User Guide for Cisco Video Assurance Management Solution 3.1

July 6, 2011

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

Text Part Number: OL-24866-01

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

User Guide for Cisco Video Assurance Management Solution, 3.1

CONTENTS

Preface

This preface describes the objectives, audience, organization, and conventions of the *User Guide for Cisco Video Assurance Management Solution 3.1*.

Note Use this document along with the documents listed in the "Related Documentation" section on page viii.

This preface contains:

In this guide, many installation and configuration procedures refer to Cisco product documentation with corresponding references made to specified product documentation guides (supplied during site installation or available online at Cisco.com). See the referenced sections of the product documentation for detailed information on the tasks you are working on.

Objectives

This guide describes the architecture, the components, and the processes necessary for the design and implementation of the Cisco Video Assurance Management Solution (Cisco VAMS), Release 3.1.

Audience

The target audience for the Cisco VAMS guide should have a basic knowledge of network management products, and experience with the installation and acceptance of these products covered by this solution.

In addition, the user should understand the procedures to upgrade and troubleshoot video systems and Ethernet switches.

Note This guide addresses Cisco components only. It does not discuss how to implement third-party components optionally supported for video management capabilities.

Document Organization

The major sections of this guide are:

Chapter	Title	Description
Chapter 1	Overview	Introduces the implementation and scope of Cisco VAMS, its components, and miscellaneous support topics.
Chapter 2	Installing and Configuring the Components of Cisco Video Assurance Management Solution 3.1	Describes how to install and configure the components of Cisco VAMS 3.1.
Chapter 3	Troubleshooting with Cisco Video Assurance Management Solution 3.1	Provides information about troubleshooting with Cisco VAMS 3.1.
Appendix A	Trap Definitions	Provides definitions of traps that the Cisco VAMS 3.1 supports.
Appendix B	End User License Agreement Supplement	Provides an end-user license agreement supplement.
Glossary	Glossary	Defines technical terms used in this guide.

Related Documentation

Refer to the following sections for information on related documentation:

- Cisco VAMS 3.1 Documentation, page ix

- Documentation for VAMS Components, page ix

Cisco VAMS 3.1 Documentation

In addition to the *User Guide for Cisco Video Assurance Management Solution, 3.1*, the Cisco VAMS documentation set comprises:

- *Release Notes for Cisco Video Assurance Management Solution, 3.1*

  Describes system requirements, and provides installation notes, information on system limitations, and a list of open caveats.

- *Documentation Guide for Cisco Video Assurance Management Solution, 3.1*

  Provides links to the documentation for the Cisco VAMS 3.1 component products and for related products. This document is viewable online at:

  http://www.cisco.com/en/US/products/ps9518/products_documentation_roadmaps_list.html

Documentation for VAMS Components

For links to the documentation for the VAMS product components, see the *Documentation Guide for Cisco Video Assurance Management Solution, 3.1,* viewable online at:

http://www.cisco.com/en/US/products/ps9518/products_documentation_roadmaps_list.html

Document Conventions

This guide uses the following conventions to convey instructions and information.

Convention	Description
boldface font	Commands and keywords.
italic font	Variables for which you supply values.
[ ]	Keywords or arguments that appear within square brackets are optional.
{x | y | z}	A choice of required keywords appears in braces separated by vertical bars. You must select one.
`screen font`	Examples of information displayed on the screen.
`boldface screen font`	Examples of information you must enter.
< >	Nonprinting characters, for example passwords, appear in angle brackets.
[ ]	Default responses to system prompts appear in square brackets.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Tip Means the following information *will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Obtaining Documentation and Submitting a Service Request

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:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

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 by using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

CHAPTER 1

Overview

This chapter provides an overview of the architecture, components, and features of Cisco Video Assurance Management Solution (Cisco VAMS) 3.1.

This chapter contains the following sections:

Introduction to Cisco VAMS 3.1

Cisco VAMS 3.1 provides service providers with a modular, end-to-end video assurance management architecture, including real-time, centralized monitoring of headends, hubs, core, distribution, regional, and aggregation networks for broadcast video services.

Cisco VAMS includes a service-aware dashboard that pinpoints and correlates alarms related to video service availability and quality from the headend or the transport network. Using Cisco VAMS you can monitor video services such as linear broadcast and video on demand (VoD) based on MPEG transport streams (TS) and uncompressed flows.

You can:

- Monitor the health and performance of the network.
- Analyze and troubleshoot faults and exceptions.
- Ensure security, accountability, and compliance with organizational policies and regulatory requirements.
- Implement inline video monitoring (VidMon) on the Cisco ASR 9000 and Cisco 7600 platforms.

See the "Solution Component Versions" section on page 1-11 for descriptions of the solution components and required software versions.

VAMS displays video services as channel services. For each video channel, one service is displayed. A service tree for the video service shows each channel. For each channel, the service view shows the multicast aliases associated with the channel in the configuration for the multiplexer transmitting the video streams.

Cisco VAMS 3.1 provides a modular architecture for monitoring video networks. VAMS 3.1 uses:

- Cisco Multicast Manager (CMM 3.1.2) for multicast monitoring and troubleshooting functions.

