## CONTENTS

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
<td>ix</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Objectives</td>
<td>ix</td>
</tr>
<tr>
<td></td>
<td>Audience</td>
<td>ix</td>
</tr>
<tr>
<td></td>
<td>Organization</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>Conventions</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>Related Documentation</td>
<td>xi</td>
</tr>
<tr>
<td></td>
<td>Obtaining Documentation, Obtaining Support, and Security Guidelines</td>
<td>xi</td>
</tr>
</tbody>
</table>

### CHAPTER 1

#### Overview of Cisco Multicast Manager 1-1

- CMM Applications and Architecture 1-1
- Multicast Monitoring and Troubleshooting 1-2
- Support for Cisco Video Solutions 1-2
- Cisco VidMon Support 1-3
- Northbound API 1-5
- Additional Product Features 1-5

### CHAPTER 2

#### Getting Started 2-1

- Logging into Cisco Multicast Manager 2-1
- Navigating the GUI 2-2
- Devices Tab 2-2
- Cisco Multicast Manager Dashboard 2-2
  - Running a Trace from the Dashboard 2-3
  - Displaying a Trap Details List from the Traps Pane 2-4
  - Viewing Performance Graphs from the Dashboard 2-4

### CHAPTER 3

#### Initial System Setup 3-1

- Basic Setup and Configuration Steps 3-1

### CHAPTER 4

#### Polling Configuration & Reports 4-1

- Event Viewer 4-1
- Trap Viewer 4-2
  - Adding Trap OIDs 4-3
  - Domain Trap/E-mail 4-3
Contents

V

User Guide for Cisco Multicast Manager, 3.4

Review Draft - Cisco Confidential

Video Probe 4-36
  Video Probe Report 4-36
  Historical Report 4-37
  Configuring Video Probe Polling 4-37
Vidmon Polling 4-38
  Viewing a Vidmon Report 4-39
  Historical Report 4-39
  Configuring Vidmon Polling 4-40
MVPN Polling 4-43
  MDT Source Report 4-43
  MDT Default Report 4-44
  VRF Interface Count Report 4-45
  VRF Count Report 4-46
  Configuring MVPN Polling 4-47
CRM Polling 4-48
  Baseline Route Polling 4-48
    Unicast Report 4-49
    Multicast Report 4-49
    Historical Report 4-49
    View Baseline 4-50
    Compare Baseline 4-50
    Configuring Route Polling 4-50
  Specific Route Polling 4-51
    Unicast Report 4-51
    Multicast Report 4-52
    Configuring Unicast Polling 4-53
    Configuring Multicast Polling 4-55

CHAPTER 5

Discovery and Trace 5-1
  Discovery 5-1
    Multicast Discovery 5-2
    L2 Device 5-17
    Video Probe 5-18
      Monitoring Application 5-20
    VidMon Device 5-20
    Unicast Device 5-21
  Trace 5-22
    Multicast Trace 5-22
    Show Groups 5-33
Contents

CHAPTER 6  Topology  6-1
  Topology  6-1
  All Device Information  6-2
  Topology Change Reflection Without Re-Discovery  6-3

CHAPTER 7  Diagnostics  7-1
  SG Diagnostics  7-1
    Packet Monitoring  7-1
  L2 Diagnostics  7-2
    L2 Multicast Information  7-2
    L2 Host IP Addresses  7-3
  Video Diagnostics  7-3
    Video Probe Status  7-3
    VidMon Flow Status  7-4
  Miscellaneous Diagnostics  7-7
    RP Status  7-8
    RP Summary  7-8
    MSDP Status  7-8
    Network Status  7-9
    Locate a Host  7-9
  Tools  7-9
    IGMP Diagnostics  7-9
    Top Talkers  7-10
    Health Check  7-10
    MVPN  7-11
    6500/7600 Troubleshooting  7-11
      Full Trace  7-11
      Diagnostics  7-12
      Troubleshooting  7-13
  SNMP Utilities  7-14
    IGMP Cache  7-14
    PIM Neighbors  7-15
  SNMP Walker  7-15
  SNMP PIM Reachability  7-16
  Explicit User Tracking  7-16
  CRM Diagnostics  7-18

Show Specific Group  5-34
Contents

Review Draft - Cisco Confidential

Create Baseline 7-18
Check Routing Table 7-19

CHAPTER 8

Configuration Management 8-1
Device Configuration 8-1
Get All Configurations 8-1
Validate All Configurations 8-1
Configuring Static RPs 8-2
Configuring SSM Devices 8-2
MVPN Configuration 8-3

CHAPTER 9

Administration 9-1
Managing Users and Access 9-1
User Configuration 9-1
Adding a User Configuration 9-1
Modifying a User File 9-2
Access Control 9-3
Authentication and Audit 9-4
ACS Server 9-4
ACS 5.x Integration with CMM 9-5
Authenticating AAA Users through TACACS+ Using Cisco Secure ACS 9-5
Authenticating AAA Users through RADIUS Using Cisco Secure ACS 9-8
Timeout Configuration 9-10

Address Management 9-10
Destination Address Database 9-11
Adding a Destination Address 9-11
Modifying a Destination Address 9-12
Source Description 9-13
Adding a Source Address and Description 9-13
Modifying a Source Address or Description 9-14
Transport Description 9-14
Adding a Transport Description 9-15
Modifying a Transport Description 9-16
Managing the Ad Zone Database 9-16
Adding a Zone 9-16
Modifying a Zone 9-17
Managing the Channel Map Database 9-18
Adding a Channel 9-18
Modifying a Channel 9-19
Managing the Multiplex Table Database  9-20
   Adding a Record to the Multiplex Table Database  9-20
   Modifying a Record in the Multiplex Table Database  9-21
Export & Import  9-22
   Exporting Data  9-22
   Importing Data  9-23
Log Management  9-23
   Logging Management  9-23
Audit Log  9-24
Debug Settings  9-24
Warning Page Configuration  9-25
License Info  9-26

CHAPTER 10
System Configuration  10-1
   Set Up Trace by Management IP Address (Optional)  10-1
Domain Management  10-2
   Creating a Domain  10-3
   Importing a Domain  10-6
Global Polling Configuration  10-6
Preface

This preface describes the objectives, audience, organization, and conventions of the User Guide for Cisco Multicast Manager, 3.4. 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 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 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
Organization

This guide is divided into the following chapters:

- **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 10, “System Configuration”** provides information on managing domains and global polling configurations.
- **Chapter 4, “Polling Configuration & Reports”** describes how to configure devices for polling, viewing of events for polling, and how to view historical data files.
- **Chapter 5, “Discovery and Trace”** provides information on discovering network devices and multicast running traces.
- **Chapter 6, “Topology”** provides information on viewing topology and reports.
- **Chapter 7, “Diagnostics”** provides information on viewing both global and router-specific diagnostics.
- **Chapter 8, “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 9, “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><em>italic</em> font</td>
</tr>
<tr>
<td>Displayed session and system information</td>
<td><em>screen</em> 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 ({</td>
</tr>
<tr>
<td>Information you enter</td>
<td><strong>boldface</strong> <em>screen</em> font</td>
</tr>
<tr>
<td>Variables you enter</td>
<td><em>italic</em> <em>screen</em> font</td>
</tr>
<tr>
<td>Menu items and button names</td>
<td><strong>boldface</strong> font</td>
</tr>
<tr>
<td>Choosing a menu item in paragraphs</td>
<td><strong>Option &gt; Network Preferences</strong></td>
</tr>
<tr>
<td>Choosing 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*
- *Release Notes for Cisco Multicast Manager*
- *Documentation Guide and Supplemental License Agreement for Cisco Multicast Manager*
- *Device Instrumentation Requirements for Cisco Multicast Manager*
- *Cisco Multicast Manager Developer’s Guide and API Reference,*

---

**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) 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

Note

CMM can run on Linux systems. CMM is not supported on Sun Solaris 10 and Windows Servers.

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.

CMM includes support for Cisco VidMon monitoring on Cisco 7600 Series routers and Cisco ASR 9000 devices.

- 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, including multicast trace for Layer 2 and Layer 3 devices by PIM neighbor address or by IP Management Address
- For VidMon devices (Cisco 7600 series devices and Cisco ASR 9000 series devices, unicast trace as well as multicast trace.
- 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. Video probe monitoring includes the ability to monitor Digital Content Managers (DCMs). The embedded address management database shows which channels are affected if there is a problem with a specific 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:


**Cisco 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 Cisco 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 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

Cisco 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 Cisco VidMon

CMM implements Cisco 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.

MLR 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 generates 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.
Chapter 1 | Overview of Cisco Multicast Manager

Review Draft - Cisco Confidential

- 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.

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.

Additional Product Features

CMM 3.4 release provides the following additional features:

- **IPv6 Server Support**—Starting from this release, CMM provides IPv6 server support and can be installed in IPv6-enabled Linux servers only.
- **P2MP Discovery**—In this release, P2MP device discovery performance has been improvised by reducing the time taken to discover all devices in a network. This is achieved by parallelly executing MIB queries from multicast discovery instead of using device CLIs, which takes more time to process.

  **Note**  
  MIB query-based device discovery is supported only for XR devices and hence no device credentials required in Domain Management interface. But for IOS devices, discovery is performed using device CLIs only and device credentials are required in Domain Management interface.

- **Trap-based Tree Report**—Starting from this release, tree polling in CMM is based on trap notifications received from ASR9k devices. Once a trap is received, CMM rediscovers devices in a network, automatically. Tree polling compares the newly generated trace with the baseline trace and when a trace change event is triggered, changes to topology are represented in both graphical and tabular formats.

  CMM receives the following traps from ASR9k devices:
  - `cmplsTeP2mpTunnelDestUp(1.3.6.1.4.1.9.10.142.0.1)
  - `cmplsTeP2mpTunnelDestDown(1.3.6.1.4.1.9.10.142.0.2)
  - `mplsTunnelUp(1.3.6.1.2.1.10.166.3.0.1)`
Additional Product Features

**Review Draft - Cisco Confidential**

- mplsTunnelDown(1.3.6.1.2.1.10.166.3.0.2)
- mplsTunnelRerouted(1.3.6.1.2.1.10.166.3.0.3)
- mplsTunnelReoptimized(1.3.6.1.2.1.10.166.3.0.4)

- **Browser Support**— CMM provides support for Firefox 27 and IE 11.x on Windows 7.
- **ESXI Support**—CMM provides support for Linux Instance of ESXI 5.5.

>Note> Cisco Multicast Manager 3.3 and later releases support Nexus 7K with version 6.1.2 for Discovery, Trace, Polling, and Diagnostic. If Nexus 7k devices are configured with multicontext VDCs, then CMM will discover the default VDC as well as other VDCs as separate devices.
Getting Started

This chapter contains the following sections:

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

Logging into Cisco Multicast Manager

Note

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

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.

The Login window 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 there are multiple methods of navigating the interface.

Menu

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

CMM Main Menu

The CMM Main Menu is the main navigation tool for CMM. To go to the main menu, from the CMM Dashboard, click the **Switch to Main** button.

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 pane at the left of the page lists the devices for the current domain.

**Step 2**
Click a device link.

The Device page for the selected device appears.

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**
Check the check box for the CLI access method you want to use:

- Telnet
- SSH v1
- SSH v2

**Step 4**
Enter the **Username** for the device.

**Step 5**
Enter the **Password**.

**Step 6**
Enter the **Enable Password** for the device.

**Step 7**
Enter an IOS command in the **Show Command** field.

**Step 8**
Click **Show** to display the output.

Cisco Multicast Manager Dashboard

Select the Dashboard view from the Main Menu page.

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

The top of the CMM Dashboard displays your username and indicates your last login time.
Chapter 2      Getting Started

Cisco Multicast Manager Dashboard

Review Draft - Cisco Confidential

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.
- Click the **RP Events** tab to view Rendezvous Point (RP) events, including RP polling events, RP group threshold events, and SG events.
- Click the **Video Events** tab to view video events, such as VidMon MLR High, DF High, video outage flow, 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

To run the trace for SG events on the CMM Dashboard:

| Step 1 | Click **SG Events** on the Event pane. |
| Step 2 | Click the link displayed on the rows. |
| Step 3 | Trace for that event runs, and the result is shown. |

**Note**
If the link is not displayed, you need to run **SG Threshold Report**.

To generate SG Threshold Report:

| Step 1 | From the Multicast Manager menu, choose **System Configuration**. |
| Step 2 | Choose **Domain Management**. |
| Step 3 | Choose "by Domain" from **Add** drop-down list. |
| Step 4 | Fill in the details and click **Save**. |
| Step 5 | Click **Discover**, to discover the device. |
| Step 6 | From the Multicast Manager menu, choose **Polling Configuration & Reports**. |
| Step 7 | From the **Traffic Polling & Reports**, choose **SG**. |
### Review Draft - Cisco Confidential

**Step 8** The SG Threshold Report window opens.

**Step 9** Click **Config SG Polling**.

**Step 10** From the SG Configurations dialog box, click **Add** drop-down list and choose “by SG”.

**Step 11** Select the Source, Group and Routers.

**Step 12** Fill the High Threshold and Low Threshold value. For eg: 10 and 2.

**Step 13** Click **Save** to trigger a link to SG Events pane, on CMM dashboard.

---

**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 performance graphs from the dashboard:

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

**Step 2** The Graphs page appears, as shown in Figure 2-1.

*Figure 2-1 Graphs Page*

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 reports requested. For example, the Graphs page shown in Figure 2-1 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.

**Step 4**
On the Graph Settings dialog, specify the settings for a new graph, as follows:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Graph Type</strong></td>
<td>From the drop-down list in the Graph Type field, choose the type of graph to display:</td>
</tr>
<tr>
<td></td>
<td>• SG—Display a Source, Group statistics graph.</td>
</tr>
<tr>
<td></td>
<td>• Video Probe—Display statistics for a video probe.</td>
</tr>
<tr>
<td></td>
<td>• Vidmon—Display statistics for a VidMon device.</td>
</tr>
<tr>
<td><strong>Units</strong></td>
<td>From the drop-down list in the Units field, choose the units for the graph.</td>
</tr>
<tr>
<td></td>
<td>The units vary depending on the type of graph selected.</td>
</tr>
<tr>
<td></td>
<td>For a SG graph, you can choose:</td>
</tr>
<tr>
<td></td>
<td>• PPS—Packets per second.</td>
</tr>
<tr>
<td></td>
<td>• BPS—Bits per second.</td>
</tr>
<tr>
<td></td>
<td>For a Video Probe graph, you can choose:</td>
</tr>
<tr>
<td></td>
<td>• DF—Delay Factor.</td>
</tr>
<tr>
<td></td>
<td>• MLR—Media Loss Rate.</td>
</tr>
<tr>
<td></td>
<td>For a VidMon device graph, you can choose:</td>
</tr>
<tr>
<td></td>
<td>• DF—Delay Factor.</td>
</tr>
<tr>
<td></td>
<td>• MLR—Media Loss Rate.</td>
</tr>
<tr>
<td></td>
<td>• MRV—Media Rate Variation.</td>
</tr>
<tr>
<td><strong>Domain</strong></td>
<td>From the drop-down list, chose the domain for the device.</td>
</tr>
<tr>
<td><strong>Device</strong></td>
<td>From the drop-down list, chose a device.</td>
</tr>
<tr>
<td><strong>Interface</strong></td>
<td>The Interface field is available only for VidMon devices. From the drop-down list, choose the interface to monitor for the graph.</td>
</tr>
<tr>
<td><strong>Direction</strong></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><strong>Source</strong></td>
<td>From the drop-down list, choose a source address.</td>
</tr>
</tbody>
</table>
Step 5  Click **Submit** to submit the settings for the graph.

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 refers 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>
<tbody>
<tr>
<td>Step 1</td>
<td>Install Cisco Multicast Manager. Install the software.</td>
</tr>
<tr>
<td></td>
<td>See the Installation Guide for Cisco Multicast Manager.</td>
</tr>
<tr>
<td>Step 2</td>
<td>(Optional) Set up Trace Using IP Management Address</td>
</tr>
<tr>
<td></td>
<td>If in your network, PIM access is restricted across particular points, you can implement trace using IP Management Address.</td>
</tr>
<tr>
<td></td>
<td>See Set Up Trace by Management IP Address (Optional), page 10-1.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Create a Domain</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>When you set up a domain, you can configure the global settings for the domain to discover routers, or to discover Layer 2 devices also.</td>
</tr>
<tr>
<td></td>
<td>See Creating a Domain, page 10-3.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Configure Global Polling</td>
</tr>
<tr>
<td></td>
<td>Specify a start and stop time for each type of polling performed by CMM. See Global Polling Configuration, page 10-6.</td>
</tr>
</tbody>
</table>
Chapter 3      Initial System Setup

Basic Setup and Configuration Steps

Step Purpose and Description

Step 5 Run Multicast Discovery Before you can configure monitoring, CMM must discover the devices in the monitored network. You can discover routers, or optionally, routers and switches. See Discovery, page 5-1.

You can run six types of multicast discovery:

- **Core/Enterprise Discovery/Contiguous** — Use Core/Enterprise Discovery/Contiguous to perform contiguous discovery of PIM-enabled devices in your core/enterprise network.
  See Core/Enterprise Discovery/Contiguous, page 5-4.

- **Core/Enterprise Discovery/Core + CE** — Use Core/Enterprise Discovery/Core + CE to discover the multicast devices in your core/enterprise network.
  See Core/Enterprise Discovery/Core + CE, page 5-5.

- **Distributed Network Discovery/CE-PE Mapping** — Use Distributed Network Discovery to discover the customer sites using Customer Edge (CE) devices and associated Provider Edge (PE) devices in a distributed network such as an IP/MPLS network.
  See Distributed Network Discovery/CE-PE Mapping, page 5-6.

- **Distributed Network Discovery/PE Only** — Use Distributed Network Discovery to discover the customer sites using Provider Edge (PE) devices in a distributed network such as an IP/MPLS network.
  See Distributed Network Discovery/PE Only, page 5-7.

- **Distributed Network Discovery/P2MP** — Use Distributed Network Discovery/P2MP to discover the customer sites in a distributed network that uses Point-to-Multipoint (P2MP) Traffic Engineering over a TE tunnel, such as a MPLS/P2MP network.
  See Distributed Network Discovery/P2MP, page 5-8.

- **Single Device Discovery** — After you have run Core Enterprise or Distributed Network discovery, use Single Device Discovery to discover a single device or a device and its adjacent PIM neighbors.
  See Single Device Discovery, page 5-11.
Step 6  Discover Additional Devices and Video Probes (as required)

After you have discovered the multicast devices in your network, as needed, run Discovery to discover additional devices and video probes. As required, choose the following options from the Discovery menu:

- **L2 Device**—Select this option to discover switches (layer 2 devices in your network, if you have not already discovered them during multicast discovery, or if you want to discover additional switches.
  
  See [L2 Device, page 5-17](#).

- **Video Probe**—Select this option to discover video probes associated with specified devices, or to discover digital content managers (DCMs).
  
  See [Video Probe, page 5-18](#).

- **Vidmon Device**—Select this option to update the inventory of VidMon devices after you have run an initial multicast discovery.
  
  See [VidMon Device, page 5-20](#).

- **Unicast Device**—Select this option to add unicast routers to the inventory of discovered devices.
  
  See [Unicast Device, page 5-21](#).

Step 7  Configure Users

To configure users:

- Add users and assign them to the appropriate user class. See [User Configuration, page 9-1](#).

- Set up access privileges for specified user classes. See [Access Control, page 9-3](#).
### Basic Setup and Configuration Steps

#### Step 8: Configure Authentication

**Purpose and Description**
Specify how users are authenticated:
- Specify the type of user authentication used by CMM. For example, local authentication, TACACS+ authentication or RADIUS authentication. See *Authentication and Audit*, page 9-4.
- (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 9-4.

#### Step 9: Configure Multicast Polling

**Configuration & Reports**
Configure the type of monitoring that you will use to monitor the devices in your multicast network. You can specify the following general types of polling:
- **Traffic Polling**—Poll multicast traffic by source and group (SG polling)
- **Tree Polling**—Set up polling for a specific part of the network tree.

