(4), mospf(5), pimSparseDense(6), cbt(7), pimSparseMode(8), pimDenseMode(9), igmpOnly(10) The address portion of the route used for this multicast forwarding entry The mask associated with the route used for this multicast forwarding entry other(1), local(2), netmamt(3), icmp(4), egp(5), ggp(6), hello(7), rip(8), isIs(9), esIs(10), ciscolgrp(11), bbnSpfIgp(12), ospf(13), bgp(14), idpr(15), ciscoligrp(16), dvmrp(17)

Figure 1-47 Viewing IP Multicast Routing Information

- (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

Done

- Value
- Description

e <u>E</u> dit ⊻iew <u>G</u> o	⊆hipmarks §	<u>B</u> ookmarks <u>T</u> ools	Help							4
• 🔶 • 🛃 (🗵 🏠 🚺	http://172.31.24	255 :8080/p	erl/home.pl				~		
Cisco Multicast M	anager 2.3.	3							Cisco Syst	TEMS
Tool: Multicast M	anager 🔽			lanagement Domain:	IPmcLab	~				
Home	Topology	Reporting	Dia	gnostics Help						
)iagnostics:			Graph L	ne 🔽						-
Show All Groups]								
Locate Host			Value b	ps 🚩						
Network Status										
RP Status			F	Plot						
RP Summary										_
IGMP Diagnostics MSDP Status		Trace selecte	d source	and group between f	the routers	below:				
Layer 2 Switches										
Health Check			FHR S	OURCE 🔽						
6500 Troubleshootir	0.0									
Top Talkers	.,		LHR A	LL 🔽						
			-	Frace						
IPmcLab - 12 multic	act 🔥									_
devices:		Group (4)	Croup (D	VS) Group (DB)	Source ID	Source (DNS)	Source (DB)	Number of Sources	
P2-7206-1			aroup (D				Source (Dits)	Source (DD)		e
		224.0.0.1		cisco-rp-announce		10.0.0.1			Sources [3]	
P2-7206-2		<u>224.0.0.1</u>		cisco-rp-discovery	[Farinacci]	10.0.0.1			Sources [6]	
D0 4		<u>224.0.0.1</u>				10.0.0.1			Sources [0]	
P2-ntv-1		224.0.0.1				10.0.0.1			Sources [0]	
P2-ntv-2			-1	h (6)	_					-
P0 -+- 0		view previou	siy saveo	source bps/pps file	S					
<u>P2-ntv-3</u>		Sel	ect File	*						
<u>P2-ntv-4</u>				Display						
<u>P3-7206-1</u>										_
P3-7206-2	_	View previou	sly saved	traces						
		Selec	t Trace n	aul99.trace 🔽 🔽						
			- 19							
P3-msfc-1				Display						

Figure 1-48 Multicast Diagnostics

- 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.



- 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**.t5rrrrrrrrrrr7

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**.

e <u>E</u> dit ⊻iew <u>G</u> o <u>C</u> hipmarks <u>B</u>	jookmarks <u>T</u> ools <u>H</u> elp					2.5 9 8
🛯 • 🔶 • 🎅 🙁 🟠 🔲	http://172.31.24.255 :8	180/perl/home.pl			~	
Cisco Multicast Manager 2.3.	3					CISCO SYSTEMS
Tool: Multicast Manager 👻		Management D	omain: IPmcLab) 💌	Licens	ed to Cisco Systems
Home Topology	Reporting	Diagnostics	Help			
)iagnostics:	Locate Host					
Show All Groups Locate Host Network Status RP Status RP Status	IP Address 10.255					
GMP Diagnostics ISDP Status ayer 2 Switches Iealth Check						
5500 Troubleshooting Top Talkers						
PmcLab - 12 multicast devices: P2-7206-1						
22-7206-2						
<u>2-ntv-1</u> <u>2-ntv-2</u>						
1 <u>2-ntv-3</u> 12-ntv-4						
<u>23-7206-1</u>						
3-7206-2						
<u>23-msfc-1</u>						

