User Guide for Cisco Multicast Manager 3.1

April 2010

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

Text Part Number: OL-17776-03
# CONTENTS

Preface ix  
Objectives ix  
Audience ix  
Organization x  
Conventions x  
Related Documentation xi  
Obtaining Documentation, Obtaining Support, and Security Guidelines xi

## CHAPTER 1

**Overview of Cisco Multicast Manager** 1-1  
CM M Applications and Architecture 1-1  
Multicast Monitoring and Troubleshooting 1-1  
Support for Cisco Video Solutions 1-2  
Vidmon Support 1-3  
Additional Product Features 1-5

## CHAPTER 2

**Getting Started** 2-1  
Logging into Cisco Multicast Manager 2-1  
Navigating the GUI 2-2  
Menu 2-2  
Devices Tab 2-2  
Cisco Multicast Manager Dashboard 2-4  
Running a Trace from the Dashboard 2-5  
Displaying a Trap Details List from the Traps Pane 2-5  
Viewing Performance Graphs from the Dashboard 2-5

## CHAPTER 3

**Initial System Setup** 3-1  
Basic Setup and Configuration Steps 3-1

## CHAPTER 4

**System Configuration** 4-1  
Domain Management 4-1  
Creating a Domain 4-1  
Importing a Domain 4-5  
Global Polling Configuration 4-5
CHAPTER 5

Polling Configuration and Reports  5-1
  Event Viewer  5-1
  Trap Viewer  5-2
  Domain Trap/Email  5-3
  Traffic & Polling Reports  5-5
    S,G  5-5
      S,G Threshold Report  5-5
      Historical Graph  5-6
      Group Gone Report  5-7
      Config S,G Polling  5-7
    L2 Polling  5-9
      Historical Graph  5-10
      Configuring L2 Polling  5-10
  Interface Polling  5-11
    Multicast Bandwidth Report  5-11
    Historical Graph  5-12
    Configuring Interface Polling  5-12
  Tree Polling & Reports  5-13
    Setting Up Tree Polling  5-13
    Configuring Tree Polling  5-14
  Tree Reports  5-15
    Viewing a Tree Report  5-15
    Viewing Historical Reports  5-15
    Viewing an S,G Delta Report  5-16
    Comparing Tree Baselines  5-16
    Viewing a Tree Changed Report from the Dashboard.  5-17
  SG Polling By Branch  5-17
  Miscellaneous Polling & Reports  5-18
    RP  5-18
      RP Report  5-19
      RP Group Threshold Report  5-20
      SSG Report  5-21
      Configuring RP Polling  5-22
      RP Global Configuration  5-23
    RPF  5-24
      RPF Polling Report  5-24
      Configuring RPF Polling  5-24
    Selective Source Monitoring  5-25
      Selective Source Monitoring Report  5-25
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selective Source Monitoring Configuration</td>
<td>5-26</td>
</tr>
<tr>
<td>Health Check</td>
<td>5-27</td>
</tr>
<tr>
<td>Health Check Failed Report</td>
<td>5-28</td>
</tr>
<tr>
<td>Configuring Health Check Polling</td>
<td>5-28</td>
</tr>
<tr>
<td>Video Probe</td>
<td>5-30</td>
</tr>
<tr>
<td>Video Probe Report</td>
<td>5-30</td>
</tr>
<tr>
<td>Historical Report</td>
<td>5-31</td>
</tr>
<tr>
<td>Configuring Video Probe Polling</td>
<td>5-32</td>
</tr>
<tr>
<td>Vidmon Polling</td>
<td>5-32</td>
</tr>
<tr>
<td>Viewing a Vidmon Report</td>
<td>5-32</td>
</tr>
<tr>
<td>Historical Report</td>
<td>5-33</td>
</tr>
<tr>
<td>Configuring Vidmon Polling</td>
<td>5-34</td>
</tr>
<tr>
<td>MVPN Polling</td>
<td>5-38</td>
</tr>
<tr>
<td>M DT Source Report</td>
<td>5-38</td>
</tr>
<tr>
<td>M DT Default Report</td>
<td>5-39</td>
</tr>
<tr>
<td>VRF Interface Count Report</td>
<td>5-40</td>
</tr>
<tr>
<td>VRF Count Report</td>
<td>5-41</td>
</tr>
<tr>
<td>Configuring MVPN Polling</td>
<td>5-42</td>
</tr>
<tr>
<td>CRM Polling</td>
<td>5-43</td>
</tr>
<tr>
<td>Baseline Route Polling</td>
<td>5-43</td>
</tr>
<tr>
<td>Unicast Report</td>
<td>5-43</td>
</tr>
<tr>
<td>Multicast Report</td>
<td>5-43</td>
</tr>
<tr>
<td>Historical Report</td>
<td>5-43</td>
</tr>
<tr>
<td>View Baseline</td>
<td>5-44</td>
</tr>
<tr>
<td>Compare Baseline</td>
<td>5-44</td>
</tr>
<tr>
<td>Configuring Route Polling</td>
<td>5-45</td>
</tr>
<tr>
<td>Specific Route Polling</td>
<td>5-45</td>
</tr>
<tr>
<td>Unicast Report</td>
<td>5-45</td>
</tr>
<tr>
<td>Multicast Report</td>
<td>5-46</td>
</tr>
<tr>
<td>Configuring Unicast Polling</td>
<td>5-47</td>
</tr>
<tr>
<td>Configuring Multicast Polling</td>
<td>5-48</td>
</tr>
</tbody>
</table>

**CHAPTER 6**

**Discovery and Trace** 6-1

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discovery</td>
<td>6-1</td>
</tr>
<tr>
<td>Multicast Discovery</td>
<td>6-1</td>
</tr>
<tr>
<td>L2 Device</td>
<td>6-6</td>
</tr>
<tr>
<td>Video Probe</td>
<td>6-7</td>
</tr>
<tr>
<td>Monitoring Application</td>
<td>6-8</td>
</tr>
<tr>
<td>Vidmon Device</td>
<td>6-9</td>
</tr>
<tr>
<td>Chapter 7: Topology</td>
<td>7-1</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----</td>
</tr>
<tr>
<td>Topology</td>
<td>7-1</td>
</tr>
<tr>
<td>All Device Information</td>
<td>7-2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 8: Diagnostics</th>
<th>8-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>SG Diagnostics</td>
<td>8-1</td>
</tr>
<tr>
<td>Packet Monitoring</td>
<td>8-1</td>
</tr>
<tr>
<td>L2 Diagnostics</td>
<td>8-2</td>
</tr>
<tr>
<td>L2 Multicast Information</td>
<td>8-2</td>
</tr>
<tr>
<td>L2 Host IP Addresses</td>
<td>8-3</td>
</tr>
<tr>
<td>Video Diagnostics</td>
<td>8-3</td>
</tr>
<tr>
<td>Video Probe Status</td>
<td>8-3</td>
</tr>
<tr>
<td>Vidmon Flow Status</td>
<td>8-5</td>
</tr>
<tr>
<td>Miscellaneous Diagnostics</td>
<td>8-9</td>
</tr>
<tr>
<td>RP Status</td>
<td>8-9</td>
</tr>
<tr>
<td>RP Summary</td>
<td>8-10</td>
</tr>
<tr>
<td>MSDP Status</td>
<td>8-11</td>
</tr>
<tr>
<td>Network Status</td>
<td>8-11</td>
</tr>
<tr>
<td>Locate a Host</td>
<td>8-12</td>
</tr>
<tr>
<td>Tools</td>
<td>8-12</td>
</tr>
<tr>
<td>IGM P Diagnostics</td>
<td>8-12</td>
</tr>
<tr>
<td>Top Talkers</td>
<td>8-12</td>
</tr>
<tr>
<td>Health Check</td>
<td>8-13</td>
</tr>
<tr>
<td>M VPN</td>
<td>8-13</td>
</tr>
<tr>
<td>6500/7600 Troubleshooting</td>
<td>8-14</td>
</tr>
<tr>
<td>Full Trace</td>
<td>8-14</td>
</tr>
<tr>
<td>Diagnostics</td>
<td>8-16</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>8-17</td>
</tr>
<tr>
<td>SNMP Utilities</td>
<td>8-17</td>
</tr>
<tr>
<td>IGM P Cache</td>
<td>8-17</td>
</tr>
<tr>
<td>PIM Neighbor</td>
<td>8-18</td>
</tr>
<tr>
<td>SNMP PIM Reachability</td>
<td>8-18</td>
</tr>
<tr>
<td>Explicit User Tracking</td>
<td>8-18</td>
</tr>
</tbody>
</table>
CRM Diagnostics  8-20
  Create Baseline  8-20
  Check Routing Table  8-21

CHAPTER 9
Configuration Management  9-1
  Device Configuration  9-1
    Get All Configurations  9-1
    Validate All Configurations  9-1
    Configuring Static RPs  9-2
    Configuring SSM Devices  9-2
  M VPN Configuration  9-3

CHAPTER 10
Administration  10-1
  Managing Users and Access  10-1
    User Configuration  10-1
      Adding a User Configuration  10-1
      Modifying a User File  10-2
    Access Control  10-3
    Authentication & Audit  10-3
    ACS Server  10-4
  Timeout Configuration  10-4
  Address Management  10-5
    Destination Address Database  10-5
      Adding a Destination Address  10-6
      Modifying a Destination Address  10-6
    Source Description  10-7
      Adding a Source Address and Description  10-7
      Modifying a Source Address or Description  10-8
    Transport Description  10-8
      Adding a Transport Description  10-8
      Modifying a Transport Description  10-9
  Managing the Ad Zone Database  10-9
    Adding a Zone  10-9
    Modifying a Zone  10-10
  Managing the Channel Map Database  10-10
    Adding a Channel  10-10
    Modifying a Channel  10-11
  Managing the Multiplex Table Database  10-12
    Adding a Record to the Multiplex Table Database  10-12
Preface

This preface describes the objectives, audience, organization, and conventions of the User Guide for Cisco Multicast Manager, 3.1. It refers you to related publications and describes online sources of technical information.

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

This preface includes:
- Objectives, page ix
- Audience, page ix
- Organization, page x
- Conventions, page x
- Related Documentation, page xi
- Obtaining Documentation, Obtaining Support, and Security Guidelines, page xi

Objectives

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

Audience

This guide is for network administrators or operators who use the CMM software to manage multicast networks. Network administrators or operators should have:
- Basic network management skills
- Basic multicast knowledge
Preface

Organization

This guide is divided into the following chapters:

- **Chapter 1, “Overview of Cisco Multicast Manager,”** provides an overview of CMM system architecture and functionality.
- **Chapter 2, “Getting Started”** describes logging into the CMM, an overview of the CMM interface, and the initial tasks to perform.
- **Chapter 3, “Initial System Setup,”** provides a list of the basic installation and configuration steps for CMM.
- **Chapter 4, “System Configuration”** provides information on managing domains and global polling configurations.
- **Chapter 5, “Polling Configuration and Reports”** describes how to configure devices for polling, viewing of events for polling, and how to view historical data files.
- **Chapter 6, “Discovery and Trace”** provides information on discovering network devices and multicast running traces.
- **Chapter 7, “Topology”** provides information on viewing topology and reports.
- **Chapter 8, “Diagnostics”** provides information on viewing both global and router-specific diagnostics.
- **Chapter 9, “Configuration Management”** describes how to view the running configuration of devices, validate device configuration using specified configuration templates, add static Rendezvous Point (RP) and SSM devices, and add a service type for multicast VPN (MVPN) trace operations.
- **Chapter 10, “Administration”** provides information on managing the address database, managing users, and configuring access control.

Conventions

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

<table>
<thead>
<tr>
<th>Item</th>
<th>Convention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commands and keywords</td>
<td><strong>boldface</strong> font</td>
</tr>
<tr>
<td>Variables for which you supply values</td>
<td><strong>italic</strong> font</td>
</tr>
<tr>
<td>Displayed session and system information</td>
<td><strong>screen</strong> font</td>
</tr>
<tr>
<td>Elements that are optional</td>
<td>Square brackets ([ ])</td>
</tr>
<tr>
<td>Alternate but required keywords that are grouped</td>
<td>Braces ({ }) and separated by a vertical bar (</td>
</tr>
<tr>
<td>Information you enter</td>
<td><strong>boldface</strong> <strong>screen</strong> font</td>
</tr>
<tr>
<td>Variables you enter</td>
<td><strong>italic</strong> <strong>screen</strong> font</td>
</tr>
<tr>
<td>Menu items and button names</td>
<td><strong>boldface</strong> font</td>
</tr>
<tr>
<td>Selecting a menu item in paragraphs</td>
<td><strong>Option &gt; Network Preferences</strong></td>
</tr>
<tr>
<td>Selecting a menu item in tables</td>
<td><strong>Option &gt; Network Preferences</strong></td>
</tr>
</tbody>
</table>
Examples use the following conventions:

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

This publication also uses the following conventions:

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

---

**Note**

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

---

**Tip**

Means *the following are useful tips*.

---

**Related Documentation**

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

- *Installation Guide for Cisco Multicast Manager 3.1*
- *Release Notes for Cisco Multicast Manager 3.1*
- *Documentation Guide and Supplemental License Agreement for Cisco Multicast Manager 3.1*
- *Supported Devices Tables for Cisco Multicast Manger 3.1*
- *Cisco Multicast Manager Developer's Guide and API Reference, 3.1*

---

**Obtaining Documentation, Obtaining Support, and Security Guidelines**

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What’s New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:


Subscribe to the *What’s New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.
Overview of Cisco Multicast Manager

Cisco Multicast Manager (CMM) 3.1 is a web-based network management application that enables monitoring and troubleshooting of IP multicast networks. CMM allows you to:

- Discover the devices in your IP multicast network.
- Determine the network topology to visualize the network architecture.
- Manage the network elements through multicast polling and monitoring of alerts.
- Troubleshoot problems by identifying the source of network faults.
- Support for Protocol Independent Multicast (PIM), PIM Sparse Mode (PIM-SM), PIM Dense Mode (PIM-DM), PIM Source Specific Multicast (PIM-SSM), and Multicast VPN (MVPN).

This chapter contains the following sections:

- CMM Applications and Architecture, page 1-1
- Additional Product Features, page 1-5

CMM Applications and Architecture

CMM is used in several industries, by:

- Financial services customers who broadcast information such as stock quotes and prices for other financial instruments over IP multicast.
- Service providers who deliver video over IP multicast. Using CMM, video service providers can monitor video quality over multiple channels, view alarms that indicate problems in the video delivery network, and isolate the source of faults that effect video broadcast.
- Service providers who need to manage their Multicast VPN (MVPN) environment.

Multicast Monitoring and Troubleshooting

CMM provides powerful features for monitoring IP multicast networks, including:

- Automated multicast discovery and topology generation
- Proactive multicast polling and monitoring
- Real-time multicast diagnostics
Chapter 1  Overview of Cisco Multicast Manager

- Alerting and reporting
- Support for Protocol Independent Multicast (PIM), PIM Sparse Mode (PIM-SM), PIM Dense Mode (PIM-DM), PIM Source Specific Multicast (PIM-SSM), and Multicast VPN (MVPN)

Figure 1-1 shows how Cisco Multicast Manager can be used to trace a multicast group. The trace is presented in tabular and graphical format. The table can update dynamically, showing the packet per second (PPS) rate, output errors, and discards for each interface along the tree. Cisco Multicast Manager also includes support for video probes that might be deployed for monitoring video quality. The embedded address management database shows which channels are affected if there is a problem with a specific multicast group.

Figure 1-1  Using Cisco Multicast Manager to Trace a Multicast Group

Support for Cisco Video Solutions

CMM can be used to monitor multicast flows used in video networks. For example, CMM is used in the Cisco Video Assurance Management Solution (VAMS), which monitors end-to-end video transmission networks. CMM receives traps from industry standard video probes such as BridgeTech probes, IneoQuest probes, and Mixed Signals probes.

Figure 1-2 shows a typical CMM architecture in a video network.
When users view CMM events in the event lists in Cisco VAMS, they can use the cross-launch capability in Cisco VAMS to launch CMM to perform a trace and other analysis of the IP multicast network.

For more information on Cisco VAMS see the User Guide for Cisco Multicast Manager, 2.0 at the following location:

**Vidmon Support**

The Cisco IOS supports video monitoring on Cisco 76xx devices and on Cisco ASR 9000 Series devices. IOS video monitoring, referred to as Vidmon, is implemented through IOS CLI commands.

CMM video monitoring includes support for the Vidmon capability provided in Cisco 7600 series routers running IOS 12.2(33)SRE and in ASR 9000 Series (Viking) devices running IOS XR 3.9.1.

The Vidmon support in CMM 3.1 varies for Cisco 7600 series routers and ASR 9000 devices. The Cisco 7600 supports VidMon metrics only on the enhanced service blade (ES+) line cards.

**Vidmon Metrics**

Vidmon provides the following video metrics:

- **Media Delivery Index (MDI) Reporting**—MDI is a metric developed in cooperation between IneoQuest and Cisco and presented in RFC 4445. MDI is a combination of two metrics that are used to measure the network’s contribution to video impairments. The two MDI metrics are:
- **MDI:MLR**—MDI: Media Loss Rate indicates whether MPEG packets were dropped.

- **MDI:DF**—MDI: Delay Factor (DF) indicates the buffering requirements for the packets in the media stream. DF represents the difference between the arrival and drain rates of a media stream. This is largely based on the arrival of the IP flow. The DF over an interval period represents the buffering required to handle variations in transmission at a point in the transmission path.

- **MRV Reporting**—Media Rate Variation (MRV) measures loss as a function of the L3/L4 header. For Constant Bitrate Flows (CBR) a normalized bit arrival rate is created based on the known media arrival rate.

  VidMon Media Rate Variation (MRV) measures loss as a function of the L3/L4 header. For Constant Bitrate Flows (CBR) a normalized bit arrival rate is created based on the known media arrival rate. The video flow is monitored for variations in the arrival rates which represent perturbations caused by excessive delay or loss in the media flow.

### CMM Implementation of Vidmon

CMM implements Vidmon support as follows:

1. When CMM monitors a video flow using Vidmon, depending on the device that is monitored, CMM uses two tables: a MDI table and a CBR table. The monitored IOS devices support MDI and CBR as follows:
   - The Cisco 7600 platform supports both MDI and CBR. The Vidmon implementation on Cisco 7600 devices uses a MDI table or a CBR table.
     
     The MDI table contains both DF and MDI information. The CBR table contains DF and MRV information.
   - ASR 9000 Series devices support only CBR through a CBR table.

2. When CMM detects a video flow it looks for the presence of an MDI table. If there is an MDI table, then CMM retrieves DF and MLR information.

3. If there is no MDI table, CMM examines the CBR table for the flow and retrieves DF and MRV information from the CBR table.

### MRV Reporting

For Cisco 7600 devices CMM allows you to set a MLR threshold in packets

### DF Reporting

For both Cisco 7600 series devices and Cisco ASR 9000 series (Viking) devices, CMM allows you to set a delay factor in milliseconds and generate a VIDEO DF HIGH event when the DF threshold is exceeded.

### MRV Reporting

For both Cisco 7600 series devices and Cisco ASR 9000 series (Viking) devices, CMM allows you to set a maximum and minimum MRV rate in millisecond percentages, and generates alerts if the maximum or minimum MRV is exceeded:

- When a specified MRV Maximum threshold is exceeded, CMM generates a VIDMON MRV HIGH alert.
- When a specified MRV Minimum threshold is reached, CMM generates a VIDMON MRV LOW alert.

Using the Graphs tab in the CMM Dashboard interface, you can view real-time graphs that compare MLR, DF, and MRV data for up to four devices at a time.
Additional Product Features

CMM 3.1 provides the following features:

- **Automated Multicast Discovery** — CMM discovers complete multicast topology from a single seed device, along with the MVPN provider and provider edge devices and VRF tables they support. Discovery bridges the provide edge to the customer edge to create an end-to-end view of the multicast environment.

CMM discovery includes the ability to discover the routers in the service provider network by starting with a single router in the service provider network (PE or P router) as well as discovery of the CE routers in the Enterprise networks. Both IOS and IOS-XR based routers are supported.

- **Alerts and Reports** — Any exceptions detected by the polling engine are sent as Simple Network Management Protocol (SNMP) traps and logged for reporting purposes. Reports are available for Rendezvous Points (RPs), Source-Group (S,G) PPS rates, tree changes, interface bandwidth, Layer 2 port PPS rates. Real-time alerts originating from an IneoQuest iVMS application are also actionable through the video operations solution (VOS) add-on.

- **Show All Groups Feature**

- **IGMP Diagnostics** — Displays all devices that have seen an Internet Group Management Protocol (IGMP) join for a particular group

- **MSDP Status** — Shows the status of all Multicast Source Discovery Protocol (MSDP)-enabled devices and their peers, including Source-Active cache information.

- **Layer 2 Diagnostics** — Shows which multicast groups are being forwarded on a particular Layer 2 switch port

- **Health Check** — Provides on-demand checking of forwarding trees; RPs and checking for the existence of specific S,Gs can also be scheduled to run automatically.

- **6500/7600 Troubleshooting** — Provides the equivalent of a Cisco IOS Software command-line interface “show tech” for multicast, along with Local Target Logic (LTL) checking and PPS rates taken from the route processor, switch processor, or distributed forwarding card. For example, you can execute the `show mls ip multicast statistics` command to output statistics on multicast flows on a specified device. Output can be e-mailed directly to the Cisco Technical Assistance Center for further analysis. For information on using this feature, see 6500/7600 Troubleshooting, page 8-14.

- **Configurable SNMP Trap Descriptor** — Support for user configuration of the descriptor for SNMP traps issued by CMM. This configuration will be on a per domain-basis.

- **Explicit User Tracking** — CMM supports the ability to identify the multicast receivers connected to a Catalyst 6500 devices with IOS version 12.2(33) and higher. Three use cases are supported:
  - **Device Query** — Generates a list of receiver information based on a specified device.
  - **Stream Query** — Generates a list of receiver information based on a specified (S,G).
  - **Receiver Query** — Generates stream flow information based on a specified receiver IP address.

- **Identify PIM Interfaces That are Down** — CMM trace logic relies on Protocol Independent Multicast (PIM) interface reachability. If any one of the PIM interfaces along the multicast tree is down, the trace will not be completed and the user does not know the problem. CMM provides a feature to show the users which PIM interfaces are down. The analysis will be done on a per-domain basis.