In addition, you can configure the following types of polling:
- Health Checks.
  
  *Health Check, page 4-33.*
- Video Probe Polling.
  
  *Video Probe, page 4-36.*
- Vidmon Polling.
  
  *Vidmon Polling, page 4-38.*
- MVPN Polling.
  
  *MVPN Polling, page 4-43.*
Polling Configuration & Reports

This chapter contains the following sections:

- **Event Viewer**, page 4-1
- **Trap Viewer**, page 4-2
- **Domain Trap/E-mail**, page 4-3
- **Traffic & Polling Reports**, page 4-4
- **Tree Polling & Reports**, page 4-17
- **Miscellaneous Polling & Reports**, page 4-23
- **CRM Polling**, page 4-48

**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**  
From the Multicast Manager menu, choose **Polling Configuration & Reports > Event Viewer**.  
The Event Viewer page opens.  
The Event Viewer is set up to show Latest Events (the default setting). The first field shown on the Event Viewer 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, choose **Report Parameters**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Type</td>
<td>Choose an event type from the drop-down list.</td>
</tr>
<tr>
<td>From Date</td>
<td>Enter or choose a start date.</td>
</tr>
<tr>
<td>To Date</td>
<td>Enter or choose an end date.</td>
</tr>
</tbody>
</table>
**Trap Viewer**

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

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

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

The Trap Viewer page appears.

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, choose **Report Parameters**. This will 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>Device</td>
<td>Choose a device from the drop-down list.</td>
</tr>
<tr>
<td>Source</td>
<td>Choose a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Choose a group from the drop-down list.</td>
</tr>
<tr>
<td>Baseline Name</td>
<td>Enter the baseline name.</td>
</tr>
</tbody>
</table>

**Field**

- **From Date**: Enter or choose a start date.
- **To Date**: Enter or choose an end date.
- **Device**: To report events for all devices, choose ALL. To report events for a specific device. Choose a device from the drop-down list.
- **Source**: N/A
- **Group**: N/A
- **Baseline Name**: Enter the baseline name.

**Step 4** Click **Submit**.

The Trap Viewer appears with the specified traps shown.
Adding Trap OIDs

During installation, the system issues the prompt “Do you want to add some other Trap OIDs with the default list (y/n) (default - n)”: Enter y and add the MIB details to the default list.

Note
If CMM is already installed, then do the following:

- Add the OID to snmptrapd.conf file located under <CMMROOT>/mmtsystsys/share/snmp folder.
- Restart the CMM Server. The traps will be listed in trap viewer.
  For example: traphandle 1.3.6.1.4.1.9.10.119.0.* /usr/local/netman/perl/bin/perl
  usr/local/netman/httpd_perl/perl/trap.pl

To add text information to the newly added OID, do the following:

Go to /<CMMROOT>/cmm/WEB-INF folder.
Where, CMMROOT is /usr/local/netman/ for Linux.
Add the OID Name in baseoid.properties file.
Add the OID Description in varbind.properties file and restart the CMM server.

Domain Trap/E-mail

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/E-mail Configuration page, then the values from the global polling configuration are used.

To configure Domain Trap/E-mail Settings:

Step 1
Choose Polling Configuration & Reports.

Step 2
Click Domain Trap/E-mail.

The Domain Trap/ E-mail page appears.

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

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

<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>
</tbody>
</table>
**Traffic & Polling Reports**

**S,G**

S,G polling helps you to monitor the S,G traffic on the routers you specify. To implement S,G polling, you must configure high and low threshold values in PPS/BPS units. CMM will alert operators when thresholds are exceeded or not met.

You can choose 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 choosing 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.
Email notification is sent to users.

Tip
Pressing shift and control simultaneously allows you to choose 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:

1. From the Multicast Manager menu, choose **Polling Configuration & Reports**.
2. Choose **Traffic Polling & Reports**.
3. Choose **S,G**.
4. Choose **Report Parameters**.

#### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Date</td>
<td>Enter or choose a start date.</td>
</tr>
<tr>
<td>To Date</td>
<td>Enter or choose an end date.</td>
</tr>
<tr>
<td>Device</td>
<td>Choose a device from the drop-down list.</td>
</tr>
<tr>
<td>Source</td>
<td>Choose a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Choose 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:

1. From the Multicast Manager menu, choose **Polling Configuration & Reports**.
2. Choose **Traffic Polling & Reports**.
3. Choose **S,G**.
4. Choose **Historical Graph**.
5. In the Units field, choose 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  Choose up to three multicast streams from the table.

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

Individual streams are indicated 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 lists all events pertaining to the stream.

To view a Group Gone report:

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

---

**Config S,G Polling**

**By S,G**

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

**Note** You can also choose By Import to import the SG configuration from a CSV file.

7. On the Configure SG Polling page, specify the following settings:
Chapter 4      Polling Configuration & Reports

Traffic & Polling Reports

**User Guide for Cisco Multicast Manager, 3.4**

Chapter 4      Polling Configuration & Reports

**Traffic & Polling Reports**

You can choose 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, choose **Polling Configuration & Reports**.
**Step 2**  Choose **Traffic Polling & Reports**.
**Step 3**  Choose **S,G**.
**Step 4**  Choose **Config SG Polling**.
**Step 5**  Click the **Add** button.
**Step 6**  Choose **By Device**.

On the **SG Polling By Device** configuration page, set the parameters for polling:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Choose a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Choose 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>Choose a router/routers to configure SG polling.</td>
</tr>
<tr>
<td>Units</td>
<td>Choose 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, CMM generates a report.</td>
</tr>
<tr>
<td>Low Threshold</td>
<td>Enter the low threshold value. If the value exceeds, CMM generates a report.</td>
</tr>
</tbody>
</table>
Traffic & Polling Reports

Chapter 4      Polling Configuration & Reports

Review Draft - Cisco Confidential

Traffic & Polling Reports

By SG Range

To configure SG polling by specifying a range of SG addresses:

Step 1  From the Multicast Manager menu, choose **Polling Configuration & Reports**.
Step 2  Choose **Traffic Polling & Reports**.
Step 3  Choose **S,G**.
Step 4  Choose **Config SG Polling**.
Step 5  Choose **By SG Range** from the **Add** drop-down list.
The By SG Range Add/Modify page appears.
Step 6  Set the following parameters on the SG Range Add/Modify page:

<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>Choose <strong>Refresh</strong> 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>Choose the router name.</td>
</tr>
<tr>
<td>Units</td>
<td>Choose 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>

Source Range

Enter an IP address range for the source. You can specify the range in the third octet or the fourth octet of the IP address, or without a range; for example, 126.0.0-2.10-15, 126.0.10.1.10-15, or 126.0.1.11.

Group Range

Enter an IP address for the group range to monitor. You can specify the range in the third octet or the fourth octet of the IP address, or without a range; for example, 224.0.10-11.1-2, 224.0.1-2, or 224.0.1.40.

Reset

Clears the entries and refreshes the source and group lists.

Select Routers

Choose routers to add to the polling configuration.
Chapter 4  Polling Configuration & Reports

Traffic & Polling Reports

Review Draft - Cisco Confidential

<table>
<thead>
<tr>
<th>Units</th>
<th>Choose either packets per sampling period (PPS) or bits per sampling period (bps).</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Threshold</td>
<td>Enter the high threshold that, if exceeded, generates a report.</td>
</tr>
<tr>
<td>Low Threshold</td>
<td>Enter the low threshold that, if exceeded, generates a report.</td>
</tr>
</tbody>
</table>

**Step 7**

Click the **Save** button to save the configuration.

---

**Note**

CMM while configuring SG polling, using a range of SG addresses, checks if SG is in the device or not. If the SG is not present in the device, then the SG is marked with * to differentiate it from other SGs in the SG configuration page.

---

**By VRF**

To configure SG polling by VRF:

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

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

**Step 3** Choose **S,G**.

**Step 4** Choose **Config SG Polling**.

**Step 5** Choose **By VRF** from the **Add** drop-down list.

The VRF Add/Modify page appears.

**Step 6** Set the following parameters on the VRF Add/Modify page:

<table>
<thead>
<tr>
<th>Select VRF</th>
<th>Choose the VRF from the list of VRFs in the discovered devices.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Device</td>
<td>Choose the device populated from the selected VRF.</td>
</tr>
<tr>
<td>Source</td>
<td>Choose the source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Choose the group from the drop-down list.</td>
</tr>
<tr>
<td>Units</td>
<td>Choose either packets per sampling period (PPS) or bytes per sampling period (bps).</td>
</tr>
<tr>
<td>High Threshold</td>
<td>Enter the high threshold that, if exceeded, generates a report.</td>
</tr>
<tr>
<td>Low Threshold</td>
<td>Enter the low threshold that, if exceeded, generates a report.</td>
</tr>
</tbody>
</table>
By Import

To configure SG polling by importing a file:

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

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

**Step 3**  Choose S,G.

**Step 4**  Choose Config SG Polling.

**Step 5**  Choose Add button.

**Step 6**  Choose By Import.

**Step 7**  Click the Browse button to upload the file.

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

**Step 9**  Click Upload.

**Import Format:**

SG,<Source>,<Group>,<Router>,<High Threshold value>,<Low Threshold value>,<RO Community String>,<BPS/PPS>,<sourceExist/notExist>,<groupExist/notExist>

Where bps=1; pps=0; sourceExist, groupExist=1; notExist=0.

**Example:**

SG,126.0.1.12,239.232.0.0,126.1.3.14,6,3,public,0,0,1

**Config Time-Based SG Polling**

To configure Time-Based SG Polling:

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

**Step 2**  On the SG Time based Configurations page, click the Add button and from the drop-down list, choose 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>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Enter or choose the IP address of the source to monitor.</td>
</tr>
<tr>
<td>Group</td>
<td>Enter or choose the IP address of the group to monitor.</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>Choose routers to add to the polling configuration.</td>
</tr>
</tbody>
</table>
Step 4
Click the Save button.

Note
The threshold polling interval should be set in the Global Polling Configuration Page.

By Import
To configure Time-based SG polling by importing a file:

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

Step 2
Choose Traffic Polling & Reports.

Step 3
Choose SG.

Step 4
Choose Config Timebased SG Polling.

Step 5
Click the Add button.

Step 6
Choose By Import.

Step 7
Click the Browse button to upload the file.

Step 8
Choose Merge to unify an existing configuration with the new configuration or choose Replace to overwrite the existing configuration.

Step 9
Click Upload.

Import Format:

SGTIME:<Source>,<Group>,<Router>,<Start Hr>,<Start Min>,<Stop Hr>,<Stop Min>,<Day>,<High Threshold value>,<Low Threshold value>,<BPS/PPS>

Where bps=1; pps=0;
Day: Sunday–0; Monday–1; Tuesday–2; Wednesday–3; Thursday–4; Friday–5; Saturday–6;

Example:

SGTIME:126.0.1.13,224.0.1.39,172.20.111.198,21,0,23,0,0,2,1,0
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.

L2 polling monitors multicast traffic on Layer 2 switches with regard to port and direction. You can also configure up to 50 different time-of-day thresholds for each port. CMM generates events for high and low threshold violations.

To view an L2 PPS Threshold Report:

Step 1 From the Multicast Manager menu, choose Polling Configuration & Reports.
Step 2 Choose Traffic Polling & Reports.
Step 3 Choose L2.
Step 4 Choose Report Parameters.
Step 5 On the L2 Polling Report Parameters page, set the parameters for the report:
Step 6 On the Configure L2 Polling page, specify the following settings:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Date</td>
<td>Enter or choose a start date.</td>
</tr>
<tr>
<td>To Date</td>
<td>Enter or choose an end date.</td>
</tr>
<tr>
<td>Device</td>
<td>Choose a device from the drop-down list.</td>
</tr>
<tr>
<td>Source</td>
<td>Choose a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Choose 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, choose Polling Configuration & Reports.
Step 2 Choose Traffic Polling & Reports.
Step 3 Choose L2.
Step 4 Choose 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 Choose one or more multicast streams from the table.
Step 8  Click the **Show Report** button to charts a graph.
Individual streams are indicated with a unique color.

---

**Configuring L2 Polling**

To configure Layer 2 switch polling:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>From the Multicast Manager menu, choose <strong>Polling Configuration &amp; Reports</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Choose <strong>Traffic Polling &amp; Reports</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Choose <strong>L2</strong>.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Choose <strong>Config L2 Polling</strong>.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click the <strong>Add</strong> button.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Choose <strong>By L2</strong>.</td>
</tr>
</tbody>
</table>

**Note**
You can also choose **By Import** to import the L2 configuration from a CSV file.

| Step 7 | On the L2 Polling Configuration page, set the parameters for the report: |

<table>
<thead>
<tr>
<th><strong>Fields and Buttons</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Switch to Monitor</td>
<td>Choose the name or IP address of the switch you want to monitor.</td>
</tr>
<tr>
<td>Select Port to Monitor</td>
<td>Choose the port to monitor. Ports appear in the following format: ifIndex:module/port.</td>
</tr>
<tr>
<td>Direction</td>
<td>Choose 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>

**By Import**

To configure L2 polling by importing a file:

| Step 1 | From the Multicast Manager menu, choose **Polling Configuration & Reports**. |
| Step 2 | Choose **Traffic Polling & Reports**. |
| Step 3 | Choose **L2**. |
| Step 4 | Choose **Config L2 Polling**. |
| Step 5 | Click the **Add** button. |
Step 6  Choose By Import.

Step 7  Click the Browse button to upload the file.

Step 8  Choose Merge to unify an existing configuration with the new configuration or choose Replace to overwrite the existing configuration.

Step 9  Click Upload.

Import Format:

<L2>,<DeviceIP>,<IfIndex>,<High Threshold>,<Low Threshold>,<RO Community String>

Example:

L2,126.2.129.23,1.3.6.1.2.1.31.1.1.2.130,4555,2,pblic
Adding Time-Based Threshold Polling

After you have set up an L2 polling configuration for a switch, you can add time-based threshold polling to the configuration.

To add time-based threshold polling:

Step 1  From the **Polling and Reports Configuration** menu, choose **L2**.
Step 2  Click **Config L2 Polling**.
Step 3  Add or edit a Layer 3 polling configuration.
Step 4  On the L2 Configurations page, click the **Configure** link in the Time-Based Threshold column. The Time-based Thresholds page appears.
Step 5  Enter time-based thresholds:
   a. Enter a high and a low threshold value.
   b. For each high and low value, use the drop-down lists to specify a start and end time for the threshold polling.
   c. Click the **Set Threshold** button.

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, choose **Polling Configuration & Reports**.
Step 2  Choose **Traffic Polling & Reports**.
Step 3  Choose **Interface**.
The Multicast Bandwidth Report page appears.

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

Step 4  Click **Report Parameters**.
Step 5  Click the calendar link (...) for the From Date and choose a From Date.
Step 6  Click the calendar link (...) for the To Date and choose a To Date.
Step 7  From the drop-down list in the Device field, choose 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, choose Polling Configuration & Reports.

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

**Step 3**
Choose Interface.

**Step 4**
Choose 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**
Choose one or more multicast streams from the table.

**Step 8**
Click the Show Report button to charts a graph.

Individual streams are indicated with a unique color.

**Configuring Interface Polling**

**By Interface**

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

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

**Step 3**
Choose Interface.

**Step 4**
Choose Config Interface Polling.

**Step 5**
Click the Add button.

**Step 6**
Choose By Interface.

**Note**
You can also choose By Import to import the Interface configuration from a CSV file.

**Step 7**
Choose the device to monitor.

**Step 8**
Choose 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.
Chapter 4  Polling Configuration & Reports

Tree Polling & Reports

**By Import**

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

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

**Step 3**  Choose **Interface**.

**Step 4**  Choose **Config Interface Polling**.

**Step 5**  Click **Add**.

**Step 6**  Choose **By Import**.

**Step 7**  Click the **Browse** button to upload the file.

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

**Step 9**  Click **Upload**.

**Import Format:**

```
MPERCENT:<routerIp>,<ifindex>,<intDesc>,<direction>,<bandwidth * 100000>,<hThr>,<lThr>
```

Where direction is Inbound=0;Outbound=1.

**Example:**

```
MPERCENT:172.20.111.198,1,Serial1/0,0,154400000000,4,2
```

**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.

During tree polling, the most recent tree created by the polling daemon is compared with the baseline tree created in the polling cycle. If the tree changes or reverts to its former state, CMM notifies the user.

If you configure tree polling with the Compare Baseline option activated, then dynamic tree baseline functionality is used. With dynamic tree baseline functionality, if the multicast tree changes, then the changed tree is then used as the baseline for further tree polling. Starting with the next polling cycle, the polling daemon compares the most recent tree with the updated baseline (the last changed tree).

To enable dynamic tree polling, check the **Compare Baseline** check box on the Tree Polling Configuration page.

Depending on whether you configure dynamic baseline functionality, CMM will enable:

- **Normal Tree**—The tree changes and reverts, because it is always compared with the configured baseline.

- **Latest Tree Baseline**—If latest tree baseline polling is configured, the configured baseline is updated when the tree is changed. Therefore, only tree change notifications are enabled.

This section describes:
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:

**Step 1**  Complete these steps to create a trace baseline:

a.  From the Main Menu, choose **Discovery & Trace**.

b.  Choose **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 4-18, for instructions on how to choose the trace baseline file and configure tree polling.

Configuring Tree Polling

To configure tree polling:

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

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

**Step 3**  Choose **Tree**.

**Step 4**  Choose **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**  Choose 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, choose 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.

---

**Editing a Tree Report Configuration**

To edit a Tree Polling configuration:

---

Step 1  On the Tree Configurations page, check the check box next to the configuration to edit, and then click the **Edit** button.

The Tree Polling Configuration page appears.

Step 2  Choose a Saved Tree from the list in the Select Trace field.

Step 3  Change the Compare Baseline setting as required.

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

Viewing a Tree Report

To view tree reports:

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

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

**Step 3** Choose **Tree**.

**Step 4** Choose **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 choose 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 choose a date from a calendar.</td>
</tr>
<tr>
<td>Device</td>
<td>Choose a device from the drop-down list.</td>
</tr>
<tr>
<td>Source</td>
<td>Choose a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Choose 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, choose **Polling Configuration & Reports**.

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

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

**Step 4** Choose **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** Choose one or more items from the table.

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

Viewing an S,G Delta Report

To view the S,G Delta Report:

Step 1 From the Multicast Manager menu, choose Polling Configuration & Reports.
Step 2 Choose Tree Polling & Reports.
Step 3 Choose Tree.
Step 4 Click the Configure link next to the saved tree that you want to use for S,G delta reporting.
   A page appears for configuring the S,G delta report parameters. It allows you to specify the routers used
   for the report.
Step 5 Choose the routers that you want to monitor for an S,G delta.
Step 6 In the Specify Max Delta Between PPS Samples field, enter the maximum change between PPS
   samples.
   If the PPS on any router deviates from the others with respect to the Max Delta value, an SNMP trap is
   generated.
Step 7 Click the Save button.

Comparing Tree Baselines

Step 1 From the Multicast Manager menu, choose Polling Configuration & Reports.
Step 2 Choose Tree Polling & Reports.
Step 3 Choose Tree.
Step 4 Choose Compare Baseline.
Step 5 From the drop-down list, choose a saved baseline.
Step 6 If you want to compare any of the saved Previous Baseline, select the baseline.
Step 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 4-1** shows a sample Trace Data page.

**Figure 4-1  Trace Data Page for a Tree Changed Event**

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**

SG polling by branch helps you to monitor a specific tree path by specifying a particular SG flow trace branch to poll.

To configure branch polling for a particular SG:

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

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

**Step 3** Choose **SG by Branch**.

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

**Step 5** On the **SG by Branch** Polling Configuration page, specify the following information:
**Chapter 4  Polling Configuration & Reports**

**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.

During RP polling, the CMM poller queries the SG information (list of SGs) from the given RP. The queried information is stored in the CMM database. This data from the database is compared with the details obtained from the subsequent polling interval.

### Step 6

Click the **Save** button.

A trace is generated and appears on the **SG by Branch** Polling Configuration page.