Figure 1-49 Locate Host

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

• 🔶 - 🥰	🛛 🏠 🗋	http://172.31.24.255	:8080/perl/home.pl			*
Cisco Multicast	Manager 2.3.	3				CISCO SYSTEMS
iool: Multicast I	Manager 💌		Managemen	t Domain:	IPmcLab 💟	Licensed to Cisco Systems
Home	Topology	Reporting	Diagnostics	Help		
iagnostics:		Network Status				
how All Groups						
ocate Host		Router Syste				
etwork Status P Status		P2-7206-1 21 day	(s, 7:01:13			
P Summary		P2-7206-2 36 day	(s, 15:16:57			
GMP Diagnostics		P2-ntv-1 36 day	(s. 10:37:26			
ISDP Status		P2-ntv-2 36 day				
ayer 2 Switches		P2-ntv-3 36 day				
ealth Check						
500 Troubleshoo	ting	P2-ntv-4 36 day				
op Talkers		P3-7206-1 21 day				
		P3-7206-2 36 day	s, 15:15:24			
	~	P3-msfc-1 36 day	s, 15:16:34			
PrincLab - 12 mul	ticast 👘	P3-msfc-2 4 days	. 1:31:42			
levices: 2-7206-1		P3-msfc-3 36 day				
2-7206-1		P3-msfc-4 36 day				
2-7206-2		F3-IIISIC-4 30 083	\$,13,10,30			
		Finished				
2-ntv-1						
2-ntv-2						
2-110/-2						
2-ntv-3						
2-ntv-4						
3-7206-1						
3-7206-2	_					
<u>'3-msfc-1</u>						
12 moto 2	~					

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

🕲 Cisco Multicast Mana	2							_ 7 🗙
~ .			Help					5,3
🔶 • 🔶 • 🔁 🗵) 🏠 🗋	http://172.31.24.25	5 :8080/perl/home.pl			~		
Cisco Multicast Man	nager 2.3.:	3						CO SYSTEMS
Tool: Multicast Mana	ager 🔽				IPmcLab 💌		Licensed to Cisc	o Systems
Home T	Гороlоду	Reporting	Diagnostics	: Help				
Diagnostics:		Active RPs	Group	State				~
Show All Groups Locate Host Network Status		P2-ntv-4						
RP Status		RP (Dynamic)	Group Address	Groun Mask				
RP Summary IGMP Diagnostics		10.0.0.1	239.0.0.2	255.255.255.244				
MSDP Status		10.0.0.1	239.0.0.2	255,255,255,244				
Layer 2 Switches		10.0.0.1	239.0.0.2					
Health Check				255.255.255.244				
6500 Troubleshooting		Active RPs	Group	State				
Top Talkers								
		P3-7206-1						
IPmcLab - 12 multicast	. ^	DD (Durania)	Group Address	Curve March				
devices:								
P2-7206-1		10.0.0.1	239.0.0.2	255.255.255.244				
		10.0.0.1	239.0.0.2	255.255.255.244				
P2-7206-2		Active RPs	Group	State				=
<u>P2-ntv-1</u>		P3-7206-2						
P2-ntv-2			Group Address	Croup Mack				
P2-ntv-3		10.0.0.1	239.0.0.2	255,255,255,244				_
DO -1-4		10.0.0.1	239.0.0.2	255,255,255,244				
<u>P2-ntv-4</u>		Active RPs	Group	State				
<u>P3-7206-1</u>								
<u>P3-7206-2</u>		P3-msfc-1						
P3-msfc-1		RP (Dynamic) 10.0.0.1	Group Address 239.0.0.2	Group Mask 265.265.265.244				A 0007A
D2 moto 2	×							÷ 5