- **Configurable Login Message** — CMM 3.1 provides a login message that is presented to users immediately after they successfully log in to the application. This message is configurable by an administrator and allow messages of at least 1600 Unicode characters. The message must be
specifically acknowledged to continue with the login. Users can disable this feature, if no login message is desired. Typical uses of such a message are an unauthorized use warning message or to remind users of planned application downtime, etc.

- **Northbound API**—CMM provides a software development kit (SDK) that allows you to develop a client application that communicates with CMM by using Web Services Definition Language (WSDL) messages. The API operations provided by the SDK allow you to perform tasks such as:
  - Getting a trace image file from the CMM server for use by your application.
  - Getting the Source and Group (S,G) in a domain or on a device.
  - Getting multicast events.
  - Getting the multicast devices in a domain.
  - Adding Layer 2 devices, Layer 3 devices, or video probes in bulk.
  - Adding, deleting, and viewing polling configurations.
Getting Started

This chapter contains the following sections:

- Logging into Cisco Multicast Manager, page 2-1
- Navigating the GUI, page 2-2

Logging into Cisco Multicast Manager

*Note*
For details on stopping and starting Cisco Multicast Manager on Solaris and Linux, see the *Installation Guide for the Cisco Multicast Manager 3.1*.

To access Cisco Multicast Manager (CMM), enter the IP address or the name of the server where the software is installed; for example: https://172.20.110.23:8080. The default port of 8080 can be changed as described in the installation instructions.

*Note*
Secure Sockets Layer (SSL) will be active by default.

**Figure 2-1  Cisco Multicast Manager Login Page**

The Login screen appears.
Enter the credentials to log into CMM. The default CMM username is admin, and the default CMM password is rmsmmt. Click Login.

If the system administrator has configured a login alert, a message displays. Click the Accept button to accept the terms of use.

**Navigating the GUI**

For Cisco Multicast Manager Version 3.1 there are multiple methods of navigating the interface.

**Menu**

When you first log into Cisco Multicast Manager, the Multicast Manager Main Menu page appears. Select a main menu item to navigate to the submenu items.

![Cisco Multicast Manager Main Menu Page](image)

**Devices Tab**

The Devices tab contains a list of devices discovered per domain.

To view the Devices tab:

**Step 1** Click the Devices tab.

The Devices tab appears, as shown in Figure 2-3. The pane at the left of the page lists the devices for the current domain.
Chapter 2      Getting Started

Navigating the GUI

Figure 2-3    Cisco Multicast Manager Device Tab

![Cisco Multicast Manager Device Tab]

Step 2  Click a device link.

The Device page for the selected device appears, as shown in Figure 2-4.

Figure 2-4    Device Page

![Device Page]

The Device page shows the Protocol Independent Multicast (PIM) neighbors, PIM Interface Mode, IGMP information, and Rendezvous Points (RPs) for the selected device.

Step 3  Enter the User Name for the device.

Step 4  Enter the Password.

Step 5  Enter the Enable Password for the device.

Step 6  Enter an IOS command in the Show Command field.
Step 7  Click Show to display the output.

Cisco Multicast Manager Dashboard

Select the Dashboard view from the Main Menu page.

Figure 2-5  CMM Dashboard

The CMM Dashboard contains two panes: a Latest Events pane that shows the latest CMM events and a Traps pane that shows the latest SNMP traps forwarded to CMM.

Each tab allows you to navigate to a different summary view:

- Click the Latest Events tab to view the latest multicast events.
- Click the SG Events tab to view the latest Source, Group events, including SG threshold events, Group Gone events, and Selective Source Monitoring events.
- Click the Bandwidth Events tab to view bandwidth events and L2 threshold events.
- Click the Tree Events tab to view tree events, including tree change events and SG Delta events.
- Click the MPVN Events tab to view MPVN events, including MDT source events, MDT default events, VRF interface count events, and VRF count events.
Chapter 2      Getting Started

Navigating the GUI

- Click the **RP Events** tab to view Rendezvous Point (RP) events, including RP polling events, RP group threshold events, and SSG events.
- Click the **Video Events** tab to view video events, such as Vidmon MLR High, DF High, or Vidmon MRV high or low events. The events on the video events view are presented in two panes: the Video Probe Events pane and the Vidmon Events pane.
- Click the **CRM Events** tab to view CRM events, including Specific Unicast Route events and Specific Multicast route events.
- Click the **Summary** tab to view statistics for events for each event defined in CMM a bar graph report showing the events in each event category. The statistical report displays the statistics for the last 24 hours. The Summary tab also shows the domain details for each domain, including the Domain name, the number of devices in each domain, and the number of events for the domain.
- Click the **Graphs** tab to display graphs that indicate real-time statistics for up to four selected devices.

Running a Trace from the Dashboard

For S,G events listed in the Events pane on the CMM Dashboard, you can click on the link shown in the event listing to bring up an S,G trace for the events.

For devices that are communicating with a video probe, the trace shows video probe information, and for devices that are communicating with Vidmon devices, the trace shows Vidmon information.

Displaying a Trap Details List from the Traps Pane

For SNMP events that are shown in the Traps pane, click on the SNMP trap name in the Details column to display the details of the SNMP trap.

Viewing Performance Graphs from the Dashboard

To view up to four performance graphs from the dashboard:

**Step 1** Click the **Graphs** tab.

**Step 2** The Graphs page appears, as shown in Figure 2-6.
The Graphs page shows up to four graphs that indicate real-time performance statistics for devices that have events showing on the Dashboard.

By default, CMM displays the last four graph report requested. For example, the Graphs page shown in Figure 2-6 displays MLR graphs for two video probes in the network, and a DF report for a Vidmon device, and a DF report for a video probe.

Step 3  
To change the settings for one of the graphs, click the **Settings** button.

The Graph Settings dialog appears, as shown in Figure 2-7.
**Step 4** On the Graph Settings dialog, specify the settings for a new graph, as indicated in Table 2-1.

**Table 2-1** Graph Settings Options

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Graph Type** | From the drop-down list in the Graph Type field, choose the type of graph to display:  
  - **SG**—Display a Source, Group statistics graph.  
  - **Video Probe**—Display statistics for a video probe.  
  - **Vidmon**—Display statistics for a Vidmon device. |
| **Units** | From the drop-down list in the Units field, choose the units for the graph.  
  The units vary depending on the type of graph selected.  
  For a SG graph, you can select:  
  - **PPS**—Packets per second.  
  - **BPS**—Bits per second.  
  For a Video Probe graph, you can select:  
  - **DF**—Delay Factor.  
  - **MLR**—Media Loss Rate.  
  For a Vidmon device graph, you can select:  
  - **DF**—Delay Factor.  
  - **MLR**—Media Loss Rate.  
  - **MRV**—Media Rate Variation. |
Step 5  Click the Submit button to submit the settings for the graph.

The Graphs page displays a graph for the selected graph type.

### Table 2-1  Graph Settings Options (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>From the drop-down list, chose the domain for the device.</td>
</tr>
<tr>
<td>Device</td>
<td>From the drop-down list, chose a device.</td>
</tr>
<tr>
<td>Interface</td>
<td>The Interface field is available only for Vidmon devices. From the drop-down list, select the interface to monitor for the graph.</td>
</tr>
<tr>
<td>Direction</td>
<td>The direction field is available only for Vidmon devices. From the drop-down list, choose <strong>Inbound</strong> or <strong>Outbound</strong>.</td>
</tr>
<tr>
<td>Source</td>
<td>From the drop-down list, choose a source address.</td>
</tr>
<tr>
<td>Group</td>
<td>From the drop-down list, choose a group address</td>
</tr>
<tr>
<td>Refresh Rate</td>
<td>From the drop-down list, choose a refresh rate.</td>
</tr>
</tbody>
</table>
Initial System Setup

This chapter describes the tasks for initial setup and configuration of Cisco Multicast Manager. The sections in the chapter describe the general steps you must complete to set up the system and refer you to the reference chapters of this guide for more detailed information.

Basic Setup and Configuration Steps

The following table indicates the main steps for setting up and configuring Cisco Multicast Manager.

<table>
<thead>
<tr>
<th>Step</th>
<th>Purpose and Description</th>
</tr>
</thead>
</table>
| Step 1 | Install Cisco Multicast Manager.  
Install the software.  
See the *Installation Guide for Cisco Multicast Manager 3.1*. |
| Step 2 | Create a Domain  
Create domains to set up different types of monitoring. For example, you might create one domain for monitoring an enterprise network and another domain to monitor core devices on the network.  
See Creating a Domain, page 4-1. |
| Step 3 | Configure Global Polling  
Specify a start and stop time for each type of polling performed by CMM. See Global Polling Configuration, page 4-5. |
| Step 4 | Run Discovery  
Before you can configure monitoring CMM must discover the devices in the monitored network. See Discovery, page 6-1.  
You can run three types of discovery:  
- **Core/Enterprise Discovery**—Use Core/Enterprise Discovery to discover the multicast devices in your core/enterprise network.  
- **Distributed Network Discovery**—Use Distributed Network Discovery to discover the customer sites using Provider Edge (PE) devices or Customer Edge (CE) devices and associated PE Devices in a distributed network such as an IP/MPLS network.  
- **Single Device Discovery**—Use Single Device Discovery to discover a single device or a device and its adjacent PIM neighbors. |
### Chapter 3      Initial System Setup

#### Basic Setup and Configuration Steps

<table>
<thead>
<tr>
<th>Step</th>
<th>Purpose and Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong></td>
<td>Configure Users</td>
</tr>
<tr>
<td>To configure users:</td>
<td></td>
</tr>
<tr>
<td>• Add users and assign them to the appropriate user class. See User Configuration, page 10-1.</td>
<td></td>
</tr>
<tr>
<td>• Set up access privileges for specified user classes. See Access Control, page 10-3.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Configure Authentication</td>
</tr>
<tr>
<td>Specify how users are authenticated:</td>
<td></td>
</tr>
<tr>
<td>• Specify the type of user authentication used by CMM, for example local authentication, TACACS+ authentication or RADIUS authentication. See Authentication &amp; Audit, page 10-3.</td>
<td></td>
</tr>
<tr>
<td>• (Optional) If you want CMM to use Cisco Secure Access Control Server (Cisco ACS) to perform user access, authentication, and audit (AAA) functions, see ACS Server, page 10-4.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Configure Multicast Polling Configuration and Reports</td>
</tr>
<tr>
<td>Configure the types of monitoring that you will use to monitor the devices in your multicast network. You can specify the following general types of polling:</td>
<td></td>
</tr>
<tr>
<td>• <strong>Traffic Polling</strong>—Poll multicast traffic by source and group (SG polling)</td>
<td></td>
</tr>
<tr>
<td>• <strong>Tree Polling</strong>—Set up polling for a specific part of the network tree.</td>
<td></td>
</tr>
<tr>
<td>In addition, you can configure the following types of polling:</td>
<td></td>
</tr>
<tr>
<td>• Health Checks.</td>
<td></td>
</tr>
<tr>
<td>Health Check, page 5-27.</td>
<td></td>
</tr>
<tr>
<td>• Video Probe Polling.</td>
<td></td>
</tr>
<tr>
<td>Video Probe, page 5-30.</td>
<td></td>
</tr>
<tr>
<td>• Vidmon Polling.</td>
<td></td>
</tr>
<tr>
<td>Vidmon Polling, page 5-32.</td>
<td></td>
</tr>
<tr>
<td>• MVPN Polling.</td>
<td></td>
</tr>
<tr>
<td>MVPN Polling, page 5-38.</td>
<td></td>
</tr>
</tbody>
</table>
System Configuration

This chapter contains the following sections:

- Domain Management, page 4-1
- Global Polling Configuration, page 4-5

Domain Management

Before you can begin managing your networks, you must create a domain. A domain is a collection of multicast routers, Layer 2 (L2) devices, video probe, and VidMon devices. Multiple domains can exist, and routers can belong to multiple domains. Using Domain Management, you can create and edit domains.

You can create a domain by in two ways:

- By adding a domain and setting the domain configuration options on the System Configuration page.
  See Creating a Domain, page 4-1.
- By importing an existing domain configuration from a comma-separated value (CSV) file.
  See Importing a Domain, page 4-5.

Creating a Domain

To create a domain:

1. From the Multicast Manager menu, select System Configuration.
2. Select Domain Management.

The Domain Management Summary page appears, as shown in Figure 4-1.
The list of domains shows any domains that have been defined previously and indicates whether they have been discovered. You can discover undiscovered domains by clicking the Start Discovery link for the domain, and you can rediscover previously discovered domains by clicking the Re-discovery link for the domain.

**Step 3** To add a new domain, click the Add button and from the drop-down list, choose By Domain.

**Step 4** To edit an existing domain, check the check box for the desired domain listing and click Edit.

If you click Add and choose By Domain or click Edit, the System Configuration page appears, as shown in Figure 4-2.

**Figure 4-1** Domain Management Summary Page

![Domain Management Summary Page](image1)

**Figure 4-2** System Configuration Page

![System Configuration Page](image2)
The System Configuration page contains the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Domain Name</td>
<td>A management domain is defined as a contiguous group of PIM neighbors sharing the same SNMP community string.</td>
</tr>
<tr>
<td>Read Only</td>
<td>SNMP read-only community string. Verify the string.</td>
</tr>
<tr>
<td>Read Write</td>
<td>SNMP read-write community string. This is required for retrieving and validating device configurations. Verify the string.</td>
</tr>
<tr>
<td>SNMP Timeout</td>
<td>Retry period if the node does not respond. Default value is 0.8.</td>
</tr>
<tr>
<td>SNMP Retries</td>
<td>Number of retries to contact a node before issuing a timeout. Default value is 2.</td>
</tr>
<tr>
<td>TFTP Server</td>
<td>TFTP server IP address. Default is the IP address of the Cisco Multicast Manager server.</td>
</tr>
<tr>
<td>VTY Password</td>
<td>Enter the VTY password and verify the password.</td>
</tr>
<tr>
<td>Enable Password</td>
<td>Enter the password and verify the password. The application will use this value for execution of some CLI commands over non-VRF aware devices.</td>
</tr>
<tr>
<td>TACACS/RADIUS Username</td>
<td>If you are using TACACS/RADIUS, you can enter a username here.</td>
</tr>
<tr>
<td></td>
<td>If you enter a TACACS/RADIUS username and password here, the application will use these values for internal CLI command execution over non-VRF aware devices regardless of who is logged in. Users can also enter their own username and password when issuing show commands.</td>
</tr>
<tr>
<td>TACACS/RADIUS Password</td>
<td>If you are using TACACS/RADIUS, you can enter a password here.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If you enter a TACACS/RADIUS username and password here, the application will use these values regardless of who is logged in. Users can also enter their own username and password when issuing show commands.</td>
</tr>
<tr>
<td>CLI Access</td>
<td>Select either Telnet or SSH.</td>
</tr>
<tr>
<td>Threshold Polling</td>
<td>Check the check box for enabling CLI mode of threshold polling. The routers being polled are the ones for which Cisco IOS and chassis information were configured in the rmspollcli.conf file.</td>
</tr>
</tbody>
</table>
## Domain Management

**Chapter 4  System Configuration**

### Step 5

Complete the fields in the System Configuration page and click **Save**, **Reset** to clear the data fields and create the new domain. Click **Cancel** to exit without creating a domain.

The new domain name appears in the list of domains on the Domain Management page.

### Step 6

If you want to discover the devices in the domain at this time, click on the Start Discovery link in the table row for the domain.

If you click on **Start Discovery**, the Multicast Discovery page appears, which allows you to enter parameters for the discovery process.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cache TACACS Info</td>
<td>Check the check box to cache the TACACS username and password until the browser is closed. This eliminates the need to enter the username and password each time that you issue a router command from the application.</td>
</tr>
<tr>
<td>Resolve Addresses</td>
<td>Performs Domain Name System (DNS) lookups on all sources found. The DNS name appears alongside the IP address on the “Show All Groups” screen. If the server is not configured for DNS, then do not check the box. If the box is checked, you may receive a slower response, because the application is trying to resolve names. We recommend disabling this option if your network contains a large number of source and groups (S,Gs). The Resolve Addresses option also causes discovery to do a reverse DNS lookup on a device name. The IP address returned by DNS is then used for management purposes. Otherwise, the IP address by which the device is found is used for management purposes.</td>
</tr>
<tr>
<td>Use Cache</td>
<td>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 S,G cache when showing lists of sources and groups, rather then retrieving them again from the RPs in the network. The cache can also be refreshed manually by clicking the <strong>Reload Cache</strong> button in the Multicast Diagnostics window. This button appears only if you have the <strong>Use Cache</strong> option selected. We highly recommend that you use the S,G cache option. If there are no RPs in the domain being discovered, then the S,G 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 S,G cache is updated only when you click the <strong>Reload Cache</strong> button.</td>
</tr>
</tbody>
</table>
Step 7 For information on the Multicast Discovery page and discovering a domain, see Multicast Discovery, page 6-1.

Rediscovering a Domain
On the Domain Management domains, domains that have been previously discovered have a Re-discovery link in the table row for the domain.
If you want to rediscover the domain, click the Re-discovery link for the domain.
If you click on Start Discovery, the Multicast Discovery page appears, which allows you to enter parameters for the discovery process.
For information on the Multicast Discovery page and discovering a domain, see Multicast Discovery, page 6-1.

Importing a Domain
To import a domain:

Step 1 From the Multicast Manager menu, select System Configuration.
Step 2 Select Domain Management.
Step 3 From the drop-down list in the Add field, choose By Import button to import a new domain.
Step 4 Click the Browse button to locate the CSV file that contains the domain information to import.
Step 5 Click the Upload button.

Note After the upload process is initiated, the System Configuration page populates with information.

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

Note You must restart the polling daemon after making changes on this page. Click the Restart button in the Polling Actions field to restart polling. Click the Stop button to stop polling.

To configure global polling:

Step 1 From the Multicast Manager menu, select System Configuration.
Step 2 Select Global Polling Configuration.
The Global Polling Configuration page appears.
Step 3 On the top part of the Global Polling Configuration page, configure polling intervals and run times for each type of polling, as indicated in Table 4-1.
Setting any one of these values to less than 1 disables that specific polling feature.

<table>
<thead>
<tr>
<th>Field or Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Run Times—Use Defaults</td>
<td>Selecting the Use Defaults check box sets all the start and stop times, and days to the default values.</td>
</tr>
<tr>
<td>DR Polling Interval</td>
<td>Checks the status of all DRs in the network. If a user changes a DR, an SNMP trap is sent.</td>
</tr>
<tr>
<td>Layer 2 Polling Interval</td>
<td>Time between polling of the Layer 2 ports.</td>
</tr>
<tr>
<td>Route Monitor Polling Interval</td>
<td>Specify a time interval for route monitor polling.</td>
</tr>
<tr>
<td>Specific Route Monitor Polling Interval</td>
<td>Specify a time interval for specific route monitor polling.</td>
</tr>
<tr>
<td>RP Polling Interval</td>
<td>Specify a time interval for RP polling.</td>
</tr>
<tr>
<td>RP Status Polling Interval</td>
<td>RP Status Polling queries the sysUpTime of the RPs configured on the RP Polling Configuration page. The purpose of this query is to report availability of the RPs. If the RP responds, an \textit{rpReachable} trap is sent. If the RP does not respond, an \textit{rpUnreachable} trap is sent. Since at least one of these traps is sent at each polling interval, you can also use them to ensure that the polling daemon is up and running.</td>
</tr>
<tr>
<td>RPF Failure Polling Interval</td>
<td>Time interval at which each router will be polled for each source and group configured, to check the number of RPF failures.</td>
</tr>
<tr>
<td>Threshold Polling Interval</td>
<td>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.</td>
</tr>
<tr>
<td>Multicast Topology Polling Interval</td>
<td>Topology polling queries the sysUpTime of each router in the multicast domain to see if it has been reloaded. If it has, the polling daemon launches a Single Router Discovery of that device in the background, to ensure that the SNMP ifIndexes have not changed.</td>
</tr>
<tr>
<td>Tree Polling Interval</td>
<td>Time interval at which the monitored trees are drawn and compared with their baselines.</td>
</tr>
<tr>
<td>Interface Polling Interval</td>
<td>Time interval where the percent of multicast bandwidth per interface is compared to the thresholds.</td>
</tr>
<tr>
<td>Health Polling Interval</td>
<td>Time interval at which the configured health checks are scheduled to run.</td>
</tr>
</tbody>
</table>
Table 4-1  Global Polling Configuration Options (continued)

<table>
<thead>
<tr>
<th>Field or Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selective Source Polling Intervals</td>
<td>Time intervals set to the source and group to be monitored for the particular time and day. The time interval configured should not be overlapping for the same source and group.</td>
</tr>
<tr>
<td>Heart Beat Polling Interval</td>
<td>Time interval at which the heart beat trap is sent to the northbound application. These traps serve as the notification about the health of the polling daemon.</td>
</tr>
<tr>
<td>MVPN Polling Interval</td>
<td>Frequency MVPN data and whose entries would be polled PE devices.</td>
</tr>
<tr>
<td>Video Probe Polling Interval</td>
<td>Time interval that the video probes are polled for MDI values.</td>
</tr>
<tr>
<td>Vidmon Polling Interval</td>
<td>Time interval that Vidmon devices (Cisco 7600 series routers and in ASR 9000 Series (Viking) devices are polled for Cisco Vidmon statistics.</td>
</tr>
<tr>
<td>Note</td>
<td>If you are monitoring 1000 or more flows, Cisco recommends that you set the Vidmon Polling interval to 1 min.</td>
</tr>
<tr>
<td>Video Probe Clear Timer</td>
<td>Interval that Cisco Multicast Manager changes a yellow warning indicator to a green OK indicator.</td>
</tr>
<tr>
<td>Save</td>
<td>Sets the values that you have entered.</td>
</tr>
</tbody>
</table>

Step 4  Scroll down the page to see the Trap Receiver and Global Default E-mail configuration sections of the page, shown in Figure 4-3.
Step 5  To enable or disable the continuous sending of PPS threshold traps, use the Enable Rising/Falling and Normalized Traps for Thresholds section:

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

Step 6  To add trap receivers, complete these steps:

a. Go to the Configure Global Default SNMP Trap Receivers section.

b. Enter the IP address for the trap receiver.

c. Click the Add button.

The IP address appears in the Configured Trap Receivers list.

d. If you want to forward Mixed Signal traps northbound to another application, check the Forward Mixed Signal Traps check box.

Note  If you enable the Mixed Signal trap forwarding option, the Mixed Signal traps are not displayed on the trap viewer page.
Note 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 Domain Trap/Email Polling Configuration page.

e. Click the Save button.