### Step 7

To view the trace table for a trace, click on a baseline link.

---

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Enter the source. You may either enter the source address or choose it from the drop-down menu.</td>
</tr>
<tr>
<td>Group</td>
<td>Enter the group. You may either enter the group address or choose it from the drop-down menu.</td>
</tr>
<tr>
<td>Service Type</td>
<td>Choose the service type from the drop-down list.</td>
</tr>
<tr>
<td>FHR</td>
<td>Choose the start destination for the first hop router.</td>
</tr>
<tr>
<td>LHR</td>
<td>Choose the end destination for the last hop router.</td>
</tr>
<tr>
<td>Select Router</td>
<td>Choose a single router or choose multiple routers by pressing the <strong>Shift</strong> key and clicking on the desired routers.</td>
</tr>
<tr>
<td>Units</td>
<td>Choose 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>
**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, choose **Polling Configuration & Reports**.

**Step 2**

Choose **Miscellaneous Polling & Reports**.

**Step 3**

Choose **RP**.

The RP Report page opens.

**Step 4**

Choose **Report Parameters**.

**Step 5**

On the Report Parameters page, specify the following settings:

<table>
<thead>
<tr>
<th><strong>Fields and Buttons</strong></th>
<th><strong>Description</strong></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 choose 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 choose a date from a calendar.</td>
</tr>
<tr>
<td>Device</td>
<td>Choose a device from the drop-down list.</td>
</tr>
<tr>
<td>Source</td>
<td>Choose a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Choose 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, choose **Polling Configuration & Reports**.

**Step 2**

Choose **Miscellaneous Polling & Reports**.

**Step 3**

Choose **RP**.

**Step 4**

Choose **RP Group Threshold Report**.

**Step 5**

Choose **Report Parameters**.
Step 6
On the RP Group Threshold Report page specify the following parameters:

<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 choose 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 choose a date from a calendar.</td>
</tr>
<tr>
<td>Device</td>
<td>Choose a device from the drop-down list.</td>
</tr>
<tr>
<td>Source</td>
<td>Choose a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Choose 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, choose Polling Configuration & Reports.
Step 2 Choose Miscellaneous Polling & Reports.
Step 3 Choose RP.
Step 4 Choose SSG Report.
Step 5 Choose Report Parameters.
**Step 6**  On the SSG Report Parameters page, specify the following settings:

<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 choose 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 choose a date from a calendar.</td>
</tr>
<tr>
<td>Device</td>
<td>Choose a device from the drop-down list.</td>
</tr>
<tr>
<td>Source</td>
<td>Choose a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Choose 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:

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

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

**Step 3**  Choose **RP**.

**Step 4**  Choose **Config RP Polling**.

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

**Step 6**  Choose **By RP**.

**Note**  You can also choose **By Import** to import the RP configuration from a CSV file.
**Step 7**

On the Configure RP Polling page, specify the following settings:

<table>
<thead>
<tr>
<th>Fields and Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select RP</td>
<td>Choose 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 <strong>Save</strong> to retain the values set in the previous fields.</td>
</tr>
<tr>
<td>Enable RP Group</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 <strong>Save</strong> to retain the values set in the previous fields.</td>
</tr>
</tbody>
</table>

**By Import**

To configure RP polling by importing a file:

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

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

**Step 3**
Choose **RP**.

**Step 4**
Choose **Config RP Polling**.

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

**Step 6**
Choose **By Import**.

**Step 7**
Click the **Browse** button to upload the file.

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

**Step 9**
Click **Upload**.

**Import Format:**

- **RP**:<RpIp>,<Ro Community String>
- **RPGLIMIT**:<RpIp>,<RpLimit>
- **RPACCEPT**:<RpIp>,<Source>,<SourceMask>,<Group>,<GroupMask>

**Example:**

- RP:172.20.111.198,public
- RPGLIMIT:172.20.111.198,222
- RPACCEPT:172.20.111.198,0.0.0.0,255.255.255.255,239.1.1.2,0.0.0.0
RP Global Configuration

To configure RP Global Configuration:

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

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

**Step 3**  Choose **RP**.

**Step 4**  Choose **RP Global Configuration**

The RP Global Configuration page appears.

**Step 5**  On the RP Global Configuration page, specify the following settings:

<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 <strong>Add</strong> button to add it to the list of S, G to monitor.</td>
</tr>
<tr>
<td>Save</td>
<td>Click the <strong>Save</strong> 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. During RPF polling, the poller performs an RPF check and reports RPF check failures.

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:

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

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

**Step 3**  Choose **RPF**.
Step 4 On RPF Polling Report Parameters page, specify the following settings:

<table>
<thead>
<tr>
<th><strong>Fields and Buttons</strong></th>
<th><strong>Description</strong></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 choose 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 choose a date from a calendar.</td>
</tr>
<tr>
<td>Device</td>
<td>Choose a device from the drop-down list.</td>
</tr>
<tr>
<td>Source</td>
<td>Choose a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Choose 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:

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

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

**Step 3** Choose **RPF**.

**Step 4** Choose **Config RPF Polling**.

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

**Step 6** Choose **By RPF**.

**Note** You can also choose **By Import** to import the RPF configuration from a CSV file.
Chapter 4  Polling Configuration & Reports

Miscellaneous Polling & Reports

Step 7  On the RPF Polling Configuration page, specify the following settings:

<table>
<thead>
<tr>
<th>Fields and Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Choose 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>Choose 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 the 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 triggers a report.</td>
</tr>
<tr>
<td>Save</td>
<td>Applies the configuration and saves the changes.</td>
</tr>
</tbody>
</table>

By Import

To configure RPF polling by importing a file:

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

Import Format:

RPFMON:<source>,<group>,<routerIp>,<delta>

Example:

RPFMON:126.0.1.13,224.0.1.39,126.1.3.14,8
Selective Source Monitoring

A source and group can be set up to monitor for a particular time and day. During selective source monitoring, the CMM poller monitors specified SG and generates events accordingly.

**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:

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

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

**Step 3** Choose **Selective Source Monitoring**.

**Step 4** On the Selective Source Monitoring Report page, specify the following settings:

<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 choose 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 choose a date from a calendar.</td>
</tr>
<tr>
<td>Device</td>
<td>Choose a device from the drop-down list.</td>
</tr>
<tr>
<td>Source</td>
<td>Choose a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Choose 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 Selective Source Monitoring for monitoring.</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:

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

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

**Step 3** Choose **Selective Source Monitoring**.

**Step 4** Choose **Config Selective Source Monitoring Polling**.

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

**Step 6** Choose **By Selective Source Monitoring**.

**Note** You can also choose **By Import** to import the SSM configuration from a CSV file.

**Step 7** On the Selective Source Monitoring Polling Configuration page, specify the following settings:

<table>
<thead>
<tr>
<th>Fields and Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Choose a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Choose a group from the drop-down list.</td>
</tr>
<tr>
<td>Reset SG Lists</td>
<td>Clears any entries and refreshes the source and group lists.</td>
</tr>
<tr>
<td>Configure threshold at ingress router</td>
<td>By default, CMM does not monitor the packet flow at ingress routers associated with the source device. If you want to monitor the packet flow at the ingress routers associated with the source, check the Configure threshold at ingress router check box and enter threshold values in the High Threshold and Low Threshold fields.</td>
</tr>
<tr>
<td>Units</td>
<td>Choose either packets per sampling period (pps) or bits per sampling period (bps).</td>
</tr>
<tr>
<td>High Threshold</td>
<td>Enter the high threshold that, if exceeded, generates a report.</td>
</tr>
<tr>
<td>Low Threshold</td>
<td>Enter the low threshold that, if exceeded, generates a report.</td>
</tr>
<tr>
<td>Run Time Intervals</td>
<td>Enter a range of time to designate when to monitor the branch. Alerts are only based on activity during a designated time frame. Enter the time based on the time zone for the location of the server.</td>
</tr>
<tr>
<td>Reload Cache</td>
<td>If you are using S,G caching, the cache contents appear. Click <strong>Reload Cache</strong> to refresh the table of sources and groups.</td>
</tr>
<tr>
<td>Save</td>
<td>Adds the selected Selective Source Monitoring polling configuration for monitoring.</td>
</tr>
</tbody>
</table>
By Import

To configure Selective Source Monitoring polling by importing a file:

---

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

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

**Step 3** Choose **Selective Source Monitoring**.

**Step 4** Choose **Config Selective Source Monitoring Polling**.

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

**Step 6** Choose **By Import**.

**Step 7** Click the **Browse** button to upload the file.

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

**Step 9** Click **Upload**.

---

**Import Format:**

SSMON:<source>,<group>,<sHr>,<sMin>,<her>,<eMin>,<days>,<hThr>,<lThr>,<unit>

Where days: Everyday–8; M-F–7; Sunday–0; Monday–1; Tuesday–2; Wednesday–3; Thursday–4; Friday–5; Saturday–6

Where unit: bps=1; pps=0.

**Example:**

SSMON:126.0.1.12,224.0.1.39,2,20,6,10,0,6,3,0

---

**Health Check**

Health check polling combines RP, SG, and tree polling. 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.

When you configure a health check, you can specify e-mail addresses to which to send notification alerts.

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, choose Polling Configuration & Reports.

Step 2
Choose Miscellaneous Polling & Reports.

Step 3
Choose Health Check.

Step 4
Choose Report Parameters.

Step 5
On the Health Check Failed Report Parameters page, specify the following settings:

<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 choose 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 choose a date from a calendar.</td>
</tr>
<tr>
<td>Device</td>
<td>Choose a device from the drop-down list.</td>
</tr>
<tr>
<td>Source</td>
<td>Choose a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Choose 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, choose Polling Configuration & Reports.

Step 2
Choose Miscellaneous Polling & Reports.

Step 3
Choose Health Check.

Step 4
Choose Config Health Check Polling.

Step 5
Click the Add button.

The Health Check Name Polling Configuration page appears.

Step 6
On the The Health Check Name Polling Configuration page, specify the following settings:

<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>`

### Step 7
On the RPs Being Checked for `<health check name>` table, specify:

<table>
<thead>
<tr>
<th>Fields and Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Addresses</td>
<td>Enter an e-mail address to which to send a notification, and click <strong>Add</strong>. To remove an e-mail address, choose it from the list and click <strong>Remove</strong>.</td>
</tr>
<tr>
<td>Save</td>
<td>Click the <strong>Save</strong> button to save the Health Check configuration for monitoring.</td>
</tr>
</tbody>
</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>Choose 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>

### Step 8
On the Current Source/Group Polling Configuration for `<health check name>` table, specify:

<table>
<thead>
<tr>
<th>Fields and Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Choose a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Choose 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>Choose one or more routers from the list. You can also click the <strong>Select All</strong> button to choose all routers.</td>
</tr>
<tr>
<td>Save</td>
<td>Adds the Health Check configuration for monitoring.</td>
</tr>
</tbody>
</table>

### Step 9
On the Forwarding Trees for `<health check name>`, specify:

<table>
<thead>
<tr>
<th>Fields and Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Saved Trees</td>
<td>Choose 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 10
To add an item to the health check configuration:

1. 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 11**
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 12**
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.

With video probe polling, devices are manually associated with video probes and CMM generates reports by polling and monitoring the data.

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, choose **Polling Configuration & Reports**.

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

**Step 3**
Choose **Video Probe**.

**Step 4**
Choose **Report Parameters**.

**Step 5**
On the Video Probe Report Parameters page, specify the following settings:

<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 choose 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 choose a date from a calendar.</td>
</tr>
<tr>
<td>Device</td>
<td>Choose a device from the drop-down list.</td>
</tr>
<tr>
<td>Source</td>
<td>Choose a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Choose 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, choose **Polling Configuration & Reports**.

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

**Step 3** Choose **Video Probe**.

**Step 4** Choose **Historical Report**. The Historical Graphs page for video probe report opens.

**Step 5** From the drop-down list in the **Units** field, choose 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, choose the From Date.

**Step 7** Click the calendar item (…) for **To Date** and from the calendar that appears, choose 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 4-2**.

![Historical Report Showing DF for Two Video Probes](image)

**Configuring Video Probe Polling**

To configure video probe polling:

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

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

**Step 3** Choose **Video Probe**.

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

**Step 5** Click the **Add** button.
From the drop-down list in the Add field, choose **By Video Probe**.

---

**Note**

You can also choose **By Import** to import the video probe polling configuration from a CSV file.

On the Configure Video Probe Polling page, specify the following settings:

### Fields and Buttons

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

---

**By Import**

To configure Video Probe polling by importing a file:

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

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

**Step 3**  
Choose **Video Probe**.

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

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

**Step 6**  
Choose **By Import**.

**Step 7**  
Click the **Browse** button to upload the file.

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

**Step 9**  
Click **Upload**.

---

**Import Format:**

VOSPROBE:<ProbeIp>,<Df>,<Loss>

**Example:**

VOSPROBE:172.20.111.213,500,1a

---

**Vidmon Polling**

With Vidmon polling, CMM polls Vidmon capable devices and generates reports if there is any violation of a configured value.
**Review Draft - Cisco Confidential**

**Viewing a Vidmon Report**

To view a Vidmon report:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>From the Multicast Manager menu, choose <strong>Polling Configuration &amp; Reports</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Choose <strong>Miscellaneous Polling &amp; Reports</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Choose <strong>Vidmon</strong>. The Vidmon Reports page opens.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Choose <strong>Report Parameters</strong>.</td>
</tr>
</tbody>
</table>

On Vidmon Report Parameters page, specify the following settings:

<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 choose 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 choose a date from a calendar.</td>
</tr>
<tr>
<td>Device</td>
<td>Choose a device from the drop-down list.</td>
</tr>
<tr>
<td>Source</td>
<td>Choose a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Choose 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:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>From the Multicast Manager menu, choose <strong>Polling Configuration &amp; Reports</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Choose <strong>Miscellaneous Polling &amp; Reports</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Choose <strong>Vidmon</strong>. The Historical Graphs page for video probe reports appears.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Choose <strong>Historical Report</strong>.</td>
</tr>
<tr>
<td>Step 5</td>
<td>From the drop-down list in the <strong>Units</strong> field, choose the units for the report:</td>
</tr>
</tbody>
</table>
Chapter 4      Polling Configuration & Reports

Miscellaneous Polling & Reports

To configure Vidmon Polling:

Step 1  From the Multicast Manager menu, choose Polling Configuration & Reports.
Step 2  Choose Miscellaneous Polling & Reports.
Step 3  Choose Vidmon.

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

Step 4  Choose Config Vidmon Polling.

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, choose By Vidmon.

  Note  You can also choose By Import to import the Vidmon configuration from a CSV file.

- 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, choose either Delete or Export.

  If you choose 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 choose Add, the Vidmon Polling Configuration page appears.

  The Vidmon Polling Configuration page lists the Vidmon devices that have been discovered in the domain.

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

  As you choose devices, a row of configuration options for the device appears.

DF  Display delay factor data.
MLR  Display Media Loss Rate data.
MRV  Display Media Rate Variation data.

User Guide for Cisco Multicast Manager, 3.4
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 choose configuration fields, the field becomes active.

Step 9
On the Vidmon Polling Configuration page, specify the following parameters:

<table>
<thead>
<tr>
<th>Configuration Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DF</strong></td>
<td>Enter a delay factor (DF) in milliseconds. When the delay factor exceeds, CMM generates a delay factor event.</td>
</tr>
<tr>
<td><strong>MLR</strong></td>
<td>For Cisco 76xx devices, enter a Media Loss Rate (MLR) threshold value (number of packets). When the MLR threshold exceeds, CMM generates an alert. <strong>Note</strong> MLR monitoring is not available for Viking devices (Cisco ASR 9000 devices).</td>
</tr>
<tr>
<td><strong>MRV max (milli %)</strong></td>
<td>Enter a milli-percentage value to specify a MRV maximum threshold. You can show values to 3 decimal places. For example, if you want to generate an event when the MRV value goes above 0.100, then enter 100. When the specified threshold exceeds, CMM generates a VIDMON MRV HIGH alert.</td>
</tr>
<tr>
<td><strong>MRV min (milli %)</strong></td>
<td>Enter a milli-percentage value to specify a MRV minimum threshold. You can show values to 3 decimal places. For example, if you want to generate an event when the MRV value drops below -0.100, then enter 100. When the MRV for the device is less than the specified threshold, CMM generates a VIDMON MRV LOW alert.</td>
</tr>
</tbody>
</table>

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 4-3.
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 the Merge radio button.
   - To replace the existing configuration, click the Replace radio button.

Step 4  Click the Upload button.

Import Format:

VIDMON :<VidmonIp>,<VidmonType>,<DF>,<MRV_max>,<MRV_min>,<MLR>
VIDMONOR :<DeviceIp>,<Source>,<Source Mask>,<Group>,<Group Mask>,<device Type>,<DF>,<MRV max>,<MRV min>,<MLR>

Example:

VIDMON:126.1.40.30,1,50,40,20,4
VIDMONOR:126.1.40.30,0.0.0.0,255.255.255.255,172.20.111.12,0.0.0.0,1,50,40,20,4

Editing an Existing Vidmon Polling Configuration

To edit an existing Vidmon polling configuration:

Step 1  On the Vidmon Configuration 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.

Vidmon Polling, page 4-38 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.

**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 Vidmon Polling, page 4-38.

**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 a Multicast Virtual Private Network (MVPN). MVPN properties such as MDT default, VRF count, and VRF interface count are monitored on PE devices.

**MDT Source Report**

To view MDT Source polling:

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

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

**Step 3**
Choose MVPN Polling.

**Step 4**
Choose Report Parameters.
Step 5  On the MDT Source Report Parameters page, specify the following settings:

<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 choose 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 choose a date from a calendar.</td>
</tr>
<tr>
<td>Device</td>
<td>Choose a device from the drop-down list.</td>
</tr>
<tr>
<td>Source</td>
<td>Choose a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Choose 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, choose **Polling Configuration & Reports**.
- **Step 2** Choose **Miscellaneous Polling & Reports**.
- **Step 3** Choose **MVPN Polling**.
- **Step 4** Choose **MDT Default Report**.
- **Step 5** Choose **Report Parameters**.
### Step 6
On the MDT Default Report page, specify the following settings:

<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 choose 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 choose a date from a calendar.</td>
</tr>
<tr>
<td>Device</td>
<td>Choose a device from the drop-down list.</td>
</tr>
<tr>
<td>Source</td>
<td>Choose a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Choose 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, choose **Polling Configuration & Reports**.

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

**Step 3** Choose **MVPN Polling**.

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

**Step 5** Choose **Report Parameters**.
Step 6  On the VRF Interface Count Report page, specify the following settings:

<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 choose 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 choose a date from a calendar.</td>
</tr>
<tr>
<td>Device</td>
<td>Choose a device from the drop-down list.</td>
</tr>
<tr>
<td>Source</td>
<td>Choose a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Choose 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, choose Polling Configuration & Reports.
Step 2  Choose Miscellaneous Polling & Reports.
Step 3  Choose MVPN Polling.
Step 4  Choose VRF Count Report.
Step 5  Choose Report Parameters.
**Chapter 4 Polling Configuration & Reports**

**Miscellaneous Polling & Reports**

---

**Step 6**

On the VRF Count Report Parameters page, specify the following settings:

<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 choose 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 choose a date from a calendar.</td>
</tr>
<tr>
<td>Device</td>
<td>Choose a device from the drop-down list.</td>
</tr>
<tr>
<td>Source</td>
<td>Choose a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Choose 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:

**Step 1**

From the Multicast Manager menu, choose Polling Configuration & Reports.

**Step 2**

Choose Miscellaneous Polling & Reports.

**Step 3**

Choose MVPN Polling.

**Step 4**

Choose Config MVPN Polling.

**Step 5**

Click the Add button.

**Step 6**

Choose By MVPN.

**Note**

You can also choose By Import to import the MVPN configuration from a CSV file.