RP Summary

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

•						
Cisco Multicast Manager 2.	3.3 - Mozilla Fir	efox				a X
jile <u>E</u> dit ⊻iew <u>G</u> o ⊆hipmarks	<u>B</u> ookmarks <u>T</u> ools	Help				0
- 🍦 - 🛃 😣 🐔	http://172.31.24	255 :8080/perl/home.pl			~	
Cisco Multicast Manager 2	.3.3				Cisco Syst	
Tool: Multicast Manager 💽	•	Manager	nent Domain:	IPmcLab 🔽		ems
Home Topolog	y Reporting	Diagnostics	Help			
Diagnostics:	RP Summary	for IPmcLab dom	ain			
Show All Groups						
Locate Host	IP Address	RP	Group Addre	ss Group Mask		
Network Status RP Status	11.51.140.1	P3-msfc-1				
RP Summary	11.51.140.1	P3-msfc-2				
IGMP Diagnostics	11.51.140.2	P3-msfc-3	239.0.0.2	255.255.255.244		
MSDP Status	11.51.140.2	P3-msfc-4	239.0.0.2	255,255,255,244		
Layer 2 Switches	11.51.70.1	P2-ntv-1	239.0.0.2	255,255,255,244		
Health Check	11.51.70.1	P2-ntv-2	239.0.0.2	255,255,255,244		
6500 Troubleshooting Top Talkers	11.51.70.2	P2-ntv-3	239.0.0.2	255.255.255.244		
Top Talkers	11.51.70.2	P2-ntv-4	239.0.0.2	255,255,255,244		
			239.0.0.2	200.200.200.244		
IPmcLab - 12 multicast	200.200.200.1					
devices:	200.200.200.1					
P2-7206-1		P2-7206-1,Phantom				
P2-7206-2	200.200.201.1	P3-7206-1,Phantom	1			
P2-ntv-1	Finished					_
P2-ntv-2						
P2-ntv-3						
P2-ntv-4						
<u>P3-7206-1</u>						
<u>P3-7206-2</u>						
P3-msfc-1	-					
D2 moto 2	~				 	

Figure 1-52 RP Summary

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

IGMP Diagnostics

<u>Note</u>

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.

🕑 Cisco Multicast Ma	anager 2.3.	3 - Mozilla Firefo	х						
Eile Edit ⊻iew Go	⊆hipmarks	Bookmarks <u>T</u> ools <u>H</u>	elp						()
🧼 • 🧼 • 🎅 (3 🏠	http://172.31.24.255	:8080/perl/home.pl					~	
Cisco Multicast M	lanager 2.3	3.3							CISCO SYSTEMS
Tool: Multicast Ma	anager 💌				IPmcLab 💌				isco Systems
Home	Topology	Reporting	Diagnostics	Help					
Diagnostics:		IGMP Diagnosti	cs						
Show All Groups Locate Host Network Status			s and GroupsUsing Note: this may tak			number of groups			
RP Status RP Summary IGMP Diagnostics			Group 224.0.0.1						
MSDP Status Layer 2 Switches Health Check 6500 Troubleshootin Top Talkers	ng	Select R	Duters P2-7206-1 P2-7206-2 P2-ntv-1 P2-ntv-2						
IPmcLab - 12 multio	cast	Select Diagnostic	:Type 💿 IGMP Last :Filter 🔲 Show Failu						
P2-7206-1 P2-7206-2			Run	105					
		IGMP Cache La	st Reporter for 224	1001 1	0				
P2-ntv-1		Rout			Interface			Last Reporter	
P2-ntv-2		P2-7206-1		itEthernet3			10.0.0.1		
P2-ntv-3		P2-7206-1	Gigab	itEthernet4	/0		10.0.0.1		
P2-ntv-4		Finished							
<u>P3-7206-1</u>									
<u>P3-7206-2</u>									
P3-msfc-1									a
D2 mefo 2		*							180478
									a l

Figure 1-53 IGMP Diagnostics

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.



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.