A message appears instructing you to start the snmptrapd processes to cause the changes in Mixed Signal trap forwarding to take effect.

Step 7 To remove trap receivers, click the IP address of the trap receiver that you want to remove and then click the Remove button, then click Save.

Step 8 To add or remove e-mail addresses, use the Configure Global Default E-mail Addresses for Event Notification section. E-mail addresses are notified of SSG exceptions and threshold related events. The e-mail addresses specified here are used only if domain-specific e-mail addresses are not specified. Domain-specific email addresses are specified from the Domain Trap/Email Polling Configuration page.
Polling Configuration and Reports

This chapter contains the following sections:

- Event Viewer, page 5-1
- Trap Viewer, page 5-2
- Domain Trap/Email, page 5-3
- Traffic & Polling Reports, page 5-5
- Tree Polling & Reports, page 5-13
- Miscellaneous Polling & Reports, page 5-18
- CRM Polling, page 5-43

**Note**

You must restart the polling daemon after making configuration changes in this section. Click the **Restart** button in the Polling Actions field to restart polling. Click the **Stop** button to stop polling.

**Event Viewer**

The Event Viewer displays the events, per domain, in descending order by time.

To use the Event Viewer:

**Step 1**

Choose **Polling Configuration & Reports > Event Viewer**.

The Event Viewer appears, as shown in Figure 5-1.
The Event Viewer shown in Figure 5-1 is set up to show Latest Events (the default setting). The first field shown on the Event Viewers is the Event ID field.

You can change the information that is shown in the other fields.

**Step 2**
To specify parameters for filtering event views, select **Report Parameters**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Type</td>
<td>Select an event type from the drop-down list.</td>
</tr>
<tr>
<td>From Date</td>
<td>Enter or select a start date.</td>
</tr>
<tr>
<td>To Date</td>
<td>Enter or select an end date.</td>
</tr>
<tr>
<td>Device</td>
<td>Select a device from the drop-down list.</td>
</tr>
<tr>
<td>Source</td>
<td>Select a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Select a group from the drop-down list.</td>
</tr>
<tr>
<td>Baseline Name</td>
<td>Enter the baseline name.</td>
</tr>
</tbody>
</table>

**Step 3**
Click **Submit**.

The Event Viewer appears with the specified events shown.

---

**Trap Viewer**

To view the SNMP traps generated by the monitored network devices:

**Step 1**
On the CMM menu, select **Polling Configuration & Reports**.

**Step 2**
Click **Trap Viewer**

The Trap Viewer page appears, as shown in Figure 5-2.
Figure 5-2  Polling Configuration Trap Viewer

The Trap Viewer page displays the traps generated by the monitored network devices. The first field shown on the Trap Viewer is always the trap ID.

**Step 3**
To modify the specification for the data shown in the other fields, select **Report Parameters** to filter the trap views.

**Note**
The Source, Group and Baseline Name fields are disabled by default.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Date</td>
<td>Enter or select a start date.</td>
</tr>
<tr>
<td>To Date</td>
<td>Enter or select an end date.</td>
</tr>
<tr>
<td>Submit</td>
<td>Sets the values that you enter.</td>
</tr>
</tbody>
</table>

**Domain Trap/Email**

You can configure CMM to use domain-specific SNMP trap receivers and to send e-mail to specified addresses when SSG exceptions or threshold-related events occur.

**Note**
The settings on this screen are domain specific. The values specified on this screen override any trap receivers or e-mail settings configured on the Global Polling Configuration screen. If trap receivers and/or e-mail addresses are not specified on the Domain Trap/Email Configuration page, then the values from the global polling configuration are used.

To configure Domain Trap/E-mail Settings:

**Step 1**
Select **Polling Configuration & Reports**.
Step 2  Click **Domain Trap/Email**.

The Domain Trap/Email page appears, as shown in Figure 5-3.

**Figure 5-3   Domain Trap/Email**

Step 3  To add or remove trap receivers, enter information on the Configure Domain Specific SNMP Trap Receivers section.

| Note | 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 **Global Polling Configuration, page 4-5**). |

Step 4  Specify the following information to add a trap receiver.

**Table 5-1   Add Trap Receiver Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Trap Receiver</td>
<td>Enter the IP address of a trap receiver, for example a video probe.</td>
</tr>
<tr>
<td>Description 1</td>
<td>Enter a description of the trap receiver.</td>
</tr>
<tr>
<td>Description 2</td>
<td>If desired, add additional text to describe the trap receiver.</td>
</tr>
</tbody>
</table>

*Note* Description1 and Description 2 are configurable trap descriptors. If these fields are configured, then all traps sent northbound from CMM will contain the specified information. This information can help users to identify the traps.

| Add                     | Adds the IP address of the trap receiver to the list of configured trap receivers. |
| Remove                  | Removes the IP address of the trap receiver from the list of configured trap receivers. |
**Step 5**  To add or remove e-mail addresses, use the Configure Domain Specific Email Addresses for Event Notification section.

**Note**  E-mail addresses are notified of SSG exceptions and threshold-related events. The e-mail addresses specified here are only used if global e-mail addresses are not specified. Global e-mail addresses are specified from the Configure Global Default Email Addresses for Event Notification (see Global Polling Configuration, page 4-5).

**Step 6**  Specify the following information to add an e-mail address.

**Table 5-2  Add Email Address Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Email Address</td>
<td>Enter an e-mail address to use for SSG exceptions and threshold events.</td>
</tr>
<tr>
<td>Add</td>
<td>Adds the specified email address to the list of configured email addresses.</td>
</tr>
<tr>
<td>Remove</td>
<td>Removes the selected email address from the list of configured email addresses.</td>
</tr>
</tbody>
</table>

**Step 7**  To save the configuration, click the **Save Domain Trap Email** button.

---

**Traffic & Polling Reports**

**S,G**

Using Cisco Multicast Manager, you can poll sources and groups with high and low thresholds. You can select a source and group from the list, or you can enter them manually. If there are many sources and groups to choose from, you can use the filter option to ensure that you are selecting an S,G that actually exists on the network. The filter option displays only the sources for a selected group, or only the groups for a selected source.

Using time-based SG polling, you can configure up to 50 times at which CMM will poll high and low thresholds for each Source and Group.

**Tip**  Pressing shift and control simultaneously allows you to select more than one item from a list.

**S,G Threshold Report**

Using the S,G Threshold Report, you can view information about PPS/BPS rate deviation on multicast routers that are configured for polling.

To view an S,G Threshold Report:
Step 1 From the Multicast Manager menu, select **Polling Configuration & Reports**.

Step 2 Select **Traffic Polling & Reports**.

Step 3 Select **S,G**.

Step 4 Select **Report Parameters**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Date</td>
<td>Enter or select a start date.</td>
</tr>
<tr>
<td>To Date</td>
<td>Enter or select an end date.</td>
</tr>
<tr>
<td>Device</td>
<td>Select a device from the drop-down list.</td>
</tr>
<tr>
<td>Source</td>
<td>Select a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Select a group from the drop-down list.</td>
</tr>
<tr>
<td>Baseline Name</td>
<td>Enter the baseline name.</td>
</tr>
<tr>
<td>Submit</td>
<td>Sets the values that you enter.</td>
</tr>
</tbody>
</table>

**Note**
You can also view the Historical Graph and Group Gone Report.

**Historical Graph**

Using historical graphs, you can view historical data in a graph format. Historical data is collected when you start to monitor the network using a specific polling configuration.

To view a historical graph for S,G polling:

Step 1 From the Multicast Manager menu, select **Polling Configuration & Reports**.

Step 2 Select **Traffic Polling & Reports**.

Step 3 Select **S,G**.

Step 4 Select **Historical Graph**.

Step 5 In the Units field, select either PPS or BPS from the drop-down menu.

Step 6 Click the **Get Report(s)** button to refresh the display of multicast streams being monitored.

Step 7 In the **From Date** field, choose a date from the calendar.

Step 8 In the **To Date** field, choose a date from the calendar.

Step 9 Select up to three multicast streams from the table.

Step 10 Click the **Show Report** button to chart a graph.

Individual streams will indicated will be color coded with a unique color.
Group Gone Report

Source and group make up a multicast stream monitor on a device. If a multicast stream that is being monitored on a device disappears from that device, then CMM generates a report called a Group Gone Report. The Group Gone Report is a list all events pertaining to the stream.

To view a Group Gone report:

- **Step 1** From the Multicast Manager menu, select **Polling Configuration & Reports**.
- **Step 2** Select **Traffic Polling & Reports**.
- **Step 3** Select **S,G**.
- **Step 4** Select **Group Gone Report**.
- **Step 5** Click **Report Parameters** and set the parameters for the report.
- **Step 6** Click the **Submit** button.

Config S,G Polling

**By S,G**

- **Step 1** From the Multicast Manager menu, select **Polling Configuration & Reports**.
- **Step 2** Select **Traffic Polling & Reports**.
- **Step 3** Select **S,G**.
- **Step 4** Select **Config SG Polling**.
- **Step 5** Click the **Add** button.
- **Step 6** Select **By S,G**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Select a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Select a group from the drop-down list.</td>
</tr>
<tr>
<td>Reset SG List</td>
<td>Refreshes the source and group lists.</td>
</tr>
<tr>
<td>Select Router</td>
<td>Select a router/routers to configure SG polling.</td>
</tr>
<tr>
<td>Units</td>
<td>Select either packets per sampling period or bytes per sampling period.</td>
</tr>
<tr>
<td>High Threshold</td>
<td>Enter the high threshold value. If the value is exceeded, Cisco Multicast Manager generates a report.</td>
</tr>
<tr>
<td>Low Threshold</td>
<td>Enter the low threshold value. If that if the value is exceeded, Cisco Multicast Manager generates a report.</td>
</tr>
</tbody>
</table>
By Device

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

To configure SG polling for a particular device:

**Step 1** From the Multicast Manager menu, select **Polling Configuration & Reports**.
**Step 2** Select **Traffic Polling & Reports**.
**Step 3** Select **S,G**.
**Step 4** Select **Config SG Polling**.
**Step 5** Click the **Add** button.
**Step 6** Select **By Device**.

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

<table>
<thead>
<tr>
<th>Fields and Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Filter Regexp</td>
<td>Enter any part of the multicast address. Only those that match appear.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Select referees to update the source and group displayed for the entered group filter regular expression and the selected router.</td>
</tr>
<tr>
<td>Select Routers</td>
<td>Select the router name.</td>
</tr>
<tr>
<td>Units</td>
<td>Select either packets per sampling period (pps) or bits per sampling period (bps).</td>
</tr>
<tr>
<td>High Threshold</td>
<td>Enter the high threshold value. If the value is exceeded, Cisco Multicast Manager generates a report.</td>
</tr>
<tr>
<td>Low Threshold</td>
<td>Enter the low threshold value. If that if the value is exceeded, Cisco Multicast Manager generates a report.</td>
</tr>
</tbody>
</table>

By Import

To configure SG polling by importing a file:

**Step 1** From the Multicast Manager menu, select **Polling Configuration & Reports**.
**Step 2** Select **Traffic Polling & Reports**.
**Step 3** Select **S,G**.
**Step 4** Select **Config SG Polling**.
**Step 5** Click the **Add** button.
**Step 6** Select **By Import**.
**Step 7** Click the **Browse** button to upload the file.
Chapter 5      Polling Configuration and Reports

Traffic & Polling Reports

Step 8  Select **Merge** to unify an existing configuration with the new configuration or select **Replace** to overwrite the existing configuration.

Step 9  Click **Upload**.

**Config Time-Based SG Polling**

To configure Time-Based SG Polling:

**Step 1**  On the SG Polling page, select **Config Time-Based SG Polling**.

**Step 2**  On the SG Time based Configurations page, click the **Add** button and from the drop-down list, select **By SG Time**.

**Note**  You can also choose **By Import** to import a CSV file with Time-Based SG polling parameters.

**Step 3**  Set the following parameters on the SG Time Based Configurations page:

<table>
<thead>
<tr>
<th><strong>Source</strong></th>
<th>Enter or select the IP address of the source to monitor.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Group</strong></td>
<td>Enter or select the IP address of the group to monitor.</td>
</tr>
<tr>
<td><strong>Reset SG List</strong></td>
<td>Clears any entries and refreshes the source and group lists.</td>
</tr>
<tr>
<td><strong>Select Routers</strong></td>
<td>Select routers to add to the polling configuration</td>
</tr>
<tr>
<td><strong>Units</strong></td>
<td>Select either packets per sampling period (PPS) or bits per sampling period (bps).</td>
</tr>
<tr>
<td><strong>High Threshold</strong></td>
<td>Enter the high threshold that, if exceeded, generates a report.</td>
</tr>
<tr>
<td><strong>Low Threshold</strong></td>
<td>Enter the low threshold that, if exceeded, generates a report.</td>
</tr>
<tr>
<td><strong>Run Time Intervals</strong></td>
<td>Enter the date and time to run the polling.</td>
</tr>
</tbody>
</table>

**Step 4**  Click the **Save** button.

**L2 Polling**

You can add Layer 2 (L2) switches to Cisco Multicast Manager individually, or you can import a list. Cisco Multicast Manager can monitor the total number of multicast packets inbound and/or outbound from any Layer 2 port.

You can also configure up to 50 different time-of-day thresholds for each port.
To view an L2 PPS Threshold Report:

Step 1  From the Multicast Manager menu, select **Polling Configuration & Reports**.
Step 2  Select **Traffic Polling & Reports**.
Step 3  Select **L2**.
Step 4  Select **Report Parameters**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Date</td>
<td>Enter or select a start date.</td>
</tr>
<tr>
<td>To Date</td>
<td>Enter or select an end date.</td>
</tr>
<tr>
<td>Device</td>
<td>Select a device from the drop-down list.</td>
</tr>
<tr>
<td>Source</td>
<td>Select a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Select a group from the drop-down list.</td>
</tr>
<tr>
<td>Baseline Name</td>
<td>Enter the baseline name.</td>
</tr>
<tr>
<td>Submit</td>
<td>Sets the values that you enter.</td>
</tr>
</tbody>
</table>

**Historical Graph**

Using historical graphs, you can view historical data in a graph format. Historical data is collected when you start to monitor the network using a specific polling configuration.

To view a historical graph for L2 polling:

Step 1  From the Multicast Manager menu, select **Polling Configuration & Reports**.
Step 2  Select **Traffic Polling & Reports**.
Step 3  Select **L2**.
Step 4  Select **Historical Graph**.
Step 5  In the **From Date** field, choose a date from the calendar.
Step 6  In the **To Date** field, choose a date from the calendar.
Step 7  Select one or more multicast streams from the table.
Step 8  Click the **Show Report** button to charts a graph.

Individual streams will indicated will be color coded with a unique color.

**Configuring L2 Polling**

To configure Layer 2 switch polling:
Step 1  From the Multicast Manager menu, select Polling Configuration & Reports.

Step 2  Select Traffic Polling & Reports.

Step 3  Select L2.

Step 4  Select Config L2 Polling.

Step 5  Click the Add button.

Step 6  Select By L2.

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

<table>
<thead>
<tr>
<th>Fields and Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Switch to Monitor</td>
<td>Select the name or IP address of the switch you want to monitor.</td>
</tr>
<tr>
<td>Select Port to Monitor</td>
<td>Select the port to monitor. Ports appear in the following format: ifIndex:module/port.</td>
</tr>
<tr>
<td>Direction</td>
<td>Select either inbound packets received at this port, or outbound packets sent from this port.</td>
</tr>
<tr>
<td>High PPS</td>
<td>Enter the high threshold that, if exceeded, generates a report.</td>
</tr>
<tr>
<td>Low PPS</td>
<td>Enter the low threshold that, if exceeded, generates a report.</td>
</tr>
</tbody>
</table>

Interface Polling

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

Multicast Bandwidth Report

Layer 3 devices on interface the user can set threshold for aggregate threshold traffic and any breach of the thresholds generate an event. This report is a listing of those events.

To configure multicast bandwidth interface polling:
Step 1 From the Multicast Manager menu, select **Polling Configuration & Reports**.
Step 2 Select **Traffic Polling & Reports**.
Step 3 Select **Interface**.
    The Multicast Bandwidth Report page appears.

Note If the Multicast Bandwidth page is not active, from the Interface pages, select **Multicast Bandwidth Report**.

Step 4 Click **Report Parameters**.
Step 5 Click the calendar link (...) for the From Date and select a From Date.
Step 6 Click the calendar link (...) for the To Date and select a To Date.
Step 7 From the drop-down list in the Device field, select a device.
Step 8 Click the **Submit** button.

**Historical Graph**

Using historical graphs, you can view historical data in a graph format. Historical data is collected when you start to monitor the network using a specific polling configuration.

To view a historical graph for interface polling:

Step 1 From the Multicast Manager menu, select **Polling Configuration & Reports**.
Step 2 Select **Traffic Polling & Reports**.
Step 3 Select **Interface**.
Step 4 Select **Historical Graph**.
Step 5 In the From Date field, choose a date from the calendar.
Step 6 In the To Date field, choose a date from the calendar.
Step 7 Select one or more multicast streams from the table.
Step 8 Click the **Show Report** button to charts a graph.
    Individual streams will indicated will be color coded with a unique color.

**Configuring Interface Polling**

**By Interface**

Step 1 From the Multicast Manager menu, select **Polling Configuration & Reports**.
Step 2 Select **Traffic Polling & Reports**.
Step 3 Select **Interface**.
**Step 4** Select **Config Interface Polling**.
**Step 5** Click the **Add** button.
**Step 6** Select **Interface Polling Configuration**.
**Step 7** Select the device to monitor.
**Step 8** Select at least one interface.
A separate list of devices appears, displaying a list of the chosen interfaces.
**Step 9** Assign an inbound and outbound status by checking the box for each device.
If a box is checked, a field appears where you can assign values for Multicast Percentage Hi/Lo. Enter millisecond percentage values as required. For example, to specify a millisecond percentage of .001, enter 100.

**Step 10** Click **Save**.

---

**By Import**

**Step 1** From the Multicast Manager menu, select **Polling Configuration & Reports**.
**Step 2** Select **Traffic Polling & Reports**.
**Step 3** Select **Interface**.
**Step 4** Select **Config Interface Polling**.
**Step 5** Click **Add**.
**Step 6** Select **By Import**.
**Step 7** Click the **Browse** button to upload the file.
**Step 8** Select **Merge** to unify an existing configuration with the new configuration or select **Replace** to overwrite the existing configuration.
**Step 9** Click **Upload**.

---

**Tree Polling & Reports**

The CMM tree polling feature notifies you of events that affect multicast trees, such as addition or removal of a router from a tree.

This section describes:
- Setting Up Tree Polling, page 5-13
- Tree Reports, page 5-15

---

**Setting Up Tree Polling**

Before you can configure tree polling, you must create a trace baseline from the Multicast Trace page. To set up tree polling:
Chapter 5  Polling Configuration and Reports

Tree Polling & Reports

Step 1  Complete these steps to create a trace baseline:

a. From the Main Menu, select **Discovery and Trace**.
b. Select **Multicast Trace**.
c. On the Multicast Trace page, enter the parameters for the trace.
d. Click the **Trace** button.
   The Trace Data page appears with the trace entries and a trace topology diagram.
e. Scroll down to the Input file field.
f. If you want to change the name of the trace baseline file, modify the filename as shown in the Input file field.
g. Click the **Save As** button to save the trace baseline.

Step 2  Go to the following section, **Configuring Tree Polling, page 5-14**, for instructions on how to select the trace baseline file and configure tree polling.

Configuring Tree Polling

To configure tree polling:

Step 1  From the Multicast Manager menu, select **Polling Configuration & Reports**.

Step 2  Select **Tree Polling & Reports**.

Step 3  Select **Tree**.

Step 4  Select **Config Tree Polling**.

The Tree Configurations page appears. Initially the list of tree configurations is empty.

Step 5  Click the **Add** button.

The Tree Polling Configuration page appears.

Step 6  Select a saved trace from the Saved Trees drop-down list.

Step 7  Click **Save**.

The saved trace appears in the Tree Configurations list.

Step 8  Click the **Configure** link next to the saved tree that you want to use for tree reporting.

A page appears for configuring the tree report parameters.

Step 9  In the Select Routers on Tree list, select the routers to include in the tree.

Step 10  In the Specify Max Delta Between PPS Samples field, enter the maximum change between PPS samples.

Step 11  Click the **Save** button.

Step 12  If you want to view a baseline trace that has been configured, click on the baseline file name on the Tree Configurations page.
Tree Reports

Viewing a Tree Report

To view tree reports:

**Step 1** From the Multicast Manager menu, select **Polling Configuration & Reports**.

**Step 2** Select **Tree Polling & Reports**.

**Step 3** Select **Tree**.

**Step 4** Select **Report Parameters**.

**Step 5** On the Tree Report Configuration page, set the parameters for the report:

<table>
<thead>
<tr>
<th>Fields and Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Date</td>
<td>Enter the start date of the Tree Report. Click the icon next to the data field to select a date from a calendar.</td>
</tr>
<tr>
<td>To Date</td>
<td>Enter the end date of the Tree Report. Click the icon next to the data field to select a date from a calendar.</td>
</tr>
<tr>
<td>Device</td>
<td>Select a device from the drop-down list.</td>
</tr>
<tr>
<td>Source</td>
<td>Select a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Select a group from the drop-down list.</td>
</tr>
<tr>
<td>Baseline</td>
<td>Enter the baseline name.</td>
</tr>
</tbody>
</table>

**Step 6** Click the **Submit** button.

Viewing Historical Reports

Using historical graphs, you can view historical data in a graph format. Historical data is collected when you start to monitor the network using a specific polling configuration.

To view a historical graph for tree polling:

**Step 1** From the Multicast Manager menu, select **Polling Configuration & Reports**.

**Step 2** Select **Traffic Polling & Reports**.

**Step 3** Select **Tree Polling & Reports**.

**Step 4** Select **Historical Graph**.

**Step 5** In the **From Date** field, choose a date from the calendar.

**Step 6** In the **To Date** field, choose a date from the calendar.

**Step 7** Select one or more items from the table.

**Step 8** Click the **Show Report** button to chart a graph.
Individual streams will indicated will be color coded with a unique color.

**Viewing an S,G Delta Report**

To view the S,G Delta Report:

1. From the Multicast Manager menu, select **Polling Configuration & Reports**.
2. Select **Tree Polling & Reports**.
3. Select **Tree**.
4. Select **S,G Delta Report**.
5. Select **Report Parameters**.

