CHAPTER 2

Installing and Configuring the Components of Cisco Video Assurance Management Solution 3.1

This chapter contains the following sections:

- Installation Overview, page 2-1
- Configuration Overview, page 2-4
- Configuring Cisco ANA, page 2-5
- Configuring CMM, page 2-5
- Configuring Video Probes, page 2-28
- Configuring the ROSA NMS, page 2-32
- Configuring Cisco Info Center, page 2-39

Installation Overview

Installing Cisco VAMS 3.1 comprises the following steps:

- Install the Cisco ANA Software (Optional), page 2-1
- Install the Cisco Multicast Manager Hardware and Software, page 2-2
- Install iVMS and Third-Party Video Probes, page 2-3
- Install the ROSA NMS, page 2-3
- Install Cisco Info Center, page 2-4

Install the Cisco ANA Software (Optional)

If you will use Cisco ANA with VAMS 3.1, the ANA Gateway and the ANA Unit on supported hardware devices, install Cisco ANA 3.7.2. For detailed installation instructions, see the *Cisco Active Network Abstraction Installation Guide 3.7.2*, viewable online at:

http://www.cisco.com/en/US/docs/net_mgmt/active_network_abstraction/3.7.2/installation/guide/ana_372_installation_guide.html

Complete these steps to install the Cisco ANA software on supported hardware devices:

Step 1 If it is not already installed, install Solaris 10 on the ANA Gateway and ANA Unit devices.

Solaris 10 is available from the Sun Microsystems download site at the following URL:

http://www.sun.com/software/solaris/get.jsp

Step 2 Install required Solaris 10 patches on the ANA Gateway and ANA Unit devices.

For information on the required patches, see the *Cisco Active Network Abstraction Installation Guide, 3.7.2* at:

http://www.cisco.com/en/US/docs/net_mgmt/active_network_abstraction/3.7.2/installation/guide/ana_372_installation_guide.html

Install Oracle 9.2.0.1 on the ANA Gateway device.

See "Oracle Requirements and Installation" in the *Cisco Active Network Abstraction Installation Guide 3.7.2* for general steps. This document is viewable online at:

http://www.cisco.com/en/US/docs/net_mgmt/active_network_abstraction/3.7.2/installation/guide/ana_372_installation_guide.html

Upgrade the Oracle installation on the ANA Gateway to Oracle 9.2.0.8.

Install the Active Network Abstraction (ANA) 3.6 Gateway, ANA Unit, and ANA client on the supported hardware devices, as described in: the *Cisco Active Network Abstraction Installation Guide 3.7.2,* viewable online at:

http://www.cisco.com/en/US/docs/net_mgmt/active_network_abstraction/3.7.2/installation/guide/ana_372_installation_guide.html

Install the Cisco Multicast Manager Hardware and Software

Complete these steps to install Cisco Multicast Manager 3.1:

Step 1 Install the Cisco Multicast Manager (CMM) 3.1 software on dedicated servers.

See the following installation guide for more information:

Cisco Multicast Manager Installation Guide, 3.1 viewable online at:

http://www.cisco.com/en/US/products/ps6337/prod_installation_guides_list.html

Step 2 Complete the following steps to download the CMM 3.1.2 patch.

a. Create a */tmp d*irectory on the target CMM host.

b. Go to the following URL on Cisco.com:

http://www.cisco.com/en/US/products/ps6337/index.html

c. Click the **Software Download** link.

d. Log in to cisco.com.

e. Click the **Cisco Multicast Manager 3.1** folder link.

f. Click the **Latest Releases > 3.1.2** link.

The patch release is contained in the following distribution files:

- **Solaris**: *cmm312_solaris.tar.gz*
- **Linux**: *cmm312_linux.tar.gz*

g. Choose the file for your operating system and click **Download Now**.

h. Enter the following commands to extract the file to a temporary directory:

```
# cd /tmp
# gunzip -c cmm312_solaris.tar.gz | tar xvf - (for Solaris)
# tar -xzvf cmm312_linux.tar.gz (for Linux)
#./install_patch.sh
```

i. When the *install_patch* script prompts you to continue, enter **y**.

The installation script installs the patch, stops the CMM processes, and then restarts them.

Install iVMS and Third-Party Video Probes

Install one of the following:

- IneoQuest Video Management System (iVMS)
- Third-party video probes for Bridge Technologies, IneoQuest, and Mixed Signals

Or if you are using both iVMS and other third-party video probes, install iVMS and also install the third-party video probes for Bridge Technologies and Mixed Signals, as required.

Step 1 If you are using iVMS, install iVMS 4.1 on a Microsoft Windows Server 2003 platform. For installation instructions, see the iVMS documentation.

Step 2 Install the video probes that you want to use to monitor your video network.

For a list of the documentation for the video probes used with Cisco VAMS 3.0, see the *Documentation Guide for Cisco Video Management Solution, 3.1,* viewable online at:

http://www.cisco.com/en/US/docs/net_mgmt/cisco_video_assurance_mgt_solution/3.1/roadmap/vams31dg.html

Install the ROSA NMS

Complete these steps to install the Cisco ROSA hardware and software:

Step 1 (Optional) Install the ROSA Element Management System (ROSA EM).

The ROSA EM is an embedded rack-mounted hardware platform that is preinstalled with the ROSA EM software.

For installation and configuration instructions, see the documentation provided with the ROSA EM device.

Step 2 Install the ROSA Copernicus Network Management System (ROSA NMS).

The ROSA NMS is provided:

- As a dedicated server that is preinstalled with the ROSA Copernicus NMS software.
- As a software version that runs on Microsoft Windows servers, Microsoft Windows XP, or Windows vista. The software version is available in three versions:
  - ROSA Client

- ROSA Single User
- ROSA Device Configuration Shell

For installation instructions, see:

- The README file for the ROSA Copernicus NMS. This file launches automatically when you insert the ROSA NMS installation CD in your Windows server or Windows workstation.
- The *ROSA Network Management System User's Guide, Version 3.0 Build 18*. This document is provided in PDF format on CD 1 of the ROSA NMS installation media.

Step 3 Install the SNMP agent on your ROSA Copernicus NMS server.

For detailed installation instructions, refer to "Installing the SNMP Agent Task Driver" in the *SNMP Agent Users Guide, Task Driver for ROSA 3.0*. This document is provided on the Documentation CD for the ROSA Copernicus Network Management System server.

Install Cisco Info Center

For information on installing Cisco Info Center, see the *Cisco VAMS 3.1 Solution Deployment Guide*. This document is available on the Cisco Developer's network website.

Configuration Overview

After completing the installation of Cisco VAMS 3.1, you are ready to configure the components of the solution for operation.

The following summary procedure describes how to configure all the components of Cisco VAMS 3.1. References to more detailed procedures and documentation are provided.

To configure the components of VAMS 3.1:

Step 1 In Cisco ANA, create new virtual network elements (VNEs) for the Cisco VAMS 3.1 components. See the C*isco Active Network Abstraction Customization User Guide, 3.7.2*. This document is available at the following URL:

http://www.cisco.com/en/US/products/ps6776/products_installation_and_configuration_guides_list.html

Step 2 Add the VAMS 3.1 devices to the Cisco ANA network map.

Step 3 Perform general configuration steps for CMM.

See General CMM Configuration, page 2-6.

The general CMM configuration steps include:

- Configuring the CMM Monitoring Domain, page 2-6
- Discovering Devices to Monitor, page 2-8
- Specifying Global Polling Configuration, page 2-9
- Configuring Address Management, page 2-11
- Adding Users, page 2-20

Note Make sure that you configure address management and channel mapping in CMM before installing Cisco Info Center. Cisco Info Center configuration requires comma separated value (CSV) files that specify the address management database, which are read by the CIC configuration utility. See Configuring Address Management, page 2-11

Step 4 Configure CMM to set thresholds and forward notifications to the Cisco Info Center Object Server. Configure the following types of monitoring:

- PPS/BPS Threshold Polling
- Tree Polling
- Health Checks
- IP Multicast Heartbeat Monitoring
- Video probe monitoring
- VidMon device monitoring

See the "Configuring CMM" section on page 2-5.

Step 5 Configure the video probes to set thresholds and send events to Cisco Info Center.

See the "Configuring Video Probes" section on page 2-28.

Step 6 Configure the ROSA NMS to forward messages to Cisco Info Center.

See Configuring the ROSA NMS, page 2-32.

Step 7 Configure the Cisco Info Center components of Cisco VAMS 3.1.

See the *Cisco VAMS 3.1 Solution Deployment Guide*. This document is available on the Cisco Developer Network (CDN) website.

All components of Cisco VAMS 3.1 are now operational. The Cisco devices in the video transport network forward notifications to the CMM, which then forwards them to Cisco Info Center. The video probes also forward notifications to CMM or directly to Cisco Info Center.

Configuring Cisco ANA

For information on configuring Cisco ANA, see the online documentation for Cisco ANA 3.7.2. The Cisco ANA documentation is available at the following URL:

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

Configuring CMM

To enable notifications and set thresholds for multicast conditions, you must configure CMM.

This section covers the following areas of CMM Configuration:

- General CMM Configuration, page 2-6
- Configuring Video Probes, page 2-28
- Configuring VidMon Polling, page 2-29.
- Setting Up Troubleshooting Configuration for IP Multicast, page 2-20—This section describes configuration of CMM for specific types of monitoring:
  - Configuring BPS/PPS Threshold Monitoring, page 2-21.
  - Configuring Tree Polling, page 2-22.
  - Configuring Health Checks, page 2-26
  - Configuring IP Multicast Heartbeat Monitoring, page 2-27

General CMM Configuration

General Configuration tasks for CMM include:

1. Configuring the CMM monitoring domain

   See Configuring the CMM Monitoring Domain, page 2-6.

2. Discovering the devices to monitor

   - Discovering multicast-capable devices in the domain
   - Discovering VidMon devices

   See Discovering Devices to Monitor, page 2-8.

3. Configuring the CMM Channel Mapping database

   See Configuring Address Management, page 2-11—This section describes configuration of CMM to match the channels used to transmit multicast flows with the IP addresses for the flows.

4. Specifying Global Polling Configuration

   See Specifying Global Polling Configuration, page 2-9.

5. Adding Users

   See Adding Users, page 2-20.

Note Summary configuration procedures follow. For complete details about these, and other configuration procedures, see the *User Guide for Cisco Multicast Manager 3.1* at the following location:

http://www.cisco.com/en/US/products/ps6337/products_user_guide_list.html

Configuring the CMM Monitoring Domain

To configure the CMM monitoring domains for Cisco VAMS 3.1:

Step 1 In a browser window, open and log in to CMM.

Step 2 Click **Switch to Main**.

Step 3 From the CMM menu, choose **System Configuration > Domain Management**.

The Domain Management page appears.

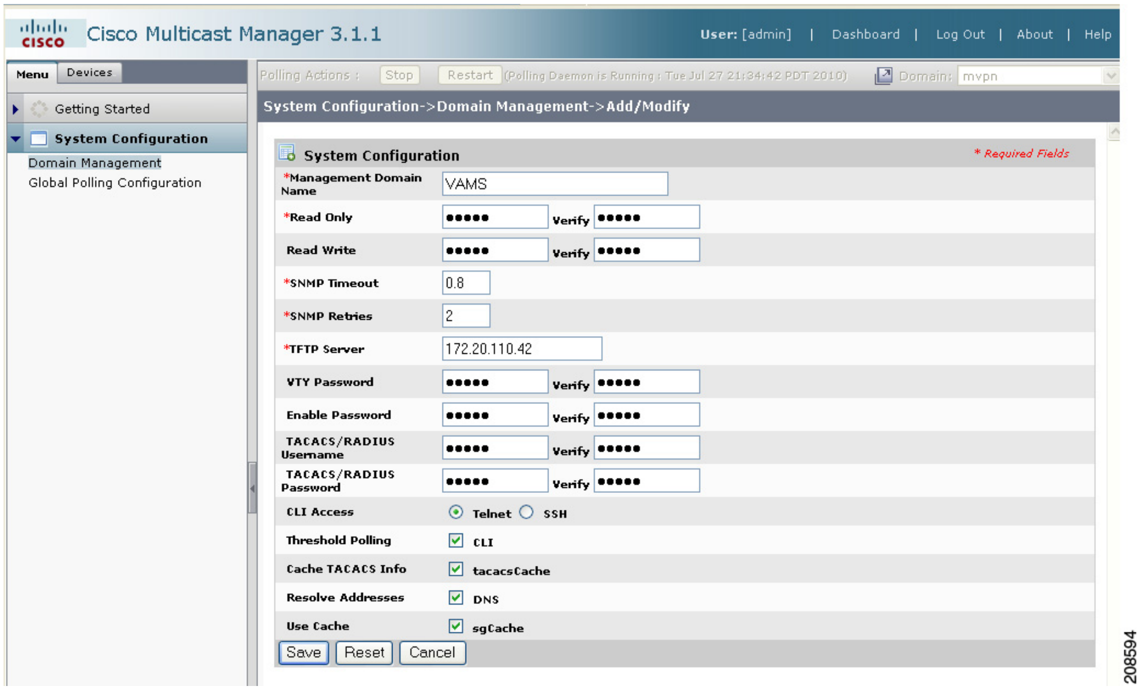
Step 4 Click the **Add** button and from the drop-down list, choose **By Domain.**

You can also click the **Add** button and specify **By Import** to import a domain from a text file. In this case you are prompted to browse for a text file containing the domain information. The following example, shows the file syntax for a domain specification file:

```
VAMS,public,private,0.8,2,172.18.135.216,lab,lab,bw,bw,Telnet,true,false,true,true
```

The System Configuration page appears, as shown in Figure 2-1.