Cisco Multicast Manager 2.3.3				
le <u>E</u> dit ⊻iew <u>G</u> o <u>C</u> hipmarks	Bookmarks Tools Help			
Þ • 🔶 • 🛃 😣 🟠 🛽	http://172.31.24.255 :8080/p	erl/home.pl		▼
Cisco Multicast Manager 2.3	.3			CISCO SYSTEM
Tool: Multicast Manager 🔽		Management Domain: IPmc	Lab 🔽	Licensed to Cisco Systems
Home Topology	Reporting Dia	gnostics Help		
Diagnostics:	MSDP Status			
Show All Groups				
Locate Host	Local	Peer	Remote IP	State
Network Status	P2-7206-1	P3-7206-1	10.0.0.1	established
RP Status	P2-7206-1		10.0.0.1	established
RP Summary IGMP Diagnostics	P2-ntv-1	P2-ntv-2	10.0.0.1	established
MSDP Status			10.0.0.1	
Layer 2 Switches	P2-ntv-2	P2-ntv-1		established
Health Check	P2-ntv-3	P2-ntv-4	10.0.0.1	established
6500 Troubleshooting	P2-ntv-4	P2-ntv-3	10.0.0.1	established
Top Talkers	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
IPmcLab - 12 multicast	P3-msfc-2	P3-msfc-1	10.0.0.1	established
devices:		13-11310-1	10.0.0.1	established
<u>P2-7206-1</u>	Select MSDP Router P2-	7206-1 🔽 Peer Info SAC	Cache Info	
P2-7206-2	Select MSDF Router F2-		Jache Inio	
1212002				
P2-ntv-1				
<u>P2-ntv-2</u>				
<u>P2-ntv-3</u>				
<u>P2-ntv-4</u>				
<u>P3-7206-1</u>				
<u>P3-7206-2</u>				
P3-msfc-1				
D2 mefe 2				

Figure 1-54 MSDP Status

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.

Back 🔹 🐑 - 💌 💈	ols Help	h 🤺 Favorites 📢 Media	<i>€</i> ≥ ⊑	3 🔜 🛍		
ess 🗿 http://172.31.24.255 :8	080/perl/home.pl				Image: A state of the state	io Links
		Reference 🥄 Highlight 📘	🕴 116 blocked 👻 🎇 S	icreensavers.com 💿 Smileys		
				•		
isco Multicast Manager :					<mark>Cisco S</mark> 	ավիս
ool: Multicast Manager 🛓	Z Do	main: ef-mcman-1 💌				stems
Home Topolog	ay Report	ing Diagnostics	Help			
agnostics: Iow All Groups	Userna	me				~
cate Host	Passwe	ard				
twork Status Status	F 05599					
Summary	Select Swi	tch efsj-4006-a5	*			
MP Diagnostics						
SDP Status		Query				
iyer 2 Switches ealth Check						
00 Troubleshooting						_
	Getting I2 s	witch 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	
mcLab - 12 multicast vices:	201	01-00-5e-7e-01-03	224.0.0.1		1/1-2,2/4	
-7206-1	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	
-7206-2	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	
?-ntv-1	203	01-00-5e-7e-01-22	224.0.0.1		1/1-2	
<u>t-ntv-1</u>	203	01-00-5e-7e-01-23	224.0.0.1		1/1-2	
<u>2-ntv-1</u> 2-ntv-2	203	01-00-5e-7e-01-24	224.0.0.1		1/1-2	
<u>?-ntv-1</u> ?-ntv-2 ?-ntv-3		01-00-58-78-01-24			1/1-2	
2 <u>-ntv-1</u> 2 <u>-ntv-2</u> 2 <u>-ntv-3</u>	203	01-00-5e-7e-01-24 01-00-5e-7e-01-25	224.0.0.1			
2-7206-2 2-ntv-1 2-ntv-2 2-ntv-3 2-ntv-4	203 203		224.0.0.1 224.0.0.1		1/1-2	~