**Step 7**

On the Configure MVPN Polling page, specify the following settings:

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

To configure MVPN polling by importing a file:

Step 1 From the Multicast Manager menu, choose Polling Configuration & Reports.
Step 2 Choose Miscellaneous Polling & Reports.
Step 3 Choose MVPN.
Step 4 Choose Config MVPN Polling.
Step 5 Choose By Import from the Add drop-down list.
Step 6 Click the Browse button to upload the file.
Step 7 Choose Merge to unify an existing configuration with the new configuration or choose Replace to overwrite the existing configuration.
Step 8 Click Upload.

Import Format:

MVPNPE:<PEIP>

Example:

MVPNPE:172.20.111.198

CRM Polling

Baseline Route Polling

To set up baseline route polling, you must provide a routing table baseline that has been previously generated in the Diagnostics interface. Baseline route polling compares the current routing table with the configured baseline, and if the configuration changes, users are notified.

Note You must first create a baseline by choosing Diagnostics > CRM Diagnostics > Create Baseline as described in Create Baseline, page 7-18.

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, choose **Polling Configuration & Reports**.
Step 2 Choose **CRM Polling**.
Step 3 Choose **Baseline Route Polling**.
Step 4 Choose **Unicast Report**.
Step 5 Click **View Report**.
Step 6 In the Select Route field, choose a date from the drop-down menu.
Step 7 Choose an object from the Filter MIB Objects field.
Step 8 Click **View**.

Multicast Report

Step 1 From the Multicast Manager menu, choose **Polling Configuration & Reports**.
Step 2 Choose **CRM Polling**.
Step 3 Choose **Baseline Route Polling**.
Step 4 Choose **Multicast Report**.
Step 5 In the Select Route field, choose a date from the drop-down menu.
Step 6 Choose an object from the Filter MIB Objects field.
Step 7 Click **View**.

Historical Report

Step 1 From the Multicast Manager menu, choose **Polling Configuration & Reports**.
Step 2 Choose **CRM Polling**.
Step 3 Choose **Baseline Route Polling**.
Step 4 Choose **Historical Report**.
Step 5 To set the Report Type, choose 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 Choose one or more stream from the table.
Step 10 Click the **Show Report** button to charts a graph.

Individual streams are color coded with a unique color.
View Baseline

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

Compare Baseline

Step 1  From the Multicast Manager menu, choose Polling Configuration & Reports.
Step 2  Choose CRM Polling.
Step 3  Choose Baseline Route Polling.
Step 4  Choose Compare Baseline.
Step 5  To specify the Report Type, click either the Unicast radio button or the Multicast radio button.
Step 6  Choose a router from the drop-down list.
Step 7  Choose the first baseline from the Baseline1 drop-down list.
Step 8  Choose 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, choose Polling Configuration & Reports.
Step 2  Choose CRM Polling.
Step 3  Choose Baseline Route Polling.
Step 4  Choose Config Route Polling.
Step 5  Click the Add button.
Step 6  Choose By Baseline Route.
Step 7  On the Add Baseline Route page, specify the following settings:
**Specific Route Polling**

To configure specific route polling, you must select S,G routes from Specific Multicast Routes lists for specified routers and add them to the list of monitored routes. For configured routes, CMM notifies users of any changes to the S,G route.

**Unicast Report**

To view the Unicast Report:

1. From the Multicast Manager menu, choose **Polling Configuration & Reports**.
2. Choose **CRM Polling**.
3. Choose **Specific Route Polling**.
4. Choose **Report Parameters**.

<table>
<thead>
<tr>
<th>Fields and Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing Table Type</td>
<td>Choose either Unicast or Multicast.</td>
</tr>
<tr>
<td>Select Router</td>
<td>Choose a router.</td>
</tr>
<tr>
<td>Baseline</td>
<td>Choose 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>
Step 5  On the Unicast Report Parameters page, specify the following settings:

<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 choose 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 choose a date from a calendar.</td>
</tr>
<tr>
<td>Device</td>
<td>Choose a device from the drop-down list.</td>
</tr>
<tr>
<td>Source</td>
<td>Choose a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Choose 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, choose **Polling Configuration & Reports**.
- **Step 2** Choose **Miscellaneous Polling & Reports**.
- **Step 3** Choose **CRM Polling**.
- **Step 4** Choose **Specific Route Polling**.
- **Step 5** Choose **Multicast Report**.
- **Step 6** Choose **Report Parameters**.
Configuring Unicast Polling

To configure Unicast Polling:

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

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

Step 8  On the Add Unicast Specific Route Config page, specify the following settings:

<table>
<thead>
<tr>
<th>Fields and Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Router</td>
<td>Choose 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

**Step 9**
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, choose **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 10**
Click the **Add** button.

### By Import

To configure Unicast SG polling by importing a file:

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

**Step 2**
Choose **CRM Polling**.

**Step 3**
Choose **Specific Route Polling**.

**Step 4**
Choose **Config Unicast Polling**.

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

**Step 6**
Choose **By Import**.

**Step 7**
Click the **Browse** button to upload the file.

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

**Step 9**
Click **Upload**.

### Import Format:

```
ROUTEMONSENGLE:<DeviceIp>,<CRM_UNICAST-0>,<Route>,<RouteMask>,<NextHop>
```

**Example:**

```
ROUTEMONSENGLE:172.20.111.198,0,126.1.1.0,255.255.255.0,126.1.1.11
```
Configuring Multicast Polling

To configure Multicast Polling:

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

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

**Step 3**
Choose **CRM Polling**.

**Step 4**
Choose **Specific Route Polling**.

**Step 5**
Choose **Config Multicast Polling**.

**Step 6**
Click **Add**.

**Step 7**
Choose **By Multicast Route**.

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

**Step 8**
On the Add Multicast Specific Route Config page, specify the following settings:

<table>
<thead>
<tr>
<th>Fields and Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Router</td>
<td>Choose a router.</td>
</tr>
<tr>
<td>CPU Threshold</td>
<td>The CPU utilization of the router is 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>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 <strong>Add Selected Routes to Polling Config</strong>.</td>
</tr>
</tbody>
</table>

**Step 9**
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, choose **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 10**
Click the **Add** button.
By Import

To configure Multicast polling by importing a file:

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

**Import Format:**

ROUTEMONSINGLE: <DeviceIp>,CRM_MULTICAST-1,<Source>,<NetworkMask>,
<getUpstreamNeighbor>,<Group>

**Example:**

ROUTEMONSINGLE:126.1.13.18,1,0.0.0.0,255.255.255.255,126.1.13.15,239.254.1.1
Discovery and Trace

This chapter contains the following sections:

- Discovery, page 5-1
- Trace, page 5-22

Discovery

Discovery is the process that CMM uses to add devices to a CMM domain. CMM provides five types of discovery:

- Multicast Discovery, page 5-2
  
  Run multicast discovery to do an initial discovery of the multicast devices in your network and add them to the domain. You can discover routers, or discover both routers and Layer 2 devices (switches).

- L2 Device, page 5-17
  
  Run L2 Device discovery to discover Layer 2 devices (switches) in the multicast network.

- Video Probe, page 5-18
  
  Run video probe discovery to associate video probes in your network with an already discovered router.

- VidMon Device, page 5-20
  
  Run VidMon device discovery to discover Cisco VidMon routers (Cisco 7700 series routers and Cisco ASR 9000 series routers)

- Unicast Device, page 5-21
  
  Run Unicast device discovery to add unicast routers to a CMM domain.

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 is the process that CMM uses to add multicast devices to a CMM domain. Multicast discovery uses Protocol Independent Multicast (PIM) neighbor relationships to locate the network routers that have PIM enabled.

When you perform discovery, you can use a Seed IP address or flat file that provides PE addresses or PE addresses and associated CE addresses, or you can use an import file that provides management IP addresses and associated SNMP community strings for Contiguous Discovery by Import.

Using a Seed IP address or flat file, you can perform these types of discovery.

- **Core/Enterprise Discovery/Contiguous** — Use Core/Enterprise Discovery/Contiguous to perform contiguous discovery of PIM-enabled devices in your core/enterprise network.
- **Core/Enterprise Discovery/Core + CE** — Use Core/Enterprise Discovery/Core + CE to discover the multicast devices in your core/enterprise network.
  
  Core/Enterprise Discovery/Core + CE requires TACACS+ access to the devices in the network. See Creating a Domain, page 10-3.

- **Distributed Network Discovery/CE-PE** — Use Distributed Network Discovery to discover the customer sites using Customer Edge (CE) devices and associated Provider Edge (PE) devices in a distributed network such as an IP/MPLS network. See CE-PE Mapping Discovery, page 5-14.
- **Distributed Network Discovery/PE Only** — Use Distributed Network Discovery to discover the customer sites using Provider Edge (PE) devices in a distributed network such as an IP/MPLS network.
- **Distributed Network Discovery/P2MP** — Use Distributed Network Discovery/P2MP to discover the customer sites in a distributed network that uses Point-to-Multipoint (P2MP) Traffic Engineering over a TE tunnel, such as a MPLS/P2MP network.
  
  Distributed Network Discovery/P2MP discovery requires TACACS+ access to the devices in the network. See Creating a Domain, page 10-3.
- **Single Device Discovery** — After you have run Core Enterprise or Distributed Network discovery, use Single Device Discovery to discover a single device or a device and its adjacent PIM neighbors.

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.
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).

If you choose **Contiguous Discovery by Import**, you have one choice for the discovery method.

To run multicast discovery:

**Step 1**  From the Multicast Manager menu, choose **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 the type of basic discovery:

- **By Seed IP/Flat File**—Choose By Seed IP/Flat File to perform most types of discovery.
- **Contiguous Discovery by Import**—Choose this method if you are implementing the Trace by IP Management address feature.

  If you choose Contiguous Discovery by Import, go to **Contiguous Discovery by Import**, page 5-12 for detailed instructions.

**Step 6**  If you choose **By Seed IP/Flat File**, the Discovery Add/Modify page appears.

The Discovery Add/Modify page contains three tabs.

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

- To perform continuous Core/Enterprise Discovery, specify discovery parameters as indicated in **Core/Enterprise Discovery/Contiguous**, page 5-4.
- To perform Core/Enterprise discovery using a mapping file that discovers the core network and associated CE routers, see **Core/Enterprise Discovery/Core + CE**, page 5-5.
- To perform Distributed Network Discovery, click the **Distributed Network** tab.

  The Distributed Network tab appears.

  - To perform distributed network discovery using a mapping file that specifies CEs and associated PEs, see **Distributed Network Discovery/CE-PE Mapping**, page 5-6.
  - To perform distributed network discovery using PEs only, see **Distributed Network Discovery/PE Only**, page 5-7.
  - To perform distributed network discovery for a network that uses P2MP TE tunnels, see **Distributed Network Discovery/P2MP**, page 5-8.

- To perform Single Device Discovery, click the **Single Device Discovery** tab.

See **Single Device Discovery**, page 5-11.
Core/Enterprise Discovery/Contiguous

This will discover the devices with PIM neighbor, up to the hop count given or up to the end of that particular network. This is the discovery type CMM used to discover all devices present in a contiguous manner with PIM enabled in a particular network. By using this discovery logic, CMM discovers all devices through PIM neighboring in core network or in a customer site network.

To perform Core/Enterprise/Contiguous Discovery:

Step 1
From CMM menu, navigate to Discovery & Trace > Discovery > Multicast Discovery.
The Multicast Discovery Add/Modify page appears. Click the Contiguous radio button.

Step 2
Provide any customer site device IP as seed IP to discover entire customer site network in a contiguous manner.

Step 3
Specify additional discovery parameters as follows:

<table>
<thead>
<tr>
<th>Table 5-1 Multicast Discovery: Core Enterprise Discovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>Community Strings</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Discovery Depth</td>
</tr>
<tr>
<td>Network Limit Type</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Network Address and Network Mask</td>
</tr>
</tbody>
</table>

Step 4
Click Start Discovery to start discovery.

**Note** Other discovery types use contiguous discovery internally to discover a core network or a customer site network.
Core/Enterprise Discovery/Core + CE

In this type of discovery, CMM performs automatic contiguous device discovery for core network by using the seed IP and then add CEs to the same domain through Single Device Discovery.

To discover the core network and CEs connected with it:

Step 1  Provide a CSV file that lists the IP addresses of the PEs that you want to discover, separated by commas.
Step 2  Save the file in an appropriate directory on the CMM server.
Step 3  From the Multicast Manager menu, choose 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 Discovery.
Step 7  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.

Step 8  Click the Core + CEs Only radio button.
Step 9  In the Seed IP/Name field, enter the IP address or the hostname of the seed device from which to start network discovery.

Seed IP — Any device IP from Core network. For example, 172.20.111.200 (cmm-6506-c1.cisco.com) in CMM lab

Step 10  In the Flat File Path field, enter the fully directory path and filename for the file that you coded to provide CE information.

Flat file — All CE devices IP address in a flat file as follows:
192.168.76.8
192.168.76.28
172.20.111.222
172.25.103.43
172.20.111.221

Step 11  Specify additional discovery parameters as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Community Strings    | Enter the SNMP RO community string. You can enter multiple community strings as needed.  
| **Note** From this release, you can validate the community strings using **Verify** option and you can view the community strings listed in the Community string box if you uncheck the **Mask** check box. |
| Discovery Depth      | Select a value for the hop count up to which the discovery will search for devices. |
Chapter 5      Discovery and Trace

**Discovery**

Step 12 Click **Start Discovery** to start discovery.

---

**Distributed Network Discovery/CE-PE Mapping**

This type of discovery is used to discover all customer site devices under a single domain by ignoring the core network. This discovery will bypass the core network by using the PE-CE flat file. This will perform a contiguous discovery for all customer sites with CE devices available in flat file as seed IP and add the discovered devices in a single domain.

---

**Note**

In this type of discovery, you have to configure Service Type to run the trace from one customer site to other customer site. Service Type can be configured by mentioning source CE and destination CE.

To discover devices in a distributed network using a file that provides CE-PE mapping information:

**Step 1** Edit a text file that provides 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

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.

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

**Step 3** From the Multicast Manager menu, choose **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** Click the **CE-PE Mapping** radio button.

**Step 8** Specify additional discovery parameters as follows:

---

**Table 5-2 Multicast Discovery: Core Enterprise Discovery (continued)**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Limit Type</td>
<td>Click the All, Include, or Exclude. radio button. The option you specify is used to restrict the discovery process. If you choose 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 Network Mask</td>
<td>If you choose Include or Exclude, allows you to filter network discovery types.</td>
</tr>
</tbody>
</table>
Discovery

Step 9
Click **Start Discovery** to start discovery.

### Distributed Network Discovery/PE Only
This discovery will prepare the CE-PE mapping file internally by executing CLI commands on PE devices and then will call CE-PE discovery to discover only customer sites.

Parameter: Flat file which contains all PE device IP addresses:

For example:
172.20.111.198
172.20.111.199
172.20.111.205
172.20.111.204
172.20.111.220

Step 1
Edit a CSV file that lists the IP addresses of the PEs that you want to discover, separated by commas.
**Discovery**

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

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

**Step 3**  
From the Multicast Manager menu, choose 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**  
Click the PE Only radio button.

**Step 8**  
Specify additional discovery parameters as follows:

<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 PEs, separated by commas.</td>
</tr>
<tr>
<td>Community Strings</td>
<td>Enter the SNMP RO community string. You can enter multiple community strings as needed.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> From this release, you can validate the community strings using Verify option and you can view the community strings listed in the Community string box if you uncheck the Mask check box.</td>
</tr>
<tr>
<td>Discovery Depth</td>
<td>Select a value for the hop count up to which the discovery will search for devices.</td>
</tr>
</tbody>
</table>
| Network Limit              | Click the All, Include, or Exclude. radio button. The option you specify is used to restrict the discovery process.  
|                           | If you choose 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 (>>) to move them to the Include or Exclude list. |
| Network Address and Network Mask | If you choose Include or Exclude, allows you to filter network discovery types.          |

**Step 9**  
Click Start Discovery to start discovery.

**Distributed Network Discovery/P2MP**  
CMM will discover all core routers in MPLS P2MP TE tunnel, including all customer sites. CMM expects all interfaces to be reachable from CMM server to core routers (PE and P routers).
You can run trace across customer sites through MPLS P2MP TE tunnels. Here core network is basically connected as MPLS P2MP TE tunnel and PIM is not enabled on the core routers involved in the P2MP TE tunnel except headend and tailend.

You can configure for this trace and if there is any violation in the trace of the SG via the PE-PE tunnel, then it will be notified as an event.

**Figure 5-1  Distributed Network Discovery/P2MP**

Figure 5-1 shows PE1 as the tunnel headend router and PE2, PE3, and PE4 as tunnel tailend routers. The following sub-LSPs are signaled from PE1 in the network:

From PE1 to PE2, the sub-LSP travels the following path: PE1 -> P01 -> P02 -> PE2

From PE1 to PE3, the sub-LSP travels the following path: PE1 -> P01 -> P03 -> PE3

From PE1 to PE4, the sub-LSP travels the following path: PE1 -> P01 -> P04 -> PE4

CMM will find the sub-LSP paths through the P2MP TE tunnel from headend to tailend. CMM will verify the tasks listed below to run multicast trace through P2MP TE tunnel.

1. CMM has to discover all core routers including all customer sites. CMM expects all interfaces to be reachable from CMM server to core routers (PE and P routers).

2. CMM assumes there is no VRF configured at PEs, and CEs and PEs (head/tail of tunnel) are interconnected as PIM neighbor devices.
Chapter 5      Discovery and Trace

3. Once CMM multicast trace reaches to the device configured for tunnel, it will check the status of the device. If the device is a headend PE router, then it will proceed with P2MP Tunnel type trace, else the multicast trace will stop.

4. If the tunnel device is a headend, then CMM will find all sub-LSP destinations and will find the explicit path for each sub-LSP.

5. Once CMM reaches to the end of the sub-LSP, then existing trace logic will be used to trace through customer site.

Follow the steps given below to start P2MP discovery:

---

**Step 1**
Edit a text file that provides 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

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

For XR devices to start P2MP discovery:
Code a CSV file that lists the IP addresses of all devices and associated PE devices in the following format:

all
CE1=PE1, CE2=PE2

This type of discovery does not require CLI access to the PE devices, instead it uses MIB queries to connect to all devices in a P2MP network. Username and password information are not required here.

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

**Step 3**
From the Multicast Manager menu, choose 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**
Click the P2MP radio button.

**Step 8**
Specify additional discovery parameters as follows:
Chapter 5  Discovery and Trace

Review Draft - Cisco Confidential

Table 5-5  Multicast Discovery: Distributed Network Discovery/P2MP

<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 and associated PEs. File format: CE1=PE1:PE2:PE3</td>
</tr>
</tbody>
</table>
| Community Strings          | Enter the SNMP RO community string. You can enter multiple community strings as needed.  
                           | **Note** From this release, you can validate the community strings using Verify option and you can view the community strings listed in the Community string box if you uncheck the Mask check box. |
| Discovery Depth            | Select a value for the hop count up to which the discovery will search for devices. |
| Network Limit              | Click the All, Include, or Exclude radio button.  
                           | The option you specify is used to restrict the discovery process.  
                           | If you choose 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 (>>) to move them to the Include or Exclude list. |
| Network Address and Network Mask | If you choose Include or Exclude, allows you to filter network discovery types. |

**Step 9**  
Click **Start Discovery** to start 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.  
CMM provides Nexus 7K support for Single Device 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, choose **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.

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

**Step 7** Specify additional discovery parameters as follows:

<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><strong>Note</strong></td>
<td>From this release, you can validate the community strings using <strong>Verify</strong> option and you can view the community strings listed in the Community string box if you uncheck the <strong>Mask</strong> check box.</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. If you choose <strong>Include</strong> or <strong>Exclude</strong>, 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><strong>Save</strong></td>
<td>Adds the selected router for discovery.</td>
</tr>
</tbody>
</table>

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

**Contiguous Discovery by Import**

If you choose **Contiguous Discovery by Import**, you are prompted to browse for a CSV file that contains the IP addresses of devices to discover. This method is used if you are implementing the Trace by IP Management Address feature.

CMM provides Nexus 7K support for Contiguous Discovery.
To perform contiguous discovery by import:

**Step 1** Make sure that you are using the Trace by IP Management Address feature. See Set Up Trace by Management IP Address (Optional), page 10-1.