Figure 2-1 CMM System Configuration Page



Cisco Multicast Manager 3.1.1
User: [admin] | Dashboard | Log Out | About | Help
Menu
Devices
Polling Actions : Stop Restart (Polling Daemon is Running : Tue Jul 27 21:34:42 PDT 2010)
Domain: mvpn
Getting Started
System Configuration
Domain Management
Global Polling Configuration
Save
Reset
Cancel
208594

System Configuration->Domain Management->Add/Modify

System Configuration * Required Fields

*Management Domain Name	VAMS		
*Read Only	●●●●●	Verify	●●●●●
Read Write	●●●●●	Verify	●●●●●
*SNMP Timeout	0.8		
*SNMP Retries	2		
*TFTP Server	172.20.110.42		
VTY Password	●●●●●	Verify	●●●●●
Enable Password	●●●●●	Verify	●●●●●
TACACS/RADIUS Username	●●●●●	Verify	●●●●●
TACACS/RADIUS Password	●●●●●	Verify	●●●●●
CLI Access	● Telnet ○ SSH		
Threshold Polling	☑ CLI		
Cache TACACS Info	☑ tacacsCache		
Resolve Addresses	☑ DNS		
Use Cache	☑ sgCache		

Step 5 Specify settings for the domain as follows:

- In the Management Domain Name field, enter the domain name.

  The domain name can be any appropriate name. In the example shown in Figure 2-1, the specified domain name is *VAMS* because this is the default name used by Cisco Info Center for cross-launching of CMM. If you specify another domain name, then you must edit the *launch_cmm_flowtrace.cg*i file in Cisco Info Center and specify the domain name configured in CMM.

- In the TFTP Server field, the IP address of the CMM server is specified by default. In general, leave this as is.

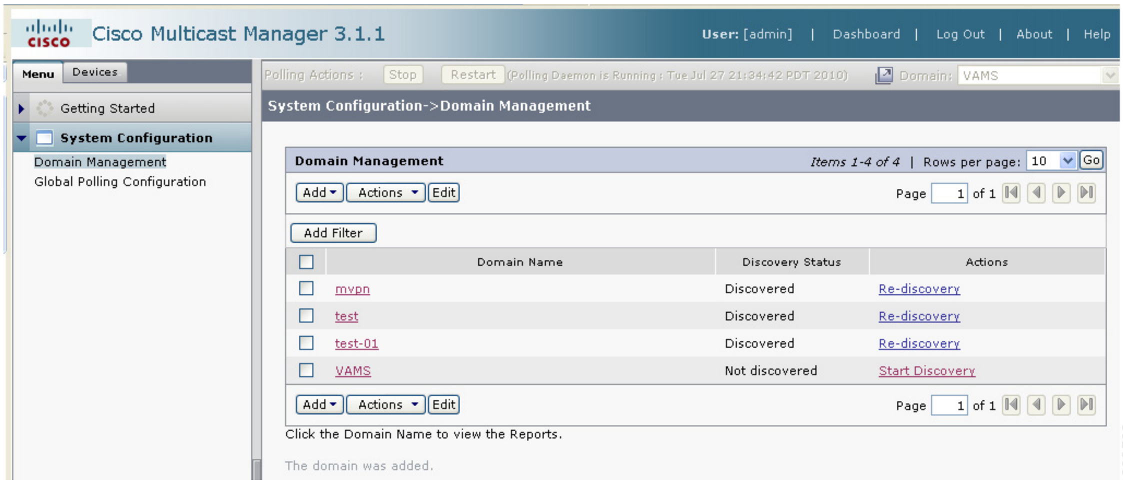
- Specify the remaining settings as described in "Creating a Domain" in the "System Configuration" chapter of the *User Guide for Cisco Multicast Manager, 3.1* at the following location:

  http://www.cisco.com/en/US/docs/net_mgmt/cisco_multicast_manager/3.1/user/guide/cm.m_dm.html#wp1056516

Step 6 Click **Save** to save the domain.

The Domain Management appears and lists the new domain, as shown in Figure 2-2.

Figure 2-2 Domain Management Page



(Polling Daemon is Running : Tue Jul 27 21:34:42 PDT 2010)

Domain: VAMS

System Configuration->Domain Management

Domain Management — Items 1-4 of 4 | Rows per page: 10

Page 1 of 1

□	Domain Name	Discovery Status	Actions
□	mvpn	Discovered	Re-discovery
□	test	Discovered	Re-discovery
□	test-01	Discovered	Re-discovery
□	VAMS	Not discovered	Start Discovery

Page 1 of 1

Click the Domain Name to view the Reports.

The domain was added.

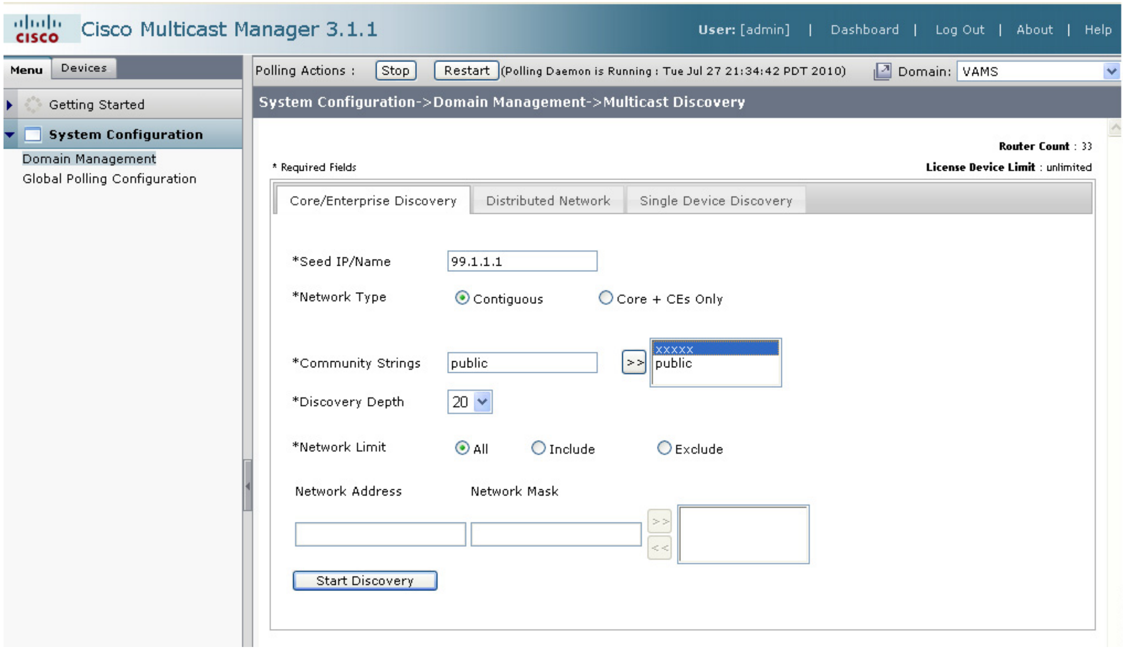
Discovering Devices to Monitor

To discover the devices and video probes in your network:

Step 1 After creating the domain, click the **Start Discovery** link in the entry for the domain on the Domain Management Screen.

The Multicast Discovery page appears, as shown in Figure 2-3.

Figure 2-3 CMM Multicast Discovery Page



(Polling Daemon is Running : Tue Jul 27 21:34:42 PDT 2010)

Domain: VAMS

System Configuration->Domain Management->Multicast Discovery

Router Count : 33

License Device Limit : unlimited

* Required Fields

*Seed IP/Name: 99.1.1.1

*Network Type: ● Contiguous ○ Core + CEs Only

*Community Strings: public — xxxxx, public

*Discovery Depth: 20

*Network Limit: ● All ○ Include ○ Exclude

Network Address | Network Mask

Step 2 Enter values as follows:

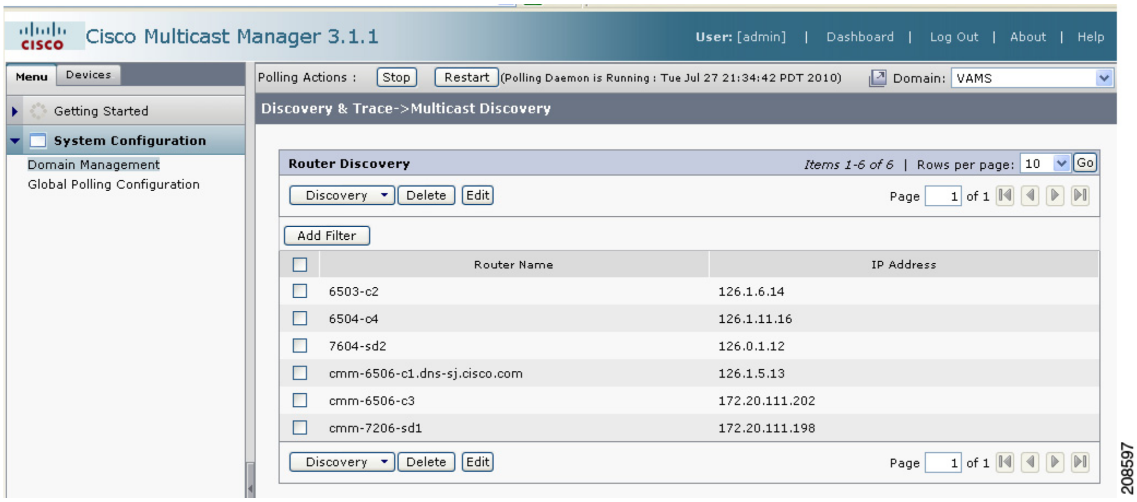
- In the Seed/IP/Name field, enter the IP address or hostname of any device in the domain.
- In the Community Strings field, enter *public* and click the right arrow to move it to the list of community strings.
- From the drop-down list in the Discovery Depth field, select the number of hops to discover from the specified seed IP address or hostname.

Step 3 Click the **Start Discovery** button.

CMM discovers the routers in your network.

The Router Discovery page appears, listing the discovered devices, as shown in Figure 2-4.

Figure 2-4 CMM Router Discovery Page



Polling Actions : (Polling Daemon is Running : Tue Jul 27 21:34:42 PDT 2010) Domain: VAMS

Discovery & Trace->Multicast Discovery

Router Discovery — Items 1-6 of 6 | Rows per page: 10 — Page 1 of 1

□	Router Name	IP Address
□	6503-c2	126.1.6.14
□	6504-c4	126.1.11.16
□	7604-sd2	126.0.1.12
□	cmm-6506-c1.dns-sj.cisco.com	126.1.5.13
□	cmm-6506-c3	172.20.111.202
□	cmm-7206-sd1	172.20.111.198

Page 1 of 1

Step 4 To discover additional devices, such as Layer 2 devices, video probes, VidMon devices, and unicast devices, from the CMM main menu, choose **Discovery and Trace**, and then from the Discovery and Trace menu, select the type of device to discover. For example:

- To discover Layer 2 devices, choose **Discovery & Trace > L2**.
- To discover video probes, choose **Discovery & Trace > Video Probe**.
- To discover VidMon devices, choose **Discovery & Trace > Vidmon Device**.
- To discover unicast devices, choose **Discovery & Trace > Unicast.**

For detailed instructions, see the “Discovery” section in the “Discovery and Trace” chapter of the *User Guide for Cisco Multicast Manager, 3.1* at the following location:

http://www.cisco.com/en/US/docs/net_mgmt/cisco_multicast_manager/3.1/user/guide/cmm_dt.html

Specifying Global Polling Configuration

When you configure global polling configuration, you specify:

- The polling interval for each type of polling in CMM
- Whether to enable rising/falling and normalized traps for thresholds

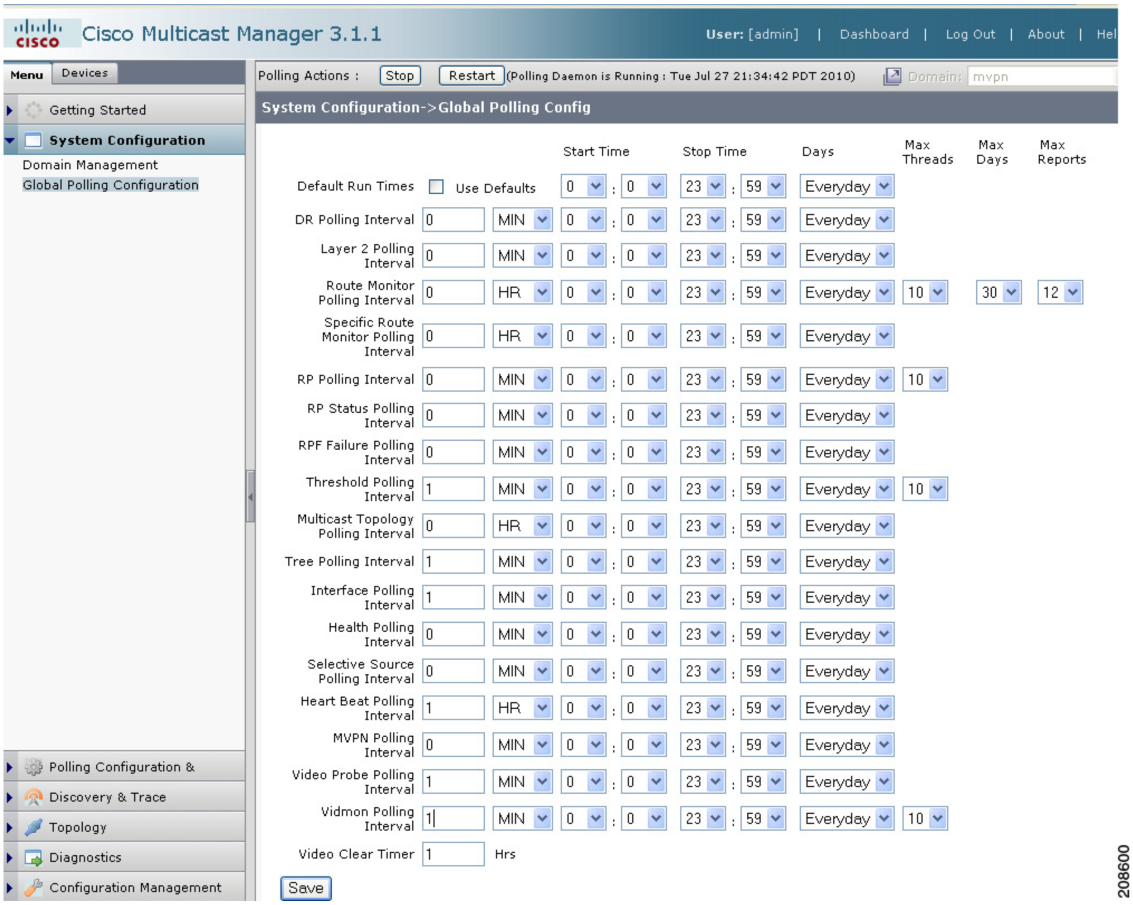
- The IP address of the CIC server, for northbound forwarding of SNMP traps

To specify the global polling configuration:

Step 1 From the CMM main menu, choose **System Configuration > Global Polling Configuration**.