Figure 1-55 Layer 2 Multicast Information

Figure 1-56 Layer 2 Host IPs

	orites <u>T</u> ools							
dress 🙋 http://es1-cn								💌 🄁 🤇
🔁 Back 🝷 🕥 🕤	🖹 🛃 (Search 🔎	📩 Favorites	🗟 • 🎍	W •	🛍 🔏		
								ISCO SYSTEMS
Cisco Multicast Ma	nager 2.3.	.3						
								սկրուսկրո
Tool: Multicast Ma	nager 🔽		Manageme	nt Domain:	gtulumba	~		o Systems
Home	Topology	Reporting	Diagnostics	Help				
iagnostics:								<u> </u>
Show All Groups		Getting multica	st port info from es1-	3750-a4.				
ocate Host		es1-3750-a4	L					-
letwork Status		VLAN	Port	M	cast IPs		Possible Host IPs	
IP Status					Cast IPS		PUSSIBLE HUST IPS	
IP Summary GMP Diagnostics		193	Gi1/0/5	239.0.0.1				
ISDP Status		-		239.0.0.1 239.0.0.1				
aver 2 Switches		-		239.0.0.1				
- L2 Multicast Infor	mation	-		239.0.0.1				
- L2 Host IPs	madon			239.0.0.1				
Health Check				239.0.0.1				
6500 Troubleshootin				239.0.0.1				
Fop Talkers	3			239.0.0.1				
	^			239.0.0.1				
Search:		-		239.0.0.1 239.0.0.1				
search				239.0.0.1				
				239.0.0.1				
IPmcLab - 12 multic	ast	193	Gi1/0/1	239.0.0.1		172.16.0.0		
devices:				239.0.0.1				
<u>P2-7206-1</u>				239.0.0.1				
P2-7206-2				239.0.0.1 239.0.0.1				
00 L				239.0.0.1				
P2-ntv-1				239.0.0.1				
	_			239.0.0.1				
<u>P2-ntv-2</u>				239.0.0.1				
				239.0.0.1				
P2-ntv-3				239.0.0.1				
				239.0.0.1 239.0.0.1				
P2-ntv-4	_			239.0.0.1				
	~			238.0.0.1				~

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**.

jie Edit ⊻iew <u>G</u> o <u>⊂</u> hipma	rks Bookmark	s Tools Help		
4				
🗣 • 🕪 • 🚰 🕓 🐧	1 🗋 http:/	/172.31.24.255 :8080/perl/home.pl		×
Cisco Multicast Manager	2.3.3			CISCO SYSTEM
Tool: Multicast Manager	v	Manageme	ent Domain: IPmcLab 🔽	للنوسيالين Licensed to Cisco Systems
Home Topolo		Reporting Diagnostics	Help	
Diagnostics:				
Show All Groups	Selec	t Health Check 🛛 London 🛛 🔽	Run	
Locate Host				
Network Status	Runni	ng (London.health) Health Che	ck	
RP Status RP Summary	T	ype	Testing	Status
IGMP Diagnostics	RP	P3-msfc-1	resulty	0:36 days, 16:00:55
MSDP Status	RP	P2-7206-1		0:21 days, 7:45:34
Layer 2 Switches	RP	P2-7208-1 P3-msfc-4		
Health Check 6500 Troubleshooting		P3-mstc-4 10.0.0.2, 224.0.0.3: P2-720	o. /	0:36 days, 16:00:59
Top Talkers	SG	10.0.0.2, 224.0.0.3: P2-720	6-1	ок
Top Talkors	SG			GONE
	SG	10.0.0.2, 224.0.0.3: P2-720	6-1	ок
IPmcLab - 12 multicast	TREE	test1.trace		CHANGED
devices:	Finish	ed		
P2-7206-1				
<u>P2-7206-2</u>				
P2-ntv-1				
P2-ntv-2				
<u>P2-ntv-3</u>				
P2-ntv-4				
<u>P3-7206-1</u>				
<u>P3-7206-2</u>				
<u>P3-msfc-1</u>				
D2 moto 2	~			

Figure 1-57 Health Check

- 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.

 \mathcal{P} Tip

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

🕲 Cisco Multicast Manager 2.3.3	- Mozilla Firefo	ж				BX
Eile Edit ⊻iew Go ⊆hipmarks E	}ookmarks <u>T</u> ools <u>H</u>	elp				0
🤃 🖓 · 🍌 · 🌮 🔇) http://172.31.24.255	:8080/perl/home.pl			~	
Cisco Multicast Manager 2.3.	3				Cisco Sys	
Tool: Multicast Manager 🔽			nt Domain: 🏽 IPmcLab 💌			tems
Home Topology	Reporting	Diagnostics	Help			
Diagnostics:	6500 Troublest	ooting				^
Show All Groups Locate Host Network Status	Router	P2-ntv-1	~			-
RP Status RP Summary	Username					
IGMP Diagnostics	Password					
MSDP Status Layer 2 Switches	Enable					
Health Check						
6500 Troubleshooting	Polling interval	5 💌				
Top Talkers	Source	10.0.0.2	filter groups	edit reset		
	300108					
IPmcLab - 12 multicast	Group	224.0.0.3	 filter sources 	edit reset		=
devices:		Run Full Trace	Run Diagnostics	1		
P2-7206-1		rtann an maoo	- Tran Blagheorice			
P2-7206-2	Command	sh ip mroute		💙 🖬 edit		
<u>F2-7200-2</u>			Bun	Command		
<u>P2-ntv-1</u>					Clear Output E-mail output to TA	ic I
P2-ntv-2						٦
<u>P2-ntv-3</u>						
<u>P2-ntv-4</u>						
<u>P3-7206-1</u>						
<u>P3-7206-2</u>						
P3-msfc-1						00040
D2 meto 2						