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

<table>
<thead>
<tr>
<th>Fields and Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Date</td>
<td>Enter the start date of the Tree Report. Click the icon next to the data field to select a date from a calendar.</td>
</tr>
<tr>
<td>To Date</td>
<td>Enter the end date of the Tree Report. Click the icon next to the data field to select a date from a calendar.</td>
</tr>
<tr>
<td>Device</td>
<td>Select a device from the drop-down list.</td>
</tr>
<tr>
<td>Source</td>
<td>Select a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Select a group from the drop-down list.</td>
</tr>
<tr>
<td>Baseline</td>
<td>Enter the baseline name.</td>
</tr>
</tbody>
</table>

6. Click the **Submit** button.

**Comparing Tree Baselines**

1. From the Multicast Manager menu, select **Polling Configuration & Reports**.
2. Select **Tree Polling & Reports**.
3. Select **Tree**.
4. Select **Compare Baseline**.
5. From the drop-down list, select a saved baseline.
6. If there are saved baselines that you want to use for the report, select them from the list of saved baselines.
7. Click **Compare Baselines**.
Viewing a Tree Changed Report from the Dashboard.

To view a Tree Changed Report from the Dashboard:

**Step 1**
From the Dashboard, click the **Tree Events** tab.
The Tree Events page appears.

**Step 2**
Locate a Tree Changed event and click on the **Changed** link in the event entry.
A Tree Trace Data page for the Tree Changed events appears. Figure 5-4 shows a sample Trace Data page.

![Figure 5-4 Trace Data Page for a Tree Changed Event](image)

On the Trace Data page, the tree report for the event shows events indicating that a router has been removed from the tree in red, and routers that have been added in green.

In the tree topology diagram, routers removed from the tree are outlined in red, and routers that have been added are outlined in green.

**SG Polling By Branch**

If you run a trace to understand a specific path, you can select a particular branch to poll.
To configure branch polling for a particular device:
Step 1  From the Multicast Manager menu, select Polling Configuration & Reports.
Step 2  Select Tree Polling & Reports.
Step 3  Select SG by Branch.
Step 4  Click Add.

Fields and Buttons | Description
--- | ---
Source | Enter the source. You may either enter the source address or select it from the drop-down menu.
Group | Enter the group. You may either enter the group address or select it from the drop-down menu.
Service Type | Select the service type from the drop-down list.
FHR | Select the start destination for the first hop router.
LHR | Select the end destination for the last hop router.
Select Router | Select a single router or select multiple routers by pressing the Shift key and clicking on the desired routers.
Units | Select either packets per sampling period (pps) or bits per sampling period (bps).
High Threshold | Enter the high threshold value. If the value is exceeded, Cisco Multicast Manager generates a report.
Low Threshold | Enter the low threshold value. If the value is exceeded, Cisco Multicast Manager generates a report.
Save | Sets the values that you have entered.

Miscellaneous Polling & Reports

RP

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

- Monitor and report all leaves and joins.
- Set a threshold on the number of groups that can join an RP. If this is exceeded, a trap is sent.
- Find out if a specific RP is available.
- Create a list of all sources and groups to be excluded from polling and send a trap if any rogue sources or groups appear on the RP.
Note

RP availability is configured from the Global Polling Configuration page. A trap is sent if an RP becomes unavailable, and a report is generated within the RP Polling Report page.

RP Report

To configure the RP Report:

Step 1  From the Multicast Manager menu, select Polling Configuration & Reports.
Step 2  Select Miscellaneous Polling & Reports.
Step 3  Select RP.

The RP Report page opens, as shown in Figure 5-5.

Figure 5-5  RP Report Page

Step 4  Select Report Parameters.
The RP Polling Configuration page contains the following fields and buttons:

<table>
<thead>
<tr>
<th>Fields and Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Date</td>
<td>Enter the start date of the RP Report. Click the icon next to the data field to select a date from a calendar.</td>
</tr>
<tr>
<td>To Date</td>
<td>Enter the end date of the RP Report. Click the icon next to the data field to select a date from a calendar.</td>
</tr>
<tr>
<td>Device</td>
<td>Select a device from the drop-down list.</td>
</tr>
<tr>
<td>Source</td>
<td>Select a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Select a group from the drop-down list.</td>
</tr>
<tr>
<td>Baseline Name</td>
<td>Enter the baseline name.</td>
</tr>
<tr>
<td>Submit</td>
<td>Adds the selected RP for monitoring.</td>
</tr>
</tbody>
</table>

**RP Group Threshold Report**

To view the RP Group Threshold Report:

*Step 1* From the Multicast Manager menu, select **Polling Configuration & Reports**.

*Step 2* Select **Miscellaneous Polling & Reports**.

*Step 3* Select **RP**.

*Step 4* Select **RP Group Threshold Report**.

*Step 5* Select **Report Parameters**.
The RP Group Threshold Report page contains the following fields and buttons:

<table>
<thead>
<tr>
<th>Fields and Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Date</td>
<td>Enter the start date of the RP Report. Click the icon next to the data field to select a date from a calendar.</td>
</tr>
<tr>
<td>To Date</td>
<td>Enter the end date of the RP Report. Click the icon next to the data field to select a date from a calendar.</td>
</tr>
<tr>
<td>Device</td>
<td>Select a device from the drop-down list.</td>
</tr>
<tr>
<td>Source</td>
<td>Select a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Select a group from the drop-down list.</td>
</tr>
<tr>
<td>Baseline</td>
<td>Enter the baseline name.</td>
</tr>
<tr>
<td>Submit</td>
<td>Adds the selected RP for monitoring.</td>
</tr>
</tbody>
</table>

**SSG Report**

To view the SSG Report:

**Step 1** From the Multicast Manager menu, select **Polling Configuration & Reports**.

**Step 2** Select **Miscellaneous Polling & Reports**.

**Step 3** Select **RP**.

**Step 4** Select **SSG Report**.

**Step 5** Select **Report Parameters**.
The SSG Report page contains the following fields and buttons:

<table>
<thead>
<tr>
<th>Fields and Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Date</td>
<td>Enter the start date of the RP Report. Click the icon next to the data field to select a date from a calendar.</td>
</tr>
<tr>
<td>To Date</td>
<td>Enter the end date of the RP Report. Click the icon next to the data field to select a date from a calendar.</td>
</tr>
<tr>
<td>Device</td>
<td>Select a device from the drop-down list.</td>
</tr>
<tr>
<td>Source</td>
<td>Select a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Select a group from the drop-down list.</td>
</tr>
<tr>
<td>Baseline</td>
<td>Enter the baseline name.</td>
</tr>
<tr>
<td>Submit</td>
<td>Adds the selected RP for monitoring.</td>
</tr>
</tbody>
</table>

## Configuring RP Polling

To configure RP Polling:

1. From the Multicast Manager menu, select **Polling Configuration & Reports**.
2. Select **Miscellaneous Polling & Reports**.
3. Select **RP**.
4. Select **Config RP Polling**.
5. Click the **Add** button.
6. Select **By RP**.
The Configure RP Polling page contains the following fields and buttons:

<table>
<thead>
<tr>
<th>Fields and Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select RP</td>
<td>Select an RP to add to the RP Exclude list. Events from RPs on the RP Exclude list are ignored.</td>
</tr>
<tr>
<td>Group Limit</td>
<td>Set the parameter for the group limit. The default is -1.</td>
</tr>
<tr>
<td>Save</td>
<td>Click Save to retain the values set in the previous fields.</td>
</tr>
<tr>
<td>Enable RP Group Add Delete Traps</td>
<td>Check the check box to monitor all leaves and joins, which are then reported on the RP Polling Report page.</td>
</tr>
<tr>
<td>Single S,G Monitoring</td>
<td>Enter the group IP address. If more than one source becomes active for this group, a report is generated.</td>
</tr>
<tr>
<td>Save</td>
<td>Click Save to retain the values set in the previous fields.</td>
</tr>
</tbody>
</table>

**RP Global Configuration**

To configure RP Global Configuration:

**Step 1**  From the Multicast Manager menu, select **Polling Configuration & Reports**.

**Step 2**  Select **Miscellaneous Polling & Reports**.

**Step 3**  Select **RP**.

**Step 4**  Select **RP Global Configuration**

The RP Global Configuration page appears.

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

<table>
<thead>
<tr>
<th>Fields and Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable RP Add/Delete Traps</td>
<td>To enable RP Add and RP Delete Traps, check the enable RP Add/Delete Traps check box. To disable RP Add and RP Delete Traps, leave the check box unchecked.</td>
</tr>
<tr>
<td>Single SG Monitoring</td>
<td>To add the IP address of a single S, G for monitoring, enter the IP address of the S, G to monitor and then click the Add button to add it to the list of S, G to monitor.</td>
</tr>
<tr>
<td>Save</td>
<td>Click the Save button to save the RP global configuration.</td>
</tr>
</tbody>
</table>
RPF

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

If any monitored source or group begin to experience RPF failures that rise above the delta, then SNMP traps can be sent, and a report generated. You can view the report on the RPF Polling Report page.

RPF Polling Report

To view the RPF Polling Report:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>From the Multicast Manager menu, select Polling Configuration &amp; Reports.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select Miscellaneous Polling &amp; Reports.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select RPF.</td>
</tr>
</tbody>
</table>

The RPF Polling Report parameter page contains the following fields and buttons:

<table>
<thead>
<tr>
<th>Fields and Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Date</td>
<td>Enter the start date of the RPF Report. Click the icon next to the data field to select a date from a calendar.</td>
</tr>
<tr>
<td>To Date</td>
<td>Enter the end date of the RPF Report. Click the icon next to the data field to select a date from a calendar.</td>
</tr>
<tr>
<td>Device</td>
<td>Select a device from the drop-down list.</td>
</tr>
<tr>
<td>Source</td>
<td>Select a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Select a group from the drop-down list.</td>
</tr>
<tr>
<td>Baseline</td>
<td>Enter the baseline name.</td>
</tr>
<tr>
<td>Submit</td>
<td>Add the selected RPF for monitoring.</td>
</tr>
</tbody>
</table>

Configuring RPF Polling

To configure RPF polling:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>From the Multicast Manager menu, select Polling Configuration &amp; Reports.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select Miscellaneous Polling &amp; Reports.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select RPF.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Select Config RPF Polling.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click the Add button.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Select By RPF.</td>
</tr>
</tbody>
</table>
Chapter 5      Polling Configuration and Reports

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

<table>
<thead>
<tr>
<th>Fields and Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Select a source from the drop-down list.</td>
</tr>
<tr>
<td>Filter Groups</td>
<td>Filters the output to contain only the relevant groups.</td>
</tr>
<tr>
<td>Group</td>
<td>Select a group from the drop-down list.</td>
</tr>
<tr>
<td>Filter Sources</td>
<td>Filters the output to contain only the relevant sources.</td>
</tr>
<tr>
<td>Reset SG List</td>
<td>Clears any entries and refreshes the source and group lists.</td>
</tr>
<tr>
<td>Router</td>
<td>Enter the router name.</td>
</tr>
<tr>
<td>Delta</td>
<td>Number of RPF failures per sampling period that trigger a report.</td>
</tr>
<tr>
<td>Save</td>
<td>Applies the configuration and saves the changes.</td>
</tr>
</tbody>
</table>

**Selective Source Monitoring**

A source and group can be set up to monitor for a particular time and day.

*Note*
The time interval configured should not be overlapping for the same source and group.

**Selective Source Monitoring Report**

To view the Selective Source Monitoring Report:

1. From the Multicast Manager menu, select Polling Configuration & Reports.
2. Select Miscellaneous Polling & Reports.

The Selective Source Monitoring Report page contains the following fields and buttons:

<table>
<thead>
<tr>
<th>Fields and Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Date</td>
<td>Enter the start date of the Selective Source Monitoring Report. Click the icon next to the data field to select a date from a calendar.</td>
</tr>
<tr>
<td>To Date</td>
<td>Enter the end date of the Selective Source Monitoring Report. Click the icon next to the data field to select a date from a calendar.</td>
</tr>
<tr>
<td>Device</td>
<td>Select a device from the drop-down list.</td>
</tr>
</tbody>
</table>
As part of the results generated, a Source Offline event is generated for the source and group (S,G) configured when the source goes offline.

A Source may be offline event will be generated for (S,G) configured under SG Polling Main, if the source is directly connected to the domain (FHR) and if there is no packet count increase for the monitoring period (typically 1 minute). This event also prevents the bogus trap occurring because of a source offline event.

### Selective Source Monitoring Configuration

To configure Selective Source Monitoring Polling:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>From the Multicast Manager menu, select <strong>Polling Configuration &amp; Reports</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select <strong>Miscellaneous Polling &amp; Reports</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select <strong>Selective Source Monitoring</strong>.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Select <strong>Config Selective Source Monitoring Polling</strong>.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click the <strong>Add</strong> button.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Select <strong>By Selective Source Monitoring</strong>.</td>
</tr>
</tbody>
</table>

The Selective Source Monitoring Polling Configuration page contains the following fields and buttons:
Health checks give you an immediate status update on several key multicast network indicators, including:

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

You can create several health checks. After you have created a health check, you can configure it to run at scheduled intervals, and add e-mail alerts that summarize the results of the health check.
**Health Check Failed Report**

To view the Health Check Failed Report:

**Step 1** From the Multicast Manager menu, select **Polling Configuration & Reports**.

**Step 2** Select **Miscellaneous Polling & Reports**.

**Step 3** Select **Health Check**.

**Step 4** Select **Report Parameters**.

The Health Check Failed Report page contains the following fields and buttons:

<table>
<thead>
<tr>
<th>Fields and Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Date</td>
<td>Enter the start date of the Health Check Report. Click the icon next to the data field to select a date from a calendar.</td>
</tr>
<tr>
<td>To Date</td>
<td>Enter the end date of the Health Check Report. Click the icon next to the data field to select a date from a calendar.</td>
</tr>
<tr>
<td>Device</td>
<td>Select a device from the drop-down list.</td>
</tr>
<tr>
<td>Source</td>
<td>Select a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Select a group from the drop-down list.</td>
</tr>
<tr>
<td>Baseline Name</td>
<td>Enter the baseline name.</td>
</tr>
<tr>
<td>Submit</td>
<td>Adds the selected health check for monitoring.</td>
</tr>
</tbody>
</table>

**Configuring Health Check Polling**

To configure health check polling:

**Step 1** From the Multicast Manager menu, select **Polling Configuration & Reports**.

**Step 2** Select **Miscellaneous Polling & Reports**.

**Step 3** Select **Health Check**.

**Step 4** Select **Config Health Check Polling**.

**Step 5** Click the **Add** button.

The Health Check Name Polling Configuration page appears. The Health Check Name Polling Configuration page contains the following fields and buttons:

<table>
<thead>
<tr>
<th>Fields and Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health Check Name</td>
<td>Enter a name for the health check.</td>
</tr>
<tr>
<td>Notify on Success</td>
<td>Check this box to generate an e-mail report if the health check completes successfully.</td>
</tr>
</tbody>
</table>
After you click the Save button, the Health Check Configuration is updated, and the following tables appear:

- **RPs Being Checked for** `<health check name>`
- **Current Source/Group Polling Configuration for** `<health check name>`
- **Forwarding Trees for** `<health check name>`

### Table 5-1  **RPs Being Checked for** `<health check name>` **Table**

<table>
<thead>
<tr>
<th>Fields and Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPs Being Checked for <code>&lt;health check name&gt;</code></td>
<td>Select the RP from the drop-down list.</td>
</tr>
<tr>
<td>Save</td>
<td>Adds the Health Check configuration for monitoring.</td>
</tr>
</tbody>
</table>

### Table 5-2  **Current Source/Group Polling Configuration for** `<health check name>` **Table**

<table>
<thead>
<tr>
<th>Fields and Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Select a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Select a group from the drop-down list.</td>
</tr>
<tr>
<td>Reset SG List</td>
<td>Clears any entries and refreshes the source and group lists.</td>
</tr>
<tr>
<td>Select Routers</td>
<td>Select one or more routers from the list. You can also click the Select All button to select all routers.</td>
</tr>
<tr>
<td>Save</td>
<td>Adds the Health Check configuration for monitoring.</td>
</tr>
</tbody>
</table>

### Table 5-3  **Forwarding Trees for** `<health check name>` **Table**

<table>
<thead>
<tr>
<th>Fields and Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Saved Trees</td>
<td>Select the a tree to trace from the drop-down list.</td>
</tr>
<tr>
<td>Save</td>
<td>Adds the Health Check configuration for monitoring.</td>
</tr>
</tbody>
</table>
Step 6  To add an item to the health check configuration:
   a.  Click the Add button in one of the tables.
   b.  On the configuration screen that appears, specify the configuration.
   c.  Click the Save button on the configuration screen.

The selected configuration now appears in the table.

Step 7  To check the status of the MSDP peers of an RP that has been added to the configuration, click the Continue link in the MSDP column for the RP.

The Select Peers to Check page for the selected RP appears.

Step 8  Click the Save button to save the health check polling configuration.

---

### Video Probe

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

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

### Video Probe Report

To view the Video Probe Report:

**Step 1**  From the Multicast Manager menu, select Polling Configuration & Reports.

**Step 2**  Select Miscellaneous Polling & Reports.

**Step 3**  Select Video Probe.

**Step 4**  Select Report Parameters.

The Video Probe Report Parameters page contains the following fields and buttons:

<table>
<thead>
<tr>
<th>Fields and Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Date</td>
<td>Enter the start date of the Video Probe Report. Click the icon next to the data field to select a date from a calendar.</td>
</tr>
<tr>
<td>To Date</td>
<td>Enter the end date of the Video Probe Report. Click the icon next to the data field to select a date from a calendar.</td>
</tr>
<tr>
<td>Device</td>
<td>Select a device from the drop-down list.</td>
</tr>
<tr>
<td>Source</td>
<td>Select a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Select a group from the drop-down list.</td>
</tr>
<tr>
<td>Baseline Name</td>
<td>Enter the baseline name.</td>
</tr>
<tr>
<td>Submit</td>
<td>Adds the selected Video Probe for monitoring.</td>
</tr>
</tbody>
</table>
Historical Report

Using historical graphs, you can view historical data in a graph format. Historical data is collected when you start to monitor the network using a specific polling configuration.

To display a graph showing historical statistics for up to three video probes:

**Step 1** From the Multicast Manager menu, select **Polling Configuration & Reports**.

**Step 2** Select **Miscellaneous Polling & Reports**.

**Step 3** Select **Video Probe**.

**Step 4** Select **Historical Report**. The Historical Graphs page for video probe reports appears, as shown in Figure 5-6.

**Figure 5-6** Historical Graphs Page for Video Probes

**Step 5** From the drop-down list in the **Units** field, select the units for the report:

<table>
<thead>
<tr>
<th>DF</th>
<th>Display delay factor data.</th>
</tr>
</thead>
<tbody>
<tr>
<td>MLR</td>
<td>Display Media Loss Rate data.</td>
</tr>
</tbody>
</table>

**Step 6** Click the calendar item (...) for **From Date** and from the calendar that appears, select the From Date.

**Step 7** Click the calendar item (...) for **To Date** and from the calendar that appears, select the To Date.

**Step 8** On the list of Video Probes, check the check boxes for up to three video probes.

**Step 9** Click the **Show Report** button.

A graph showing the statistics for the selected video probes appears, as shown in Figure 5-7.
Configuring Video Probe Polling

To configure video probe polling:

**Step 1** From the Multicast Manager menu, select Polling Configuration & Reports.

**Step 2** Select Miscellaneous Polling & Reports.

**Step 3** Select Video Probe.

**Step 4** Select Config Video Probe Polling.

**Step 5** Click the Add button.

**Step 6** From the drop-down list in the Add field, select By Video Probe.

The Configure Video Probe Polling page contains the following fields and buttons:

<table>
<thead>
<tr>
<th>Fields and Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Video Probe(s)</td>
<td>Select one or more probes from the list. Assign Delay Factor (DF) Threshold (mSec) and Loss Threshold (MLR) values to each probe.</td>
</tr>
<tr>
<td>Save</td>
<td>Adds the video probe configuration for monitoring.</td>
</tr>
</tbody>
</table>

Vidmon Polling

Viewing a Vidmon Report

To view a Vidmon report:

**Step 1** From the Multicast Manager menu, select Polling Configuration & Reports.

**Step 2** Select Miscellaneous Polling & Reports.

**Step 3** Select Vidmon.
The Vidmon Reports page opens.

**Step 4** Select **Report Parameters**.

The Vidmon Report Parameters page contains the following fields and buttons:

<table>
<thead>
<tr>
<th>Fields and Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Date</td>
<td>Enter the start date of the Vidmon Report. Click the icon next to the data field to select a date from a calendar.</td>
</tr>
<tr>
<td>To Date</td>
<td>Enter the end date of the Vidmon Report. Click the icon next to the data field to select a date from a calendar.</td>
</tr>
<tr>
<td>Device</td>
<td>Select a device from the drop-down list.</td>
</tr>
<tr>
<td>Source</td>
<td>Select a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Select a group from the drop-down list.</td>
</tr>
<tr>
<td>Baseline Name</td>
<td>This field is not enabled for Vidmon reports.</td>
</tr>
<tr>
<td>Submit</td>
<td>Adds the selected Vidmon device for monitoring.</td>
</tr>
</tbody>
</table>

The Vidmon Reports page displays the Vidmon report.

### Historical Report

Using historical graphs, you can view historical data in a graph format. Historical data is collected when you start to monitor the network using a specific polling configuration.

To display a graph showing historical statistics for up to three Vidmon devices:

**Step 1** From the Multicast Manager menu, select **Polling Configuration & Reports**.

**Step 2** Select **Miscellaneous Polling & Reports**.

**Step 3** Select **Vidmon**.

**Step 4** Select **Historical Report**. The Historical Graphs page for video probe reports appears.

**Step 5** From the drop-down list in the **Units** field, select the units for the report:

<table>
<thead>
<tr>
<th>DF</th>
<th>Display delay factor data.</th>
</tr>
</thead>
<tbody>
<tr>
<td>MLR</td>
<td>Display Media Loss Rate data.</td>
</tr>
<tr>
<td>MRV</td>
<td>Display Media Rate Variation data.</td>
</tr>
</tbody>
</table>

**Step 6** Click the calendar item (...) for **From Date** and from the calendar that appears, select the From Date.

**Step 7** Click the calendar item (...) for **To Date** and from the calendar that appears, select the To Date.

**Step 8** On the list of interfaces on Vidmon devices, check the check boxes for up to three interfaces.

**Step 9** Click the **Show Report** button.
A graph showing the statistics for the selected Vidmon devices appears.

Configuring Vidmon Polling

To configure Vidmon Polling:

Step 1  From the Multicast Manager menu, select **Polling Configuration & Reports**.