The Global Polling Configuration page appears, shown in Figure 2-5.

Figure 2-5 CMM Global Polling Configuration Page



Polling Actions : Stop Restart (Polling Daemon is Running : Tue Jul 27 21:34:42 PDT 2010) Domain: mvpn

System Configuration->Global Polling Config

			Start Time		Stop Time		Days	Max Threads	Max Days	Max Reports
Default Run Times	☐ Use Defaults		0	0	23	59	Everyday			
DR Polling Interval	0	MIN	0	0	23	59	Everyday			
Layer 2 Polling Interval	0	MIN	0	0	23	59	Everyday			
Route Monitor Polling Interval	0	HR	0	0	23	59	Everyday	10	30	12
Specific Route Monitor Polling Interval	0	HR	0	0	23	59	Everyday			
RP Polling Interval	0	MIN	0	0	23	59	Everyday	10		
RP Status Polling Interval	0	MIN	0	0	23	59	Everyday			
RPF Failure Polling Interval	0	MIN	0	0	23	59	Everyday			
Threshold Polling Interval	1	MIN	0	0	23	59	Everyday	10		
Multicast Topology Polling Interval	0	HR	0	0	23	59	Everyday			
Tree Polling Interval	1	MIN	0	0	23	59	Everyday			
Interface Polling Interval	1	MIN	0	0	23	59	Everyday			
Health Polling Interval	0	MIN	0	0	23	59	Everyday			
Selective Source Polling Interval	0	MIN	0	0	23	59	Everyday			
Heart Beat Polling Interval	1	HR	0	0	23	59	Everyday			
MVPN Polling Interval	0	MIN	0	0	23	59	Everyday			
Video Probe Polling Interval	1	MIN	0	0	23	59	Everyday			
Vidmon Polling Interval	1	MIN	0	0	23	59	Everyday	10		
Video Clear Timer	1	Hrs								

Step 2 Configure the following Global Polling intervals:

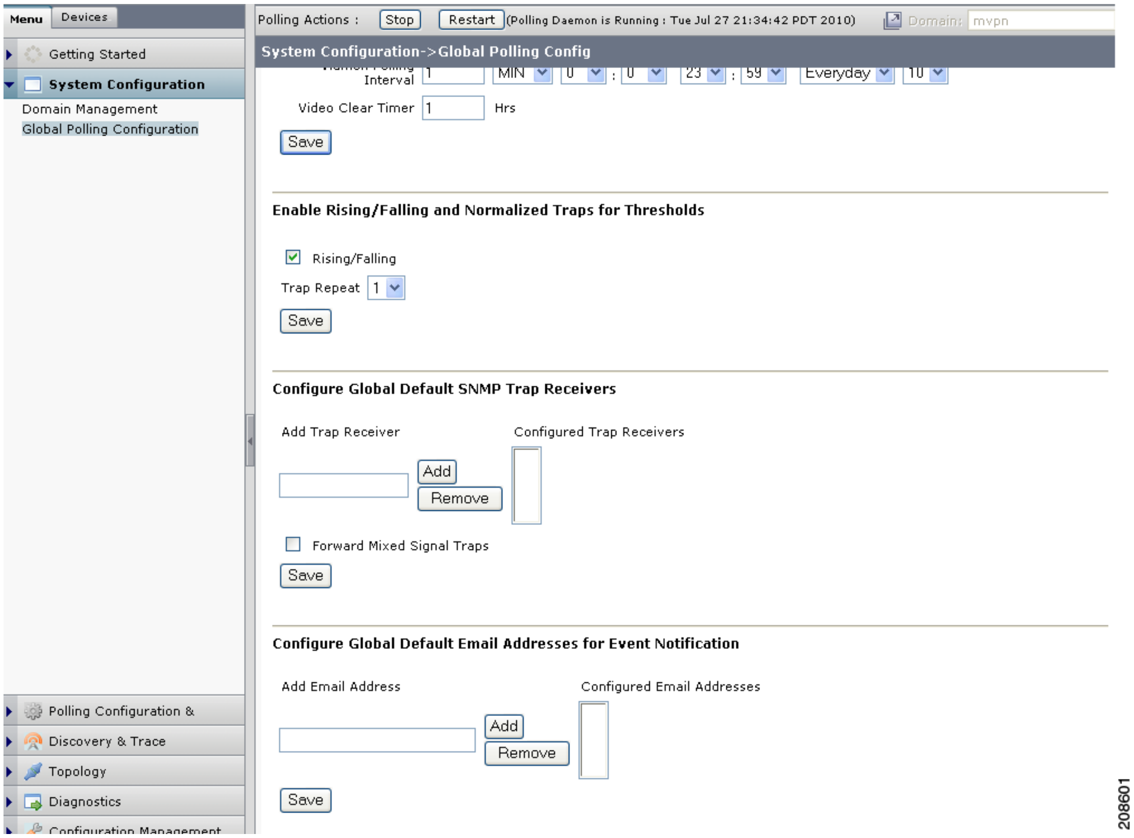
- Threshold Polling Interval
- Tree Polling Interval
- Heart Beat Polling Interval
- Video Probe Polling Interval

Step 3 Configure the Vidmon Polling Interval.

In the example shown in Figure 2-5, the Vidmon Polling Interval is set to 1 minute. We recommend that you set this interval to 1 minute or more, especially if you have a large number (thousands) of VidMon flows configured.

Step 4 Scroll down the Global Polling Configuration page to view the Enable Rising/Falling and Normalized Traps for Thresholds, Configure Global Default SNMP Trap Receivers, and Configure Global Default Email Addresses for Event Notification sections, as shown in Figure 2-6.

Figure 2-6 Bottom Portion of the CMM Global Polling Configuration Page



Polling Actions : Stop Restart (Polling Daemon is Running : Tue Jul 27 21:34:42 PDT 2010)

System Configuration->Global Polling Config

Interval 1 MIN 0 : 0 23 : 59 Everyday 10

Video Clear Timer 1 Hrs

Enable Rising/Falling and Normalized Traps for Thresholds

☑ Rising/Falling

Trap Repeat 1

Configure Global Default SNMP Trap Receivers

Add Trap Receiver

Configured Trap Receivers

□ Forward Mixed Signal Traps

Configure Global Default Email Addresses for Event Notification

Add Email Address

Configured Email Addresses

Step 5 In the Configure Global Default SNMP Trap Receivers section, enter the IP address of the Cisco Info Center server click the **Add** button, and then click the **Save** button.

This adds the Cisco Info Center Object Server IP address to the Configured Trap Receivers drop-down list.

Step 6 Go to the **Domain Trap/Email section o**f the Global Polling Config page, and if you want to send an email when event notifications are generated, enter an email address in the Add Email Address field and then click the Add button.

Step 7 To activate your changes, click the **Restart** button.

CMM forwards notifications to Cisco Info Center, the designated trap receiver.

Configuring Address Management

To configure CMM to associate video flows with the IP addresses used to transmit video flows and monitor multiplexed channels and ad zones, you must:

1. Configure several databases for CMM.

   You can specify the information in the database in two ways, by:

   - By importing CSV files into the CMM address management database
   - By manually entering the information using the CMM GUI

For general information on configuring the address management database in CMM, see "Address Management" in chapter 10 of the *User Guide for Cisco Multicast Manager 3.1* "Administration." This information is viewable online at:

http://www.cisco.com/en/US/products/ps6337/products_user_guide_list.html

2. Configure the databases in the order listed here:
   - **Channel Map Database**—Specifies details about the channels used to transmit video flows, such as the channel name, type of CODEC used for the channel, and the screen format.
   - **AdZone Database**—Identifies ad zones defined by the service provider. The ad zones are linked to the IP Address Table.
   - **Multiplex Table Database**—Describes the channels transmitted in multicast video flows.
   - **Destination Address Database**—Associates multicast IP addresses with channel names defined in the Multiplex Table database.
   - **Source Description Database**—Specifies a source IP address and a description for it.
   - **Transport Description Database (optional)** —Describes the transport streams (TS) in a multicast flow.

To configure Cisco Info Center, you must copy the information from four of these databases information to the TIP/TBSM host as CSV files. You must name the CSV files as required by CIC:

- **Channel Map Data CSV File**—*channels.csv*
- **Multiplex Table Database CSV File**—*muxid.csv.*
- **Destination Address Database CSV File**—*addresses.csv*
- **Source Description CSV File**—*source.csv.*

You can create the CSV files in several ways.

- If you are importing the CSV files into the CMM database, by creating them as text files on the CMM server.

  However if you make any changes to the CSV files, you must re-import them into CMM.
- If you use the CMM GUI to create the database tables, you must export them from the CMM database using the CMM export feature in the Address Management user interface.

  See Exporting CMM Address Management Database Information, page 2-19

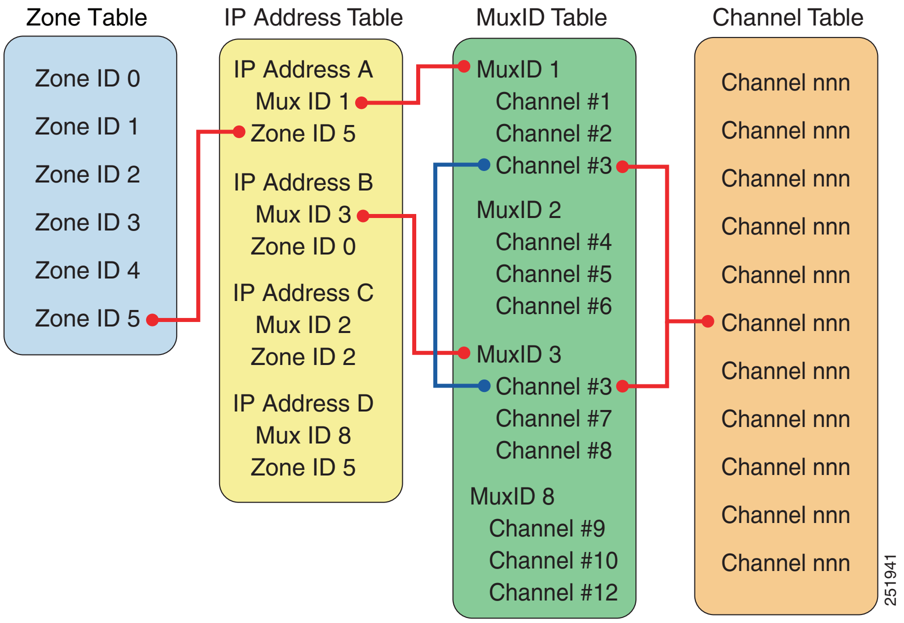
Note Ensure that you configure the CMM databases before you install and configure Cisco Info Center. During Cisco Info Center installation, you must place CSV files containing the database information into a directory used for CIC installation and which is accessible to the *customize_vams.sh* script.

During Cisco Info Center installation, sample CSV files are written to the *$NCHOME/cmm* directory on the Cisco Info Center host. You can use the formats of these files as an example for editing the CSV files that you copy from CMM to get them into the format required for Cisco Info Center Impact.

For information on importing the CSV files into Cisco Info Center, See the *Cisco VAMS 3.1 Solution Deployment Guide*. This document is available on the Cisco Developer Network (CDN) website.

CMM indexes the address management database tables by using relational keys that point from entries in one table to entries in the other tables, as shown in Figure 2-7.

Figure 2-7 CMM Database Table Index Relationships



Configuring the Channel Table

The channel table contains details about the video flows being transported across the IP network. The fields for this table include:

- Channel number

  A unique number identifying the channel.

- Channel Name

  Channel name

- Short name
- Codec type
- Screen format
- Service type

Using CMM, you can either add channels individually, or import multiple channels in a CSV file having the following format:

```
address_channel@<channel_number>,<channel_name>,<short_name>,<CODEC_type>,<screen_format>,
Service_type>
```

For example:

```
address_channel@CHE-MPTS-2,CHE-MPTS-2 BBC1 BBC2 ITV CH4 CH5 HD, CHE-MPTS-2, MPEG-2,
Widescreen, SDV
```

You can add the channel map in two ways:

- By importing it into the CMM database
- By entering the channel map data manually

To import the channel map into CMM:

Step 1 From the CMM main menu, choose **Administration > Address Management > Channel Map Database**.

The Channel Database page appears.

Step 2 From the Channel Database page, click the **Add** button, and from the drop-down list, choose **By Import**.

Step 3 Browse for the Channel Map *.csv* file.

Step 4 Click the **Upload** button.