Figure 1-58 6500 Troubleshooting

The 6500 Troubleshooting page contains:

Fields and Buttons	Description	
Router	Select a 6500 or 7600 router.	
Username	Enter your username.	
PasswordEnter the MSFC password.		
Enable	Enter the enable password.	
Polling Interval Interval at which the statistics are upd		
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 CommandRuns the selected show command. Or 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.

🗿 Top Talkers (from: es1-7606	-sd2 - Microsoft Internet Explore	r provided by Cisco Systems,	Inc.
Top Talkers f	rom: es1-760	5-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)
		11 2 1 3 7	,	

Figure 1-59 Top Talkers

Router Diagnostics

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

🕲 Cisco Multicast Manager 2.3.3 💿 - Mozilla Firefox Eile Edit View Go Chipmarks Bookmarks Iools Help 🛯 🗸 🧼 🖌 🛃 区 🏫 🗋 http://172.31.24.255 :8080/perl/home.pl ~ ISCO SYSTEMS Cisco Multicast Manager 2.3.3 лн. jement Domain: IPmcLab 🔽 Tool: Multicast Manager 🔽 Licensed to Cisco Syster Topology Horo Reporting Diagnostics Helr Reporting: 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 Historical Graphs Display All IOS Versions Run Diagnostics on P2-7206-1 Show Command Show Command Select ~ Username Password Set Source and Group to work on: Source 0.0.0.0 Filter Groups IPmcLab - 12 multicast 0.0.0.0 * P2-7206-1 Filter Sources Group P2-7206-2 224.0.1.39 ~ RESET SG LISTS <u>P2-ntv-1</u> <u>P2-ntv-2</u> SNMP Queries Query Select ~ P2-ntv-3 P2-ntv-4 Compare bps/pps between P2-7206-1 and: P3-7206-1 P2-7206-2 🔺 P2-ntv-1 P3-7206-2 Dest Router P2-ntv-2 2 P2-ntv-3 ~ 8087 P3-msfc-1 Samples 3 02.0

Figure 1-60 Router Diagnostics

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.

🕑 Untitled Document - Mozilla	Firefox		
jle <u>E</u> dit ⊻iew <u>G</u> o ⊆hipmarks	<u>B</u> ookmarks <u>T</u> ools <u>H</u> elp		
🗘 • 🎝 • 🎅 😣 🏠	http://172.31.24.255 :8080/perl	/home.pl	×
Show Command	Show		
Username			
Password			
igmpCacheEntry Query for F	92-7206-1 (10.0.0.1) ()	0	
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	

Figure 1-61 IGMP Cache Entries

- Multicast Information—Shows multicast topology information.