Step 2  Select **Miscellaneous Polling & Reports**.

Step 3  Select **Vidmon**.

The Vidmon Report page appears, and shows a current Vidmon Polling report.

Step 4  Select **Config Vidmon Polling**.

The Config Vidmon Polling page appears, as shown in Figure 5-8.

![Config Vidmon Polling Page](image)

The Config Vidmon Polling page lists the current Vidmon polling configurations.

From the Config Vidmon Polling page, you can add a new Vidmon polling configuration, delete or export an existing Vidmon polling configuration, or edit an existing configuration.

Step 5  Do one of the following:

- To add a new configuration, click the **Add** button, and from the drop-down list, select **By Vidmon**.
- To delete an existing configuration or export it to file to use on another device, check the check box next to a configuration, click the **Actions** button, and from the drop-down list, select either **Delete** or **Export**.

If you select **Export**, you are prompted for the folder path and filename for a CSV file containing the exported configuration.

Step 6  If you selected **Export**, browse to the folder where you want to save the CSV file, enter a file name, and click the **Save** button to save the file.

If you select **Add**, the Vidmon Polling Configuration page appears, as shown in Figure 5-9.
The Vidmon Polling Configuration page lists the Vidmon devices that have been discovered in the domain.

**Step 7**
To select a Vidmon device to discover, click a device name in the list of Vidmon Devices.

As you select devices, a row of configuration options for the device appears. Figure 5-10 shows all of the devices that are shown in Figure 5-9 selected.

**Figure 5-10 Selected Vidmon Devices**

**Step 8**
To configure polling for a device, check the check box next to the configuration option for the device. For example, to configure a delay factor for a device, click the DF field.

As you select configuration fields, the field becomes active.

Figure 5-11 shows all configuration fields for all devices listed in Figure 5-10 selected.

**Figure 5-11 Vidmon Polling Configuration Fields**

**Step 9**
Enter Vidmon polling configuration parameters as indicated in Table 5-3.
Step 10  To save the Vidmon polling configuration, click the **Save** button.

### Importing a Vidmon Configuration

If you have previously saved a CSV file containing a polling configuration for a Vidmon Device, you can import the existing polling configuration.

To import a Vidmon polling configuration:

**Step 1**  On the Config Vidmon Polling page, click the **Add** button, and from the drop-down list, choose **By Import**.

The Vidmon Import page appears, as shown in Figure 5-11.
Chapter 5      Polling Configuration and Reports

Figure 5-12     Vidmon Import Page

Step 2  Browse for the CSV file to import.
Step 3  Do one of the following:
   • To merge the saved configuration with your existing configuration, click to Merge radio button.
   • To replace the existing configuration, click the Replace radio button.
Step 4  Click the Upload button.

Editing an Existing Vidmon Polling Configuration
To edit an existing VidMon polling configuration:

Step 1  On the Vidmon Configurations page, check the check box next to an existing Vidmon polling configuration.
Step 2  Click the Edit button.
The Vidmon Polling Configuration page appears and shows the existing configuration.
Step 3  Edit the values as required.
   Table 5-3 describes the Vidmon Polling Configuration options.
Step 4  Click the Save button to save the configuration.
Step 5  To begin using the new polling configuration, at the top of the page, click the Restart button.

Specifying an Override Configuration for Vidmon Polling
You can override the specified Vidmon polling configuration for specified devices, on a Source, Group basis.
To override the Vidmon polling configuration for specified devices:

Step 1  On the Vidmon Configuration page, in the SG-Based Threshold column, click the Configure link for a device.
The Vidmon Threshold Override Configuration page for the selected device appears, as shown in Figure 5-13.
Step 2  On the Vidmon Threshold Override Configuration page, specify a mask for the Source and Group to which the override configuration will apply, as follows:

a. In the Source field, specify an IP address for a Source or Source Range. The value you enter in the Source field is modified by the value you enter in the Source Mask field.

b. To override the configuration for an exact IP address, enter the IP address of the device to which the override will apply in the Source field, and enter 0.0.0.0 in the Source Mask field. To specify a bit mask that applies the override to a range of source IP addresses, enter a value in the Source Mask field. For example, to match IP addresses 172.20.111.0 through 172.20.111.255, enter 172.20.111.242 in the Source field and 0.0.0.255 in the Source Mask field.

c. To specify the Destination override information, enter IP addresses in the Destination field and the Destination Mask field in the same manner as for the Source field and the Source Mask field.

Step 3  Enter override values for the Vidmon polling threshold configuration fields as required. For a description of the Vidmon polling configuration options, see Table 5-3 on page 5-36.

Step 4  Click the Save button to save the override configuration.

Step 5  To enable the new configuration, click the Restart button at the top of the page.

MVPN Polling

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

MDT Source Report

To view MDT Source polling:
Step 1 From the Multicast Manager menu, select **Polling Configuration & Reports**.
Step 2 Select **Miscellaneous Polling & Reports**.
Step 3 Select **MVPN Polling**.
Step 4 Select **Report Parameters**.

The MDT Source Report page contains the following fields and buttons:

<table>
<thead>
<tr>
<th>Fields and Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Date</td>
<td>Enter the start date of the MDT Source Report. Click the icon next to the data field to select a date from a calendar.</td>
</tr>
<tr>
<td>To Date</td>
<td>Enter the end date of the MDT Source Report. Click the icon next to the data field to select a date from a calendar.</td>
</tr>
<tr>
<td>Device</td>
<td>Select a device from the drop-down list.</td>
</tr>
<tr>
<td>Source</td>
<td>Select a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Select a group from the drop-down list.</td>
</tr>
<tr>
<td>Baseline</td>
<td>Enter the baseline name.</td>
</tr>
<tr>
<td>Submit</td>
<td>Adds the selected MDT source for monitoring.</td>
</tr>
</tbody>
</table>

**MDT Default Report**

To view MDT default polling:

Step 1 From the Multicast Manager menu, select **Polling Configuration & Reports**.
Step 2 Select **Miscellaneous Polling & Reports**.
Step 3 Select **MVPN Polling**.
Step 4 Select **MDT Default Report**.
Step 5 Select **Report Parameters**.
The MDT Default Report page contains the following fields and buttons:

<table>
<thead>
<tr>
<th>Fields and Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Date</td>
<td>Enter the start date of the MDT Default Report. Click the icon next to the data field to select a date from a calendar.</td>
</tr>
<tr>
<td>To Date</td>
<td>Enter the end date of the MDT Default Report. Click the icon next to the data field to select a date from a calendar.</td>
</tr>
<tr>
<td>Device</td>
<td>Select a device from the drop-down list.</td>
</tr>
<tr>
<td>Source</td>
<td>Select a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Select a group from the drop-down list.</td>
</tr>
<tr>
<td>Baseline</td>
<td>Enter the baseline name.</td>
</tr>
<tr>
<td>Submit</td>
<td>Adds the selected MDT default for monitoring.</td>
</tr>
</tbody>
</table>

**VRF Interface Count Report**

To view the Virtual Routing and Forwarding (VRF) Interface Count Report:

**Step 1** From the Multicast Manager menu, select **Polling Configuration & Reports**.

**Step 2** Select **Miscellaneous Polling & Reports**.

**Step 3** Select **MVPN Polling**.

**Step 4** Select **VRF Interface Count Report**.

**Step 5** Select **Report Parameters**.
The VRF Interface Count Report page contains the following fields and buttons:

<table>
<thead>
<tr>
<th>Fields and Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Date</td>
<td>Enter the start date of the VRF Interface Count Report. Click the icon next to the data field to select a date from a calendar.</td>
</tr>
<tr>
<td>To Date</td>
<td>Enter the end date of the VRF Interface Count Report. Click the icon next to the data field to select a date from a calendar.</td>
</tr>
<tr>
<td>Device</td>
<td>Select a device from the drop-down list.</td>
</tr>
<tr>
<td>Source</td>
<td>Select a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Select a group from the drop-down list.</td>
</tr>
<tr>
<td>Baseline</td>
<td>Enter the baseline name.</td>
</tr>
<tr>
<td>Submit</td>
<td>Adds the selected VRF interface count for monitoring.</td>
</tr>
</tbody>
</table>

**VRF Count Report**

To view the VRF Count Report:

**Step 1** From the Multicast Manager menu, select **Polling Configuration & Reports**.

**Step 2** Select **Miscellaneous Polling & Reports**.

**Step 3** Select **MVPN Polling**.

**Step 4** Select **VRF Count Report**.

**Step 5** Select **Report Parameters**.
The VRF Count Report page contains the following fields and buttons:

<table>
<thead>
<tr>
<th>Fields and Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Date</td>
<td>Enter the start date of the VRF Count Report. Click the icon next to the data field to select a date from a calendar.</td>
</tr>
<tr>
<td>To Date</td>
<td>Enter the end date of the VRF Count Report. Click the icon next to the data field to select a date from a calendar.</td>
</tr>
<tr>
<td>Device</td>
<td>Select a device from the drop-down list.</td>
</tr>
<tr>
<td>Source</td>
<td>Select a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Select a group from the drop-down list.</td>
</tr>
<tr>
<td>Baseline</td>
<td>Enter the baseline name.</td>
</tr>
<tr>
<td>Submit</td>
<td>Adds the selected VRF count for monitoring.</td>
</tr>
</tbody>
</table>

### Configuring MVPN Polling

To configure MVPN polling:

1. From the Multicast Manager menu, select **Polling Configuration & Reports**.
2. Select **Miscellaneous Polling & Reports**.
3. Select **MVPN Polling**.
4. Select **Config MVPN Polling**.
5. Click the **Add** button.
6. Select **By MVPN**.

The Configure MVPN Polling page contains the following fields and buttons:

<table>
<thead>
<tr>
<th>Fields and Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PE Device</td>
<td>Select one or more devices from the list.</td>
</tr>
<tr>
<td>Save</td>
<td>Adds the MVPN configuration for monitoring.</td>
</tr>
</tbody>
</table>
CRM Polling

Baseline Route Polling

**Note** You must first create a baseline as described in *Create Baseline, page 8-20.*

**Note** You must restart the polling daemon after making configuration changes in this section. Click the Restart button in the Polling Actions field to restart polling. Click the Stop button to stop polling.

Unicast Report

**Step 1** From the Multicast Manager menu, select **Polling Configuration & Reports**.

**Step 2** Select **CRM Polling**.

**Step 3** Select **Baseline Route Polling**.

**Step 4** Select **Unicast Report**.

**Step 5** Click **View Report**.

**Step 6** In the Select Route field, select a date from the drop-down menu.

**Step 7** Select an object from the Filter MIB Objects field.

**Step 8** Click **View**.

Multicast Report

**Step 1** From the Multicast Manager menu, select **Polling Configuration & Reports**.

**Step 2** Select **CRM Polling**.

**Step 3** Select **Baseline Route Polling**.

**Step 4** Select **Multicast Report**.

**Step 5** In the Select Route field, select a date from the drop-down menu.

**Step 6** Select an object from the Filter MIB Objects field.

**Step 7** Click **View**.

Historical Report

**Step 1** From the Multicast Manager menu, select **Polling Configuration & Reports**.

**Step 2** Select **CRM Polling**.
Step 3 Select **Baseline Route Polling**.
Step 4 Select **Historical Report**.
Step 5 To set the Report Type, select either Unicast or Multicast from the drop-down menu.
Step 6 Click the **Get Report(s)** button to refresh the display of the streams being monitored.
Step 7 In the **From Date** field, choose a date from the calendar.
Step 8 In the **To Date** field, choose a date from the calendar.
Step 9 Select one or more stream from the table.
Step 10 Click the **Show Report** button to chart a graph.

Individual streams are color coded with a unique color.

---

**View Baseline**

Step 1 From the Multicast Manager menu, select **Polling Configuration & Reports**.
Step 2 Select **CRM Polling**.
Step 3 Select **Baseline Route Polling**.
Step 4 Select **View Baseline**.
Step 5 Select either Unicast or Multicast in the Report Type field.
Step 6 Select a router from the drop-down list.
Step 7 Select a baseline.
Step 8 Click **View**.

---

**Compare Baseline**

Step 1 From the Multicast Manager menu, select **Polling Configuration & Reports**.
Step 2 Select **CRM Polling**.
Step 3 Select **Baseline Route Polling**.
Step 4 Select **Compare Baseline**.
Step 5 To specify the Report Type, click either the **Unicast** radio button or the **Multicast** radio button.
Step 6 Select a router from the drop-down list.
Step 7 Select the first baseline from the Baseline1 drop-down list.
Step 8 Select the second baseline from the Baseline2 drop-down list.
Step 9 Click **View**.
Configuring Route Polling

To configure route polling:

**Step 1** From the Multicast Manager menu, select **Polling Configuration & Reports**.

**Step 2** Select **CRM Polling**.

**Step 3** Select **Baseline Route Polling**

**Step 4** Click the **Add** button.

**Step 5** Select **By Baseline Route**.

The Configure Baseline Route page contains the following fields and buttons:

<table>
<thead>
<tr>
<th>Fields and Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing Table Type</td>
<td>Select either Unicast or Multicast.</td>
</tr>
<tr>
<td>Select Router</td>
<td>Select a router.</td>
</tr>
<tr>
<td>Baseline</td>
<td>Select a baseline.</td>
</tr>
<tr>
<td>CPU Threshold</td>
<td>The CPU utilization of the router will be checked first to determine if a query of the routing table is acceptable based upon the configured CPU threshold. A value of -1, indicates that the routing table should be queried without checking CPU utilization.</td>
</tr>
<tr>
<td>Add/Modify</td>
<td>Updates the baseline route for monitoring.</td>
</tr>
</tbody>
</table>

Specific Route Polling

Unicast Report

To view the Unicast Report:

**Step 1** From the Multicast Manager menu, select **Polling Configuration & Reports**.

**Step 2** Select **CRM Polling**.

**Step 3** Select **Specific Route Polling**.

**Step 4** Select **Report Parameters**.
The Unicast Report page contains the following fields and buttons:

<table>
<thead>
<tr>
<th>Fields and Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Date</td>
<td>Enter the start date of the Unicast Report. Click the icon next to the data field to select a date from a calendar.</td>
</tr>
<tr>
<td>To Date</td>
<td>Enter the end date of the Unicast Report. Click the icon next to the data field to select a date from a calendar.</td>
</tr>
<tr>
<td>Device</td>
<td>Select a device from the drop-down list.</td>
</tr>
<tr>
<td>Source</td>
<td>Select a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Select a group from the drop-down list.</td>
</tr>
<tr>
<td>Baseline</td>
<td>Enter the baseline name.</td>
</tr>
<tr>
<td>Submit</td>
<td>Adds the selected Unicast parameters for monitoring.</td>
</tr>
</tbody>
</table>

**Multicast Report**

To view the Multicast Report:

**Step 1** From the Multicast Manager menu, select **Polling Configuration & Reports**.

**Step 2** Select **Miscellaneous Polling & Reports**.

**Step 3** Select **CRM Polling**

**Step 4** Select **Specific Route Polling**.

**Step 5** Select **Multicast Report**.

**Step 6** Select **Report Parameters**.
The Multicast Report page contains the following fields and buttons:

<table>
<thead>
<tr>
<th>Fields and Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Date</td>
<td>Enter the start date of the Multicast Report. Click the icon next to the data field to select a date from a calendar.</td>
</tr>
<tr>
<td>To Date</td>
<td>Enter the end date of the Multicast Report. Click the icon next to the data field to select a date from a calendar.</td>
</tr>
<tr>
<td>Device</td>
<td>Select a device from the drop-down list.</td>
</tr>
<tr>
<td>Source</td>
<td>Select a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Select a group from the drop-down list.</td>
</tr>
<tr>
<td>Baseline</td>
<td>Enter the baseline name.</td>
</tr>
<tr>
<td>Submit</td>
<td>Adds the selected Multicast report parameters for monitoring.</td>
</tr>
</tbody>
</table>

### Configuring Unicast Polling

To configure Unicast Polling:

**Step 1** From the Multicast Manager menu, select **Polling Configuration & Reports**.
**Step 2** Select **Miscellaneous Polling & Reports**.
**Step 3** Select **CRM Polling**.
**Step 4** Select **Specific Route Polling**.
**Step 5** Select **Config Unicast Polling**.
**Step 6** Click **Add**.
**Step 7** Select **By Unicast Route**.

**Note** You can also select **By Import** to import the unicast route from a CSV file.

The Unicast Report page contains the following fields and buttons:

<table>
<thead>
<tr>
<th>Fields and Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Router</td>
<td>Select a router.</td>
</tr>
<tr>
<td>CPU Threshold</td>
<td>The CPU utilization of the router will be checked first to determine if a query of the routing table is acceptable based upon the configured CPU threshold. A value of -1, indicates that the routing table should be queried without checking CPU utilization.</td>
</tr>
</tbody>
</table>
CRM Polling

### Fields and Buttons

<table>
<thead>
<tr>
<th>Field and Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Current Routes</td>
<td>Updates the baseline route for monitoring</td>
</tr>
<tr>
<td>Specific Unicast Routes List</td>
<td>To generate a specific unicast list, check the box and click <strong>Add Selected Routes to Polling Config.</strong></td>
</tr>
</tbody>
</table>

#### Step 8

If you want to search for multicast routes for specified Devices, Sources, or Groups:

1. Click the **Add Filter** button.
2. From the drop-down list in the Filter field, select **Device**, **Source**, or **Group**.
3. In the Containing Text field, enter a search string that contains part of the Device name, Source IP address, or Group IP address.
4. Click the **Search** button.
5. Check the check boxes next to any items that are found and which you want to add.

#### Step 9

Click the **Add** button.

### Configuring Multicast Polling

To configure Multicast Polling:

1. From the Multicast Manager menu, select **Polling Configuration & Reports**.
2. Select **Miscellaneous Polling & Reports**.
3. Select **CRM Polling**.
4. Select **Specific Route Polling**.
5. Select **Config Multicast Polling**.
6. Click **Add**.
7. Select **By Multicast Route**.
8. **Note**: You can also select **By Import** to import the multicast route from a CSV file.

The Multicast Route Configuration page contains the following fields and buttons:

<table>
<thead>
<tr>
<th>Fields and Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Router</td>
<td>Select a router.</td>
</tr>
<tr>
<td>CPU Threshold</td>
<td>The CPU utilization of the router will be checked first to determine if a query of the routing table is acceptable based upon the configured CPU threshold. A value of -1, indicates that the routing table should be queried without checking CPU utilization.</td>
</tr>
</tbody>
</table>
### Chapter 5 Polling Configuration and Reports

#### CRM Polling

#### Step 8

If you want to search for multicast routes for specified Devices, Sources, or Groups:

a. Click the **Add Filter** button.
b. From the drop-down list in the Filter filed, select **Device**, **Source**, or **Group**.
c. In the Containing Text field, enter a search string that contains part of the Device name, Source IP address, or Group IP address.
d. Click the **Search** button.
e. Check the check boxes next to any items that are found and which you want to add.

#### Step 9

Click the **Add** button.

<table>
<thead>
<tr>
<th>Fields and Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Current Routes</td>
<td>Updates the baseline route for monitoring</td>
</tr>
<tr>
<td>Specific Multicast Routes List</td>
<td>To generate a specific multicast list, check the check box and click Add Selected Routes to Polling Config.</td>
</tr>
</tbody>
</table>
Discovery and Trace

This chapter contains the following sections:

- Discovery, page 6-1
- Trace, page 6-10

Discovery

You can discover devices by device category, such as multicast devices, Vidmon devices (devices that provide Cisco Vidmon capability), Layer 2 devices, or unicast devices, and you can also discover video probes.

When you discover devices or video probes, you can enter parameters that tell the Discovery process where to start looking for devices (for example, by specifying a seed IP address or a flat file that contains router IP addresses), or you can import the discovery parameters by specifying the name of a CSV file that contains discovery information.

**Note**

Run one discovery run at a time.

**Note**

Stop the poller if devices have already been discovered in the domain.

Multicast Discovery

Multicast Discovery allows you to carry out three types of discovery:

- **Core/Enterprise Discovery**—Use Core/Enterprise Discovery to discover the multicast devices in your core/enterprise network.
- **Distributed Network Discovery**—Use Distributed Network Discovery to discover the customer sites using Provider Edge (PE) devices or Customer Edge (CE) devices and associated PE Devices in a distributed network such as an IP/MPLS network.
- **Single Device Discovery**—Use Single Device Discovery to discover a single device or a device and its adjacent PIM neighbors.

You can perform discovery in two ways:
By specifying a Seed IP address from which to start discovery or a directory path and file name for a flat file that contains discovery information. To do this, choose the **By Seed IP/Flat File** from the pull-down menu for **Discovery**.

- By importing a CSV file that contains discovery information. To do this, choose **Contiguous Discovery by Import** on the pull-down menu for **Discovery**.

The first time that you perform multicast discovery, use Core/Enterprise Discovery or Distributed Network Discovery. CMM will build a network topology database based on what it discovers.

**Tip**

After performing initial discovery, if you need to add additional devices to the inventory of discovered devices, use Single Device Discovery. If you run Core/Enterprise Discovery or Distributed Network Discovery a second time after the initial run, all of the topology that was discovered initially is lost and replaced by the revised discovery information.

Using Single Device Discovery, however, will not overwrite your additional discovery information—it will retain the initial information and add the single device (as well as its PIM neighbors if you specify this option).

To run multicast discovery:

---

**Step 1**  
From the Multicast Manager menu, select **Discovery & Trace**.

**Step 2**  
Select **Discovery**.

**Step 3**  
Select **Multicast Discovery**.  
The Router Discovery page appears, showing the list of routers that have been discovered so far.

**Step 4**  
Click **Discover**.

**Step 5**  
From the pull-down menu in the Discovery field, choose **By Seed IP/Flat File**.

**Step 6**  
The Discovery Add/Modify page appears, as shown in Figure 6-1.

---

**Figure 6-1 Discovery Add/Modify Page**

The Discovery Add/Modify page contains three tabs.
Step 7 Do one of the following:

- If you want to perform Core/Enterprise Discovery, specify discovery parameters as indicated in Core/Enterprise Discovery, page 6-3.
- To perform Distributed Network Discovery, click the Distributed Network tab. See Distributed Network Discovery, page 6-4.
- To perform Single Device Discovery, click the Single Device Discovery tab. See Single Device Discovery, page 6-6.