**Step 2** Code a comma-separated value (CSV) file that specifies the Management IP addresses and associated SNMP community strings for the devices to discover. See Coding a CSV File to Provide Management IP Addresses, page 10-2.

**Step 3** From the Multicast Manager menu, choose **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 **Discovery**.

**Step 7** From the pull-down menu in the Discovery field, choose **Contiguous Discovery by Import**.

The Multicast Discovery Import Page appears.

**Step 8** Click the **Browse** button and browse for the CSV file specifying the devices to discover.

**Step 9** Select the CSV file.

**Step 10** Click the **Upload** button.

**Import Format:**

```
<device_ip>,<ro_community>
```

**Example:**

```
172.20.111.233,public
```

**Deleting a Device**

You can delete a device from the domain in the event that the device is no longer operational.

To delete a device:

**Step 1** If the device has a video probe associated with it, complete these steps to delete the video probe:

a. Go to **Discovery & Trace > Discovery > Video Probe**.

b. On the Video Probe Discovery page, check the check box next to the video probe that you want to delete, then from the drop-down menu in the Actions button, choose **Delete**.

c. When prompted to delete the video probe, click **OK**.

**Step 2** Go to **Discovery > Multicast Discovery**.

**Step 3** On the Multicast Discovery page, complete these steps:

a. Check the check box next to the device that you want to delete.

b. From the drop-down menu in the Actions button, choose **Delete**.

c. When prompted to delete the device, click **OK**.
CE-PE Mapping Discovery

CE-PE Mapping ignores the core network and helps discover all the customer site devices under a single domain, using CE-PE flat file. This flat file contains all the customer sites with CE devices, as a seed IP. CE-PE Mapping performs a contiguous discovery of all the devices and adds it under a single domain.

Note

In this discovery, the user has to configure Service Type in order to run the trace from one customer site to the other customer sites. To configure Service Type, enter the source and destination CEs.

The format for CE-PE Mapping is

CE1=PE1:PE2
CE2=PE3

Given below is an example of the flat file as per MVPN Topology:

- 11.1.1.13=11.1.1.12
- 12.1.1.19=12.1.1.18:14.1.2.17
- 12.1.6.19=12.1.6.18:14.1.1.17
- 13.1.1.12=13.1.1.11
- 15.1.1.22=15.1.1.19

All the five customer sites given in the example will be discovered as shown in the Figure 5-2.
CE-PE Mapping discovery will discover only customer sites like 1, 2, 3, 4 and 5. This will ignore core.
Service Type Configuration

After CE-PE discovery, the user has to manually configure CE-to-CE connection in CMM to launch multicast trace across the customer sites.

To configure CE-to-CE connection:

---

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

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

The MVPN Configuration page opens.

**Step 3**  Enter the Name for **Service Type**.

**Step 4**  Select the Source CE (from which the flow will be connected to other customer site CEs) from the CE Devices drop-down list.

An expanded MVPN Configuration page pops up. The pane at the left lists the devices that were discovered using CE-PE mapping.

**Step 5**  Select the outgoing interface of the Source CE from the **CE’s Interface List** to **SEL Interface List** (Ifindex:IP Address).

**Step 6**  Select the destination CEs from the **CE Device(s)** to **SEL CE Device(s)** (the SG flow should go from Source CE to Destination CEs).

**Step 7**  Click **Continue** to save this Service Type configuration.

---

**How to Trace using Service Type**

To trace the flow of the Source CE on the other customer sites:

---

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

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

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

The Multicast Trace page appears.

**Step 4**  Select the **Device**.

**Step 5**  Select the **Source**.

**Step 6**  Select the **Group**.

**Step 7**  Select the **Service Type**.

**Step 8**  Click **Trace**.
L2 Device

L2 discovery adds Layer 2 devices to an already discovered CMM domain.

To run L2 device discovery:

1. From the Multicast Manager menu, choose **Discovery & Trace**.
2. Select **Discovery**.
3. Select **L2 Device**.
4. Click **Add**, and from the drop-down list, choose **By L2**.
5. The Add/Rediscover a L2 Device page appears.
6. On the Add/Rediscover a L2 Device page, specify the following settings:

<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></td>
<td><strong>Note</strong> From this release, you can validate the community strings using <strong>Verify</strong> option.</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.

**By Import**

To import a CSV file listing Layer 2 devices, on the L2 Discovery page:

1. From the Multicast Manager menu, choose **Discovery & Trace**.
2. Choose **Discovery**.
3. Choose **L2 Device**.
4. Click the **Add** button in the **L2 Discovery** page.
5. Choose **By Import**.
6. Click the **Browse** button to upload the CSV file.
7. Choose **Merge** to unify an existing configuration with the new configuration or choose **Replace** to overwrite the existing configuration.
8. Click **Upload**.
**Video Probe**

To run video probe discovery:

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

**Step 2**  Select Discovery.

**Step 3**  Select Video Probe.

**Step 4**  Click the Add button.

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

   The Add/Rediscover a Video Probe configuration page appears.

**Step 6**  On the Add/Rediscover a Video Probe configuration page, specify the following settings:

---

**Import Format:**

<device_ip>,<ro_community>

**Example:**

172.20.111.206,public
**By Import**

To import a Video Probe file:

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

**Step 2** Choose **Discovery**.

**Step 3** Choose **Video Probe**.

**Step 4** Click the **Add** button in the **Video Probe Discovery** page.

**Step 5** Choose **By Import**.

**Step 6** Click the **Browse** button to upload the CSV file.

**Step 7** Choose **Merge** to unify an existing configuration with the new configuration or choose **Replace** to overwrite the existing configuration.
**Discovery**

Step 8  Click **Upload**.

**Import Format:**

<Probe IP>,<Probe RO Community String>,< Probe Write Community String>,<Router IP>,<Router Community String>,<Interface Description>,<Probe Type>,<DCM URL>

**Example:**

172.20.111.213,public,public,172.20.111.198,public,eth0,2,null

**Monitoring Application**

To configure monitoring applications:

Step 1  From the Multicast Manager menu, choose **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, choose **By Monitoring Application**.

Step 7  On the Monitoring Application configuration page, specify the following settings:

<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></td>
<td><strong>Note</strong> From this release, you can validate the community strings using <strong>Verify</strong> option.</td>
</tr>
<tr>
<td>Application Type</td>
<td>From the pull-down list, choose 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, choose 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:

| Matching | From the drop-down list, choose either All or Any. |
| Filter | You can specify up to two filters to filter the discovery by device name or by IP address. From the drop-down list(s), choose either Device Name or Device IP Address |
| Containing Text | Enter a partial search string for either the Device Name or the Device IP Address |
| Search | To search for devices matching the specified search parameters, click the Search button |

**Step 5**
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, choose Discovery & Trace.

**Step 2**
Select Discovery.

**Step 3**
Select Unicast Device.

**Step 4**
Click Add.

**Step 5**
Select By Unicast Router.

**Step 6**
On the Unicast Router Discovery configuration page, specify the following settings:
By Import

To import a Unicast Device file:

Step 1 From the Multicast Manager menu, choose Discovery & Trace.
Step 2 Choose Discovery.
Step 3 Choose Unicast Device.
Step 4 Click the Add button in the Unicast Discovery page.
Step 5 Choose By Import.
Step 6 Click the Browse button to upload the CSV file.
Step 7 Choose Merge to unify an existing configuration with the new configuration or choose Replace to overwrite the existing configuration.
Step 8 Click Upload.

Import Format:
<device_name>,<device_ip>,<ro_community>

Example:
qpm7200.cisco.com,10.77.210.159,public

Trace

Multicast Trace

The multicast trace process displays:

- A graphical tree showing connectivity between a source router and two or more destination routers
- Trace tables showing detailed information about the data flowing between the devices shown in the trace.

CMM provides Nexus 7K support for Multicast Trace and Unicast Trace.
The trace data tables that appear depend on the type of device being traced and the type of data in the multicast. The trace data tables include:

- **Flow Description**—A description of the flow, which includes the multicast group and source. If additional information on the flow is configured in CMM, the description can include information such as the Channel Name, Transport Description, Source description (for video flows).

- **Trace Data Table**—Lists the routers, interfaces, and PIM neighbors that transport the multicast flow.

- **Video Probe Data Table**—For flows that include video probe data, the trace data tables include a video probe data table that lists all video probes known to CMM that are present on the distribution tree. This table shows the router/interface to which the probe is connected, and MDI metrics like DF and MLR.

- **VidMon Data Table**—For traces that include VidMon devices, the trace tables include a VidMon data table showing the VidMon-enabled routers present in the distribution tree. The table includes the router, interface, direction, status, and VidMon metrics like DF, MLR, and MRV.

- **Channel Data Table**—For multi-channel video flows, the trace includes a channel data table showing the related multicast groups for each of the video channels carried in the traced multicast flow. The table shows the channels, related multicast groups for each channel, and additional video format information.

If any DF or MLR thresholds have been exceeded, the Vidmon data area indicates these with a red circle in the Status column. If the DF and MLR values are within the defined thresholds, the Status column shows green circles.

To launch Multicast Trace across customer sites, the user has to manually configure CE-to-CE connection in CMM. See Service Type Configuration, page 5-16.

To perform a multicast trace:

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

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

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

**Step 4** The Multicast Trace page appears.

**Step 5** On the Multicast Trace configuration page, specify the following settings:

<table>
<thead>
<tr>
<th>Fields and Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select a Device</td>
<td>From the drop-down list of devices, choose the device for which to run a trace.</td>
</tr>
<tr>
<td>Source</td>
<td>From the drop-down list, choose the IP address of the source to monitor.</td>
</tr>
<tr>
<td>Filter Groups</td>
<td>Click <strong>Filter Groups</strong> to filter the list of groups to show only groups relevant to the selected Source.</td>
</tr>
<tr>
<td>Group</td>
<td>From the drop-down list, choose the IP address of the group to monitor.</td>
</tr>
<tr>
<td>Filter Sources</td>
<td>Click Filter Sources to filter the list of sources to show only sources relevant to the selected Group.</td>
</tr>
<tr>
<td>Clear SG Filter</td>
<td>Click <strong>Clear SG Filter</strong> to clear the Source and Group fields.</td>
</tr>
</tbody>
</table>
**Step 6**

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).”

Figure 5-3 shows a sample trace data table.

### Figure 5-3 Trace Data Tables

<table>
<thead>
<tr>
<th>Trace Data</th>
<th>Source</th>
<th>Forwarding</th>
<th>Out Errors/sec</th>
<th>In Errors/sec</th>
<th>Neighbor IP</th>
<th>Neighbor ID</th>
<th>Out Errors/sec</th>
<th>In Errors/sec</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>CORE-710-1</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>CORE-710-1</td>
<td>171.15.1.16</td>
<td>171.15.1.16</td>
<td>0.0</td>
<td>-</td>
</tr>
<tr>
<td>CORE-710-2</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>CORE-710-1</td>
<td>171.15.1.16</td>
<td>171.15.1.16</td>
<td>0.0</td>
<td>-</td>
</tr>
<tr>
<td>CORE-710-3</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>CORE-710-2</td>
<td>171.15.1.16</td>
<td>171.15.1.16</td>
<td>0.0</td>
<td>-</td>
</tr>
<tr>
<td>CORE-710-4</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>CORE-710-3</td>
<td>171.15.1.16</td>
<td>171.15.1.16</td>
<td>0.0</td>
<td>-</td>
</tr>
<tr>
<td>CORE-710-5</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>CORE-710-4</td>
<td>171.15.1.16</td>
<td>171.15.1.16</td>
<td>0.0</td>
<td>-</td>
</tr>
<tr>
<td>CORE-710-6</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>CORE-710-5</td>
<td>171.15.1.16</td>
<td>171.15.1.16</td>
<td>0.0</td>
<td>-</td>
</tr>
<tr>
<td>CORE-710-7</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>CORE-710-6</td>
<td>171.15.1.16</td>
<td>171.15.1.16</td>
<td>0.0</td>
<td>-</td>
</tr>
</tbody>
</table>

Figure 5-4 shows the graphical tree portion of the trace page.
If the trace includes switches, the topology map shows the switches in the trace. And for traces that show CE-PE connections for VRFs, the trace shows which VRF is connected through the CE and PE.

L2 Devices will be shown in the Trace only when devices are connected directly with L3 devices. The Imported L2 devices will not be shown.

**Figure 5-5** shows a topology map that includes switches and VRF connections.

CMM displays multicast receiver information when you click UT-enabled devices on the Multicast Trace page.
Routers are shown with a UT-enabled icon on the Trace page for explicit user tracking supported devices. When you click the devices in the trace image (Figure 5-6) in the show command page, one more table is shown for user tracking details (Figure 5-7).

**Figure 5-6**  
**Routers with UT-enabled devices**

**Figure 5-7**  
**User Tracking Details**

Step 7  
If you want to save the trace, complete these steps:

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

**Performing a Unicast Trace**

You can also perform a trace on a unicast device.

To perform a unicast trace:
Step 1  From the Multicast Manager menu, choose **Discovery & Trace**.

Step 2  Select **Trace**.

Step 3  Select **Multicast Trace**.

Step 4  On the Multicast Trace page, choose a device that is configured for unicast and has unicast flows.

Step 5  Enter the parameters for the trace and then click the **Trace** button.

Figure 5-8 shows a trace table for a unicast trace.

**Figure 5-8  Trace Table for a Unicast Trace**

<table>
<thead>
<tr>
<th>VidMon Data</th>
<th>Interface</th>
<th>Direction</th>
<th>Status</th>
<th>DF</th>
<th>MLR</th>
<th>Min MRV</th>
<th>Max MRV</th>
</tr>
</thead>
<tbody>
<tr>
<td>WD2036-VMON</td>
<td>TenGigabitEthernet/1</td>
<td>Outbound</td>
<td>✔️</td>
<td>0.945</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>VAHR-7556-VMON</td>
<td>TenGigabitEthernet/4</td>
<td>Inbound</td>
<td>✔️</td>
<td>0.839</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>WD2061-EDGE</td>
<td>TenGigabitEthernet/3</td>
<td>Inbound</td>
<td>✔️</td>
<td>1.055</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>VAHR-7556-EDGE</td>
<td>TenGigabitEthernet/3</td>
<td>Outbound</td>
<td>✔️</td>
<td>0.99</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

If the unicast device is a VidMon device with channels defined for a multicast channel, the trace table includes a Channel Data table. The Channel Data table identifies the channel and also lists related multicast groups for the channel.

Figure 5-9 shows the graphical tree portion of the unicast trace.
Step 6  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.
Viewing Additional Information About a Device in a Trace

To view additional information about a device or video probe shown in a trace:

Click the icon for a device or video probe.

If you click on a:

- Router icon or a core router icon—CMM issues an ipMRouteEntry query for the device, and shows a trace data table summarizing the values in the MIB event that is returned. You can also log into the device and issue additional IOS commands monitor the device.

- Icon for a VidMon device (Cisco 7600 series router or Cisco ASR 9000 series device), a trace table appears showing the VidMon flows on the device.

  For more information on VidMon flows, see Viewing VidMon Flows From a Trace, page 5-29.

- Video 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.

- Icon for a Cisco 7600 device or a Cisco 6500 device—A trace table appears showing multicast receiver information for the device.

Viewing VidMon Flows From a Trace

To view VidMon flows from a CMM trace page:

Step 1

On the trace page, click on the icon for a VidMon device.

The Vidmon Flow Status page appears, as shown in Figure 5-10. The Video Flow Status page shows the status of the VidMon flows on the device interfaces.

Figure 5-10   Vidmon Flow Status Page

The stoplights in the Status column show the status of the flow on the interface:

- **Green**—Normal Flow
- **Red**—A threshold is exceeded on the flow
- **Yellow**—A threshold is exceeded, but the flow is normal at present
- **Black**—There is an outage

Step 2

To refresh monitoring data, click the Monitor Flows button.

Step 3

To more detailed status for the interfaces on the VidMon device, click an interface name on the Video Flow Status page.
The Vidmon Interface Flows page appears, as shown in Figure 5-11. The Vidmon Interface Flows page shows detailed statistics for the current flows on the interface.

**Figure 5-11   Vidmon Interface Flows Page**

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:
  - Green indicates that the flow is being transmitted with no errors.
  - Yellow indicates a minor fault in the TS.
  - Red indicates a major fault in the TS.
- 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 4**  
To clear yellow indicators, click the **Clear** button.

**Step 5**  
To perform a multicast trace for the flow, click on the IP address of the Destination Port for the flow.

**Step 6**  
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 5-12.
The Vidmon Interface Flows Page shown in Figure 5-12 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.
- **MDC**—Indicates the Medic Discontinuity Counter (MDC) value for the flow.

Figure 5-13 shows a 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.
**Review Draft - Cisco Confidential**

**Viewing Multicast Receivers in a Forwarding Tree**

You can view the multicast receivers in a forwarding tree for devices that are running Cisco IOS SXI or SXH releases. To view trace data for multicast receivers in a forwarding tree:

---

**Step 1**
In the trace topology view, click on an icon for a Cisco 7600 or Cisco 6500 Series device. **Figure 5-14** shows a portion of a trace topology that includes Cisco 6500 Series devices.

![Figure 5-14 Topology Trace with Multicast Receivers](image1)

**Figure 5-14**

---

**Step 2**
Click on an icon for a Cisco 6500 series device that has a receiver device associated with it (shown by a PC icon); for example, click on **cmm-6504-c4**.

**Step 3**
A trace table showing ipMRouteEntry trace data and a Receiver table appears, as shown in **Figure 5-15**.
Chapter 5  Discovery and Trace

Figure 5-15  Trace Table with Receiver Table

The trace table shows ipMRouteEntry trace data for the device.
The Receiver table shows information for the VLANs containing the receivers.

Show Groups

The Show Groups process shows a trace for a specified Source and Group.

In CMM, upto 18000 source groups can be shown in the S, G Trace table.

To configure and run a Show Groups trace:

Step 1  From the Multicast Manager menu, choose Discovery & Trace.
Step 2  Select Trace.
Step 3  Select Show Groups.
Step 4  From the Select a Device drop-down list, choose a device.
Step 5  If you want to filter the groups, click the Add Filter button enter a text string, and then click the Search button.
The groups shown will be limited to ones containing the entered text.
To remove the filter, click the Remove button.
Step 6  Click the Show Trace button.
Step 7  The trace appears in the S,G Trace table.
Step 8  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 9  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. If you want to run a trace from a saved trace file, choose a trace file from the pull-own list in the Load from previously saved traces field and then click the Show Trace button.

Step 10 To remove the trace, click the Remove Trace button.

---

**Show Specific Group**

The Show Specific Group allows user to retrieve the configuration details of specific Source Groups of a device.

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

Step 2  Select Trace.

Step 3  Select Show Specific Groups.

Step 4  Choose a device from Select a Device from here drop-down list.

Step 5  Enter the Group IP address in the Enter Group IP field.

Step 6  Click Submit.
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 6-1
- All Device Information, page 6-2

**Topology**

**Step 1**  
From the Multicast Manager menu, choose **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 6-1.
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, choose Topology.
Step 2  Click All Device Information.
The Topology - One Hop Neighbors window appears.
Step 3  From the Select a Router drop-down list, choose a device.
Step 4  Click Show.
A table displaying the PIM neighbors for the selected device appears as shown in . The table displays the PIM neighbors for the selected device and a separate pane for each PIM neighbor that shows its PIM neighbors.

**Step 5**
To view the PIM neighbors of a device that is listed in one of the panes, click the router ID in the Neighbor column.

---

**Topology Change Reflection Without Re-Discovery**

In CMM, the Topology changes are automatically reflected for PIM Neighbor Loss trap. The user need not manually re-discover the domain for the Topology changes.

When the trap, “PIM Neighbor loss” is triggered by the device, CMM receives a trap notification. CMM runs a single device discovery for the device and reflects the topology changes.