Figure 1-62 Multicast Information

🕑 Untitled Document - Mozilla	a Firefox			. 8
jle <u>E</u> dit ⊻iew <u>G</u> o <u>C</u> hipmarks	; <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp			()
þ • 🧼 • 🛃 😣 🟠	http://172.31.24.255 :8080/perl/home.	pl		▼
Show Command	Show			4
Username				
Password				
lulticast Info for P2-7206	1 (10.0.0.1)			
PIM Neighbors				
	Local Int	Neighbor		ghbor 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		20.2007.0	10.0.0.1	
SRP1/0		P2-7206-2	10.0.01	
SRP1/0		P3-7206-1	10.0.0.1	
SRP1/0 Funnel22		P3-7206-2	10.0.0.1 10.0.0.1	
runneizz PIM Interface Mode			10.0.0.1	
Local Interface Mode	Local IP	PIM Mode	DE	
RP1/0	224.0.0.1	sparse	P3-7206-2 (224.0.0.1)	
igabitEthernet4/0	224.0.0.1	sparse	P2-ntv-2 (224.0.0.1)	
unnel22	224.0.0.1	sparse	N/A (0.0.0.0)	
_oopback1	224.0.0.1	sparse	P2-7206-1 (224.0.0.1)	
.oopback2	224.0.0.1	sparse	P3-7206-1 (224.0.0.1)	
runnel0	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
Funnel22		224.0.0.1		2
.oopback1		224.0.0.1		2
Loopback2		224.0.0.1		2
FunnelA				2

- Multicast Routing Table—Shows the multicast routing table.

Untitled Document	- Mozilla Firefox			- C - C - C - C - C - C - C - C - C - C
jie <u>E</u> dit <u>V</u> iew <u>G</u> o	⊆hipmarks <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp			0
(3 🕋 🗋 http://172.31.24.255 :80	201	×	
🗘 - 🔷 - 🔁 🜔	3 1 http://172.31.24.255 :80	su/peri/nome.pi		
Show Command	Show			1
	0.00			
Username				
Password				
ipMRouteEntry Quer	y for P2-7206-1 (10.0.0.1	0		
Shortest Path Tree				
Group	Source		Shortest Path Tree	
224.0.1.39	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	False		
224.0.1.40	0.0.0	True		
224.0.1.40	0.0.0	True		
224.0.1.40	0.0.0	True		
224.0.1.40	0.0.0	True		
224.0.1.40	0.0.0	True		
224.0.1.40	0.0.0	True		
224.0.1.40	0.0.0	True		
224.0.1.40	0.0.0	True		
224.0.1.40	0.0.0	True		
224.0.1.40	0.0.0	True		
224.0.1.40	0.0.0	True		
224.0.1.40	0.0.0	False		
224.0.1.40	0.0.0.0	False		
224.0.1.40	0.0.0	True		
224.0.1.40	0.0.0	True		
224.0.1.40	0.0.0	False		
224.0.1.40	0.0.0	True		
224.0.1.40	0.0.0	True		
224.0.1.40	0.0.0	True		
224.0.1.40	0.0.0	True		
224.0.1.40	0.0.0	True		
224.0.1.40	0.0.0	True		

Figure 1-63 Multicast Routing Table

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.



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.



Α

Admin Utilities 1-16 Apache Log Files 1-81 Application Maintenance and Troubleshooting 1-81

В

Backups 1-82

С

Compare bps/pps **1-80** Configuration **1-49** Configuration Files **1-81**

D

Databases 1-82 Device Configurations 1-82 Diagnostics 1-61 Discovery 1-9 Display All IOS Versions 1-60

Ε

Error Log File 1-17 events.log 1-81

G

Graphs (Trends) 1-59

Η

Health Check 1-74 Historical Data 1-82

L

IGMP Diagnostics 1-70

L

Layer 2 PPS Threshold Report 1-54 Layer 2 Switches 1-72 Licensing 1-6 Linux Installation Instructions 1-4 Locate Sender 1-66 Log Files 1-81

Μ

MSDP Status 1-71

Ν

Network Status 1-67

R

Reinitialize Address Management Database 1-17 Remove Baseline 1-17 Remove Device 1-17 Remove Domain 1-17 Reporting 1-49

User Guide for the Cisco Multicast Manager 2.3.3

rmspolld.log **1-81** Router Diagnostics **1-77** Routing Table Check **1-77** RP Group Threshold Report **1-51** RP Polling Report **1-50** RP Status **1-68** RP Summary **1-69**

S

S,G PPS Threshold Report 1-52 SG Delta Report 1-58 Show All Groups 1-62 Solaris Installation Instructions 1-2 SSG Report 1-55 Standard Multicast MIBs 1-82 Starting and Stopping the Application 1-6

Т

Topology 1-45 Tree Report 1-56

V

Validate Router Configurations 1-22

I