To add channel map information by channel:

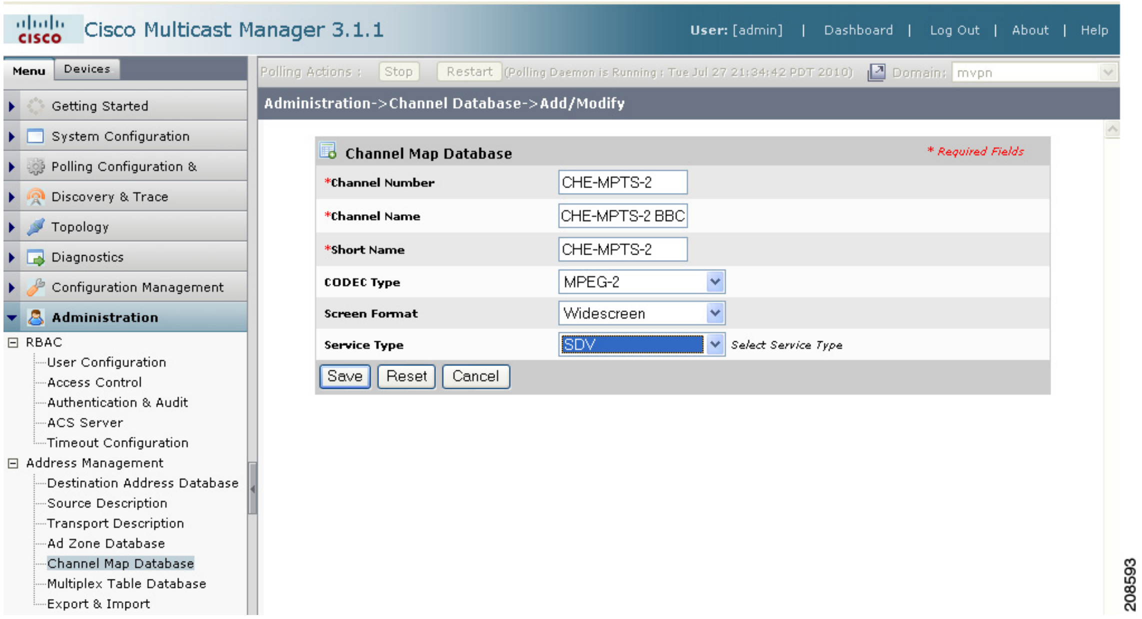
Step 1 From the CMM main menu, choose **Administration > Address Management > Channel Map Database**.

The Channel Database page appears.

From the Channel Database page, click the **Add** button, and from the drop-down list, choose **By Channel.**

The Channel Map Database page appears, shown in Figure 2-8.

Figure 2-8 Channel Map Database Page



*Channel Number	CHE-MPTS-2
*Channel Name	CHE-MPTS-2 BBC
*Short Name	CHE-MPTS-2
CODEC Type	MPEG-2
Screen Format	Widescreen
Service Type	SDV

Step 2 Enter the channel map information as indicated in Figure 2-8.

Step 3 Click the **Save** button.

Configuring the Ad Zone Table

Service providers can insert national, regional, or local advertising content into a given video channel.This enables the SP to realize increased revenue. Ad zones describe the scope of the network where specific advertisements are inserted.

Ad insertion creates challenges for SPs. In each ad zone, the multicast destination address must be changed to reflect ad modifications. One program can be put into multiple ad zones. It is important to not only track the program in a single ad zone, but also to the program across all ad zones, along with the program state before ad splicing.

The Ad Zone database identifies the IP address (and related video channels) to the ad zone in advertising for that IP flow was inserted.

The table fields are:

- **Zone Number**—A unique ID created by the SP.
- **Zone Name**—A unique name describing the ad zone.

Using CMM, you can either add ad zones individually, or import multiple ad zones in a CSV file having the following format:

```
address_zone@<ad_zone_number>,<ad_zone_name>
```

For example:

```
address_zone@201,Ad_Zone_1
```

To import a CSV file containing AD Zone database information:

Step 1 From the CMM menu, choose **Administration > Address Management > Ad Zone Database.**

Step 2 From the Ad Zone Database page, click the **Add** button and from the drop-down list, choose **By Import**.

Step 3 On the Add/Modify Add Zone, page, browse for the CSV file containing the Ad Zone data, and then click the **Upload** button.

To add an Ad Zone entry manually:

Step 1 From the CMM menu, choose **Administration > Address Management > Ad Zone Database.**

Step 2 From the Ad Zone Database page, click the **Add** button and from the drop-down list, choose **By Zone**.

Step 3 On the Add/Modify Add Zone, page, enter the Zone Number and Zone Name and then click the **Save** button.

Configuring the Multiplex Table Database

The Multiplex Table database enables one or more channels to be associated in a group. Video flows can be carried in single program transport streams (SPTSs) or multiple program transport streams (MPTSs). MPTS flows aggregate many channels into one IP flow, while SPTS uses a one-to-one mapping between channel and flows. Cisco VAMS supports both types of transport stream.

A MuxID is used to describe the channels in a given flow. For example, MuxID 1 might contain the channel numbers for an MPTS carrying Discovery, ESPN, TNT, and Fox News.

The Multiplex table fields are:

- Channel Number: The Channel table key
- Program ID (PID): A value describing the video and audio of the channel.

You enter Multiplex Table database information manually into CMM or import it from a muxid.csv file. The same data, with modifications to the filed names, must be added to the Cisco Info Center Object Server configuration, either as a CSV file, or as a MySQL database table.

When you create a CSV file to import into Cisco Info Center, use this format:

```
address_mux@<mux_number>,<channel_number>,<channel_name>,<channel_program_ID>
```

For example,:

```
address_mux@CHE-MPTS-2,55,CH5-HD,25
```

For a multiprogram transport stream (MPTS), enter multiple lines using the same mux number, but with each line having a different channel name and number. For example:

```
address_mux@CHE-MPTS-2,55,CH5-HD,25
address_mux@CHE-MPTS-2,51,BBC1-SD,21
```

For example, a MPTS with six channels requires six “address_mux@<mux_number>” lines:

To create a Multiplex Table entry in CMM and associate channels and program IDs with it:

1. Add one or more channels.

   See Adding a Channel, page 2-16.

2. Add Mux IDs

   See Adding a Multiplex Table Entry, page 2-17.

Adding a Channel

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

Step 2 Select **Address Management**.

Step 3 Select **Channel Map Database.**

Step 4 Click the **Add** button.

Step 5 Select **By Channel**.

Note You can also import a file by selecting **By Import** from the pull-down list for the **Add** button. Browse to the file location and select **Upload**.

Field	Description
Channel Number	Enter a channel number.
Channel Name	Enter a channel name.
Short Name	Enter a short name for the channel.
CODEC Type	From the drop-down list in the CODEC Type field, select the type of CODEC the channel uses.

Field	Description
Screen Format	From the drop-down list in the Screen Format field, select the screen format for the channel.
Service Type	From the drop-down list in the Service Type field, select the service type for the channel.
Save	Apply the new record to the database.

Note 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.

Adding a Multiplex Table Entry

Step 1 In CMM, from the Multicast Manager menu, select **Administration**.

Step 2 Click **Address Management > Multiplex Table Database**.

The Multiplex Table Database page opens.

Step 3 From the Multiplex Table Database drop-down menu, click the **Add** button, and from the drop-down list, choose one of the following:

- To add a Mux ID manually, choose **By Mux**.
- To import Mux IDs from a file, choose **By Import**.

If you choose **By Mux**, the Mux Database page appears.

Step 4 If you chose **By Mux**, enter the Mux ID in the Mux ID field and select the channel number from the list of channel numbers, and then click the **Save** button.

Step 5 If you chose **By Import**, enter the filename and directory path for the muxid.csv file and then click the **Upload** button.

Configuring the Destination Address Database

To enable CMM to map the video channels that it monitors to the multicast addresses associated with the channels, you must configure the CMM IP address table.

The IP address table associates multicast addresses with video channel information. This enables easy, quick recognition of a channel by name rather than by IP address.

The IP address table that you configure in CMM must be added to the Cisco Info Center Object Server configuration to enable Cisco Info Center to interpret the events it receives from CMM.

The IP Address table contains the following fields:

- **IP Address**—A unique multicast address.
- **Description**—Information displayed during diagnostics.
- **Ad Zone ID**—The Ad Zone Table key.
- **MuxID**—The MuxID table key.

Using CMM, you can either add addresses individually, or import multiple addresses in a comma-separated variables (CSV) file. The CSV file. for the IP address table must have this format:

```
address_db@<Destination_ip>,<Description (Transport)>,<Ad Zone>,<Mux Number>
```

For example:

```
address_db@232.1.1.20,CHE-MPTS-2 BBC1 BBC2 ITV CH4 CH5 HD 11-1-0-2 as source,CHE
AdZone,CHE-MPTS-2
```

To import the Destination Address table into CMM:

Step 1 From the CMM main menu, select **Administration**.

Step 2 Choose **Address Management > Destination Address Database**.

The Destination Address Database window appears.

Step 3 Click the **Add** button and from the drop-down list, select **By Import**.

Step 4 Click the **Browse** button next to the Import from File field, locate the CSV file for the IP address table, and select it.

Step 5 Click **Import**.

Adding a Transport Description

You can add a transport description by importing a CSV file or by using the CMM interface.

If importing a Transport CSV file for the database, use the following format:

```
address_sgdesc@<Source IP>,<Destination IP>,<Description>
```

For example:

```
address_sgdesc@10.10.20.9,225.1.190.4,CHE to RHE ENC1
```

To add a transport description:

Step 1 In CMM, from the Multicast Manager menu, select **Administration**.

Step 2 Select **Address Management**.

Step 3 Select **Transport Description.**

Step 4 Click the **Add** button.

Step 5 From the drop-down list, select **By Transport Description.**

Note You can also import an address file by selecting **By Import** from the Add button. Browse to the file location and select **Upload**.

Field	Description
Source IP Address	Enter the IP address of the source.
Group IP Address	Enter the IP address for the group.

Field	Description
Description	Enter a description for the TS.
Save	Apply the new address to the database.

Adding a Source Address and Description

You can add a source address and a description for the source address by importing a CSV file or by using the CMM user interface.

The format of the CSV file for a source address and description must be as follows:

```
address_source@<source ip >,<description>
```

For example:

```
address_source@10.10.20.9,CHE_ENC1
```

To add a source address and description:

Step 1 In CMM, from the Multicast Manager menu, select **Administration**.

Step 2 Select **Address Management**.

Step 3 Select **Source Description.**

Step 4 Click the **Add** button.

Step 5 From the drop-down list, select **By Source Address**.

Note You can also import an address file by selecting **By Import** from the **Add** button. Browse to the file location and select **Upload**.

Field	Description
IP Address	Enter the IP address of the source.
Description	Create and enter a description.
Save	Apply the new address to the database.

Exporting CMM Address Management Database Information

If you use the CMM user interface to configure the address management database, then you must export the data to CSV files that you can copy to the Cisco Info Center host.

The following example shows a sample

Example 2-1 Sample Channel Datase File Extracted form CMM

```
address_channel@1,Reg_DB_M_001-11,R_DB_M_001-11,MPEG-2,4:3,DT
```

For information on the fields, see, Configuring the Channel Table, page 2-13.

To export address management data from CMM:

Step 1 In CMM, from the Multicast Manager menu, select **Administration**.

Step 2 Select **Address Management**.

Step 3 Select **Destination Address Database** and complete these steps.

- **a.** On the Destination Address Database page, check the check box for each Destination IP address you want to export data for.
- **b.** Click the **Actions** button, and from the drop-down list, select **Export**.
- **c.** When you save the data file, name it *addresses.csv*.

Step 4 Select **Source Description** and complete these steps.

- **a.** On the Source Description Address Database page, check the check box for each Source IP address you want to export data for.
- **b.** Click the **Actions** button, and from the drop-down list, select **Export**.
- **c.** When you save the data file, name it *source.csv*.

Step 5 Select **Channel Map Database** and complete these steps.

- **a.** On the Source Description Address Database page, check the check box for each Channel Number address you want to export data for.
- **b.** Click the **Actions** button, and from the drop-down list, select **Export**.
- **c.** When you save the data file, name it *channels.csv*.

Step 6 Select **Multiplex Table Database** and complete these steps.

- **a.** On the Multiplex Database page, check the check box for each Mux Number you want to export data for.
- **b.** Click the **Actions** button, and from the drop-down list, select **Export**.
- **c.** When you save the data file, name it *muxid.csv*.

Adding Users

To add users, from the CMM menu, choose **Administration > RBAC > User Configuration**.

For detailed information, see “Managing Users and Access” in the *User Guide for Cisco Multicast Manager, 3.1* at the following location:

http://www.cisco.com/en/US/docs/net_mgmt/cisco_multicast_manager/3.1/user/guide/cmm_admin.html#wp1057710

Setting Up Troubleshooting Configuration for IP Multicast

Configuring IP multicast configuration settings in CMM for VAMS 3.1 includes the following tasks:

- Configuring BPS/PPS Threshold Monitoring, page 2-21
- Configuring Tree Polling, page 2-22
- Configuring Health Checks, page 2-26

- Configuring IP Multicast Heartbeat Monitoring, page 2-27

Configuring BPS/PPS Threshold Monitoring

CMM 3.1 enables polling of flows from Cisco 7600 routers and Cisco 6500 devices without the use of video probes. This is referred to as probeless monitoring.

To set up BPS/PPS Threshold Monitoring:

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

Step 2 Select **Domain Management**.

The Domain Management Summary page appears,.

Step 3 Check the check box for the domain where you will configure BPS/PPS threshold monitoring and then click the **Edit** button.

The System Configuration page appears, as shown in Figure 2-1.

Step 4 On the System Configuration page, click the Telnet radio button to specify telnet as the CLI Access method, and check the CLI check box for **Threshold Polling.**

a. Enter a valid password VTY password in the VTY Password field and in the Verify field.

b. Click **Save** to save the domain configuration.

Step 5 To configure SG polling and set up PPS/BPS thresholds, from the CMM menu, select **Polling Configuration & Reports > Traffic Polling & Reports> SG.**

Step 6 On the SG Threshold Report page, click **Config SG Polling**.