**Note**
Automatic Topology Reflection happens only when the trap, PIM Neighbor loss is generated by the device. When the PIM neighbor is up, you must manually re-discover the domain for Topology Reflection. Automatic Topology Reflection is applicable only for Contiguous discovery.
Chapter 6  Topology

Topology Change Reflection Without Re-Discovery

Review Draft - Cisco Confidential
Diagnostics

This chapter contains the following sections:

- SG Diagnostics, page 7-1
- L2 Diagnostics, page 7-2
- Video Diagnostics, page 7-3
- Miscellaneous Diagnostics, page 7-7
- Tools, page 7-9
- CRM Diagnostics, page 7-18

SG Diagnostics

Packet Monitoring

To plot Packet Monitoring:

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

**Step 2** Choose S,G Diagnostics.

**Step 3** Choose Packet Monitoring.

**Step 4** On the Packet Monitoring page, specify the following settings:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select a Device</td>
<td>Choose a device from the drop-down list.</td>
</tr>
<tr>
<td>Source</td>
<td>Choose a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Choose a group from the drop-down list.</td>
</tr>
<tr>
<td>Reset SG List</td>
<td>Clears the 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>Choose the graph type.</td>
</tr>
</tbody>
</table>
L2 Diagnostics

L2 Multicast Information

To query L2 Multicast Information:

Step 1 From the Multicast Manager menu, choose Diagnostics.
Step 2 Choose L2 Diagnostics.
Step 3 Choose L2 Multicast Info.
Step 4 On the Layer 2 Multicast Information page, specify the following settings:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLI Access</td>
<td>Allows you to specify the type of CLI access for the operation. The default CLI access method configured for the domain is initially selected. You can choose Telnet, SSH v1, or SSH v2. Choose the type of CLI access enabled on the device.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the username.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password.</td>
</tr>
<tr>
<td>Select a Switch</td>
<td>Choose a switch.</td>
</tr>
<tr>
<td>Query</td>
<td>Run the query using the set parameters.</td>
</tr>
</tbody>
</table>
L2 Host IP Addresses

To query L2 Host IP Addresses:

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

**Step 2** Choose L2 Diagnostics.

**Step 3** Choose L2 Host IPs.

**Step 4** On the Layer 2 Host IPs page, specify the following settings:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLI Access</td>
<td>Allows you to specify the type of CLI access for the operation. The default CLI access method configured for the domain is initially selected. You can choose Telnet, SSH v1, or SSH v2. Choose the type of CLI access enabled on the device.</td>
</tr>
<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>Choose switches.</td>
</tr>
<tr>
<td>Query</td>
<td>Runs the query using the set parameters.</td>
</tr>
</tbody>
</table>

Video Diagnostics

CMM provides the following tools to diagnose multicast of video:

- Video Probe Status, page 7-3
- VidMon Flow Status, page 7-4

Video Probe Status

To view Video Probe status:

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

**Step 2** Choose Video Diagnostics.

**Step 3** Choose Video Probe Status.

The Video Probe Status page opens. The Video Probe Status page shows the currently monitored video probes, the number of flows monitored by each probe, and the status indicator for each probe.
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 Flow page for the selected probe appears.

Step 6 To perform multicast trace on one of the Group Ports listed on the Video Probes Flow page, click the IP address of the Group Port.

VidMon Flow Status

To view VidMon Flow Status:

Step 1 From the Multicast Manager menu, choose Diagnostics.

Step 2 Choose Video Diagnostics.

Step 3 Choose Vidmon Flow Status

The Vidmon Flow Status page appears. The Video Flow Status page shows the status of the VidMon devices in the CMM network topology.

Step 4 To view the interfaces on the VidMon device, click the link shown on Video Flow Status page.

The Vidmon Flows Status page appears. The Vidmon Flows Status page shows the status of the current video flow on each interface on the device.
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. The VidMon Interface Flows page shows detailed statistics for the current flows on the interface.

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 the IP address of the Destination Port for the flow.

Step 7 To perform a trace on a unicast flow, click the IP address of the Destination Port for the unicast flow.

Step 8 To view additional details regarding the flow, such as the number of intervals and metrics for the flow, click More in the More Details column.
Figure 7-2  Vidmon Interface Flows Page for a 76xx Device

The Vidmon Interface Flows Page shown in Figure 7-2 indicates flow information for a Cisco 76xx device.

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

- **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 7-3 shows a Vidmon Interface Flows page for an ASR 9000 device.

Figure 7-3  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, choose **Diagnostics**.

**Step 2**  
Choose **Video Diagnostics**.

**Step 3**  
Choose **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.  
The Vidmon Diagnostics page allows you to enter CLI commands to troubleshoot the selected VidMon device.

**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.

**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.

**Step 12**  
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 7-8
- **RP Summary**, page 7-8
- **MSDP Status**, page 7-8
- **Network Status**, page 7-9
- **Locate a Host**, page 7-9
RP Status

To view Rendezvous Point (RP) status:

Step 1  From the Multicast Manager menu, choose Diagnostics.
Step 2  Choose Miscellaneous Diagnostics.
Step 3  Choose RP Status.
        The RP status page appears.
Step 4  From the drop-down list in the Select a Router field, choose a router and click Show.
        The RP status page for the router appears, including RP set and RP state.

RP Summary

To view the RP summary:

Step 1  From the Multicast Manager menu, choose Diagnostics.
Step 2  Choose Miscellaneous Diagnostics.
Step 3  Choose RP Summary.
        The RP Summary page appears.
Step 4  Click an RP link.
        The RP Summary page for the link appears. 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, choose Diagnostics.
Step 2  Choose Miscellaneous Diagnostics.
Step 3  Choose 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.
Step 4: From the MSDP Status page, you choose 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 SA Cache information.

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

Step 6: Choose 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, choose **Diagnostics**.

**Step 2:** Choose **Miscellaneous Diagnostics**.

**Step 3:** Choose **Network Status**.

## Locate a Host

To locate a host:

**Step 1:** From the Multicast Manager menu, choose **Diagnostic**.

**Step 2:** Choose **Miscellaneous Diagnostics**.

**Step 3:** Choose **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, choose **Diagnostics**.

**Step 2:** Choose **Tools**.
**Tools**

**Step 3** Choose IGMP Diagnostics.

**Step 4** On the IGMP Diagnostics page, specify the following settings:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select a Group</td>
<td>Choose a group from the drop-down list.</td>
</tr>
<tr>
<td>Select a Router</td>
<td>Choose one or more routers.</td>
</tr>
<tr>
<td>Select Diagnostic Type</td>
<td>Choose 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, choose Diagnostics.

**Step 2** Choose Tools.

**Step 3** Choose Top Talkers.

**Step 4** On the Top Talkers page, specify the following settings:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLI Access</td>
<td>Allows you to specify the type of CLI access for the operation. The default CLI access method configured for the domain is initially selected. You can choose Telnet, SSH v1, or SSH v2. Choose the type of CLI access enabled on the device.</td>
</tr>
<tr>
<td>Select a Device</td>
<td>Choose 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>Choose 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:
**Diagnostics**

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

**Step 2** Choose **Tools**.

**Step 3** Choose **Health Check**.

**Step 4** Choose 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, choose **Diagnostics**.

**Step 2** Choose **Tools**.

**Step 3** Choose **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, choose **Diagnostics**.

**Step 2** Choose **Tools**.

**Step 3** Choose **6500/7600 Troubleshooting**.

**Step 4** Choose **Full Trace**.

**Step 5** On the Full Trace page, specify the following settings:
Diagnostics

To view 6500/7600 Troubleshooting Diagnostics:

**Step 1** From the Multicast Manager menu, choose **Diagnostics**.
**Step 2** Choose **6500/7600 Troubleshooting**.
**Step 3** Choose **Diagnostics**. On the Diagnostics page, specify the following settings:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select a Device</td>
<td>Choose a device from the drop-down list.</td>
</tr>
<tr>
<td>Source</td>
<td>Choose a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Choose 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>Choose a service type from the drop-down list.</td>
</tr>
<tr>
<td>Run Full Trace</td>
<td>Click the <strong>Run Full Trace</strong> button to launch a full trace.</td>
</tr>
<tr>
<td>CLI Access</td>
<td>Allows you to specify the type of CLI access for the operation. The default CLI access method configured for the domain is initially selected. You can choose <strong>Telnet</strong>, <strong>SSH v1</strong>, or <strong>SSH v2</strong>. Choose the type of CLI access enabled on the device.</td>
</tr>
<tr>
<td>Select a Device</td>
<td>Choose a device from the drop-down list.</td>
</tr>
<tr>
<td>Source</td>
<td>Choose a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Choose 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, choose Diagnostics.
Step 2  Choose 6500/7600 Troubleshooting.
Step 3  Choose Troubleshooting.
Step 4  On the Troubleshooting page, specify the following settings:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLI Access</td>
<td>Allows you to specify the type of CLI access for the operation. The default CLI access method configured for the domain is initially selected. You can choose <strong>Telnet</strong>, <strong>SSH v1</strong>, or <strong>SSH v2</strong>. Choose the type of CLI access enabled on the device.</td>
</tr>
<tr>
<td>Select a Device</td>
<td>Choose a device from the drop-down list.</td>
</tr>
<tr>
<td>Source</td>
<td>Choose a source from the drop-down list.</td>
</tr>
<tr>
<td>Group</td>
<td>Choose 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 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>Command</td>
<td>Choose 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:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>From the Multicast Manager menu, choose <strong>Diagnostics</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Choose <strong>SNMP Utils</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Choose <strong>IGMP Cache</strong>.</td>
</tr>
<tr>
<td>Step 4</td>
<td>On the IGMP Cache page, specify the following settings:</td>
</tr>
</tbody>
</table>

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

To view a PIM neighbor:

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

**Step 2** Choose **SNMP Utils**.

**Step 3** Choose **PIM Neighbors**.

**Step 4** On the PIM Neighbor page, specify the following settings:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select a Device</td>
<td>Choose a device from the drop-down list.</td>
</tr>
<tr>
<td>Select a Neighbor Router</td>
<td>Choose 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 Walker

The SNMP walker gathers the SNMP information and allows you to troubleshoot behavior or verify configuration of devices.

To run the SNMP walker:

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

**Step 2** Choose **Tools**.

**Step 3** Choose **SNMP Walker**.

**Step 4** On the SNMP Walker page, specify the following settings:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLI Access</td>
<td>Specify the type of CLI access for the operation.</td>
</tr>
<tr>
<td></td>
<td>Choose the type of CLI access enabled on the device.</td>
</tr>
<tr>
<td>RO Community String</td>
<td>Enter the SNMP RO community string. You can enter multiple community strings as needed.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> From this release, you can validate the community strings using <strong>Verify</strong> option.</td>
</tr>
<tr>
<td>Select/Edit OID</td>
<td>The default OIDs will be listed. You can select the OID from the default list or add known OIDs.</td>
</tr>
</tbody>
</table>

**Step 5** Click **Submit**.
CMM retrieves a MIB subtree and prints the results to the console.

SNMP PIM Reachability

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

To run the SNMP PIM Reachability tool:

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

**Step 2** Choose **Tools**.

**Step 3** Choose **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, choose the routers to query.
- To choose 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 is 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:

- A specific router
- A transmission stream (TS) using a specified S,G
- A specified receiver

**Device Query**

To track user activities:

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

**Step 2** Choose **Tools**.

**Step 3** Choose **Explicit User Tracking**.

The Explicit User Tracking page for router usage appears.

**Step 4** On the Explicit User Tracking page, specify the following settings:
Stream Query

To query user activity in monitoring a specified TS:

**Step 1** Choose **Explicit User Tracking**.

The Explicit User Tracking page for router usage appears.

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

**Step 3** On the Explicit User Tracking page for stream query, specify the following settings:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLI Access</td>
<td>Allows you to specify the type of CLI access for the operation. The default CLI access method configured for the domain is initially selected. You can choose <strong>Telnet</strong>, <strong>SSH v1</strong>, or <strong>SSH v2</strong>. Choose the type of CLI access enabled on the device.</td>
</tr>
<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, choose a router.</td>
</tr>
<tr>
<td>VLAN Name</td>
<td>From the pull-down menu, choose 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>

---

**Field**

**Description**

CLI Access

Allows you to specify the type of CLI access for the operation. The default CLI access method configured for the domain is initially selected. You can choose **Telnet**, **SSH v1**, or **SSH v2**. Choose the type of CLI access enabled on the device.

Username

Enter the username.

Password

Enter the password for the user.

Source

From the pull-down menu, choose a source.

Group

From the pull-down menu, choose a Group.

Reset SG List

To clear the current S,G information click **Reset SG List**.

Submit

Click **Submit** to submit the request.
Review Draft - Cisco Confidential

Receiver Query

To query user activity in monitoring a specified TS:

---

**Step 1** Choose **Explicit User Tracking**.

The Explicit User Tracking page for router usage appears.

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

**Step 3** On the Explicit User Tracking page for a receiver query, specify the following settings:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLI Access</td>
<td>Allows you to specify the type of CLI access for the operation. The default CLI access method configured for the domain is initially selected. You can choose <strong>Telnet</strong>, <strong>SSH v1</strong>, or <strong>SSH v2</strong>. Choose the type of CLI access enabled on the device.</td>
</tr>
<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, choose **Diagnostics**.

**Step 2** Choose **CRM Diagnostics**.

**Step 3** Choose **Create Baseline**.

**Step 4** On the Create Routing Table Baseline page, specify the following settings:
### Diagnostics

#### CRM Diagnostics

To check a routing table baseline configuration:

**Step 1** From the Multicast Manager menu, choose **Diagnostics**.
**Step 2** Choose **CRM Diagnostics**.
**Step 3** Choose **Check Routing Table**.
**Step 4** On the Check Routing Table Baseline page, specify the following settings:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing Table Type</td>
<td>Choose either <strong>Unicast</strong> or <strong>Multicast</strong>.</td>
</tr>
<tr>
<td>Select a Router</td>
<td>Choose 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 <strong>Run</strong> 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, choose **Diagnostics**.
**Step 2** Choose **CRM Diagnostics**.
**Step 3** Choose **Check Routing Table**.
**Step 4** On the Check Routing Table Baseline page, specify the following settings:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing Table Type</td>
<td>Choose either <strong>Unicast</strong> or <strong>Multicast</strong>.</td>
</tr>
<tr>
<td>Select a Router</td>
<td>Choose a router.</td>
</tr>
<tr>
<td>Baseline</td>
<td>Choose 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>
Configuration Management

This chapter contains the following sections:

- Device Configuration, page 8-1
- MVPN Configuration, page 8-3

Device Configuration

Get All Configurations

To get all configurations:

Step 1 From the Multicast Manager menu, choose Configuration Management.
Step 2 Choose Device Configuration.
Step 3 Choose Get All Configuration.
Step 4 Choose a router.

Note Click Select All to include all listed routers.

Validate All Configurations

To validate all configurations:

Step 1 From the Multicast Manager menu, choose Configuration Management.
Step 2 Choose Device Configuration.
Step 3 Choose Validate All Configurations.
Step 4 Choose a configuration name.
Step 5 Choose a router.
**Note** Click **Select All** to include all listed routers.

**Step 6** Click **View**.

---

### 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, choose **Configuration Management**.

**Step 2** Choose **Device Configuration**.

**Step 3** Choose **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 choose. 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, choose **Configuration Management**.

**Step 2** Choose **Device Configuration**.

**Step 3** Choose **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 choose. The Source Specific Multicast Devices table is populated.
MVPN Configuration

To configure the MVPN service type:

Step 1  From the Multicast Manager menu, choose Configuration Management.
Step 2  Choose MVPN Configuration.
Step 3  Click Add.
Step 4  Choose By MVPN.

The MVPN Configuration configuration page specify the following settings:

<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>Choose the CE Device.</td>
</tr>
<tr>
<td>Save</td>
<td>Adds the MVPN configuration.</td>
</tr>
</tbody>
</table>

By Import

To configure a MVPN:

Step 1  From the Multicast Manager menu, choose Configuration Management.
Step 2  Choose MVPN Configuration.
Step 3  Click the Add button in the MVPN - Service Type Configuration page.
Step 4  Choose By Import.
Step 5  Click the Browse button to upload the CSV file.
Step 6  Choose Merge to unify an existing configuration with the new configuration or choose Replace to overwrite the existing configuration.
Step 7  Click Upload.

Import Format:

<Service Type>#$<Source CE Name>@<Ifindex:ip>§<Destination CE’s name with comma separated>

Example:

mvpn#3845-ce3@4:13.1.2.12§cmm-ce1,cmm-ce2.cisco.com
Administration

System administrators can configure CMM by using CMM Administration.
This chapter contains the following sections:

- Managing Users and Access, page 9-1
- Address Management, page 9-10
- Logging Management, page 9-23
- Warning Page Configuration, page 9-25
- License Info, page 9-26

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 9-1
- Access Control, page 9-3
- Authentication and Audit, page 9-4
- ACS Server, page 9-4

User Configuration

Adding a User Configuration

Step 1  From the Multicast Manager menu, choose Administration.
Step 2  Choose RBAC.
Step 3  Choose User Configuration.
Step 4  Click the Add button.
Step 5 Specify the following settings:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>Enter the username</td>
</tr>
<tr>
<td>Password</td>
<td>Enter a password associated with this username.</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 choosing one or more role from the list.</td>
</tr>
<tr>
<td></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>

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 username and role.

Note Super admin tracks the logs of all guest/local users and has permission to delete the audit logs. The local/guest users do not have permission to delete the audit logs.

Modifying a User File

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

**Step 2** Choose **RBAC**.

**Step 3** Choose **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>

**Step 5** Click **Delete**, **Edit** or **Change Password** to modify the User File.
Unlocking a User ID

After five unsuccessful login attempts, or if the user has not changed their password after 60 days, the user is locked out of the system. You can then unlock the User ID to allow the user to log in again and change the user’s password.

If users have not changed their password within the last 60 days, they are reminded to change their password starting 10 days before the password expiration date.

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

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 username.

Step 2
Check the check box next to the username 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, choose Administration.

Step 2
Choose RBAC.

Step 3
Choose Access Control.

Step 4
Choose 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.
Changing a User Password

If a user forgets their password, is locked out of the system, or does not change their password after 60 days, you can reset the user’s password manually.

To reset a user password:

---

**Step 1** Choose **Administration > RBAC > User Administration**.

**Step 2** On the User Configuration page, check the check box next to the user’s user ID and then click the **Change Password** button.

**Step 3** On the User Administration Screen, enter a new password for the user and then click the **Save** button.

---

### Authentication and Audit

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

**Step 2** Choose **RBAC**.

**Step 3** Choose **Authentication & Audit**.

**Step 4** Choose 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.

**Note**
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, choose **Administration**.

**Step 2** Choose **RBAC**.

**Step 3** Choose **ACS Server**.

**Step 4** Specify the following settings:
ACS 5.x Integration with CMM

This section describes the integration of Cisco Multicast Manager (CMM) with ACS 5.x and contains the following topics:

- Authenticating AAA Users through TACACS+ Using Cisco Secure ACS
- Authenticating AAA Users through RADIUS Using Cisco Secure ACS

Authenticating AAA Users through TACACS+ Using Cisco Secure ACS

This section contains the following topics:

- Creating a New User Group in ACS
- Creating a New User and Adding to a User Group in ACS
- Creating a New Shell Profile in ACS
- Creating an Authorization Policy Rule in ACS

Creating a New User Group in ACS

To create a new user group in ACS:

Step 1 From the Cisco Secure ACS menu, choose Users and Identity Stores > Identity Groups.
Step 2 Click Create to create a new identity group.
   The User Identity Groups page appears.
Step 3 Enter the name and provide a brief description, for example, ‘Create a User Group CMM-Confman’.
Step 4 Click Submit.
   A new user group is created in ACS.
Creating a New User and Adding to a User Group in ACS

To create a new user in ACS and map that user to a user group,

**Step 1** From the Cisco Secure ACS menu, choose **Users and Identity Stores > Internal Identity Stores > Users**.

**Step 2** Click **Create** to create a new user.

**Step 3** Enter values in the mandatory fields such as Name and Password.

**Step 4** Select the group from the Identity Group drop-down list to which you wish to map that user.

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

A new user is created and added to a user group in ACS.

Creating a New Shell Profile in ACS

To create a new shell profile in ACS;

**Step 1** From the Cisco Secure ACS menu, choose **Policy Elements > Authorization and Permissions > Device Administration**.