Core/Enterprise Discovery

When you perform Core/Enterprise Discovery, you can choose to discover contiguous devices using a seed device IP address or hostname, or to discover the core network and the CEs connected to it.

To perform Core/Enterprise Discovery:

Step 1 If you want to discover the core network and CEs connected with it, complete these steps:

a. Provide a CSV file that lists the IP addresses of the PEs that you want to discover, separated by commas.

b. Save the file in an appropriate directory on the CMM server.

Step 2 From the Multicast Manager menu, select Discovery & Trace.

Step 3 Select Discovery.

Step 4 Select Multicast Discovery.

The Router Discovery page appears, showing the list of routers that have been discovered so far.

Step 5 Click Discovery.

Step 6 From the pull-down menu in the Discovery field, choose By Seed IP/Flat File.

The Multicast Discovery configuration page appears and shows the Core/Enterprise Discovery tab, as shown in Figure 6-2.

Step 7 Do one of the following:

- If you want to discover contiguous devices, click the Contiguous radio button.
- If you want to discover the core network and connected CEs, click the Core + CEs Only radio button.
In the Seed IP/Name field, enter the IP address or the hostname of the seed device from which to start network discovery.

If you clicked the Core + CEs Only radio button, then in the Flat File Path field, enter the fully directory path and filename for the file that you coded to provide CE information.

Specify additional discovery parameters as shown in Table 6-1.

Click Start Discovery to complete the configuration of multicast discovery.

### Distributed Network Discovery

To discover devices in a distributed network:

**Step 1**  Edit a text file that provides IP addresses for the discovery process:
If you want to discover customer site devices but know only the addresses for the PE devices, provide a CSV file that lists the IP addresses of the PEs that you want to discover, separated by commas.

This type of discovery requires CLI access to the PE devices, to enable identification of the CE devices and other connected devices. To provide CLI access, ensure that the System Configuration page in the Domain Management interface specifies username and password information to enable CLI access.

If you want to discover the customer site devices and you know the IP addresses of the CE devices and associated PE devices, code a CSV file that lists the IP addresses for CE devices and associated PE devices in the following format:

CE1=PE1:PE2:PE3, CE2=PE1:PE2:PE3

**Step 2**  
Save the file in an appropriate directory on the CMM server.

**Step 3**  
From the Multicast Manager menu, select **Discovery & Trace**.

**Step 4**  
Select **Discovery**.

**Step 5**  
Select **Multicast Discovery**.

The Router Discovery page appears, showing the list of routers that have been discovered so far.

**Step 6**  
Click the **Distributed Network** tab.

**Step 7**  
Do one of the following:

- To discover PEs only, click the **PE Only** radio button.
- To discover CEs and associated PEs, click the **CE-PE Mapping** radio button.

**Step 8**  
Specify additional discovery parameters as shown in **Table 6-2**.

**Table 6-2 Multicast Discovery: Distributed Network Discovery**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flat File Address</td>
<td>Enter the fully qualified name of the server file that contains CEs. File format: CE1=PE1:PE2:PE3</td>
</tr>
<tr>
<td>Community Strings</td>
<td>Enter the community strings.</td>
</tr>
<tr>
<td>Discovery Depth</td>
<td>Select a value.</td>
</tr>
<tr>
<td>Network Limit</td>
<td>Click the <strong>All</strong>, <strong>Include</strong>, or <strong>Exclude</strong>. radio button. If you select Include or Exclude, use the IP address and network mask fields to enter IP addresses and network masks that you want to include or exclude in the discovery and click the right arrows (&gt;&gt;) to move them to the Include or Exclude list.</td>
</tr>
<tr>
<td>Network Address and Mask</td>
<td>If you select Include or Exclude, allows you to filter network discovery types.</td>
</tr>
</tbody>
</table>

**Step 9**  
Click **Start Discovery** to complete the configuration of multicast discovery.
**Single Device Discovery**

Run Single Device Discovery to add individual devices to CMM’s network topology after discovering the network or network segments using the other types of discovery.

Running Single Device Discovery does not overwrite the information from previous discovery operations.

To run Single Device Discovery:

---

**Step 1**
From the Multicast Manager menu, select **Discovery & Trace**.

**Step 2**
Select **Discovery**.

**Step 3**
Select **Multicast Discovery**.

The Router Discovery page appears, showing the list of routers that have been discovered so far.

**Step 4**
Click **Discovery**.

**Step 5**
From the pull-down menu in the Discovery field, choose **By Seed IP/Flat File**.

The Multicast Discovery configuration page appears and shows the Core/Enterprise Discover tab, as shown in Figure 6-2.

**Step 6**
Click the **Single Device Discovery** tab.

**Step 7**
Specify additional discovery parameters as shown in **Table 6-3**.

---

**Table 6-3**  **Multicast Discovery: Single Device Discovery**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Seed IP/Name</td>
<td>Enter the router name or IP address.</td>
</tr>
<tr>
<td>Community Strings</td>
<td>Specify community strings for the router.</td>
</tr>
<tr>
<td>Discovery Depth</td>
<td>Click either the <strong>This Device Only</strong> radio button or the <strong>One hop from the device</strong> radio button.</td>
</tr>
<tr>
<td>Network Limit</td>
<td>Click the <strong>All</strong>, <strong>Include</strong>, or <strong>Exclude</strong> radio button.</td>
</tr>
<tr>
<td></td>
<td>If you select Include or Exclude, use the IP address and network mask fields to enter IP addresses and network masks that you want to include or exclude in the discovery and click the right arrows (&gt;&gt;&gt;) to move them to the Include or Exclude list.</td>
</tr>
</tbody>
</table>

**Step 8**
Click the **Add/Rediscover button**.

---

**L2 Device**

To run L2 device discovery:
**Discovery**

**Step 1**
From the Multicast Manager menu, select **Discovery & Trace**.

**Step 2**
Select **Discovery**.

**Step 3**
Select **L2 Device**.

The L2 Discovery page opens.

**Step 4**
Click **Add**, and from the drop-down list, select **By L2**.

The Add/Rediscover a L2 Device page appears.

The add or rediscover a L2 Device configuration page contains the following fields and buttons:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch Name/IP Address</td>
<td>Enter the switch name or IP address.</td>
</tr>
<tr>
<td>RO Community String</td>
<td>The read only community string for the router.</td>
</tr>
<tr>
<td>Save</td>
<td>Adds the selected L2 for discovery.</td>
</tr>
</tbody>
</table>

**Adding L2 Devices for Discovery by Import**

If you have previously saved a list of discovered Layer 2 devices in a CSV file, you can import the devices for discovery by importing the file.

To import a CSV file listing Layer 2 devices, on the L2 Discovery page, click **Add**, and from the drop-down list, select By Import. Then, from the L2 Discovery > Import page, browse for the CSV file to import and click the **Import** button.

**Video Probe**

To run video probe discovery:

**Step 1**
From the Multicast Manager menu, select **Discovery & Trace**.

**Step 2**
Select **Discovery**.

**Step 3**
Select **Video Probe**

**Step 4**
Click the **Add** button.

**Step 5**
From the pull-down menu, select **By Video Probe**.

The Add / Rediscover a Video Probe configuration page appears, as shown in Figure 6-3.
Chapter 6  Discovery and Trace

Figure 6-3  Add/Rediscover Video Probe Page

The Add / Rediscover a Video Probe configuration page contains the following fields and buttons:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Probe Name/IP Address</td>
<td>Enter the probe name or IP address.</td>
</tr>
<tr>
<td>Probe RO Community String</td>
<td>Enter the SNMP read-only community string for the probe.</td>
</tr>
<tr>
<td>Probe RW Community String</td>
<td>SNMP read-write community string for the probe.</td>
</tr>
<tr>
<td>Application Type</td>
<td>From the pull-down list in the Application type field, a video probe application to discover. CMM 3.1 supports the BridgeTech, iVMS v 3.x and 4.x, and Mixed Signals probes. To discover another type of probe select Others.</td>
</tr>
<tr>
<td>Router Name/IP Address</td>
<td>Enter hostname or IP address of the router on which the probe is running.</td>
</tr>
<tr>
<td>Router RO Community String</td>
<td>Enter read only community string for the router.</td>
</tr>
<tr>
<td>Interface Description</td>
<td>Enter brief description of the interface that the probe is monitoring.</td>
</tr>
<tr>
<td>Save</td>
<td>Adds the selected video probe for discovery.</td>
</tr>
</tbody>
</table>

**Monitoring Application**

To configure monitoring applications:

**Step 1** From the Multicast Manager menu, select **Discovery & Trace**.

**Step 2** Select **Discovery**.

**Step 3** Select **Video Probe**.

**Step 4** Click **Monitoring Application**.

**Step 5** Click **Add**.
**Step 6** From the pull-down menu, select **By Monitoring Application**.

The Monitoring Application configuration page contains the following fields and buttons:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Name</td>
<td>Enter the name of the monitoring application</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the application.</td>
</tr>
<tr>
<td>HostIp</td>
<td>Enter the IP address of the host where the application is running.</td>
</tr>
<tr>
<td>URL Port</td>
<td>Enter the URL port for the application.</td>
</tr>
<tr>
<td>Community String on Application</td>
<td>Enter the SNMP Community String for the application.</td>
</tr>
<tr>
<td>Application Type</td>
<td>From the pull-down list, select the application type.</td>
</tr>
<tr>
<td>Save</td>
<td>Adds the selected monitoring application for discovery.</td>
</tr>
</tbody>
</table>

**Vidmon Device**

Use Vidmon device discovery to discover Vidmon capable devices in your network (Cisco 7600 series routers or Cisco ASR 9000 devices).

To run Vidmon device discovery:

**Step 1** From the Multicast Manager menu, select **Discovery & Trace**.

**Step 2** Select **Discovery**.

**Step 3** Select **Vidmon Device**.

The Discovery > Vidmon Device page appears. This page is initially empty, and after a successful discovery lists the currently discovered Vidmon devices.

**Step 4** If you want to use a filter to control the discovery of Vidmon devices:

a. Click the **Add Filter** button.

b. On the Add Filter page, specify the filter:

<table>
<thead>
<tr>
<th>Matching</th>
<th>From the drop-down list, select either <strong>All</strong> or <strong>Any</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter</td>
<td>You can specify up to two filters to filter the discovery by device name or by IP address. From the drop-down list (s), select either <strong>Device Name</strong> or <strong>Device IP Address</strong></td>
</tr>
</tbody>
</table>
To update the inventory of Vidmon devices, click the **Update Vidmon Capable** button.

---

## Unicast Device

To configure unicast discovery:

**Step 1**  From the Multicast Manager menu, select **Discovery & Trace**.

**Step 2**  Select **Discovery**.

**Step 3**  Select **Unicast**.

**Step 4**  Click **Add**.

**Step 5**  Select **By Unicast Router**.

The Unicast Router Discovery configuration page contains the following fields and buttons:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router Name/IP Address</td>
<td>Enter the or IP address for the router.</td>
</tr>
<tr>
<td>RO Community String</td>
<td>The read only community string for the router.</td>
</tr>
<tr>
<td>Add/Modify</td>
<td>Adds the selected Unicast router for discovery.</td>
</tr>
</tbody>
</table>

---

## Trace

### Multicast Trace

To configure multicast trace:

**Step 1**  From the Multicast Manager menu, select **Discovery & Trace**.

**Step 2**  Select **Trace**.

**Step 3**  Select **Multicast Trace**.

The Multicast Trace configuration page contains the following fields and buttons:
### Discovery and Trace

#### Trace

**Step 4** Click the **Trace** button.

The Trace Data page appears, showing the trace data and a topology diagram for the devices included in the trace.

The trace name at the top of the page has the following format:

Group (**Group Description**) transport (**Transport_Description**) Source (**Source_Description**), for example, “Tracing multicast group 211.22.2.0 (Midwest Region) transport (TBS Sports Network) Source (Region One).”

**Step 5** If you want to save the trace, complete these steps:

- a. Scroll down to the Input File field.
- b. If you want to change the trace name, edit the trace filename shown in the Input File field.
- c. Click the **Save As** button.

**Step 6** To view additional information about the probe used in the trace, click on the probe icon.

If you click on the probe icon:

- For the MixedSignal probe, the latest traps for the probe are displayed.
- If the probe is a probe other than the MixedSignal, iVMS, or BridgeTech probe, a video probe application page for the probe launches.

---

### Show Groups

To configure and run a Show Groups trace:

**Step 1** From the Multicast Manager menu, select **Discovery & Trace**.

**Step 2** Select **Trace**.

**Step 3** Select **Show Groups**.

**Step 4** Select a device from the pull-down list.

**Step 5** The trace appears in the S,G Trace table.

---

<table>
<thead>
<tr>
<th>Fields and Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select a Device</td>
<td>Select a device.</td>
</tr>
<tr>
<td>Source</td>
<td>Select a source from the drop-down menu.</td>
</tr>
<tr>
<td>Group</td>
<td>Select a group from the drop-down menu.</td>
</tr>
<tr>
<td>Reset SG List</td>
<td>Click <strong>Clear SG Filter</strong> to reset the values from the source and group lists.</td>
</tr>
<tr>
<td>Select Service Type</td>
<td>Select a service type from the drop-down menu.</td>
</tr>
<tr>
<td>FHR</td>
<td>Select the start destination for the First Hop Router.</td>
</tr>
<tr>
<td>LHR</td>
<td>From the pull-down list in the LHR field, select the end destination for the Last Hop Router.</td>
</tr>
</tbody>
</table>
Step 6  To run a trace on a listed Multicast Group, click on the IP address for the group at the left of the group entry.

Step 7  If you want to see a trace for one of the sources for the group, click on the sources link to the right of the entry and then click on a source IP address on the page that appears.

Step 8  If you want to run a trace from a saved trace file, select a trace file from the pull-down list in the Load from previously saved traces field and then click the Show Trace button.
Topology

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

This chapter contains the following sections:

- Topology, page 7-1
- All Device Information, page 7-2

**Step 1** From the Multicast Manager menu, select **Topology**.

**Step 2** Select **Topology**.
Step 3 A topology view window opens in your browser and a network topology map appears, as shown in Figure 7-1.

Figure 7-1 Topology View Window

Step 4 Click on any of the topology graphics to move them.

Note The Search button allows you to specify the device name or IP address to conduct a search. If the search is successful, the device will be highlighted.

Note Checking the Link Label box will enable the map to display the interface names for all of the devices that the link is connected to.

Step 5 Click the Save Layout button.

All Device Information

To view Protocol Independent Multicast (PIM) neighbors and multicast information of one hop neighbors:

Step 1 From the Multicast Manager menu, select Topology.

Step 2 Click All Device Information.

The Topology - One Hop Neighbors window appears.
Step 3  From the pull-down list in the Select a Router field, choose a device for which to display information and click the **Show** button.

A network topology table appears. The table displays PIM neighbors for the selected device and a separate pane for each PIM neighbor that shows its PIM neighbors.

**Figure 7-2  Topology - All Devices**

Step 4  To view the PIM neighbors of a device that is listed in one of the panes, click the router ID in the Neighbor column.
Diagnostics

This chapter contains the following sections:

- SG Diagnostics, page 8-1
- L2 Diagnostics, page 8-2
- Video Diagnostics, page 8-3
- Miscellaneous Diagnostics, page 8-9
- Tools, page 8-12
- CRM Diagnostics, page 8-20

SG Diagnostics

Packet Monitoring

To plot packet monitoring:

**Step 1** From the Multicast Manager menu, select **Diagnostics**.
**Step 2** Select **S,G Diagnostics**.
**Step 3** Select **Packet Monitoring**.

The Packet Monitoring page contains the following fields and buttons:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select a Device</td>
<td>Select a device from the drop-down list.</td>
</tr>
<tr>
<td>Source</td>
<td>Select a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Select a group from the drop-down list.</td>
</tr>
<tr>
<td>Reset SG List</td>
<td>Clears any entries and refreshes the source and group lists.</td>
</tr>
<tr>
<td>Samples</td>
<td>Enter the sample value.</td>
</tr>
<tr>
<td>Interval</td>
<td>Enter the interval value.</td>
</tr>
<tr>
<td>Graph</td>
<td>Select the graph type.</td>
</tr>
</tbody>
</table>
L2 Diagnostics

L2 Multicast Information

To query L2 multicast information:

Step 1  From the Multicast Manager menu, select Diagnostics.
Step 2  Select L2 Diagnostics.
Step 3  Select L2 Multicast Info.

The Layer 2 Multicast Information page contains the following fields and buttons:
### Video Diagnostics

CMM provides the following tools to diagnose multicast of video:

- Video Probe Status, page 8-3
- Vidmon Flow Status, page 8-5

#### Video Probe Status

To view video probe status:

**Step 1** From the Multicast Manager menu, select **Diagnostics**.
**Step 2** Select **Video Diagnostics**.
**Step 3** Select **Video Probe Status**.

### L2 Host IP Addresses

To query host IP addresses:

**Step 1** From the Multicast Manager menu, select **Diagnostics**.
**Step 2** Select **L2 Diagnostics**.
**Step 3** Select **L2 Host IPs**.

The Layer 2 Host IPs page contains the following fields and buttons:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Enter the username.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password.</td>
</tr>
<tr>
<td>Select Switches</td>
<td>Select a switch.</td>
</tr>
<tr>
<td>Query</td>
<td>Run the query using the set parameters.</td>
</tr>
</tbody>
</table>
The Video Probe Status page opens, as shown in Figure 8-2. The Video Probe Status page shows the currently monitored video probes, the number of flows monitored by each probe, and a status indicator for the probe.

**Figure 8-2  Video Probe Status Page**

![Video Probe Status Page](image)

**Step 4** To change the monitoring interval for the video probes, click the **Monitor** button, and then change the monitoring interval as required.

**Step 5** To monitor a specific video probe, click a probe link.

The Video Probes Flows page for the selected probe appears, as shown in Figure 8-3.

**Figure 8-3  Video Probes Flow Page**

![Video Probes Flow Page](image)
Step 6  To perform a multicast trace on one of the Group Ports listed on the Video Probes Flow Page, click on the IP address for the Group Port.

**Vidmon Flow Status**

To view video probe status:

**Step 1**  From the Multicast Manager menu, select **Diagnostics**.

**Step 2**  Select **Video Diagnostics**.

**Step 3**  Select **Vidmon Flow Status**

The Vidmon Flow Status page appears, as shown in Figure 8-4. The Video Flow Status page shows the status of the Vidmon devices in the CMM network topology.

**Figure 8-4  Vidmon Flow Status Page**

---

**Step 4**  To view more detailed status, for the interfaces on the Vidmon device, click a device name on the Video Flow Status page.

The Vidmon Flows Status page appears, as shown in Figure 8-5. The Vidmon Flows Status page shows the status of the current video flow on each interface on the device.

**Figure 8-5  Vidmon Flows Status Page with Interfaces**

---

**Step 5**  To view detailed statistics on the current video flow on the interface, click on an interface name in the list.
The Vidmon Interface Flows page appears, as shown in Figure 8-6. The Vidmon Interface Flows page shows detailed statistics for the current flows on the interface.

**Figure 8-6   Vidmon Interface Flows Page**

![Vidmon Interface Flows Page](image)

The Vidmon Interface Flows Page shows the following information for the video flows:

- The IP address of the Source port.
- The IP address of the Destination port.
- The status of the flow.
- For Cisco 76xx devices, the Media Loss Rate (MLR)

**Note** MLR is not monitored for Cisco ASR 9000 devices.

- The minimum Media Rate Variation (MRV).
- The maximum MRV.
- The direction of the flow (outbound or inbound).

**Step 6** To perform a multicast trace for the flow, click on the IP address of the Destination Port for the flow.

**Step 7** To view additional details regarding the flow, such as the number of intervals and metrics for the flow, click on the More link in the More Details column.

The Vidmon Interface Flows page for the interface appears, as shown in Figure 8-7.
Chapter 8  Diagnostics

Video Diagnostics

Figure 8-7  Vidmon Interface Flows Page for a 76xx Device

![Vidmon Interface Flows Page for a 76xx Device]

The Vidmon Interface Flows Page shown in Figure 8-7 indicates flow information for a Cisco 76xx device.

The Vidmon Interface Flow for a Cisco 76xx devices shows:

- **Type**—The flow table maintained for Cisco 76xx is an MDI table.
- **MLR**—Indicates the MLR for the flow.
- **DF**—Indicates the DF for the flow.

Figure 8-8 shows a Vidmon Interface Flows page for an ASR 9000 device.

Figure 8-8  Vidmon Interface Flows Page for an ASR 9000 Device.

![Vidmon Interface Flows Page for an ASR 9000 Device]

The Vidmon Interface Flows page shows the following information:

- **Type**—The flow table maintained for Cisco ASR 9000 series devices is a CBR table.
- **MRV %**—The MRV value in millisecond percentage.
- **DF**—The delay factor.
Running Vidmon Troubleshooting

From the Vidmon Flow Status page, you can telnet into the Vidmon devices monitored by CMM and run CLI commands to troubleshoot problems with the flows on a device interface.

To run Vidmon troubleshooting:

**Step 1** From the Multicast Manager menu, select **Diagnostics**.

**Step 2** Select **Video Diagnostics**.

**Step 3** Select **Vidmon Flow Status**

**Step 4** The Vidmon Flow Status page appears.

**Step 5** On the Vidmon Flow Status page, click **Vidmon Troubleshooting**.

The Vidmon Diagnostics page appears, as shown in Figure 8-9.

**Figure 8-9 Vidmon Diagnostics Page**

The Video Diagnostics page shows the Max DF, Max MLR, Min MRS, and Max MRV value for each stream.

**Step 6** From the drop-down list in the Device field, choose a device.

**Step 7** From the drop-down list in the Interface field, choose an interface on the device to troubleshoot.

**Step 8** Enter the User ID, Password, and Enable Password for the device.

**Step 9** From the drop-down list in the Select/Edit command, choose a command.

**Note** The commands available for selection from the drop-down list are configurable in a text file. On the Linux platform, add the Vidmon command in a file named `VidmonCommand.txt` in the `/usr/local/netman/mmtsys/sys` directory. On the Solaris platform, add the Vidmon command in the `VidmonCommand.txt` file in the `/opt/RMSMT/mmtsys/sys` directory.

**Step 10** Click the **Edit** button and edit the command.

For example for the `show policy-map type performance-traffic int <INT>` command, enter the interface number required for the command.