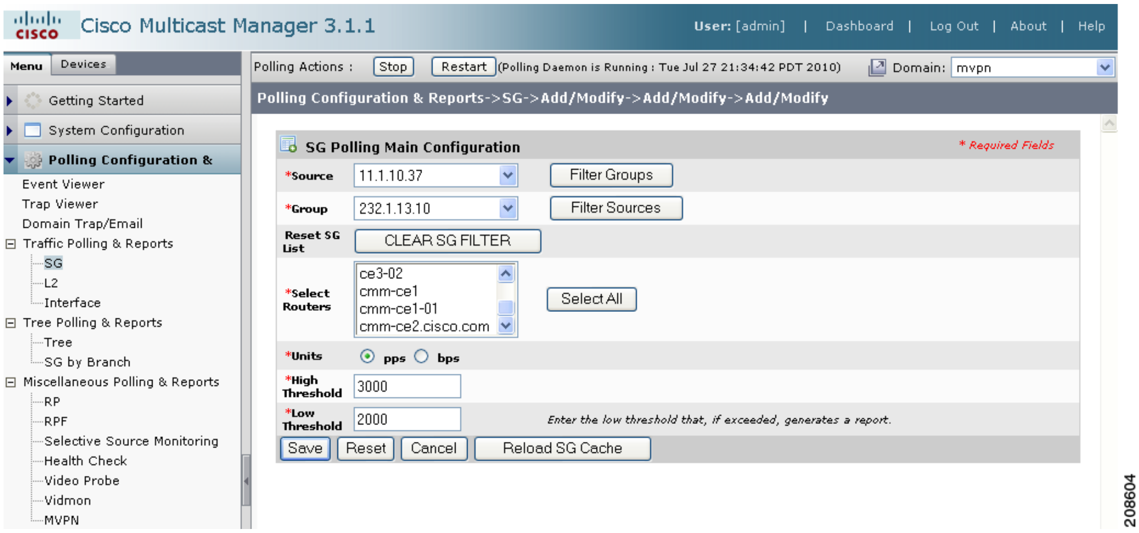
The SG Configurations page opens.

Step 7 On the SG Configurations page, do one of the following:

- To add a new SG polling configuration, click the **Add** button, and from the pull-down menu, choose By SG.
- To edit an existing SG polling configuration, check the check box for an existing configuration and click the **Edit** button.

The main SG Polling Configuration page opens, as shown in Figure 2-9.

Figure 2-9 SG Polling Configuration Page



(Polling Daemon is Running : Tue Jul 27 21:34:42 PDT 2010)

Domain: mvpn

Polling Configuration & Reports->SG->Add/Modify->Add/Modify->Add/Modify

SG Polling Main Configuration

* Required Fields

*Source	11.1.10.37
*Group	232.1.13.10
Reset SG List	
*Select Routers	ce3-02 cmm-ce1 cmm-ce1-01 cmm-ce2.cisco.com
*Units	● pps ○ bps
*High Threshold	3000
*Low Threshold	2000

Enter the low threshold that, if exceeded, generates a report.

Step 8 Configure PPS/BPS thresholds as described in the "Config S,G Polling" section of the "Polling Configuration and Reports" chapter in the "*User Guide for Cisco Multicast Manager 3.1* at the following location:

http://www.cisco.com/en/US/docs/net_mgmt/cisco_multicast_manager/3.1/user/guide/cmm_pc.html#wp1081147

Configuring Tree Polling

Multicast trees can change due to network outages or in response to establishment of more optimal flow paths. Because tree changes might impact video quality immediately or in the future, it is important for network operators to be notified of changes in multicast trees.

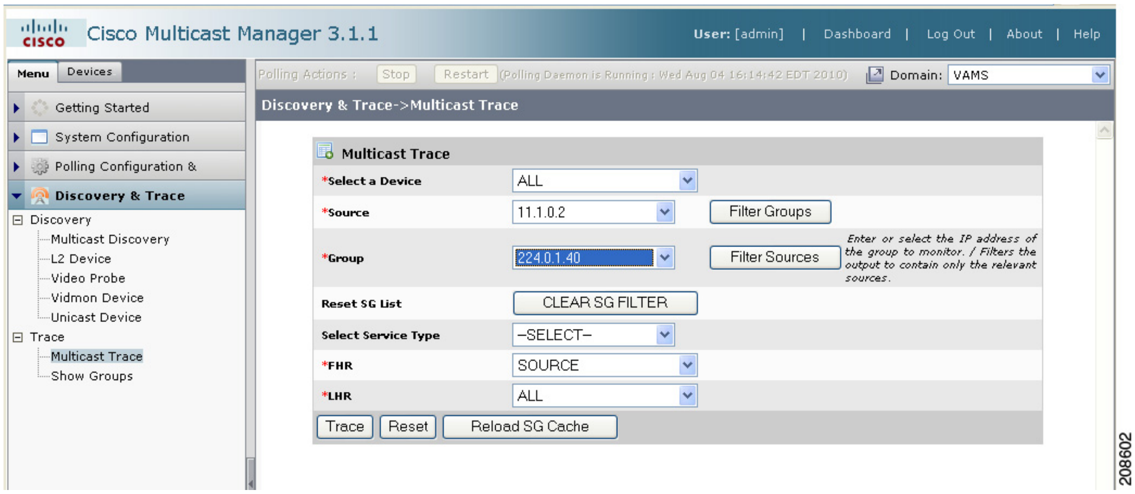
To configure tree polling, you must first create a trace file by drawing a multicast tree and saving it.

To configure tree polling:

Step 1 From the CMM main menu, select **Discovery & Trace > Trace > Multicast Trace**.

The Multicast Trace page appears, as shown in Figure 2-10.

Figure 2-10 Multicast Trace Page



*Select a Device: ALL

*Source: 11.1.0.2

*Group: 224.0.1.40

Enter or select the IP address of the group to monitor. / Filters the output to contain only the relevant sources.

Reset SG List: CLEAR SG FILTER

Select Service Type: --SELECT--

*FHR: SOURCE

*LHR: ALL

Step 2 From the drop-down list in the **Select a Device** field, select the device for the trace.

Step 3 From the drop-down list in the **Source** field, select a source to work on.

Step 4 From the drop-down list in the **Group** field, select a group to work on.

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

Step 5 For additional details, see the "Multicast Trace" section in the *User Guide for Cisco Multicast Manager 3.1* at this location:

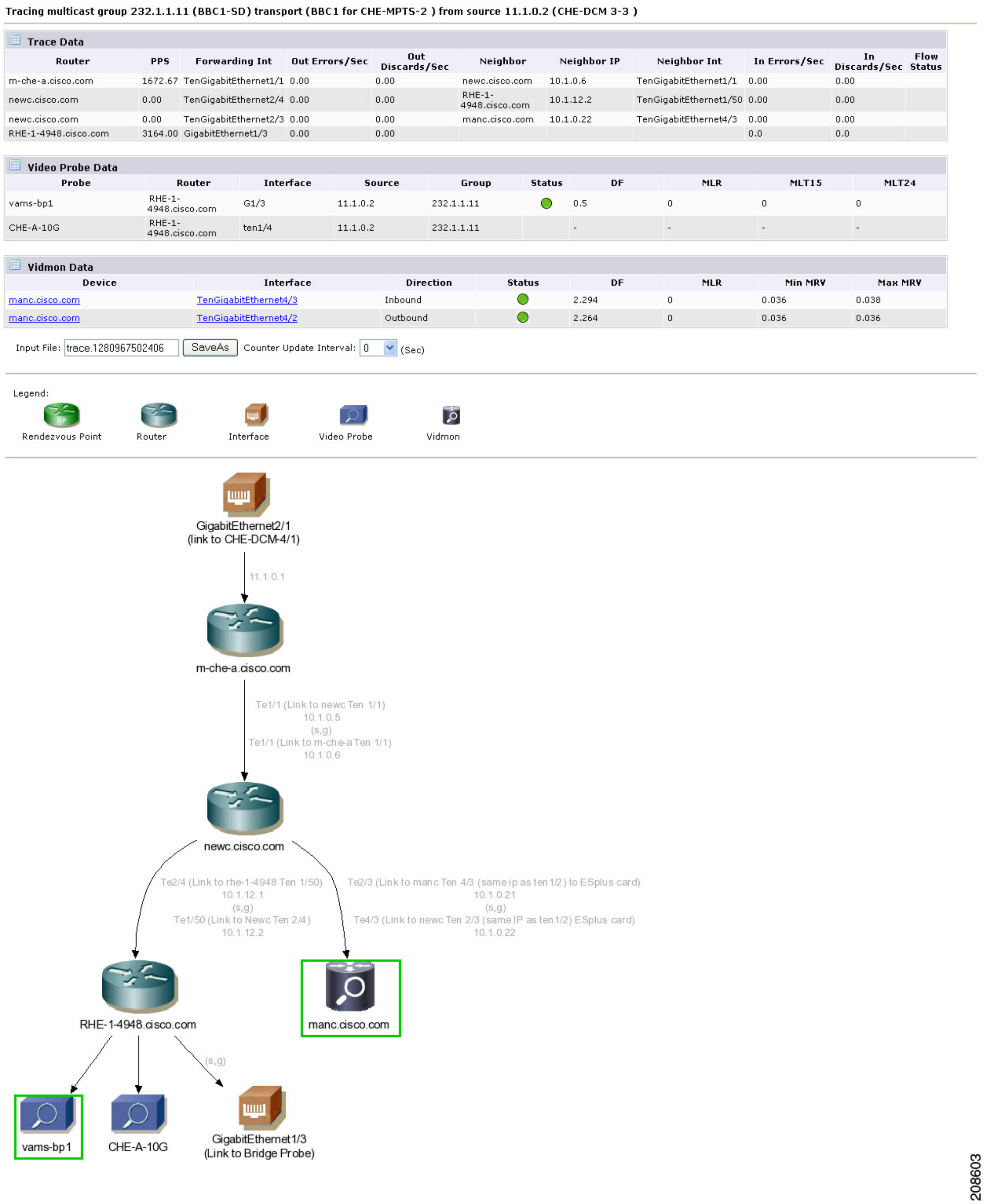
http://www.cisco.com/en/US/docs/net_mgmt/cisco_multicast_manager/3.1/user/guide/cmm_dt.html#wp1054116

Step 6 Click the **Trace** button.

CMM displays a Trace Data page for the trace and draws a tree diagram of the tree.

Figure 2-11 shows the Trace Data page.

Figure 2-11 CMM Trace Data Page



Tracing multicast group 232.1.1.11 (BBC1-SD) transport (BBC1 for CHE-MPTS-2) from source 11.1.0.2 (CHE-DCM 3-3)

Trace Data

Router	PPS	Forwarding Int	Out Errors/Sec	Out Discards/Sec	Neighbor	Neighbor IP	Neighbor Int	In Errors/Sec	In Discards/Sec	Flow Status
m-che-a.cisco.com	1672.67	TenGigabitEthernet1/1	0.00	0.00	newc.cisco.com	10.1.0.6	TenGigabitEthernet1/1	0.00	0.00	
newc.cisco.com	0.00	TenGigabitEthernet2/4	0.00	0.00	RHE-1-4948.cisco.com	10.1.12.2	TenGigabitEthernet1/50	0.00	0.00	
newc.cisco.com	0.00	TenGigabitEthernet2/3	0.00	0.00	manc.cisco.com	10.1.0.22	TenGigabitEthernet4/3	0.00	0.00	
RHE-1-4948.cisco.com	3164.00	GigabitEthernet1/3	0.00	0.00				0.0	0.0	

Video Probe Data

Probe	Router	Interface	Source	Group	Status	DF	MLR	MLT15	MLT24
vams-bp1	RHE-1-4948.cisco.com	G1/3	11.1.0.2	232.1.1.11	●	0.5	0	0	0
CHE-A-10G	RHE-1-4948.cisco.com	ten1/4	11.1.0.2	232.1.1.11		-	-	-	-

Vidmon Data

Device	Interface	Direction	Status	DF	MLR	Min MRV	Max MRV
manc.cisco.com	TenGigabitEthernet4/3	Inbound	●	2.294	0	0.036	0.038
manc.cisco.com	TenGigabitEthernet4/2	Outbound	●	2.264	0	0.036	0.036

Input File: trace.1280967502406 SaveAs Counter Update Interval: 0 (Sec)

The Trace Data page shows the following information:

- **Flow Description**—Includes Multicast Group, Channel Name, Transport Description, Source IP and Source description, as configured in CMM for the flow.
- **Trace Data table**—Includes the routers, interfaces, and PIM neighbors that transport the multicast flow.

- **Video Probe Data table**,—Shows 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 such as delay factor (DF) and media loss rate (MLR).
- **VidMon Data table**—Shows all the VidMon-enabled routers present in the distribution tree media rate variation (MRV). Clicking on a hostname displays the VidMon flow status for the flows transmitted by the selected host. Clicking on an interface name in the table displays the status of the flows transmitted over the interface.
- **Channel Data Table**—For multicast flows that have data transmitted over multiple channels, shows 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.
- **Topology Diagram—**Shows a topology diagram of the devices and video probes in the trace.

Step 7 To save the trace to use as a baseline for tree polling, in the Trace File field, enter a name the trace file, and then click **Save As**.

Step 8 To set up tree polling for the saved baseline, complete these steps:

a. From the CMM menu, select **Polling Configuration & Reports > Tree Polling & Reports > Tree.**

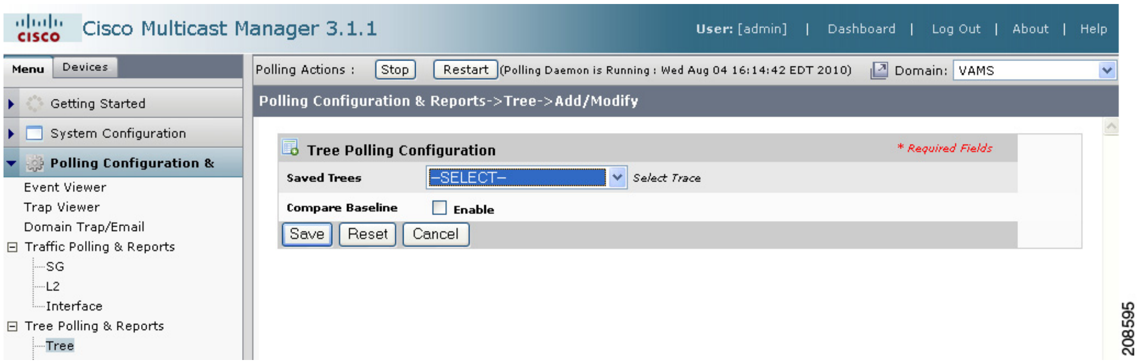
The Tree Report page opens.

b. Click **Config Tree Polling**.

c. Click the **Add** button.