**Step 2** Click **Create** to create a new shell profile.

**Step 3** Enter the Name and provide a brief description, for example, ‘Create a shell profile Conf Manager’.

**Step 4** Click the **Custom Attributes** tab.

If you click the **Add** button you can manually add Role, Tasks and Virtual Domain for TACACS+ Custom Attributes one after another.

**Step 5** Follow the steps listed below to add Custom Attributes:

a. Type “priv-lvl” in the Attribute field

b. Type “1” in the Value field.

Please refer to the following table to understand the role combinations and the corresponding privilege value.

<table>
<thead>
<tr>
<th>Possible Role Combinations</th>
<th>Privilege Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NETWORK_ADMIN</td>
<td>1</td>
</tr>
<tr>
<td>SYS_ADMIN</td>
<td>2</td>
</tr>
<tr>
<td>NETWORK_ADMIN,SYSADMIN</td>
<td>3</td>
</tr>
<tr>
<td>OPERATOR</td>
<td>4</td>
</tr>
<tr>
<td>NETWORK_ADMIN,OPERATOR</td>
<td>5</td>
</tr>
<tr>
<td>SYSADMIN,OPERATOR</td>
<td>6</td>
</tr>
<tr>
<td>NETWORKADMIN,MACADMIN,OPERATOR</td>
<td>7</td>
</tr>
<tr>
<td>HELPDESK</td>
<td>8</td>
</tr>
<tr>
<td>NETWORK_ADMIN,HELPDESK</td>
<td>9</td>
</tr>
<tr>
<td>SYSADMIN,HELPDESK</td>
<td>10</td>
</tr>
<tr>
<td>NETWORK_ADMIN,SYSADMIN,HELPDESK</td>
<td>11</td>
</tr>
</tbody>
</table>
**Review Draft - Cisco Confidential**

### Chapter 9      Administration

#### Managing Users and Access

**c.** Click **Add** to add the custom attribute.

**Step 6** Add the "virtual domain" attribute at the end of TACACS+ Custom attribute.

**Note** To log in, the Virtual Domain custom attributes must be exported to the TACACS+ server.

A new shell profile is created in ACS.

**Creating an Authorization Policy Rule in ACS**

To create an authorization policy rule in ACS:

**Step 1** From the Cisco Secure ACS menu, choose **Access Policies > Access Services > Default Device Admin > Authorization**.

**Step 2** On the Device Administration Authorization Policy page, click **Create** to create a rule.

**Step 3** Enter a name in the Name field.

**Step 4** From the Status drop-down list, choose **Enabled**.

**Step 5** Check the **Identity Group** check box. Click **Select** to select the required Identity Group.

See **Creating a New User Group in ACS** for information on creating Identity User Groups.

**Step 6** Check the **Protocol** check box. Click **Select** to select **TACACS**.

**Step 7** Choose the Shell Profile by clicking the select button against it.

See **Creating a New Shell Profile in ACS** for information on creating a new shell profile.

**Step 8** Click **OK** to save the Authorization rule.

Once it is configured you can test the authentication and confirm with the number of hit counts.

**Hit counts** — Displays the number of times a rule matched an incoming request since the last reset of the policy’s hit counters. ACS counts hits for any monitored or enabled rule whose conditions all matched an incoming request.

**Step 9** Log out of CMM.

**Step 10** Log in again into CMM as an AAA user, defined in ACS.

An Authorization Policy Rule is created in ACS.

**Note** **First-Match Rule Tables**: Cisco ACS 5.1 provides policy decisions by using first-match rule tables to evaluate a set of rules. Rule tables contain conditions and results. Conditions can be either simple or compound. Simple conditions consist of attribute operator value which is either true or false. Compound conditions contain more complex conditions combined with AND or OR operators.
Review Draft - Cisco Confidential

The default rule specifies the policy result that ACS uses, when no other rules exist, or when the attribute values in the access request do not match any rules.

Authenticating AAA Users through RADIUS Using Cisco Secure ACS

This section contains the following topics:

- Adding CMM as an AAA client in ACS
- Creating a New User Group in ACS
- Creating a New User and Adding to a User Group in ACS
- Creating a New Authorization Profile in ACS
- Creating an Authorization Policy Rule in ACS

Adding CMM as an AAA client in ACS

To add CMM as an AAA client in ACS:

Step 1  From the Cisco Secure ACS menu, choose Network Resources > Network Devices and AAA Clients.
Step 2  Click Create.
Step 3  Enter the details in the respective fields as shown below:
   - Name - The name of the AAA Client.
   - Description - A brief description about the AAA client.
   - IP Address - Click the Single IP Address radio-button and enter CMM server IP address in the IP address field. For example, enter 10.77.240.235 as the IP address.
   - Under Authentication Options, check the RADIUS checkbox to enable the RADIUS.
   - Enter a Shared Secret in the Shared Secret box.
Step 4  Click Submit.

CMM is added as an AAA client in ACS.

Creating a New User Group in ACS

To create a new Identity Group in ACS, see Creating a New User Group in ACS.

Creating a New User and Adding to a User Group in ACS

To create a new user and adding to a user group, see Creating a New User and Adding to a User Group in ACS.

Creating a New Authorization Profile in ACS

To create a new Authorization Profile in ACS;
**Review Draft - Cisco Confidential**

**Step 1** From the Cisco Secure ACS menu, choose **Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles**.

**Step 2** Click **Create**.

**Step 3** Enter a name in the Name field.

**Step 4** Provide a brief description in the description field. For example, ‘Create an Authorization profile Config Manager’.

**Step 5** Click the **RADIUS Attributes** tab.

   If you click the **Add** button you can manually add Role, Tasks and Virtual Domain for RADIUS Attributes one after another.

**Step 6** To add RADIUS Attributes:

   a. Select Dictionary type as **RADIUS-Cisco**.
   b. Select RADIUS attribute as **priv-lvl**.
   c. Select Attribute Type as **String**.
   d. Select Attribute Value as **Static**.
   e. Enter "1" as the RADIUS Attribute value in the text box.
   f. Click **Add** to add the RADIUS attribute.

**Step 7** Add the "virtual domain" attribute at the end of RADIUS attribute.

---

**Note**

To log in, the Virtual Domain custom attributes must be exported to the RADIUS server.

**Note**

Unlike ACS 4, it is not possible to copy and paste the list of attributes from the Cisco CMM GUI to ACS 5 GUI. In ACS 5 they must be entered one by one.

A new Authorization Profile is created in ACS.

---

**Creating an Authorization Policy Rule in ACS**

To create an authorization policy rule in ACS:

**Step 1** From the Cisco Secure ACS menu, choose **Access Policies > Access Services > Default Device Admin > Authorization**.

**Step 2** On the Device Administration Authorization Policy page, click **Create** to create a rule.

**Step 3** Enter a name in the Name field.

**Step 4** From the Status drop-down list, choose **Enabled**.

**Step 5** Check the **Identity Group** check box. Click **Select** to select the required Identity Group.

See **Creating a New User Group in ACS** for information on creating Identity User Groups.

**Step 6** Check the **Protocol** check box. Click **Select** to select **Radius**.

**Step 7** Choose the Authorization check box by clicking the select button against it.
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 9-11
- Transport Description, page 9-14
- Managing the Ad Zone Database, page 9-16
- Managing the Channel Map Database, page 9-18

Note

First-Match Rule Tables: Cisco ACS 5.1 provides policy decisions by using first-match rule tables to evaluate a set of rules. Rule tables contain conditions and results. Conditions can be either simple or compound. Simple conditions consist of attribute operator value which is either true or false. Compound conditions contain more complex conditions combined with AND or OR operators.

The default rule specifies the policy result that ACS uses, when no other rules exist, or when the attribute values in the access request do not match any rules.

An Authorization Policy Rule is created in ACS.

Timeout Configuration

To change the session timeout settings:

Step 1  From the Multicast Manager menu, choose Administration.
Step 2  Choose RBAC.
Step 3  Choose Timeout Configuration.
Step 4  Enter the amount of time in minutes.
Step 5  Click Save.
Note
The database is already populated with all of the reserved address space.

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, choose Administration.

Step 2
Choose Address Management.

Step 3
Choose Destination Address Database.

The Destination Address Database page appears. This page lists the default and configured Destination addresses.

Step 4
Choose By Address from the Add drop-down list.

Note
You can also import an address file by choosing By Import from the Add button. Browse to the file location and choose Upload.

Step 5
Specify the following settings:

<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, choose a zone from the drop-down list.</td>
</tr>
<tr>
<td>Mux ID</td>
<td>If you have entered data for the Mux ID database, choose 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.

By Import

To import an address file:
Step 1  From the Multicast Manager menu, choose Administration.
Step 2  Choose Address Management.
Step 3  Choose Destination Address Database.
Step 4  Click the Add button in the Destination Address Database page.
Step 5  Choose By Import.
Step 6  Click the Browse button to upload the CSV file.
Step 7  Choose Merge to unify an existing configuration with the new configuration or choose Replace to overwrite the existing configuration.
Step 8  Click Upload.

Import Format:
address_db@<destination ip>,<destination description>,<Ad Zone>,<Mux No>

Example:
address_db@224.0.2.1,Description,zone1,1000

Note  To add AD Zone and MUX no., first you need to add entries in AD Zone Database and Multiplex Table Database.

Modifying a Destination Address

Step 1  From the Multicast Manager menu, choose Administration.
Step 2  Choose Address Management.
Step 3  Choose 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.
Step 6  Edit the following settings as required:

<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>Choose a zone from the drop-down list.</td>
</tr>
<tr>
<td>Mux ID</td>
<td>Choose 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>

Note  To delete a file, click the Actions button and choose Delete from the drop-down menu.
To export a file, click the Actions button and choose 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, choose Administration.

**Step 2**
Choose Address Management.

**Step 3**
Choose Source Description.

**Step 4**
Choose By Source Address from the Add drop-down list.

**Note**
You can also import an address file by choosing By Import from the Add button. Browse to the file location and choose Upload.

**Step 5**
Specify the following settings:

<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.

**By Import**

To import an address file:

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

**Step 2**
Choose Address Management.
Review Draft - Cisco Confidential

Address Management

Step 3 Choose Source Description.
Step 4 Click the Add button in the Address - Source Database page.
Step 5 Choose By Import.
Step 6 Click the Browse button to upload the CSV file.
Step 7 Choose Merge to unify an existing configuration with the new configuration or choose Replace to overwrite the existing configuration.
Step 8 Click Upload.

Import Format:
address_source@<source_ip>,<source_description>

Example:
address_source@12.23.34.56,source1

Modifying a Source Address or Description

To modify a source address:

Step 1 From the Multicast Manager menu, choose Administration.
Step 2 Choose Address Management.
Step 3 Choose 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 choose 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.

This section contains the following topics:
- Adding a Transport Description
- Modifying a Transport Description
Review Draft - Cisco Confidential

Chapter 9  Administration

Address Management

Adding a Transport Description

To add a transport description:

Step 1  From the Multicast Manager menu, choose Administration.
Step 2  Choose Address Management.
Step 3  Choose Transport Description.
Step 4  Click the Add button.
Step 5  From the drop-down list, choose By Transport Description.

Note  You can also import an address file by choosing By Import from the Add button. Browse to the file location and choose Upload.

Step 6  Specify the following settings:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP Address</td>
<td>Enter the IP address of the source.</td>
</tr>
<tr>
<td>Group IP Address</td>
<td>Enter the IP address for the group.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the TS.</td>
</tr>
<tr>
<td>Save</td>
<td>Apply the new address to the database.</td>
</tr>
</tbody>
</table>

By Import

To import an address file:

Step 1  From the Multicast Manager menu, choose Administration.
Step 2  Choose Address Management.
Step 3  Choose Transport Description.
Step 4  Click the Add button in the Transport Description page.
Step 5  Choose By Import.
Step 6  Click the Browse button to upload the CSV file.
Step 7  Choose Merge to unify an existing configuration with the new configuration or choose Replace to overwrite the existing configuration.
Step 8  Click Upload.

Import Format:

address_sgdesc@<Source Ip>,<Destination IP>,<Transport Description>

Example:
Modifying a Transport Description

To modify a transport description:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>From the Multicast Manager menu, choose Administration.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Choose Address Management.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Choose Transport Database.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Check the check box next to the IP address for the transport description that you want to modify.</td>
</tr>
<tr>
<td>Step 5</td>
<td>If you want to delete the transport description, click the Actions button and choose Delete from the pull-down menu.</td>
</tr>
<tr>
<td>Step 6</td>
<td>To edit the transport description information:</td>
</tr>
<tr>
<td></td>
<td>a. Click the Edit button.</td>
</tr>
<tr>
<td></td>
<td>b. Modify the Description field as required</td>
</tr>
<tr>
<td></td>
<td>c. Click the Save button.</td>
</tr>
</tbody>
</table>

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.

This section contains the following topics:

- Adding a Zone
- Modifying a Zone

Adding a Zone

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>From the Multicast Manager menu, choose Administration.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Choose Address Management.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Choose Ad Zone Database.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Choose By Zone from the Add drop-down list.</td>
</tr>
</tbody>
</table>

**Note** You can also import a file by choosing By Import from the Add button. Browse to the file location and choose Upload.

| Step 5 | Specify the following settings:                                                             |
By Import

To import a Zone database file:

Step 1  From the Multicast Manager menu, choose Administration.
Step 2  Choose Address Management.
Step 3  Choose Ad Zone Database.
Step 4  Click the Add button in the Ad Zone Database page.
Step 5  Choose By Import.
Step 6  Click the Browse button to upload the CSV file.
Step 7  Choose Merge to unify an existing configuration with the new configuration or choose Replace to overwrite the existing configuration.
Step 8  Click Upload.

Import Format:

address_zone@<Zone No>,<Zone Name>

Example:

address_zone@123,zone1

Modifying a Zone

Step 1  From the Multicast Manager menu, choose Administration.
Step 2  Choose Address Management.
Step 3  Choose Ad Zone Database.
Step 4  Click the Edit button.
Step 5  Edit the following settings as required:

<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.

This section contains the following topics:
- Adding a Channel
- Modifying a Channel

Adding a Channel

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

**Step 2**  Choose **Address Management**.

**Step 3**  Choose **Channel Map Database**.

**Step 4**  Choose **By Channel** from the Add drop-down list.

**Note**  You can also import a file by choosing **By Import** from the Add button. Browse to the file location and choose **Upload**.

**Step 5**  Specify the following settings:

<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, choose 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, choose the screen format for the channel.</td>
</tr>
<tr>
<td>Service Type</td>
<td>From the drop-down list in the Service Type field, choose 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.

### By Import

To import a Channel database file:

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

**Step 2** Choose Address Management.

**Step 3** Choose Channel Map Database.

**Step 4** Click the Add button in the Channel Database page.

**Step 5** Choose By Import.

**Step 6** Click the Browse button to upload the CSV file.

**Step 7** Choose Merge to unify an existing configuration with the new configuration or choose Replace to overwrite the existing configuration.

**Step 8** Click Upload.

**Import Format:**

```
address_channel@<Channel Number>,<Channel Name>,<short Name>,<Codec Type>,<Screen Format>,<Service Type>
```

Where

- Codec types are: MPEG-2, MPEG-4, H.264, FLV, WM, REAL, 3GPP, Other.
- Screen Formats are: Widescreen, 4:3, CIF, 56, Other.
- Service Types are: SIM, SDV, OD, DT, AN, MC, Other.

**Example:**

```
address_channel@12345,sunTV,sun,MPEG-2,Widescreen,SIM
```

### Modifying a Channel

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

**Step 2** Choose Address Management.

**Step 3** Choose Channel Map Database.

**Step 4** Check the check box next to the channel number that you want to modify.

**Step 5** Click the Edit button.

**Step 6** Edit the following settings as required:
### Address Management

#### Adding a Record to the Multiplex Table Database

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

**Step 2**  Choose **Address Management**.

**Step 3**  Choose **Multiplex Table Database**.

**Step 4**  Choose **By Mux** from the **Add** drop-down list.

**Note**  You can also import a file by choosing **By Import** from the **Add** button. Browse to the file location and choose **Upload**.

**Step 5**  Specify the following settings:

<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, choose 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, choose the screen format for the channel.</td>
</tr>
<tr>
<td>Service Type</td>
<td>From the drop-down list in the Service Type field, choose the service type for the channel.</td>
</tr>
<tr>
<td>Add/Modify</td>
<td>Apply the changes to the record in the database.</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.

This section contains the following topics:

- **Adding a Record to the Multiplex Table Database**
- **Modifying a Record in the Multiplex Table Database**
### By Import

To import a file:

1. From the Multicast Manager menu, choose **Administration**.
2. Choose **Address Management**.
3. Choose **Multiplex Table Database**.
4. Click the **Add** button in the **Multiplex Database** page.
5. Choose **By Import**.
6. Click the **Browse** button to upload the CSV file.
7. Choose **Merge** to unify an existing configuration with the new configuration or choose **Replace** to overwrite the existing configuration.
8. Click **Upload**.

**Import Format:**

```
address_mux@<Mux Number>,<Channel Number>,<Channel Name>,<Program Id>
```

**Example:**

```
address_mux@1000000,12345,sunTV,1234
```

**Note**  
Add the Channel Map Database before proceeding for mapping.

### Modifying a Record in the Multiplex Table Database

1. From the Multicast Manager menu, choose **Administration**.
2. Choose **Address Management**.
3. Choose **Multiplex Table Database**.
4. Check the check box next to the record that you want to modify.
5. Click the **Edit** button.
Step 6  Edit the following settings as required:

<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>Choose 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 choose **Delete** from the drop-down menu.

**Note**
To export a file, click the **Actions** button and choose **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 choosing the **Import** button.

See **Importing Data**, page 9-23.

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.

See **Exporting Data**, page 9-22.

---

**Exporting Data**

To export address management data:

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

Step 2  Choose **Address Management**.

Step 3  Choose **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**

To import address management data:

**Step 1** From the Multicast Manager menu, choose **Administration**.
**Step 2** Choose **Address Management**.
**Step 3** Choose **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 choose the file.
**Step 6** Click the **Upload** button.
CMM imports the address management data.

**Note**

You should give all details in the address management before going for Address Management Export option. These exported address management details can be imported to another server for reusability. This eliminates the overhead of exporting the data from individual databases.

**Log Management**

**Logging Management**

To manage the different types of logs:

**Step 1** From the Multicast Manager menu, choose **Administration**.
**Step 2** Choose **Log Management**.
**Step 3** Choose **Logging Management**.
**Step 4** Specify the following settings:
Audit Log

Use the Audit Log feature to view Audit Log messages. To view audit log messages:

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

**Step 2** Choose **Log Management**.

**Step 3** Choose **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.

Debug Settings

In CMM, the logging level can be set to info, warn or debug mode.

Navigate to **Administration > Log Management > Debug settings**, to set the following logs:

- UI Log—security.log, audit.log, controller.log, crmcontroller.log, spring.log
  pollConfigResults.log, cliInfo.log,service.log, discovery.log, cmmWebservice.log
- Database Logs—persistence.log, profiler.log, hibernate.log
- Performance Logs—purge.log
License Logs
SNMP Logs
Topology Logs

Note
By default the logs are set to warn mode.

Warning Page Configuration

The Warning Page Configuration feature allows you to configure an alert page that appears when user log into CMM. If no Warning Page configuration is enabled, then no warning page appears when users log in.

To configure a Warning Page:

Step 1  Choose Administration.
Step 2  Choose Warning Page.

The Warning Page configuration page appears.

Step 3  Specify the following settings:
The License Info page allows you to view your existing FlexLm licenses and update them as required. For a detailed description of how CMM licensing works, see “Licensing,” in Chapter 1 of the *Installation Guide for Cisco Multicast Manager*, “Installing Cisco Multicast Manager.”

To view license information and change it as required:

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

**Step 2** Choose **License Info**.

**Step 3** On the License Information page, specify the following settings:

<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>Host ID</td>
<td>Indicates the host ID for the license. If the license is an evaluation license, the host ID is ANY.</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>

**Step 4** To update the license(s) complete the following steps:

a. Click the **Update License** button.
You are prompted to choose a file to upload.

b. Click the **Browse** button and then browse for a license that you have saved on the CMM server.