**Step 11** Click the **Run Command** button.

The command output appears in the output area at the bottom of the page.
If you want to e-mail the output command to the Cisco Technical Assistance Center (TAC), click **E-Mail Output to TAC**, edit the e-mail in the window that appears, and click the **Send E-Mail** button to send the E-mail.

## Miscellaneous Diagnostics

From the Miscellaneous Diagnostics menu, you can run the following diagnostic procedures:

- RP Status, page 8-9
- RP Summary, page 8-10
- MSDP Status, page 8-11
- Network Status, page 8-11
- Locate a Host, page 8-12

## RP Status

To view Rendezvous Point (RP) status:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>From the Multicast Manager menu, select <strong>Diagnostics</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Select <strong>Miscellaneous Diagnostics</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select <strong>RP Status</strong>. The RP status page appears.</td>
</tr>
<tr>
<td>Step 4</td>
<td>From the drop-down list in the <strong>Select a Router</strong> field, choose a router and click <strong>Show</strong>. The RP status page for the router appears, including RP set and RP state.</td>
</tr>
</tbody>
</table>

![Figure 8-10 RP Status Page](image-url)
RP Summary

To view the RP summary:

**Step 1** From the Multicast Manager menu, select **Diagnostics**.

**Step 2** Select **Miscellaneous Diagnostics**.

**Step 3** Select **RP Summary**.

The RP Summary page appears, as shown in **Figure 8-11**.

**Step 4** Click an RP link.

The RP Summary page for the link appears as shown in Figure 8-11. The RP Summary page shows the following information for the RP:

- PIM Neighbors
- PIM Interface Mode
- IGMP Interface Version
- RP Information

**Step 5** To telnet to the device to run a `show` command, enter the username, password, enable password, and a `show` command, and then click the **Show** button.
MSDP Status

To view Multicast Source Discovery Protocol (MSDP) status:

**Step 1** From the Multicast Manager menu, select **Diagnostics**.

**Step 2** Select **Miscellaneous Diagnostics**.

**Step 3** Select **MSDP Status**.

The MSDP Status page appears. The MSDP Status page shows the devices, MSDP peers, remote IP addresses, and MSDP status for the devices in the current domain.

**Figure 8-12 MSDP Status Page**

**Step 4** From the MSDP Status page, you select an MSDP router and do the following:

- Click the **Peer Info** button to display MSDP statistics for the device.
- Click the **SA Cache Info** button to display SACache information.

**Step 5** Select a MSDP Router from the drop-down menu and click **Peer Info** to view the peer information.

**Step 6** Select a MSDP Router from drop-down and click **SA Cache Info** to view SA Cache information.

Network Status

The Network Status page displays the status of all routers. This table displays each router name and the amount of time that the system has been up. Routers that are not responding are highlighted in red.

To view network status:

**Step 1** From the Multicast Manager menu, select **Diagnostics**.

**Step 2** Select **Miscellaneous Diagnostics**.

**Step 3** Select **Network Status**
## Locate a Host

To locate a host:

**Step 1** From the Multicast Manager menu, select **Diagnostic**.

**Step 2** Select **Miscellaneous Diagnostics**.

**Step 3** Select **Locate Host**.

**Step 4** Enter an IP address.

**Step 5** Click **Locate**.

## Tools

### IGMP Diagnostics

To run IGMP diagnostics:

**Step 1** From the Multicast Manager menu, select **Diagnostics**.

**Step 2** Select **Tools**.

**Step 3** Select **IGMP Diagnostics**.

The IGMP Diagnostics page contains the following fields and buttons:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select a Group</td>
<td>Select a group from the drop-down list.</td>
</tr>
<tr>
<td>Select a Router</td>
<td>Select one or more routers.</td>
</tr>
<tr>
<td>Select Diagnostic Type</td>
<td>Select the diagnostic type.</td>
</tr>
<tr>
<td>Output Filter</td>
<td>To display failures, check the Show Failure box.</td>
</tr>
<tr>
<td>Run</td>
<td>Create an IGMP cache.</td>
</tr>
</tbody>
</table>

## Top Talkers

To view top talkers:

**Step 1** From the Multicast Manager menu, select **Diagnostics**.

**Step 2** Select **Tools**.

**Step 3** Select **Top Talkers**.
The Top Talkers page contains the following fields and buttons:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select a Device</td>
<td>Select a device from the drop-down list.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the username.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password.</td>
</tr>
<tr>
<td>Polling Interval</td>
<td>Select a polling interval.</td>
</tr>
<tr>
<td>Top Talker</td>
<td>Create a list of top talkers.</td>
</tr>
</tbody>
</table>

**Health Check**

To run a health check:

**Step 1** From the Multicast Manager menu, select **Diagnostics**.

**Step 2** Select **Tools**.

**Step 3** Select **Health Check**.

**Step 4** Select a baseline from the Select Health Check list.

**Step 5** Click **Run**.

**MVPN**

The MVPN tool displays the Virtual Routing and Forwarding (VRF) Table configurations and Provider Edge (PE) Device configurations.

To view MVPN diagnostics:

**Step 1** From the Multicast Manager menu, select **Diagnostics**.

**Step 2** Select **Tools**.

**Step 3** Select **MVPN**.

Every VRF and PE configuration is displayed.

**Step 4** Click on a device to view the details.

**Note** You can update the VRF information in the inventory by clicking on the device name link. If the device is a non-VRF aware device, CMM attempts to use the CLI to update the inventory details.
6500/7600 Troubleshooting

Full Trace

To view a full trace:

Step 1  From the Multicast Manager menu, select Diagnostics.
Step 2  Select Tools.
Step 3  Select 6500/7600 Troubleshooting.
Step 4  Select Full Trace.

The Full Trace page contains the following fields and buttons:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select a Device</td>
<td>Select a device from the drop-down list.</td>
</tr>
<tr>
<td>Source</td>
<td>Select a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Select a group from the drop-down list.</td>
</tr>
<tr>
<td>Reset SG List</td>
<td>Clears any entries and refreshes the source and group lists.</td>
</tr>
<tr>
<td>Service Type</td>
<td>Select a service type from the drop-down list.</td>
</tr>
<tr>
<td>Run Full Trace</td>
<td>Click the Run Full Trace button to launch a full trace.</td>
</tr>
</tbody>
</table>

Diagnostics

To view 6500/7600 Troubleshooting Diagnostics:

Step 1  From the Multicast Manager menu, select Diagnostics.
Step 2  Select 6500/7600 Troubleshooting.
Step 3  Select Diagnostics.

The Diagnostics page contains the following fields and buttons:
Chapter 8  Diagnostics

To view 6500/7600 troubleshooting diagnostics:

Step 1  From the Multicast Manager menu, select **Diagnostics**.

Step 2  Select **6500/7600 Troubleshooting**.

Step 3  Select **Troubleshooting**.

The Troubleshooting page contains the following fields and buttons:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select a Device</td>
<td>Select a device from the drop-down list.</td>
</tr>
<tr>
<td>Source</td>
<td>Select a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Select a group from the drop-down list.</td>
</tr>
<tr>
<td>Reset SG List</td>
<td>Clears any entries and refreshes the source and group lists.</td>
</tr>
<tr>
<td>Service Type</td>
<td>Enter the service type.</td>
</tr>
<tr>
<td>Polling Interval</td>
<td>Enter the interval value.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the user name.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password.</td>
</tr>
<tr>
<td>Enable Password</td>
<td>Enter the enable password.</td>
</tr>
<tr>
<td>Run Diagnostics</td>
<td>Launch a diagnostic trace.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select a Device</td>
<td>Select a device from the drop-down list.</td>
</tr>
<tr>
<td>Source</td>
<td>Select a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Select a group from the drop-down list.</td>
</tr>
<tr>
<td>Reset SG List</td>
<td>Clears any entries and refreshes the source and group lists.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the user name.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password.</td>
</tr>
<tr>
<td>Enable Password</td>
<td>Enter the Enable password.</td>
</tr>
<tr>
<td>Command</td>
<td>Select a command from the drop-down list.</td>
</tr>
<tr>
<td>Run Command</td>
<td>Launch a troubleshooting trace.</td>
</tr>
</tbody>
</table>


To view 6500/7600 Troubleshooting Diagnostics:

**Step 1** From the Multicast Manager menu, select **Diagnostics**.

**Step 2** Select **6500/7600 Troubleshooting**.

**Step 3** Select **Diagnostics**.

The Diagnostics page contains the following fields and buttons:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select a Device</td>
<td>Select a device from the drop-down list.</td>
</tr>
<tr>
<td>Source</td>
<td>Select a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Select a group from the drop-down list.</td>
</tr>
<tr>
<td>Reset SG List</td>
<td>Clears any entries and refreshes the source and group lists.</td>
</tr>
<tr>
<td>Service Type</td>
<td>Enter the service type.</td>
</tr>
<tr>
<td>Polling Interval</td>
<td>Enter the interval value.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the username.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password.</td>
</tr>
<tr>
<td>Enable Password</td>
<td>Enter the enable password.</td>
</tr>
<tr>
<td>Run Diagnostics</td>
<td>Launch a diagnostic trace.</td>
</tr>
</tbody>
</table>
Troubleshooting

To view 6500/7600 troubleshooting diagnostics:

**Step 1**  From the Multicast Manager menu, select **Diagnostics**.
**Step 2**  Select **6500/7600 Troubleshooting**.
**Step 3**  Select **Troubleshooting**.

The Troubleshooting page contains the following fields and buttons:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select a Device</td>
<td>Select a device from the drop-down list.</td>
</tr>
<tr>
<td>Source</td>
<td>Select a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Select a group from the drop-down list.</td>
</tr>
<tr>
<td>Reset SG List</td>
<td>Clears any entries and refreshes the source and</td>
</tr>
<tr>
<td></td>
<td>group lists.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the user name.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password.</td>
</tr>
<tr>
<td>Enable Password</td>
<td>Enter the Enable password.</td>
</tr>
<tr>
<td>Command</td>
<td>Select a command from the drop-down list.</td>
</tr>
<tr>
<td>Run Command</td>
<td>Launch a troubleshooting trace.</td>
</tr>
</tbody>
</table>

SNMP Utilities

IGMP Cache

To view the IGMP cache:

**Step 1**  From the Multicast Manager menu, select **Diagnostics**.
**Step 2**  Select **SNMP Utils**.
**Step 3**  Select **IGMP Cache**.

The IGMP Cache page contains the following fields and buttons:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select a Router</td>
<td>Select a router from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Select a group from the drop-down list.</td>
</tr>
<tr>
<td>Show</td>
<td>Display the IGMP cache.</td>
</tr>
</tbody>
</table>
**PIM Neighbor**

To view a PIM neighbor:

**Step 1**  
From the Multicast Manager menu, select **Diagnostics**.

**Step 2**  
Select **SNMP Utils**.

**Step 3**  
Select **PIM Neighbor**.

The PIM Neighbor page contains the following fields and buttons:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select a Device</td>
<td>Select a device from the drop-down list.</td>
</tr>
<tr>
<td>Select a Neighbor Router</td>
<td>Select a neighbor router from the drop-down list.</td>
</tr>
<tr>
<td>Show</td>
<td>Display the relationship between the device and its neighbor.</td>
</tr>
</tbody>
</table>

**SNMP PIM Reachability**

Use the SNMP PIM Reachability tool to determine what a PIM interfaces are down.

To run the SNMP PIM Reachability tool:

**Step 1**  
From the Multicast Manager menu, select **Diagnostics**.

**Step 2**  
Select **Tools**.

**Step 3**  
Select **SNMP PIM Reachability**.

The SNMP PIM Reachability page appears.

**Step 4**  
Do one of the following:

- On the SNMP PIM Reachability page, from the drop-down list in the Router field, select the routers to query.
- To select all routers, click the **Select All** button.

**Step 5**  
Click **Submit**.

CMM queries the selected router for PIM reachability and checks connectivity with CMM for all of the PIM interfaces.

A list of unreachable routers appears. If none of the routers in unreachable, the list is empty.

**Explicit User Tracking**

The Explicit User Tracking tool allows you to track the activities of a specified user. You can track the user’s actions in monitoring:
To track user activities:

**Step 1**  From the Multicast Manager menu, select **Diagnostics**.

**Step 2**  Select **Tools**.

**Step 3**  Select **Explicit User Tracking**.

The Explicit User Tracking page for router usage appears.

The Explicit User Tracking page contains the following fields and buttons:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Enter the username.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password for the user.</td>
</tr>
<tr>
<td>Router</td>
<td>From the pull-down menu, select a router.</td>
</tr>
<tr>
<td>VLAN Name</td>
<td>From the pull-down menu, select a VLAN connected to the router.</td>
</tr>
<tr>
<td>Submit</td>
<td>Click <strong>Submit</strong> to submit the request.</td>
</tr>
</tbody>
</table>

### Stream Query

To query user activity in monitoring a specified TS:

**Step 1**  Select **Explicit User Tracking**.

The Explicit User Tracking page for router usage appears.

**Step 2**  Click **Stream Query**.

**Step 3**  From the Explicit User Tracking page for stream query use following fields and buttons:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Enter the username.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password for the user.</td>
</tr>
<tr>
<td>Source</td>
<td>From the pull-down menu, select a source.</td>
</tr>
<tr>
<td>Group</td>
<td>From the pull-down menu, select a Group.</td>
</tr>
<tr>
<td>Reset SG List</td>
<td>To clear the current S,G information click <strong>Reset SG List</strong>.</td>
</tr>
<tr>
<td>Submit</td>
<td>Click <strong>Submit</strong> to submit the request.</td>
</tr>
</tbody>
</table>
Receiver Query
To query user activity in monitoring a specified TS:

### Step 1
Select **Explicit User Tracking**.
The Explicit User Tracking page for router usage appears.

### Step 2
Click **Receiver Query**.

### Step 3
From the Explicit User Tracking page for a receiver query appears use the following fields and buttons:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Enter the username.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password for the user.</td>
</tr>
<tr>
<td>Receiver IP</td>
<td>Enter the IP address of the receiving device.</td>
</tr>
<tr>
<td>Submit</td>
<td>Click <strong>Submit</strong> to submit the request.</td>
</tr>
</tbody>
</table>

---

**CRM Diagnostics**

### Create Baseline

To create a routing table baseline:

### Step 1
From the Multicast Manager menu, select **Diagnostics**.

### Step 2
Select **CRM Diagnostics**.

### Step 3
Select **Create Baseline**.

The Create Routing Table Baseline page contains the following fields and buttons:
Check Routing Table Baseline Configuration

To check a routing table baseline configuration:

**Step 1** From the Multicast Manager menu, select **Diagnostics**.

**Step 2** Select **CRM Diagnostics**.

**Step 3** Select **Check Routing Table**.

The Check Routing Table Baseline page contains the following fields and buttons:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing Table Type</td>
<td>Select either Unicast or Multicast.</td>
</tr>
<tr>
<td>Select a Router</td>
<td>Select a router.</td>
</tr>
<tr>
<td>Baseline</td>
<td>Enter a baseline. If you check the box next to the baseline name, you can replace an existing value.</td>
</tr>
<tr>
<td>CPU Threshold</td>
<td>The CPU utilization of the router will be checked first to determine if a query of the routing table is acceptable based upon the configured CPU threshold. A value of -1, indicates that the routing table should be queried without checking CPU utilization.</td>
</tr>
<tr>
<td>Run</td>
<td>Click Run to create a routing table baseline.</td>
</tr>
</tbody>
</table>

**Check Routing Table**

To check a routing table baseline configuration:

**Step 1** From the Multicast Manager menu, select **Diagnostics**.

**Step 2** Select **CRM Diagnostics**.

**Step 3** Select **Check Routing Table**.

The Check Routing Table Baseline page contains the following fields and buttons:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing Table Type</td>
<td>Select either Unicast or Multicast.</td>
</tr>
<tr>
<td>Select a Router</td>
<td>Select a router.</td>
</tr>
<tr>
<td>Baseline</td>
<td>Select a baseline from the drop-down list.</td>
</tr>
<tr>
<td>CPU Threshold</td>
<td>The CPU utilization of the router will be checked first to determine if a query of the routing table is acceptable based upon the configured CPU threshold. A value of -1, indicates that the routing table should be queried without checking CPU utilization.</td>
</tr>
<tr>
<td>Run</td>
<td>Run a check on the routing table baseline.</td>
</tr>
</tbody>
</table>
9

Configuration Management

This chapter contains the following sections:

- Device Configuration, page 9-1
- MVPN Configuration, page 9-3

Device Configuration

Get All Configurations

To get all configurations:

1. From the Multicast Manager menu, select Configuration Management.
2. Select Device Configuration.
3. Select Get All Configuration.
4. Select a router.

Note: Click Select All to include all listed routers.

Validate All Configurations

To validate all configurations:

1. From the Multicast Manager menu, select Configuration Management.
2. Select Device Configuration.
3. Select Validate All Configurations.
4. Select a configuration name.
5. Select a router.
Configuring Static RPs

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

To configure static RPs:

Step 1 From the Multicast Manager menu, select Configuration Management.
Step 2 Select Device Configuration.
Step 3 Select Configure Static RPs.
Step 4 In the Add Static RP Search field, enter the IP address of the RP. The Search field is address sensitive, so as you enter the IP address, a list of routers appear.
Step 5 Click Add next to the router(s) you want to select. The Static RPs table is populated.

Configuring SSM Devices

The CMM currently supplies you with a list of all active sources and groups when requested. In a network containing RPs, the CMM visits each RP and collates a list to provide this information when requested. This is not possible in a Source Specific Multicast (SSM) network that does not contain RPs.

To provide you with a list of all active sources and groups in SSM networks, you can input routers to the CMM that it visits when asked for this information. You can decide which routers are considered RP-type devices that contain most of the active sources and groups in the network, and then specify those routers. When you request to Show All Groups, the CMM visits the specified routers and builds the list from them.

To configure SSM devices:

Step 1 From the Multicast Manager menu, select Configuration Management.
Step 2 Select Device Configuration.
Step 3 Select Configure SSM Devices.
Step 4 Within the Add Source Specific Multicast Device Search field, enter the IP address of the RP. The Search field is address sensitive, so as you type in the IP address, a list of routers appear.
Step 5 Click Add next to the router(s) that you want to select. The Source Specific Multicast Devices table is populated.
MVPN Configuration

To configure the MVPN service type:

**Step 1** From the Multicast Manager menu, select **Configuration Management**.

**Step 2** Select **MVPN Configuration**.

**Step 3** Click **Add**.

**Step 4** Select **By MVPN**.

The MVPN Configuration configuration page contains the following fields and buttons:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Type</td>
<td>Enter the service type.</td>
</tr>
<tr>
<td>CE Device</td>
<td>Select the CE Device.</td>
</tr>
<tr>
<td>Save</td>
<td>Adds the MVPN configuration.</td>
</tr>
</tbody>
</table>
Administration

System administrators can configure CMM by using CMM Administration.

This chapter contains the following sections:

- Managing Users and Access, page 10-1
- Address Management, page 10-5
- Logging Management, page 10-14
- Warning Page Configuration, page 10-15
- License Information, page 10-17

Managing Users and Access

CMM provides four privilege levels: NETWORKADMIN, SYSADMIN, OPERATOR, and HELPDESK. You need an administrator account to configure multicast domains, run discovery, create users, create health checks, and use the Admin Utilities functions.

This topic contains the following information:

- User Configuration, page 10-1
- Access Control, page 10-3
- Authentication & Audit, page 10-3
- ACS Server, page 10-4

User Configuration

Adding a User Configuration

0571624632

Step 1 From the Multicast Manager menu, select Administration.
Step 2 Select RBAC.
Step 3 Select User Configuration.
Step 4 Click the Add button.
Managing Users and Access

### Tip
After files have been configured and added to the User Configuration List, you can sort the data by clicking on the **Add Filter** button. This will allow you to build up to two filters based on user name and role.

### Modifying a User File

**Step 1**
From the Multicast Manager menu, select **Administration**.

**Step 2**
Select **RBAC**.

**Step 3**
Select **User Configuration**.

**Step 4**
Check the box next to the username for the file that you want to modify.

<table>
<thead>
<tr>
<th>Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete</td>
<td>Deletes the user file.</td>
</tr>
<tr>
<td>Edit</td>
<td>Allows a modification to the user file.</td>
</tr>
<tr>
<td>Change Password</td>
<td>Allows the modification to a user’s password.</td>
</tr>
</tbody>
</table>

### Unlocking a User ID
After five unsuccessful login attempts, a user is locked out of the system. You can then unlock the User ID to allow the user to log in again.

After you reset the user ID, the first time that the user logs in again, CMM prompts the user to change their password.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>Enter the user name</td>
</tr>
<tr>
<td>Password</td>
<td>Enter a password associated with this user name.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Re-enter the password from the previous field.</td>
</tr>
<tr>
<td>Mail ID</td>
<td>Enter the user’s mail ID.</td>
</tr>
<tr>
<td>Authorities</td>
<td>Assign the user access permissions by selecting one or more role from the list.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>Authorities</td>
<td>CMM provides four privilege levels: NETWORKADMIN, SYSADMIN, OPERATOR, and HELPDESK. You need an administrator account to configure multicast domains, run discovery, create users, create health checks, and use the Admin Utilities functions.</td>
</tr>
<tr>
<td>Add/ Modify</td>
<td>Click the Add/Modify button to add the record to the database.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
To unlock a user ID:

**Step 1** Go to Administration > RBAC > User Administration.
A list of the configured users appears. A lock icon appears next to the user name.

**Step 2** Check the check box next to the user name and then click the Edit button.
The User Configuration page for the user appears. The Is Account Locked check box is checked and a lock icon appears on the page.

**Step 3** Uncheck the Is Account Locked check box to unlock the User ID.
**Step 4** Check the Reset Password check box.
**Step 5** Click the Save button.
The user account is now unlocked and the user can log in again. When the user logs in, they are prompted to reset their login password.

**Access Control**

Access Control allows you to specify the CMM system features and capabilities that a specified user privilege level can access.

To specify set access control settings for the CMM user types:

**Step 1** From the Multicast Manager menu, select Administration.
**Step 2** Select RBAC.
**Step 3** Select Access Control.
**Step 4** Select a role from the list.
**Step 5** Check the boxes next to the features that you want to assign to the role.
**Step 6** Click the Save button.