Step 9 The Tree Polling Configuration page opens, as shown in Figure 2-12.

Figure 2-12 Tree Polling Configuration Page



(Polling Daemon is Running : Wed Aug 04 16:14:42 EDT 2010)

Domain: VAMS

Polling Configuration & Reports->Tree->Add/Modify

Tree Polling Configuration * Required Fields

Saved Trees: –SELECT– Select Trace

Compare Baseline: □ Enable

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

Fields and Buttons	Description
Refresh Status	The status line indicates how long the polling daemon has been running and how it was started. Click **Refresh Status** to update the status information.
Restart	Starts the polling daemon globally.
Stop	Stops the polling daemon globally.
Saved Trees	The drop-down list in the Saved Trees field lists saved trace files.

Fields and Buttons	Description
Reset	Resets the tree polling configuration.
Compare Baseline	Allows you to perform polling by comparing with a baseline trace file.

Step 10 To monitor a tree, from the drop-down menu in the **Saved Trees field,** select the tree name.

Step 11 Leave the **Compare Baseline** check box unchecked.

Step 12 Click the **Save** button.

Step 13 To specify how often the tree is polled:

a. From the CMM main menu, select **System Configuration > Global Polling Configuration.**

The Global Polling Configuration Page appears.

b. Specify the tree polling interval and click the **Save** button.

The tree is drawn in the background for every interval that you set up for tree polling. This tree is compared with the tree saved in the database. If it is different, a trap is sent, and a report is generated.

Configuring Health Checks

CMM provides the ability to set up health checks that check and report on the status of critical components of your IP multicast network. Health checks can check the status of RPs, MSDP peering, the presence of sources and groups, and the status of multicast trees.

You should create a health check for every important source and group in your multicast network.

To configure health check polling:

Step 1 From the CMM main menu, choose **Polling Configuration & Reports > Miscellaneous Polling & Reports > Health Check.**

The Health Check Report page opens.

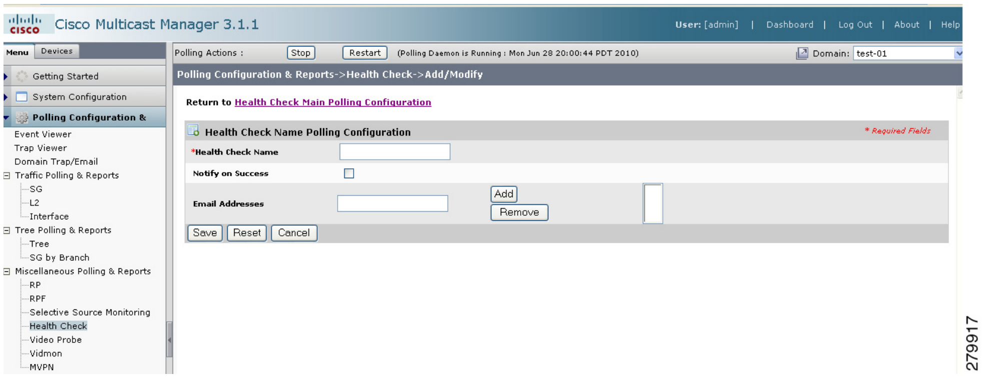
Step 2 Click **Config Health Check Polling**.

The Health Check Polling Configurations page opens.

Step 3 Click the **Add** button.

The Health Check Name Polling Configuration page appears, as shown in Figure 2-13.

Figure 2-13 Health Check Name Polling Configuration Page



(Polling Daemon is Running : Mon Jun 28 20:00:44 PDT 2010)

Domain: test-01

Return to Health Check Main Polling Configuration

The Health Check Config/Polling page contains the following fields and buttons:

Fields and Buttons	Description
Health Check Name	Enter a name for the health check.
Save	Saves the new health check.
Cancel	Cancels the configuration and returns you to the previous page.
Resets	Resets the information in the fields.
Notify on Success	Generates an email report if the health check completes successfully.
Email Addresses	Enter the email addresses to be notified. Click the **Add button** add an email address to the list of email addresses. Click the Remove button to remove an email address from the list.

Configuring IP Multicast Heartbeat Monitoring

Cisco routers can monitor the data plane of a multicast group and detect when that group is no longer receiving multicast packets. This is useful to confirm that the traffic stream is active.

To set up heartbeat monitoring requires that a downstream router or host has joined a multicast group or a static IGMP has been set; a data path must be established through the router that is configured for heartbeat monitoring.

Configuring heartbeat monitoring consists of two steps:

1. Configuring IP multicast on a router.
2. Enabling monitoring for the router.

Configuring IP Multicast Heartbeat on the Router

To configure IP multicast heartbeat on a router for which you want to enable IP multicast heartbeat, enter the following commands:

```
snmp-server enable traps ipmulticast
```

```
ip multicast heartbeat <ip_address> <minimum_number> <intervals> <interval_length>
```

where *ip_address* is the IP address of the router, *minimum_number* is the minimum number of intervals, *intervals* is the number of intervals, and *interval_length* is the length of the intervals in seconds.

The following is an example configuration of the ip multicast heartbeat command:

```
snmp-server enable traps ipmulticast-heartbeat
ip multicast heartbeat 224.0.1.53 1 1 10
```

Configuring Video Probes

Each video probe in Cisco VAMS 3.1 monitors various parameters of the video flow through the network. For example, you might configure a video probe to monitor the amount of jitter or delay in a video stream.

For each video probe deployed in the network, you must configure the thresholds for the conditions that you want to monitor. Only probes not supported by CMM should trap directly to Cisco Info Center—for these probes you must also configure the video probes to forward traps to Cisco Info Center. (See the probe documentation for information on adding the Cisco Info Center IP addresses and related SNMP information to the video probe settings.)

After you configure the video probe, if a monitored condition exceeds a configured threshold, the probe sends a corresponding trap to Cisco Info Center, which shows the event in the TBSM GUI and the CIC GUI.

Note CMM 3.1 will poll the IneoQuest probes even though the probes may also be sending traps to Cisco Info Center.

Bridge Technologies Video Probe

You can configure the Bridge Technologies video probe to send traps directly to Cisco Info Center. To configure the Bridge Technologies video probe for operation in the video transport network, see the documentation that comes with the product. The *VB120 Broadcast IP-Probe User's Manual v. 4.0* assists the network planner when integrating the Bridge Technologies video probes with Cisco VAMS 3.1.

IneoQuest Video Probe

You can configure the IneoQuest video probe to send alerts to CMM and configure CMM to forward the alerts to Cisco Info Center.

To configure the IneoQuest video probe for operation in the video transport network, see the documentation that comes with the product. These documents assist the network planner when integrating the IneoQuest video probes with Cisco VAMS 3.1:

- *Hardware User's Guide*
- *IQMediaAnalyzer Application User's Guide*

Mixed Signals Video Probe

You can configure the Mixed Signals video probe to send traps directly to Cisco Info Center. To configure the Mixed Signals video probe for operation in the video transport network, see the documentation that comes with the product. The *Mixed Signals Sentry Digital Content Monitor User Guide* assists the network planner when integrating the Mixed Signals video probes with Cisco VAMS 3.1.

Configuring VidMon Polling

You can configure VidMon polling by importing a text file that specifies VidMon polling configuration or by entering the polling configuration in the CMM interface.

If you use a text file, the file must have the following format:

```
VIDMON:10.1.0.22,0,50000,10000,-10000,20
```

To configure Vidmon alerts in CMM:

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

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

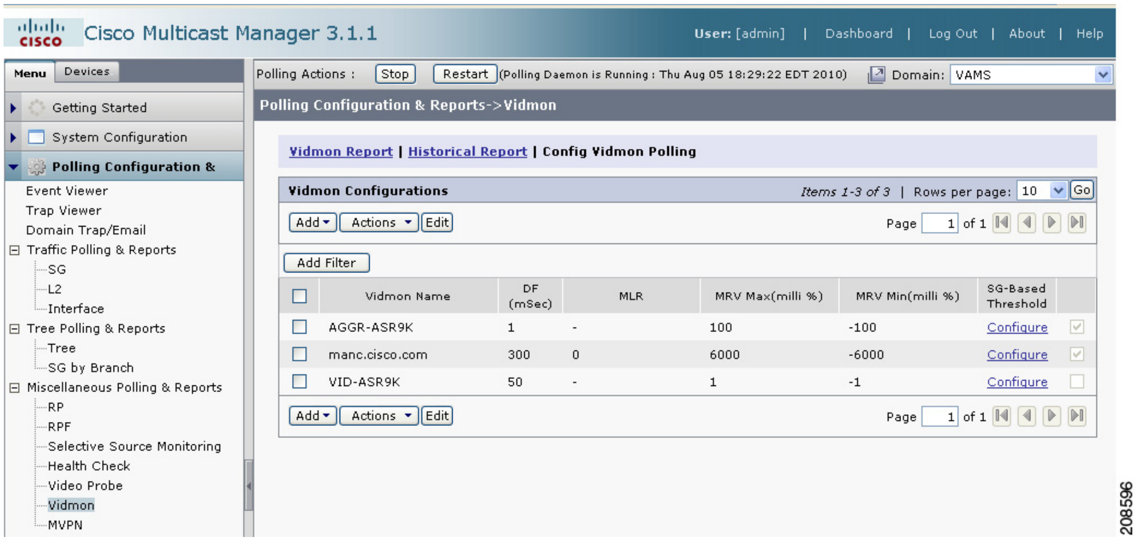
Step 3 Select **Vidmon**.

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

Step 4 Select **Config Vidmon Polling.**

The Config Vidmon Polling page appears, as shown in Figure 2-14.

Figure 2-14 Config Vidmon Polling Page



(Polling Daemon is Running : Thu Aug 05 18:29:22 EDT 2010)

Domain: VAMS

Rows per page: 10

□	Vidmon Name	DF (mSec)	MLR	MRV Max(milli %)	MRV Min(milli %)	SG-Based Threshold	
□	AGGR-ASR9K	1	-	100	-100	Configure	☑
□	manc.cisco.com	300	0	6000	-6000	Configure	☑
□	VID-ASR9K	50	-	1	-1	Configure	□

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 To add a VidMon polling configuration, do one of the following:

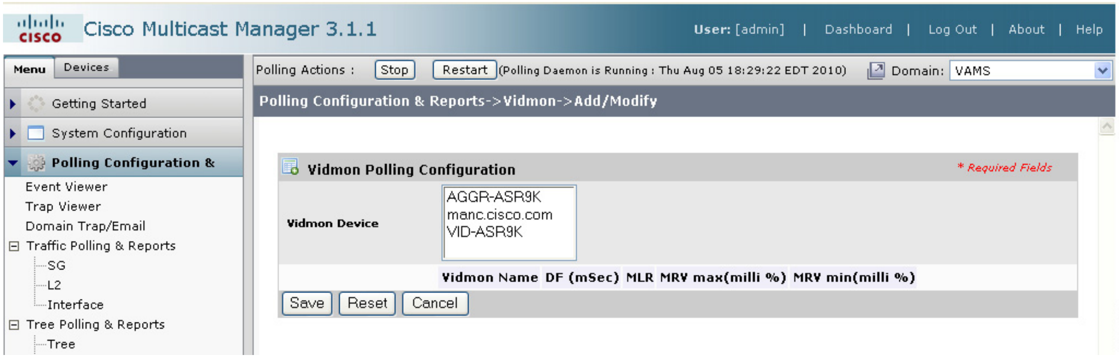
- To add a new configuration using the CMM interface, click the **Add** button, and from the drop-down list, select **By Vidmon**.
- To add a VidMon configuration by importing a text file, click the **Add** button and from the drop-down list, select **By Import**.

If you select **By Import,** you are prompted for the folder path and filename for a CSV file containing the Vidmon configuration.

Step 6 If you selected **By Import**, browse for the import file containing the VidMon polling configuration and then click the **Upload** button.

If you select **By Vidmon**, the Vidmon Polling Configuration page appears, as shown in Figure 2-15.

Figure 2-15 Vidmon Polling Configuration Page with List of Vidmon Devices



Polling Actions : (Polling Daemon is Running : Thu Aug 05 18:29:22 EDT 2010) Domain: VAMS

Polling Configuration & Reports->Vidmon->Add/Modify

Vidmon Polling Configuration * Required Fields

Vidmon Device: AGGR-ASR9K, manc.cisco.com, VID-ASR9K

Vidmon Name	DF (mSec)	MLR	MRV max(milli %)	MRV min(milli %)

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

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

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

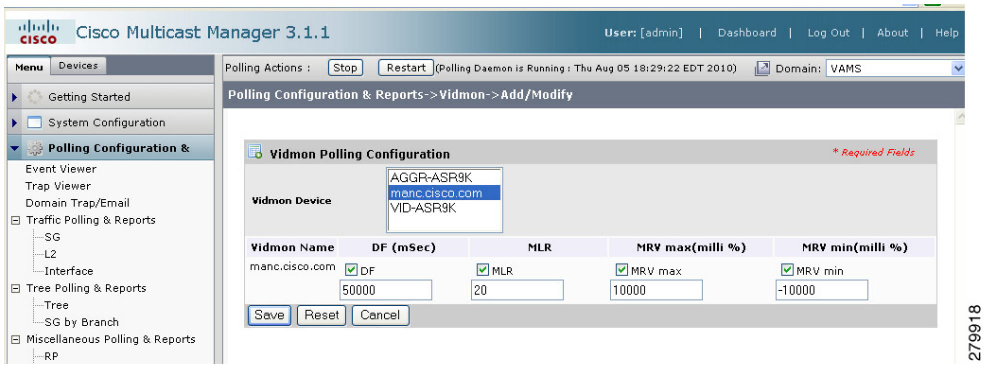
Step 8 To configure polling for a device, check the check box next to the configuration option for the device.