For information on obtaining a CMM license, see For a detailed description of how CMM licensing works, see “Obtaining a CMM License,” in Chapter 1 of the *Installation Guide for Cisco Multicast Manager*, “Installing Cisco Multicast Manager.”

c. Choose the license file and then click the **Upload** button.

CMM uploads the license and validates it.

---

The following features in CMM require a MVPN license:

- MVPN Polling
- MVPN Diagnostics
- MVPN Configuration
- P2MP Trace

---

**Note**

In the CMM dashboard, the MVPN Events tab will be shown only if a MVPN license is available.

The following features in CMM require a VOS license:

- Vidmon device and Video probe Discovery
- Vidmon Polling
- Video probe Polling
- Video Diagnostics

---

**Note**

In the CMM dashboard, the Video Events tab will be shown only if a VOS license is available.
System Configuration

This chapter contains the following sections:

- Set Up Trace by Management IP Address (Optional), page 10-1
- Domain Management, page 10-2
- Global Polling Configuration, page 10-6

Set Up Trace by Management IP Address (Optional)

The trace function in CMM 3.1 and previous releases required access to the PIM interface of the device. From CMM 3.2, trace functionality is available in the multicast network even if the PIM interface is not accessible. This is an optional configuration in the event that in your network PIM interface access is restricted across particular points. In most cases, you can use the default setting (trace using PIM interface IP address).

Note

The feature is domain specific. The same router can be in multiple domains with some domains using autodiscovery and PIM interfaces for CMM multicast trace and other domains using IP Management addresses for CMM multicast trace.

The Trace by IP Management Address feature is implemented in two files:

- The `multicast_trace_type.properties` file—A trace configuration file that specifies whether CMM uses the IP management address of the device or the PIM neighbor address of the device to perform a trace. See Coding the `multicast_trace_type.properties` File, page 10-2.
- A CSV file that you provide to list the Management IP addresses and associated SNMP community strings for the devices you will manage using the feature. See Coding a CSV File to Provide Management IP Addresses, page 10-2.

Implementing Discovery for Trace by Management IP Address

To use the Trace by IP Management Feature, you must perform Discovery using the Contiguous Discovery by Import setting. For information on this setting, see Contiguous Discovery by Import, page 5-12.
Coding the *multitrace_type.properties* File

The *multicasttrace_type.properties* file is located in the following directory:

`CMMROOT/mmtsys/sys`

Example 10-1 shows a sample *multicasttrace_type.properties* file.

**Example 10-1 Sample multicasttrace_type.properties File**

```
#************************************************
#         Copyright (c) 2010 Cisco Systems, Inc.
#         All rights reserved.
#************************************************

# Give 1 -> for Trace using management Ip address and 0 -> for PIM interface ip address
useManagementIp=0

If you need to change the default trace functionality, edit this file to specify the type of trace functionality your CMM installation uses. To specify:

- Trace using IP management address - set `useManagementIp=1`
- Trace using PIM interface IP address - set `useManagementIp=0`

In the example above, trace functionality is set to use the PIM interface IP address. In the CMM trace page, trace functionality shows the same output for both types of trace.

Coding a CSV File to Provide Management IP Addresses

If you are using the Trace by IP Management address feature, then before you perform device discovery, you must code a comma-separated value (CSV) file that provides the management IP address and associated SNMP community string for each device in your multicast network.

The CSV file has the following format:

`<ip address>, <snmp community string>`

Example 10-2 shows a sample CSV file.

**Example 10-2 Sample CSV file for a Domain Using Management by IP Address**

```
10.1.255.1, snmp-ro
10.1.255.1, snmp-ro
```

Domain Management

The first step in CMM for monitoring the multicast network is to create a domain. A domain is the grouping that you assign to the multicast network. A domain can include Layer 2 (L2) devices, Layer 3 (L3) devices, video probes, 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 the domain and setting the configuration manually.
  See Creating a Domain, page 10-3.
- By importing an existing domain configuration from a comma-separated value (CSV) file.
  See Importing a Domain, page 10-6.
Creating a Domain

To create a domain:

**Step 1**  
From the Multicast Manager menu, choose **System Configuration**.

**Step 2**  
Select **Domain Management**.  
The Domain Management Summary page appears.

The Domain Management Summary page contains all the domain information specific to the server and also indicates whether the domains in the server are discovered. Click **Start Discovery** to discover the domains that are undiscovered. To re-discover the previously discovered domains, click 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 and click **Edit**.

The System Configuration page contains the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Management Domain Name | A management domain is defined as a contiguous group of PIM neighbors sharing the same SNMP community string.  
                         The domain name that you specify can contain alphanumeric characters and underscores (_). |
| Read Only            | Specify the SNMP read-only community string.  
                         Also specify the same string in the “verify” field.  
                         This string is required for retrieving device configurations. |
| Read Write           | Specify the SNMP read-write community string.  
                         Specify the same string in the “verify” field.  
                         This string is required to write any configuration settings to the device. |
| SNMP Timeout         | Retry period if the node does not respond. You can set the SNMP Timeout value based on the optimum value required for your network. The default value is 0.8. |
| SNMP Retries         | Number of retries to contact a node before issuing a timeout. You can set the SNMP Retries value based on the optimum value required for your network. The default value is 2. |
| TFTP Server          | Specify the TFTP server IP address. The default is the IP address of the Cisco Multicast Manager server. |
| VTY Password         | Enter the device password to communicate with the devices in the domain. This password will be used for all CLI communication for this domain. |
### Domain Management

**Enable Password**
Enter the password and verify the password. The application will use this value for execution of some CLI commands over non-VRF aware devices.

**TACACS/RADIUS Username**
If a TACACS/RADIUS server is used to authenticate users, enter a username here. If you plan to use Core/Enterprise Discovery/Core + CE discovery or Distributed Network Discovery/P2MP to discover your network, you must enter a TACACS+ username and password.

- **Note** When the network consists of XR-IOS (ASR9K devices), TACACS+ username and password are not required.

- **Note** 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.

**TACACS/RADIUS Password**
If you are using TACACS/RADIUS, you can enter a password here. If you plan to use Core/Enterprise Discovery/Core + CE discovery or Distributed Network Discovery/P2MP to discover your network, you must enter a TACACS+ username and password.

- **Note** When the network consists of XR-IOS (ASR9K devices), TACACS+ username and password are not required.

- **Note** 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.

**CLI Access**
Select *Telnet*, *SSH v1*, or *SSH v2*.

Based on this selection, CMM will use Telnet, SSH v1, or SSH v2 to communicate to the devices on this domain. You can change the CLI access method on several CMM pages that issue CLI commands, as required for the device that CMM needs to communicate with.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 a TACACS/RADIUS server is used to authenticate users, enter a username here. If you plan to use Core/Enterprise Discovery/Core + CE discovery or Distributed Network Discovery/P2MP to discover your network, you must enter a TACACS+ username and password.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Note</strong> When the network consists of XR-IOS (ASR9K devices), TACACS+ username and password are not required.</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 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. If you plan to use Core/Enterprise Discovery/Core + CE discovery or Distributed Network Discovery/P2MP to discover your network, you must enter a TACACS+ username and password.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Note</strong> When the network consists of XR-IOS (ASR9K devices), TACACS+ username and password are not required.</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 <em>Telnet</em>, <em>SSH v1</em>, or <em>SSH v2</em>. Based on this selection, CMM will use Telnet, SSH v1, or SSH v2 to communicate to the devices on this domain. You can change the CLI access method on several CMM pages that issue CLI commands, as required for the device that CMM needs to communicate with.</td>
</tr>
</tbody>
</table>
**Chapter 10      System Configuration**

**Domain Management**

**Step 5**
Complete the fields in the System Configuration page and click **Save** and then **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.

**Step 7**
For information on the Multicast Discovery page and discovering a domain, see **Multicast Discovery**, page 5-2.

---

**Rediscovering a Domain**

On the Domain Management page, 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.

---

### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
<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>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 than 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>
<tr>
<td>Auto L2 Discovery</td>
<td>Check the <strong>Auto L2 Discovery</strong> check box to automatically discover Layer 2 devices in your network.</td>
</tr>
</tbody>
</table>
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 5-2.

**Importing a Domain**

To import a domain:

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

**Import Format:**

<Domain Name>,<ROString>,<RWString>,<SNMP Timeout>,<SNMP Retries>,<TFTP Server>,<Enable password>,<Device User Name>,<Device Password>,<CLI Access option>,<CLI Threshold Polling Enable/Disable>,<TACACS cache Enable/Disable>,<SG cache Enable/Disable>,<Auto L2 Discovery Enable/Disable>

**Example:**

CMM,public,,0.8,2,172.20.111.233,null,,,Telnet,false,false,false,false,true

**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:

1. From the Multicast Manager menu, choose System Configuration.
2. Select Global Polling Configuration.
   
   The Global Polling Configuration page appears.

3. On the top part of the Global Polling Configuration page, configure polling intervals and run times for each type of polling, as shown in the following table.
### Global Polling Configuration

#### Note
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>Checking the <strong>Use Defaults</strong> check box sets all the start and stop times, and days to the default values.</td>
</tr>
<tr>
<td>DR Polling Interval</td>
<td>Enter the polling interval to check the status of all DRs in the network. If a DR is changed, CMM polling alerts CMM users.</td>
</tr>
<tr>
<td>Layer 2 Polling Interval</td>
<td>Enter the polling interval to monitor the routing table when creating baselines.</td>
</tr>
<tr>
<td>Route Monitor Polling Interval</td>
<td>Enter the polling interval to monitor specific multicast routes.</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>Enter the polling interval to monitor the number of Multicast Groups present on an RP, and so on.</td>
</tr>
<tr>
<td>RP Status Polling Interval</td>
<td>Enter the polling interval for RP Status Polling. RP status polling queries the <code>sysUpTime</code> 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 <code>rpReachable</code> trap is sent. If the RP does not respond, an <code>rpUnreachable</code> 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 every configured source and group, to check on 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. CMM will ensure that no thresholds are exceeded.</td>
</tr>
<tr>
<td>Multicast Topology Polling Interval</td>
<td>Topology polling queries the <code>sysUpTime</code> 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 <code>ifIndexes</code> 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>
</tbody>
</table>
## Global Polling Configuration

<table>
<thead>
<tr>
<th>Field or Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
<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. Note If you are monitoring 1000 or more flows, We recommend 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 opens..
**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.
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/E-mail 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/E-mail Polling Configuration page.
<table>
<thead>
<tr>
<th>Index</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td></td>
</tr>
<tr>
<td>Access Control</td>
<td>9-3</td>
</tr>
<tr>
<td>ACS Server</td>
<td>9-4</td>
</tr>
<tr>
<td>Adding a Channel</td>
<td>9-18</td>
</tr>
<tr>
<td>Adding an Address</td>
<td>9-11</td>
</tr>
<tr>
<td>Adding a Record to the Multiplex Table Database</td>
<td>9-20</td>
</tr>
<tr>
<td>Adding a User Configuration</td>
<td>9-1</td>
</tr>
<tr>
<td>Adding a Zone</td>
<td>9-16</td>
</tr>
<tr>
<td>Address Management</td>
<td>9-10</td>
</tr>
<tr>
<td>All Device Information</td>
<td>6-2</td>
</tr>
<tr>
<td>Authentication &amp; Audit</td>
<td>9-4</td>
</tr>
<tr>
<td>B</td>
<td></td>
</tr>
<tr>
<td>By Device</td>
<td>4-7</td>
</tr>
<tr>
<td>By S,G</td>
<td>4-6</td>
</tr>
<tr>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Check Routing Table</td>
<td>7-19</td>
</tr>
<tr>
<td>CMM</td>
<td></td>
</tr>
<tr>
<td>logging in</td>
<td>2-1</td>
</tr>
<tr>
<td>cmm_cm1</td>
<td>8-1</td>
</tr>
<tr>
<td>cmm_pc10</td>
<td>4-12</td>
</tr>
<tr>
<td>Config L2 Polling</td>
<td>4-13, 4-21</td>
</tr>
<tr>
<td>Config S,G Polling</td>
<td>4-6</td>
</tr>
<tr>
<td>Config Tree Polling</td>
<td>4-21</td>
</tr>
<tr>
<td>Configure Health Check Polling</td>
<td>4-34</td>
</tr>
<tr>
<td>Configure Interface Polling</td>
<td>4-16</td>
</tr>
<tr>
<td>Configure MVPN Polling</td>
<td>4-47</td>
</tr>
<tr>
<td>Configure Route Polling</td>
<td>4-50</td>
</tr>
<tr>
<td>Configure RPF Polling</td>
<td>4-29</td>
</tr>
<tr>
<td>Configure RP Polling</td>
<td>4-26</td>
</tr>
<tr>
<td>Configure Tree Polling</td>
<td>4-21</td>
</tr>
<tr>
<td>Configure Unicast Polling</td>
<td>4-53</td>
</tr>
<tr>
<td>Configure Video Probe Polling</td>
<td>4-37</td>
</tr>
<tr>
<td>Configuring L2 Polling</td>
<td>4-13</td>
</tr>
<tr>
<td>Create Baseline</td>
<td>7-18</td>
</tr>
<tr>
<td>creating domains</td>
<td>10-3</td>
</tr>
<tr>
<td>D</td>
<td></td>
</tr>
<tr>
<td>Device Configuration</td>
<td>8-1</td>
</tr>
<tr>
<td>Domain Management</td>
<td>10-2</td>
</tr>
<tr>
<td>domains</td>
<td></td>
</tr>
<tr>
<td>creating</td>
<td>10-3</td>
</tr>
<tr>
<td>Domain Trap/Email</td>
<td>4-3</td>
</tr>
<tr>
<td>E</td>
<td></td>
</tr>
<tr>
<td>Event Viewer</td>
<td>4-1</td>
</tr>
<tr>
<td>Export &amp; Import</td>
<td>9-22</td>
</tr>
<tr>
<td>F</td>
<td></td>
</tr>
<tr>
<td>Full Trace</td>
<td>7-11</td>
</tr>
<tr>
<td>G</td>
<td></td>
</tr>
<tr>
<td>Get All Configurations</td>
<td>8-1</td>
</tr>
<tr>
<td>Global Polling Configuration</td>
<td>10-6</td>
</tr>
<tr>
<td>H</td>
<td></td>
</tr>
<tr>
<td>Health Check</td>
<td>4-33, 7-10</td>
</tr>
<tr>
<td>Index</td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td></td>
</tr>
<tr>
<td><strong>Health Check Failed Report</strong></td>
<td>4-33</td>
</tr>
<tr>
<td><strong>MVVPN</strong></td>
<td>7-11</td>
</tr>
<tr>
<td><strong>MVVPN Configuration</strong></td>
<td>8-3</td>
</tr>
<tr>
<td><strong>IGMP Cache</strong></td>
<td>7-14</td>
</tr>
<tr>
<td><strong>IGMP Diagnostics</strong></td>
<td>7-9</td>
</tr>
<tr>
<td><strong>Interface Polling</strong></td>
<td>4-15</td>
</tr>
<tr>
<td><strong>interface polling</strong></td>
<td>4-15</td>
</tr>
<tr>
<td><strong>L2 Discovery</strong></td>
<td>5-17</td>
</tr>
<tr>
<td><strong>L2 Host IPs</strong></td>
<td>7-3</td>
</tr>
<tr>
<td><strong>L2 Multicast Information</strong></td>
<td>7-2</td>
</tr>
<tr>
<td><strong>L2 polling</strong></td>
<td>4-12</td>
</tr>
<tr>
<td><strong>License Information</strong></td>
<td>9-26</td>
</tr>
<tr>
<td><strong>Local Host</strong></td>
<td>7-9</td>
</tr>
<tr>
<td><strong>logging into CMM</strong></td>
<td>2-1</td>
</tr>
<tr>
<td><strong>Logging Management</strong></td>
<td>9-23</td>
</tr>
<tr>
<td><strong>Managing the Ad Zone Database</strong></td>
<td>9-16</td>
</tr>
<tr>
<td><strong>Managing the Channel Map Database</strong></td>
<td>9-18</td>
</tr>
<tr>
<td><strong>Managing the Multiplex Table Database</strong></td>
<td>9-20</td>
</tr>
<tr>
<td><strong>Managing Users &amp; Access</strong></td>
<td>9-1</td>
</tr>
<tr>
<td><strong>MDT Default Report</strong></td>
<td>4-44</td>
</tr>
<tr>
<td><strong>MDT Source Report</strong></td>
<td>4-43</td>
</tr>
<tr>
<td><strong>Miscellaneous Diagnostics</strong></td>
<td>7-7</td>
</tr>
<tr>
<td><strong>Modifying a Channel</strong></td>
<td>9-19</td>
</tr>
<tr>
<td><strong>Modifying an Address</strong></td>
<td>9-12</td>
</tr>
<tr>
<td><strong>Modifying a Record in the Multiplex Table Database</strong></td>
<td>9-21</td>
</tr>
<tr>
<td><strong>Modifying a User File</strong></td>
<td>9-2</td>
</tr>
<tr>
<td><strong>Modifying a Zone</strong></td>
<td>9-17</td>
</tr>
<tr>
<td><strong>Monitoring Application</strong></td>
<td>5-20</td>
</tr>
<tr>
<td><strong>MSDP Status</strong></td>
<td>7-8</td>
</tr>
<tr>
<td><strong>Multicast Discovery</strong></td>
<td>5-2</td>
</tr>
<tr>
<td><strong>Multicast Report</strong></td>
<td>4-52</td>
</tr>
<tr>
<td><strong>Network Status</strong></td>
<td>7-9</td>
</tr>
<tr>
<td><strong>Packet Monitoring</strong></td>
<td>7-1</td>
</tr>
<tr>
<td><strong>PIM Neighbor polling</strong></td>
<td>4-15</td>
</tr>
<tr>
<td><strong>L2</strong></td>
<td>4-12</td>
</tr>
<tr>
<td><strong>Routers with UT Enabled devices</strong></td>
<td>5-26</td>
</tr>
<tr>
<td><strong>RP</strong></td>
<td>4-23</td>
</tr>
<tr>
<td><strong>RPF</strong></td>
<td>4-28</td>
</tr>
<tr>
<td><strong>RPF Polling Report</strong></td>
<td>4-28</td>
</tr>
<tr>
<td><strong>RP Group Threshold Report</strong></td>
<td>4-24</td>
</tr>
<tr>
<td><strong>RP Report</strong></td>
<td>4-24</td>
</tr>
<tr>
<td><strong>RP Status</strong></td>
<td>7-8</td>
</tr>
<tr>
<td><strong>RP Summary</strong></td>
<td>7-8</td>
</tr>
<tr>
<td><strong>S,G</strong></td>
<td>4-4</td>
</tr>
<tr>
<td><strong>S,G Threshold Report</strong></td>
<td>4-5</td>
</tr>
<tr>
<td><strong>Selective Source Monitoring</strong></td>
<td>4-31</td>
</tr>
<tr>
<td><strong>SG Delta Report</strong></td>
<td>4-21</td>
</tr>
<tr>
<td><strong>SG Polling- By Branch</strong></td>
<td>4-22</td>
</tr>
<tr>
<td><strong>SNMP Utilities</strong></td>
<td>7-14, 7-22</td>
</tr>
<tr>
<td><strong>SSG Report</strong></td>
<td>4-25</td>
</tr>
<tr>
<td><strong>SSM Configuration</strong></td>
<td>4-32</td>
</tr>
</tbody>
</table>
Review Draft - Cisco Confidential

Index

T

Timeout Configuration 9-10
Topology 6-1
Top Talkers 7-10
Traffic & Polling Reports 4-4
Trap Viewer 4-2
Tree Polling & Reports 4-17
Tree Report 4-20

U

Unicast 5-21
User Tracking Details 5-26

V

Validate All Configurations 8-1
Video Probe 4-36, 5-18
Video Probe Report 4-36
Video Probe Status 7-3
VRF Count Report 4-46
VRF Interface Count Report 4-45