**Authentication & Audit**

**Step 1** From the Multicast Manager menu, select Administration.
**Step 2** Select RBAC.
**Step 3** Select Authentication & Audit.
**Step 4** Select an authentication mode from the drop-down menu.
**Step 5** Check the Enable check box to create an audit log.
**Step 6** Click the Save button.
There are three modes for authentication: LOCAL, TACACS, and RADIUS. The default authentication mode is LOCAL.

### ACS Server

**Step 1** From the Multicast Manager menu, select *Administration*.

**Step 2** Select *RBAC*.

**Step 3** Select *ACS Server*.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Choose either RADIUS or TACACS.</td>
</tr>
<tr>
<td>Primary Server</td>
<td>Enter the IP address of the TACACS server.</td>
</tr>
<tr>
<td>Primary Port</td>
<td>This field is dynamically populated based on the Protocol field. The TACACS port number default is 49 and the Radius port number default is 1812.</td>
</tr>
<tr>
<td>Secondary Server</td>
<td>Enter the IP address of the TACACS server.</td>
</tr>
<tr>
<td>Secondary Port</td>
<td>Enter the secondary TACACS port number. The default is 49.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>Enter the key.</td>
</tr>
<tr>
<td>Apply</td>
<td>Apply the configuration changes to the database.</td>
</tr>
</tbody>
</table>

### Timeout Configuration

To change the session timeout settings:

**Step 1** From the Multicast Manager menu, select *Administration*.

**Step 2** Select *RBAC*.

**Step 3** Select *Timeout Configuration*.

**Step 4** Enter the amount of time in minutes.

**Step 5** Click *Save*. 
Address Management

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

This topic contains the following information:
- Destination Address Database, page 10-5
- Destination Address Database, page 10-5
- Transport Description, page 10-8
- Managing the Ad Zone Database, page 10-9
- Managing the Channel Map Database, page 10-10
- Managing the Multiplex Table Database, page 10-12

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

Destination Address Database

To add an address to the destination address database:

**Step 1** Select Administration->Destination Address Database.
**Step 2** Click the Add button and from the drop-down list, select By Address.
**Step 3** On the Destination Address Database page, specify:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Enter the IP address.</td>
</tr>
<tr>
<td>Description</td>
<td>Create and enter a description.</td>
</tr>
<tr>
<td>Ad Zone</td>
<td>If you have entered data for the Ad Zone database, select zone from the drop-down list.</td>
</tr>
<tr>
<td>Mux ID</td>
<td>If you have entered data for the Mux ID database, select a Mux ID from the drop-down list.</td>
</tr>
<tr>
<td>Save</td>
<td>Apply the new address to the database.</td>
</tr>
</tbody>
</table>

Destination Address Database

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

**Step 1**  
From the Multicast Manager menu, select Administration.

**Step 2**  
Select Address Management.

**Step 3**  
Select Destination Address Database.

The Destination Address Database page appears. This page lists the default and configured Destination addresses.

**Step 4**  
Click the Add button.

**Step 5**  
Select By Address.

**Note**  
You can also import an address file by selecting By Import from the Add button. Browse to the file location and select Upload.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Enter the IP address.</td>
</tr>
<tr>
<td>Description</td>
<td>Create and enter a description.</td>
</tr>
<tr>
<td>Ad Zone</td>
<td>If you have entered data for the Ad Zone database, select zone from the drop-down list.</td>
</tr>
<tr>
<td>Mux ID</td>
<td>If you have entered data for the Mux ID database, select a Mux ID from the drop-down list.</td>
</tr>
<tr>
<td>Save</td>
<td>Apply the new address to the database.</td>
</tr>
</tbody>
</table>

**Tip**  
After files have been configured and added to the Address Database, you can sort the data by clicking on the Add Filter button. This will allow you to build up to two filters based on address and description.

Modifying a Destination Address

**Step 1**  
From the Multicast Manager menu, select Administration.

**Step 2**  
Select Address Management.

**Step 3**  
Select Destination Address Database.

**Step 4**  
Check the check box next to the IP address that you want to modify.

**Step 5**  
Click the Edit button.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Enter the IP address.</td>
</tr>
<tr>
<td>Description</td>
<td>Create and enter a description.</td>
</tr>
</tbody>
</table>
Chapter 10  Administration

Address Management

Note
To delete a file, click the Actions button and select Delete from the drop-down menu.

Note
To export a file, click the Actions button and select Export from the drop-down menu. This will give you the option to save the file.

Source Description

The Source Description selection on the Address Management menu allows you to add a source IP address and enter a description for it. When a trace is performed that involves the source, the source description you enter is shown in the trace title on the Multicast Trace page.

Adding a Source Address and Description

To add a source address and description:

Step 1  From the Multicast Manager menu, select Administration.
Step 2  Select Address Management.
Step 3  Select Source Description.
Step 4  Click the Add button.
Step 5  Select By Source Address.

Note  You can also import an address file by selecting By Import from the Add button. Browse to the file location and select Upload.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Enter the IP address of the source.</td>
</tr>
<tr>
<td>Description</td>
<td>Create and enter a description.</td>
</tr>
<tr>
<td>Save</td>
<td>Apply the new address to the database.</td>
</tr>
</tbody>
</table>
Tip
After files have been configured and added to the Address Database, you can sort the data by clicking on the Add Filter button. This will allow you to build up to two filters based on address and description.

Modifying a Source Address or Description

To modify a source address:

Step 1 From the Multicast Manager menu, select Administration.
Step 2 Select Address Management.
Step 3 Select Source Database.
Step 4 Check the check box next to the IP address that you want to modify.
Step 5 If you want to delete the source address, click the Actions button and select Delete from the pull-down menu.
Step 6 To edit the source address information:
   a. Click the Edit button.
   b. Modify the Description field as required
   c. Click the Save button.

Transport Description

You can add entries to the address database describing the transport streams (TS) in a multicast flow. When a trace is performed that involves the TS, the transport description that you enter is shown in the trace title on the Multicast Trace page.

Adding a Transport Description

To add a transport description:

Step 1 From the Multicast Manager menu, select Administration.
Step 2 Select Address Management.
Step 3 Select Transport Description.
Step 4 Click the Add button.
Step 5 From the drop-down list, select By Transport Description.

Note You can also import an address file by selecting By Import from the Add button. Browse to the file location and select Upload.
Chapter 10      Administration

Address Management

Modifying a Transport Description

To modify a transport description:

Step 1   From the Multicast Manager menu, select Administration.
Step 2   Select Address Management.
Step 3   Select Transport Database.
Step 4   Check the check box next to the IP address for the transport description that you want to modify.
Step 5   If you want to delete the transport description, click the Actions button and select Delete from the pull-down menu.
Step 6   To edit the transport description information:
   a.  Click the Edit button.
   b.  Modify the Description field as required
   c.  Click the Save button.

Managing the Ad Zone Database

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

Adding a Zone

Step 1   From the Multicast Manager menu, select Administration.
Step 2   Select Address Management.
Step 3   Select Ad Zone Database.
Step 4   Click the Add button.
Step 5   Select By Zone.

Note   You can also import a file by selecting By Import from the Add button. Browse to the file location and select Upload.
Address Management

Chapter 10      Administration

Modifying a Zone

Step 1  From the Multicast Manager menu, select Administration.
Step 2  Select Address Management.
Step 3  Select Ad Zone Database.
Step 4  Click the Edit button.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zone Number</td>
<td>Create and enter a zone number.</td>
</tr>
<tr>
<td>Zone Name</td>
<td>Create and enter a zone name.</td>
</tr>
<tr>
<td>Save</td>
<td>Apply the edit the zone in the database.</td>
</tr>
</tbody>
</table>

Managing the Channel Map Database

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

Adding a Channel

Step 1  From the Multicast Manager menu, select Administration.
Step 2  Select Address Management.
Step 3  Select Channel Map Database.
Step 4  Click the Add button.
Step 5  Select By Channel.
You can also import a file by selecting **By Import** from the Add button. Browse to the file location and select **Upload**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel Number</td>
<td>Enter a channel number.</td>
</tr>
<tr>
<td>Channel Name</td>
<td>Enter a channel name.</td>
</tr>
<tr>
<td>Short Name</td>
<td>Enter a short name for the channel.</td>
</tr>
<tr>
<td>CODEC Type</td>
<td>From the drop-down list in the CODEC Type field, select the type of CODEC the channel uses.</td>
</tr>
<tr>
<td>Screen Format</td>
<td>From the drop-down list in the Screen Format field, select the screen format for the channel.</td>
</tr>
<tr>
<td>Service Type</td>
<td>From the drop-down list in the Service Type field, select the service type for the channel.</td>
</tr>
<tr>
<td>Save</td>
<td>Apply the new record to the database.</td>
</tr>
</tbody>
</table>

After files have been configured and added to the channel map database, you can sort the data by clicking on the **Add Filter** button. This will allow you to build up to two filters based on channel name and short name.

**Modifying a Channel**

1. From the Multicast Manager menu, select **Administration**.
2. Select **Address Management**.
3. Select **Channel Map Database**.
4. Check the check box next to the channel number that you want to modify.
5. Click the **Edit** button.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel Number</td>
<td>Enter the IP address.</td>
</tr>
<tr>
<td>Channel Name</td>
<td>Enter the channel number.</td>
</tr>
<tr>
<td>Short Name</td>
<td>Enter a short name for the channel.</td>
</tr>
<tr>
<td>CODEC Type</td>
<td>From the drop-down list in the CODEC Type field, select the type of CODEC the channel uses.</td>
</tr>
<tr>
<td>Screen Format</td>
<td>From the drop-down list in the Screen Format field, select the screen format for the channel.</td>
</tr>
</tbody>
</table>
**Managing the Multiplex Table Database**

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

**Adding a Record to the Multiplex Table Database**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>From the Multicast Manager menu, select <strong>Administration</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select <strong>Address Management</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select <strong>Multiplex Table Database</strong>.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click the <strong>Add</strong> button.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Select <strong>By Mux</strong>.</td>
</tr>
</tbody>
</table>

**Note**
You can also import a file by selecting **By Import** from the Add button. Browse to the file location and select **Upload**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mux Number</td>
<td>Enter the Mux number.</td>
</tr>
<tr>
<td>Channel Number</td>
<td>Select a channel number.</td>
</tr>
<tr>
<td>Add/Modify</td>
<td>Apply the new entry to the database.</td>
</tr>
</tbody>
</table>

**Note**
After files have been configured and added to the address database, you can sort the data by clicking on the **Add Filter** button. This will allow you to build up to two filters based on address and description.
Modifying a Record in the Multiplex Table Database

**Step 1**  
From the Multicast Manager menu, select **Administration**.

**Step 2**  
Select **Address Management**.

**Step 3**  
Select **Multiplex Table Database**.

**Step 4**  
Check the check box next to the record that you want to modify.

**Step 5**  
Click the **Edit** button.

---

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mux Number</td>
<td>Enter the Mux number.</td>
</tr>
<tr>
<td>Channel Number</td>
<td>Select a channel number.</td>
</tr>
<tr>
<td>Add/Modify</td>
<td>Apply the new entry to the database.</td>
</tr>
</tbody>
</table>

---

**Note**  
To delete a file, click the **Actions** button and select **Delete** from the drop-down menu.

**Note**  
To export a file, click the **Actions** button and select **Export** from the drop-down menu. This will give you the option to save the file.

---

Export & Import

To simplify the process of configuring the address management database, you can import and export database table information from a database dump.

If you exported the address management database, you can import the database dump by selecting the file name and clicking the **Import** button.

If you want to export the database information for later use, you can save the database to a database dump file by entering a file name and clicking the **Export** button.

The export method is useful if you have multiple CMM installations that use the same address management database: you can set up a database on one CMM server and then import it into another server.

---

Exporting Data

To export address management data:

**Step 1**  
From the Multicast Manager menu, select **Administration**.

**Step 2**  
Select **Address Management**.

**Step 3**  
Select **Export & Import**.

**Step 4**  
Click **Export** to export all address management entries and save the file locally.
You are prompted to save the export file.

**Step 5** Enter a filename and browse for the directory in which to save the export file.

**Step 6** Click the **Save** button

CMM saves the SQL data for the address management database in a text file. You can use this data to import the file on the current CMM device or on another CMM device running the same operating system.

---

### Importing Data

**Step 1** From the Multicast Manager menu, select **Administration**.

**Step 2** Select **Address Management**.

**Step 3** Select **Export & Import**.

**Step 4** Click the **Import** button to replace existing address management entries that you have imported

You are prompted for the name of the file to upload.

**Step 5** Click the **Browse** button and browse to the directory where the upload file resides, then select the file.

**Step 6** Click the **Upload** button.

CMM imports the address management data.

---

### Log Management

#### Logging Management

**Step 1** From the Multicast Manager menu, select **Administration**.

**Step 2** Select **Log Management**.

**Step 3** Select **Logging Management**.
Audit Log

Use the Audit Log feature to view Audit Log messages. To view audit log messages:

**Step 1** From the Multicast Manager menu, select Administration.

**Step 2** Select Log Management.

**Step 3** Select Audit Log.

The Audit Log page appears. The Audit Log page shows the audit log messages generated by CMM.

**Step 4** To view messages, scroll up and down the screen using the arrow icons.

**Step 5** If you want to delete a message:

a. Click Delete Logs.

b. In the Delete Logs older than x Days field, enter the number of days of logs to delete.

c. Click the Delete Audit Logs button.

Warning Page Configuration

The Warning Page Configuration feature allows you to configure an alert page that appears when user log in to CMM. If no Warning Page configuration is enabled, then no warning page appears when users log in.

To configure a Warning Page:

**Step 1** Select Administration.
Step 2 Select **Warning Page**.

The Warning Page configuration page appears, as shown in Figure 10-1.

**Figure 10-1 Warning Page Configuration Page**

```
<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Warning Page</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Enable/Disable</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Language</strong></td>
<td>English (en)</td>
</tr>
<tr>
<td><strong>Title</strong></td>
<td>warning</td>
</tr>
<tr>
<td><strong>Message Body</strong></td>
<td>CMF test</td>
</tr>
<tr>
<td><strong>Policy Link</strong></td>
<td><a href="http://www.cisco.com">www.cisco.com</a></td>
</tr>
<tr>
<td><strong>Company Name</strong></td>
<td>cisco</td>
</tr>
</tbody>
</table>
```

Save  Reset
The Warning Page Configuration page has the following fields and buttons:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable/Disable</td>
<td>To enable the Warning Message page check the Enable/Disable check box. To disable the page, leave the check box unchecked.</td>
</tr>
<tr>
<td>Language</td>
<td>From the pull-down menu, select a language. The default language for the warning message is English.</td>
</tr>
<tr>
<td>Title</td>
<td>Enter a title for the Warning Message page.</td>
</tr>
<tr>
<td>Message Body</td>
<td>Enter the text for the warning message.</td>
</tr>
<tr>
<td>Policy Link</td>
<td>Enter the URL for a web page that contains a policy to execute for the page.</td>
</tr>
<tr>
<td>Company Name</td>
<td>Enter the name of your company.</td>
</tr>
<tr>
<td>Save</td>
<td>Click <strong>Save</strong> to save the Warning Message configuration.</td>
</tr>
</tbody>
</table>

### License Information

To view license information:

**Step 1** From the Multicast Manager menu, select **Administration**.

**Step 2** Select **License Information**.

Product licensing information is displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Licensed To</td>
<td>Who the product is licensed to.</td>
</tr>
<tr>
<td>IP</td>
<td>IP address</td>
</tr>
<tr>
<td>Expire Date</td>
<td>This field displays the date on which the software license is set to expire.</td>
</tr>
<tr>
<td>Features</td>
<td>Features that have been enabled.</td>
</tr>
<tr>
<td>Device Limit</td>
<td>The maximum number of devices.</td>
</tr>
<tr>
<td>Version</td>
<td>Cisco Multicast Manager software version.</td>
</tr>
</tbody>
</table>
**Numerics**

6500/7600 Troubleshooting  8-14

**A**

Access Control  10-3
ACS Server  10-4
Adding a Channel  10-10
Adding an Address  10-6
Adding a Record to the Multiplex Table Database  10-12
Adding a User Configuration  10-1
Adding a Zone  10-9
Address Management  10-5
All Device Information  7-2
angle brackets  xi
Authentication & Audit  10-3

**B**

Baseline Route Polling  5-43
boldface font  x
braces  x
By Device  5-8
By S,G  5-7

**C**

Check Routing Table  8-21
CMM
logging in  2-1
Config L2 Polling  5-10, 5-16
Config S,G Polling  5-7

Config Tree Polling  5-16
Configure Health Check Polling  5-28
Configure Interface Polling  5-12
Configure MVPN Polling  5-42
Configure Route Polling  5-45
Configure RPF Polling  5-24
Configure RP Polling  5-22
Configure Tree Polling  5-16
Configure Unicast Polling  5-47
Configure Video Probe Polling  5-32
Configuring L2 Polling  5-10
Create Baseline  8-20
creating domains  4-1
CRM Polling  5-43

**D**

Device Configuration  9-1
document
audience  ix
conventions  x
objectives  ix
organization  x
documentation
related  xi
Domain Management  4-1
domains
creating  4-1
Domain Trap/Email  5-3

**E**

Event Viewer  5-1
**Index**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export &amp; Import</td>
<td>10-13</td>
</tr>
<tr>
<td><strong>F</strong></td>
<td></td>
</tr>
<tr>
<td>font x</td>
<td></td>
</tr>
<tr>
<td>boldface xi</td>
<td></td>
</tr>
<tr>
<td>boldface screen xi</td>
<td></td>
</tr>
<tr>
<td>italic x</td>
<td></td>
</tr>
<tr>
<td>italic screen xi</td>
<td></td>
</tr>
<tr>
<td>screen xi</td>
<td></td>
</tr>
<tr>
<td>Full Trace 8-14</td>
<td></td>
</tr>
<tr>
<td><strong>G</strong></td>
<td></td>
</tr>
<tr>
<td>Get All Configurations 9-1</td>
<td></td>
</tr>
<tr>
<td>Global Polling Configuration 4-5</td>
<td></td>
</tr>
<tr>
<td><strong>H</strong></td>
<td></td>
</tr>
<tr>
<td>Health Check 5-27, 8-13</td>
<td></td>
</tr>
<tr>
<td>Health Check Failed Report 5-28</td>
<td></td>
</tr>
<tr>
<td><strong>I</strong></td>
<td></td>
</tr>
<tr>
<td>IGMP Cache 8-17</td>
<td></td>
</tr>
<tr>
<td>IGMP Diagnostics 8-12</td>
<td></td>
</tr>
<tr>
<td>Interface Polling 5-11</td>
<td></td>
</tr>
<tr>
<td>interface polling 5-11</td>
<td></td>
</tr>
<tr>
<td>italic font x</td>
<td></td>
</tr>
<tr>
<td><strong>L</strong></td>
<td></td>
</tr>
<tr>
<td>L2 Discovery 6-6</td>
<td></td>
</tr>
<tr>
<td>L2 Host IPs 8-3</td>
<td></td>
</tr>
<tr>
<td>L2 Multicast Information 8-2</td>
<td></td>
</tr>
<tr>
<td>L2 polling 5-9</td>
<td></td>
</tr>
<tr>
<td>License Information 10-17</td>
<td></td>
</tr>
<tr>
<td>Local Host 8-12</td>
<td></td>
</tr>
<tr>
<td>Logging into CMM 2-1</td>
<td></td>
</tr>
<tr>
<td>Logging Management 10-14</td>
<td></td>
</tr>
<tr>
<td><strong>M</strong></td>
<td></td>
</tr>
<tr>
<td>Managing the Ad Zone Database 10-9</td>
<td></td>
</tr>
<tr>
<td>Managing the Channel Map Database 10-10</td>
<td></td>
</tr>
<tr>
<td>Managing the Multiplex Table Database 10-12</td>
<td></td>
</tr>
<tr>
<td>Managing Users &amp; Access 10-1</td>
<td></td>
</tr>
<tr>
<td>MDT Default Report 5-39</td>
<td></td>
</tr>
<tr>
<td>MDT Source Report 5-38</td>
<td></td>
</tr>
<tr>
<td>Miscellaneous Diagnostics 8-9</td>
<td></td>
</tr>
<tr>
<td>Modifying a Channel 10-11</td>
<td></td>
</tr>
<tr>
<td>Modifying an Address 10-6</td>
<td></td>
</tr>
<tr>
<td>Modifying a Record in the Multiplex Table Database 10-13</td>
<td></td>
</tr>
<tr>
<td>Modifying a User File 10-2</td>
<td></td>
</tr>
<tr>
<td>Modifying a Zone 10-10</td>
<td></td>
</tr>
<tr>
<td>Monitoring Application 6-8</td>
<td></td>
</tr>
<tr>
<td>MSDP Status 8-11</td>
<td></td>
</tr>
<tr>
<td>Multicast Discovery 6-1</td>
<td></td>
</tr>
<tr>
<td>Multicast Report 5-46</td>
<td></td>
</tr>
<tr>
<td>MVPN 8-13</td>
<td></td>
</tr>
<tr>
<td>MVPN Configuration 9-3</td>
<td></td>
</tr>
<tr>
<td>MVPN Polling 5-38</td>
<td></td>
</tr>
<tr>
<td><strong>N</strong></td>
<td></td>
</tr>
<tr>
<td>Network Status 8-11</td>
<td></td>
</tr>
<tr>
<td><strong>P</strong></td>
<td></td>
</tr>
<tr>
<td>Packet Monitoring 8-1</td>
<td></td>
</tr>
<tr>
<td>PIM Neighbor 8-18</td>
<td></td>
</tr>
<tr>
<td>polling x</td>
<td></td>
</tr>
<tr>
<td>interface 5-11</td>
<td></td>
</tr>
<tr>
<td>L2 5-9</td>
<td></td>
</tr>
</tbody>
</table>
### R
- RP 5-18
- RPF 5-24
- RPF Polling Report 5-24
- RP Group Threshold Report 5-20
- RP Report 5-19
- RP Status 8-9
- RP Summary 8-10

### S
- S,G 5-5
- S,G Threshold Report 5-5
- Selective Source Monitoring 5-25
- SG Delta Report 5-16
- SG Polling- By Branch 5-17
- SNMP Utilities 8-17, 8-18
- Specific Route Polling 5-45
- square brackets x
- SSG Report 5-21
- SSM Configuration 5-26

### T
- Timeout Configuration 10-4
- Topology 7-1
- Top Talkers 8-12
- Traffic & Polling Reports 5-5
- Trap Viewer 5-2
- Tree Polling & Reports 5-13
- Tree Report 5-15

### U
- Unicast 6-10
- Unicast Report 5-45