For example, to configure a delay factor for a device, click the **DF** field.

As you select configuration fields, the field becomes active.

Figure 2-16 shows all configuration fields for the devices selected in Figure 2-15 selected.

Figure 2-16 Vidmon Polling Configuration Fields



Polling Actions : (Polling Daemon is Running : Thu Aug 05 18:29:22 EDT 2010) Domain: VAMS

Polling Configuration & Reports->Vidmon->Add/Modify

Vidmon Polling Configuration * Required Fields

Vidmon Device: AGGR-ASR9K, manc.cisco.com, VID-ASR9K

Vidmon Name	DF (mSec)	MLR	MRV max(milli %)	MRV min(milli %)
manc.cisco.com	☑ DF 50000	☑ MLR 20	☑ MRV max 10000	☑ MRV min -10000

Step 9 Enter Vidmon polling configuration parameters as indicated in Table 2-1.

Table 2-1 Vidmon Polling Configuration Options

Configuration Option	Description
DF	Enter a delay factor (DF) in milliseconds. When the delay factor is exceeded, CMM generates a delay factor event.
MLR	For Cisco 76xx devices, enter a Media Loss Rate (MLR) threshold value (number of packets). When the MLR threshold is exceeded, CMM generates an alert. **Note** MLR monitoring is not available for Viking devices (Cisco ASR 9000 devices).
MRV max (milli %)	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 is exceeded, CMM generates a VIDMON MRV HIGH alert.
MRV min (milli %)	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.

Step 10 To save the Vidmon polling configuration, click the **Save** button.

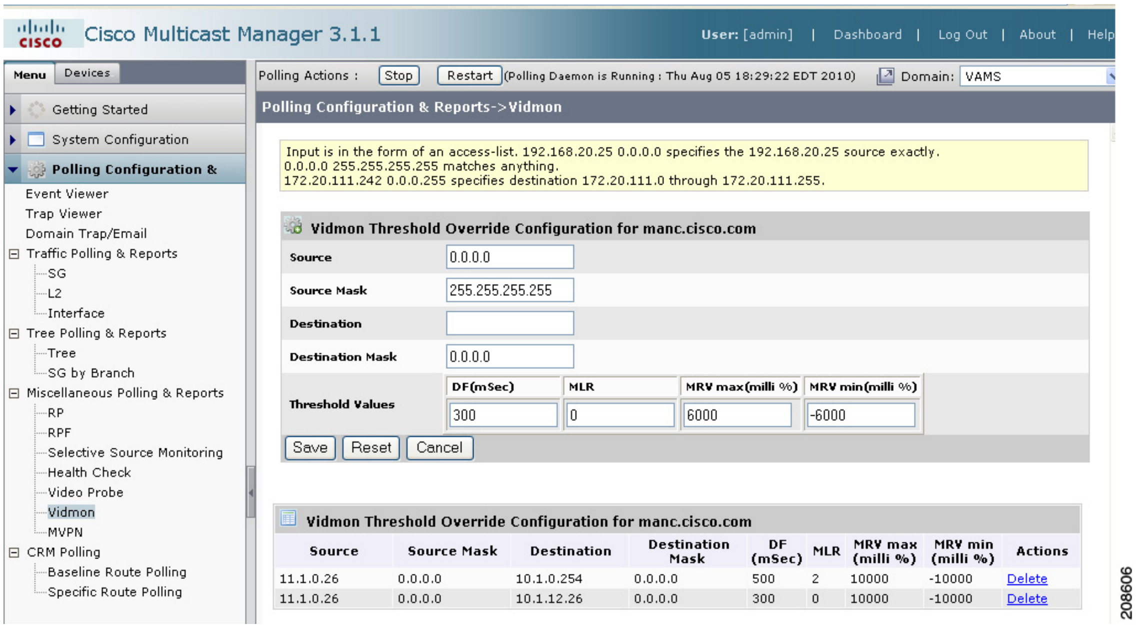
After you have saved the device-level VidMon threshold configuration, you can configure individual thresholds for the flows on the device.

Step 11 To configure VidMon thresholds at the flow level:

a. Click the **Configure** link in the SG-Based Threshold column in the entry for a device.

The Vidmon Threshold Override Configuration page appears, as shown in Figure 2-17.

Figure 2-17 Vidmon Threshold Override Configuration Page



(Polling Daemon is Running : Thu Aug 05 18:29:22 EDT 2010)

Polling Configuration & Reports->Vidmon

Input is in the form of an access-list. 192.168.20.25 0.0.0.0 specifies the 192.168.20.25 source exactly.
0.0.0.0 255.255.255.255 matches anything.
172.20.111.242 0.0.0.255 specifies destination 172.20.111.0 through 172.20.111.255.

Vidmon Threshold Override Configuration for manc.cisco.com

Source	0.0.0.0			
Source Mask	255.255.255.255			
Destination				
Destination Mask	0.0.0.0			
Threshold Values	DF(mSec)	MLR	MRV max(milli %)	MRV min(milli %)
	300	0	6000	-6000

Vidmon Threshold Override Configuration for manc.cisco.com

Source	Source Mask	Destination	Destination Mask	DF (mSec)	MLR	MRV max (milli %)	MRV min (milli %)	Actions
11.1.0.26	0.0.0.0	10.1.0.254	0.0.0.0	500	2	10000	-10000	Delete
11.1.0.26	0.0.0.0	10.1.12.26	0.0.0.0	300	0	10000	-10000	Delete

CMM uses an Access Control List (ACL) to identify the flow. You can specify the exact IP address for the ACL, a wildcard that matches any IP address, or an IP address range. The information area at the top of the Vidmon Threshold Override Configuration page describes how the ACL mask works:

```
192.168.20.25 0.0.0.0 specifies the 192.168.20.25 source exactly.
0.0.0.0 255.255.255.255 matches anything.
172.20.111.242 0.0.0.255 specifies destination 172.20.111.0 through 172.20.111.255.
```

Step 12 Check the configuration for the selected router to verify the ACL list configuration.

Step 13 On the Vidmon Threshold Override Configuration page, specify the following:

- An Access Control List (ACL) to identify the flow on the device. Enter information in the following fields:
  - **Source**—Specifies the IP address of the source router.
  - **Source Mask**—Specifies either 0.0.0.0 to indicate the exact IP address of the router or a mask to specify a range of IP addresses.
  - **Destination**—Specifies the IP address of the destination router.
  - **Destination Mask**—Specifies either 0.0.0.0 to indicate the exact IP address of the router or a mask to specify a range of IP addresses.
- **Threshold Values for the Flow**—Specifies the threshold settings. For a description of the settings, see Table 2-1 on page 2-31.

Step 14 Click the **Save** button to save the flow level threshold configuration.

Configuring the ROSA NMS

This section describes specific ROSA NMS configuration tasks that are required to configure the application to work with Cisco VAMS 3.1. For more detailed information, see:

- The README file for the ROSA Copernicus NMS. This file launches automatically when you insert the ROSA NMS installation CD in your Windows server or Windows workstation.
- The *ROSA Network Management System User's Guide, Version 3.0 Build 18*. This document is provided in PDF format on CD 1 of the ROSA NMS installation media.
- *SNMP Agent Users Guide, Task Driver for ROSA 3.0*. This document is provided on the Documentation CD for the ROSA Copernicus Network Management System server.

This section describes:

- Configuring the SNMP Agent, page 2-33
- Configuring a Northbound Trap Destination, page 2-34
- Ensuring That the Alarm Suppression Rule is Disabled, page 2-36

Configuring the SNMP Agent

ROSA Copernicus Network Management System server software includes SNMP agent software for the ROSA system. To enable Cisco VAMS 3.1 monitoring of ROSA NMS events, you must configure the SNMP agent to send ROSA NMS traps to Cisco Info Center

To configure the SNMP Agent for the Copernicus NMS server:

Step 1 Install the SNMP agent on your ROSA Copernicus NMS server.

For detailed installation instructions, refer to “Installing the SNMP Agent Task Driver” in the *SNMP Agent Users Guide, Task Driver for ROSA 3.0*. This document is provided on the Documentation CD for the ROSA Copernicus Network Management System server.

Step 2 On the ROSA client, go to the Server Explorer window.

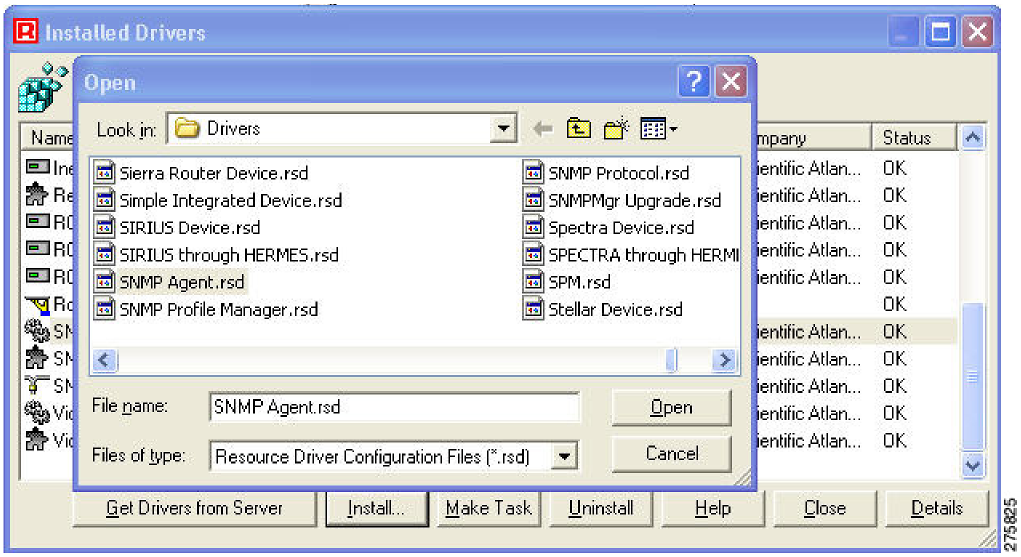
Step 3 Select **Config > Drivers.**

The Installed Drivers dialog appears.

Step 4 Click the **Install** button.

A list of installed drivers appears, as shown in Figure 2-18:

Figure 2-18 SNMP Install Screen



File name: SNMP Agent.rsd

Files of type: Resource Driver Configuration Files (*.rsd)

Step 5 Highlight the *SNMP Agent.rsd* driver and click **Open**.

The Make Task dialog appears.

Step 6 On the Make Task dialog, enter a task name, such as *SNMP Agent*, and then click **OK**.

The SNMP Agent task now appears in the Global Inventory directory on the ROSA interface.

Configuring a Northbound Trap Destination

After you add the SNMP task, you must specify a northbound trap destination to configure ROSA to send SNMP traps to Cisco Info Server.

To configure the northbound trap destination:

Step 1 On the ROSA interface, click the **Global** tab.

Step 2 In the Global Inventory directory tree, right-click the SNMP task, for example **SNMP Agent**.

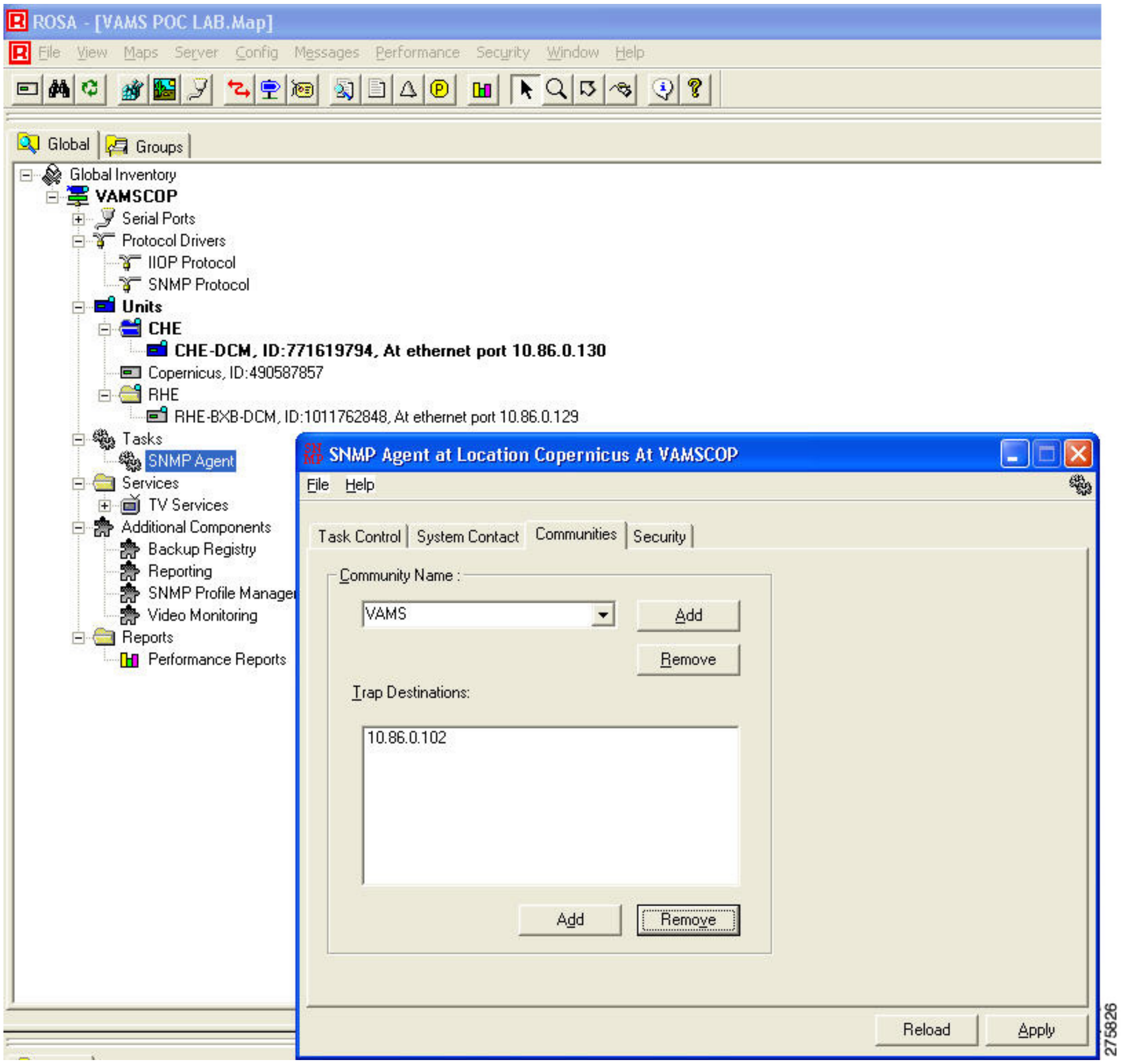
Step 3 From the pull-down menu for the task, select Properties.

The SNMP User Agent dialog appears.

Step 4 Click the **Communities** tab.

The Communities dialog appears, as shown in Figure 2-19:

Figure 2-19 Northbound Configuration Screen



Community Name : VAMS

Trap Destinations: 10.86.0.102

Step 5 In the Community Name field, enter the name of an SNMP community for the SNMP agent, for example, *VAMS*.

Step 6 Click **Apply**.

Step 7 After you have added the community for VAMS, complete these steps to add a northbound trap destination.

a. On the SNMP dialog, click the **Communities** tab.

The Add Trap Destination dialog appears.

b. Enter the IP address of the Cisco Info Center Object Server.

c. Click **OK**.

Step 8 Click **Apply**.

The SNMP Agent is now configured to forward traps to Cisco Info Center.

Ensuring That the Alarm Suppression Rule is Disabled

By default, the ROSA NMS is configured to disable the Repetitive Alarm Distribution Rule. However, if your ROSA NMS has this rule enabled, ROSA events might not clear automatically in Cisco Info Center, because the Repetitive Alarm Distribution Rule causes the ROSA NMS to generate Summary messages in the place of individual alarm messages. Because these Summary messages use incremented *trpMSGID* values, Cisco Info Center cannot associate them with the initial alarm event and clear that event.

To prevent this situation from occurring, if the ROSA NMS has the Repetitive Alarm Distribution Rule configured, Cisco recommends that you perform the following steps:

- Disable the Repetitive Alarm Distribution Rule—See Disabling the Repetitive Alarm Distribution Rule, page 2-36.
- Configure End Debouncing Timers on the DCM—See Configuring End Debouncing Timers on the DCM, page 2-37.

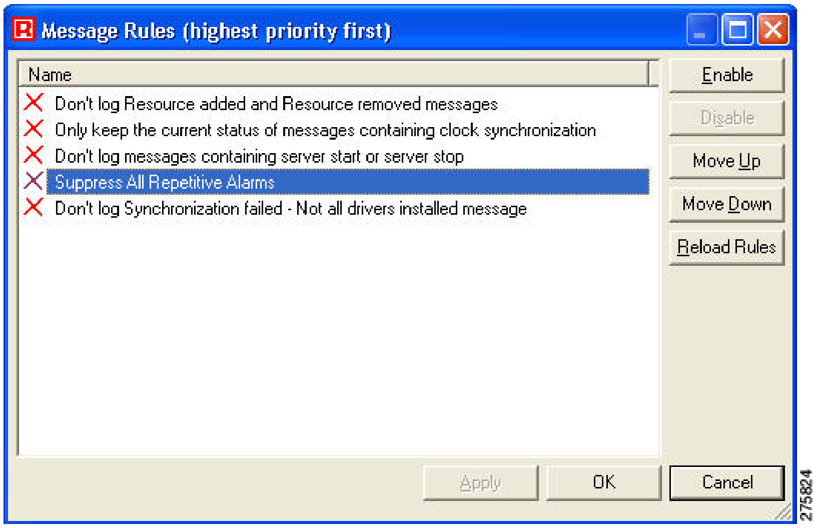
Disabling the Repetitive Alarm Distribution Rule

To disable the Repetitive Alarm Distribution Rule on the ROSA NMS:

Step 1 In the Server Explorer or Group Explorer directory tree on the ROSA system, select the server on which message rule scripts are added and from the pull-down menu, select **Rules**.

The Message Rules dialog appears, as shown in Figure 2-20:

Figure 2-20 ROSA Message Rules



Message Rules (highest priority first)

Name

- Don't log Resource added and Resource removed messages
- Only keep the current status of messages containing clock synchronization
- Don't log messages containing server start or server stop
- Suppress All Repetitive Alarms
- Don't log Synchronization failed - Not all drivers installed message

Step 2 Check the **Suppress All Repetitive Alarms** check box.

Step 3 Check the check boxes next to any other alarms that you want to disable.

Step 4 Click **Disable**.

Configuring End Debouncing Timers on the DCM

Enabling debouncing timers on the DCM will not completely resolve the issue of nonclearing ROSA events in Cisco Info Center if the ROSA Alarm Suppression Rule is enabled. However, properly configured DCM debouncing timers should greatly reduce the possibility of DCM events not automatically clearing in Cisco Info Center when the ROSA Alarm Suppression Rule is enabled. If DCM debouncing timers are configured, situations where the ROSA Alarm Suppression rule is needed are reduced, because the DCM will not generate as many alerts.

To configure End Debouncing timers:

Step 1 On the web browser user interface of the DCM, click the **Configuration** link.

The Configuration page appears.

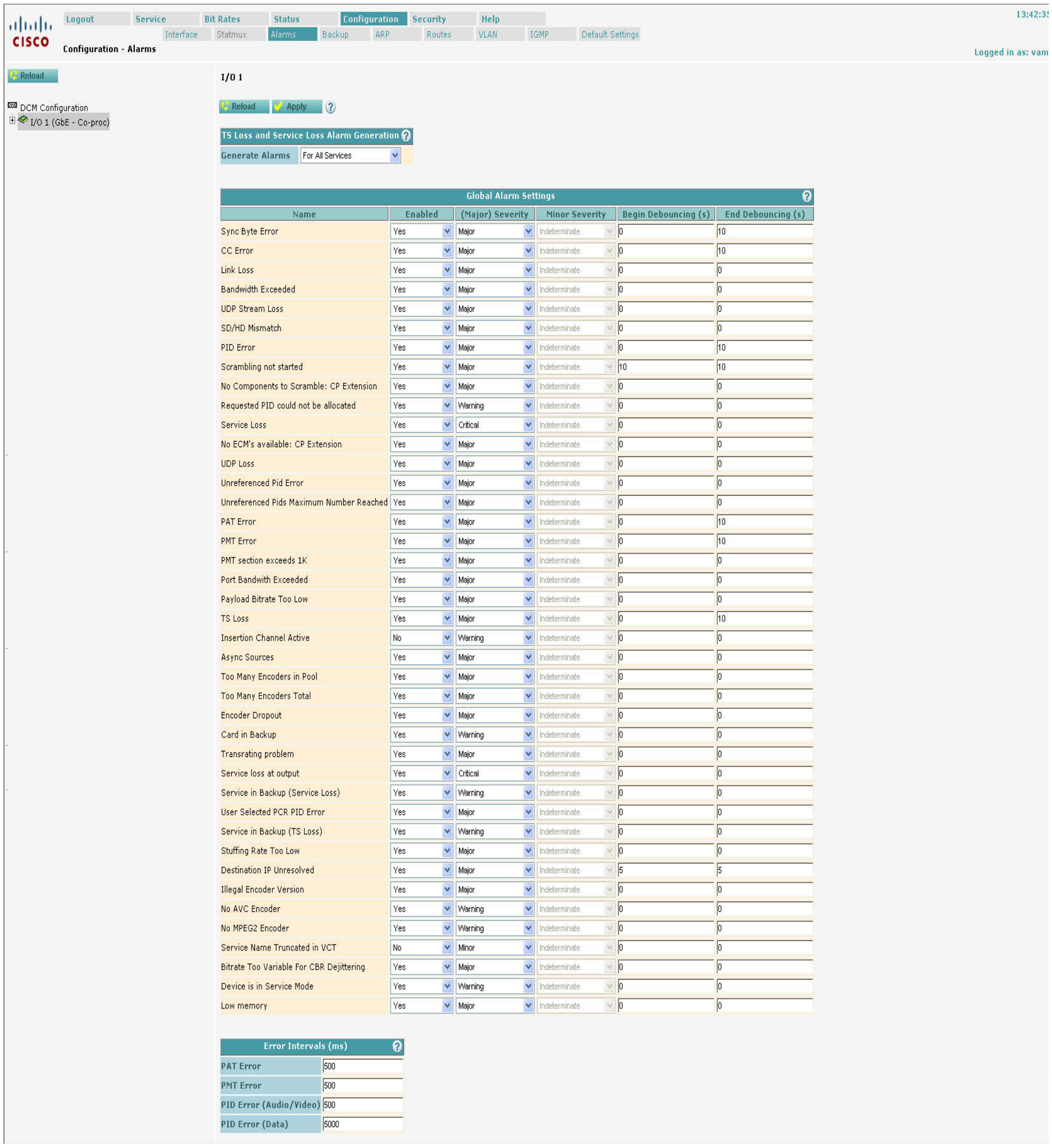
Step 2 In the DCM configuration tree, double-click on the interface card for which alarm settings must be configured.

The Configuration-Interface page for the selected interface card appears.

Step 3 Click the **Alarms** link.

The Configuration-Alarms dialog for the specified interface card appears, as shown in Figure 2-21.

Figure 2-21 ROSA End Debouncing Timer



Configuration - Alarms

I/O 1

TS Loss and Service Loss Alarm Generation

Generate Alarms	For All Services

Global Alarm Settings

Name	Enabled	(Major) Severity	Minor Severity	Begin Debouncing (s)	End Debouncing (s)
Sync Byte Error	Yes	Major	Indeterminate	0	10
CC Error	Yes	Major	Indeterminate	0	10
Link Loss	Yes	Major	Indeterminate	0	0
Bandwidth Exceeded	Yes	Major	Indeterminate	0	0
UDP Stream Loss	Yes	Major	Indeterminate	0	0
SD/HD Mismatch	Yes	Major	Indeterminate	0	0
PID Error	Yes	Major	Indeterminate	0	10
Scrambling not started	Yes	Major	Indeterminate	10	10
No Components to Scramble: CP Extension	Yes	Major	Indeterminate	0	0
Requested PID could not be allocated	Yes	Warning	Indeterminate	0	0
Service Loss	Yes	Critical	Indeterminate	0	0
No ECM's available: CP Extension	Yes	Major	Indeterminate	0	0
UDP Loss	Yes	Major	Indeterminate	0	0
Unreferenced Pid Error	Yes	Major	Indeterminate	0	0
Unreferenced Pids Maximum Number Reached	Yes	Major	Indeterminate	0	0
PAT Error	Yes	Major	Indeterminate	0	10
PMT Error	Yes	Major	Indeterminate	0	10
PMT section exceeds 1K	Yes	Major	Indeterminate	0	0
Port Bandwith Exceeded	Yes	Major	Indeterminate	0	0
Payload Bitrate Too Low	Yes	Major	Indeterminate	0	0
TS Loss	Yes	Major	Indeterminate	0	10
Insertion Channel Active	No	Warning	Indeterminate	0	0
Async Sources	Yes	Major	Indeterminate	0	0
Too Many Encoders in Pool	Yes	Major	Indeterminate	0	0
Too Many Encoders Total	Yes	Major	Indeterminate	0	0
Encoder Dropout	Yes	Major	Indeterminate	0	0
Card in Backup	Yes	Warning	Indeterminate	0	0
Transrating problem	Yes	Major	Indeterminate	0	0
Service loss at output	Yes	Critical	Indeterminate	0	0
Service in Backup (Service Loss)	Yes	Warning	Indeterminate	0	0
User Selected PCR PID Error	Yes	Major	Indeterminate	0	0
Service in Backup (TS Loss)	Yes	Warning	Indeterminate	0	0
Stuffing Rate Too Low	Yes	Major	Indeterminate	0	0
Destination IP Unresolved	Yes	Major	Indeterminate	5	5
Illegal Encoder Version	Yes	Major	Indeterminate	0	0
No AVC Encoder	Yes	Warning	Indeterminate	0	0
No MPEG2 Encoder	Yes	Warning	Indeterminate	0	0
Service Name Truncated in VCT	No	Minor	Indeterminate	0	0
Bitrate Too Variable For CBR Dejittering	Yes	Major	Indeterminate	0	0
Device is in Service Mode	Yes	Warning	Indeterminate	0	0
Low memory	Yes	Major	Indeterminate	0	0

Error Intervals (ms)	
PAT Error	500
PMT Error	500
PID Error (Audio/Video)	500
PID Error (Data)	5000

275823

Step 4 Enter a timer value in the End Debouncing column for each enabled alarm. Make sure that you enter values for the following alarms:

- Sync Byte Error
- CC Error
- PID Error
- Scrambling not started
- PAT Error
- PMT Error

- TS Loss

Step 5 Click **Apply**

Configuring Cisco Info Center

For information on configuring Cisco Info Center for use with Cisco VAMS 3.1, see the *Cisco VAMS 3.1 Solution Deployment Guide*. This document is available on the Cisco Developer Network (CDN) website.