  Cisco Multicast Manager is a web-based network management application that simplifies the discovery, visualization, monitoring, and troubleshooting of multicast networks to help ensure business continuity. Cisco Multicast Manager provides:

  - Multicast flow tracing with video probe status
  - Multicast tree monitoring
  - Probeless monitoring of CBR video flows using PPS/BPS Source, Group (SG) polling
  - A channel mapping database for multicast address to video service correlation
  - Inline video monitoring using Cisco VidMon to collect video metrics, including Media Loss Rate (MLR), Delay Factor (DF), Media Discontinuity Counter (MDC) metrics, and for constant bit rate (CBR) flows, Media Rate Variation (MRV).
  - Historical graphs of video probe performance and VidMon device performance
  - View real-time performance graphs showing video probe and VidMon device performance

- The ROSA Copernicus Network Management System (NMS) and the ROSA Element Management System (EMS), version 4.2 to monitor events from Digital Content Managers (DCMs) and devices in the video headend.

  The ROSA Copernicus NMS is available as a dedicated hardware platform with preloaded ROSA NMS software or as a client application that runs on Microsoft Windows 2000, Microsoft Windows XP, Microsoft Windows Vista, or Microsoft Windows Server 2003 and communicates with the ROSA NMS Server.

  The ROSA NMS manages Telco, CATV, HFC networks, Multichannel Multipoint Distribution System (MMDS) sites, satellite uplinks, and broadcast stations in accordance with basic telecom network management principles. Some of the features provided by the ROSA NMS are:

  - Automatic RF levelling
  - Headend redundancy backup
  - Filtering and correlation of alarm messages
  - Service management
  - Scheduling
  - Synchronous Data Hierarchy/Synchronous Optical Network (SDH/SONET) fiber-optic network management
  - Aggregated Service Status Reflection (ASSR) alerts, including RF-QAM alerts

  The ROSA EMS is a hardware and software platform that allows network operators to monitor the video headend using a web browser client. The ROSA EMS:

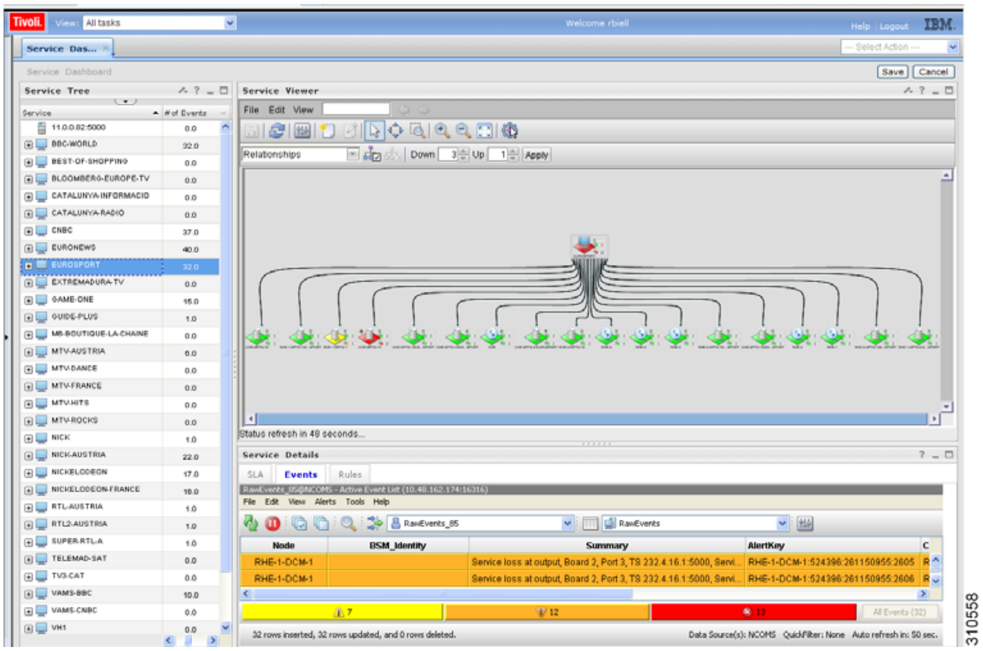
  - Polls the devices that it manages and reports any problems that occur as SNMP alarms.
  - If configured to perform backup protection, automatically indicates predefined backup schemes that reroute signals and activate and configure standby devices within seconds of a device failure.
  - Can pass alarms to the ROSA NMS

- **Cisco Info Center** —Cisco Info Center is the Manager of Managers, and monitors events from CMM, Cisco ANA, the ROSA NMS, video probes, and Cisco devices. The Cisco Info Center product suite includes:
  - **IBM Tivoli Integrated Portal** —IBM Tivoli Integrated Portal (TIP) is the high level interface for Cisco Info Center. It communicates with the Cisco Info Center/Netcool ObjectServer (central database) and includes IBM Tivoli Business and Services Manager (TBSM), a service dashboard and visualization tool, and the Tivoli Netcool/OMNIbus Web GUI.

    TIP/TBSM enables definition and display of network services. In Cisco VAMS, the network services are video channels. TIP TBSM includes a Service Dashboard that displays the video services (channels) in a service tree showing the devices that provide the service.

    Figure 1-1 shows a video service view on the TIP/TBSM Service Dashboard.

Figure 1-1 TIP/TBSM Service Dashboard



Service	# of Events
11.0.0.82:5000	0.0
BBC-WORLD	32.0
BEST-OF-SHOPPING	0.0
BLOOMBERG-EUROPE-TV	0.0
CATALUNYA-INFORMACIO	0.0
CATALUNYA-RADIO	0.0
CNBC	37.0
EURONEWS	40.0
EUROSPORT	32.0
EXTREMADURA-TV	0.0
GAME-ONE	15.0
GUIDE-PLUS	1.0
M6-BOUTIQUE-LA-CHAINE	0.0
MTV-AUSTRIA	6.0
MTV-DANCE	0.0
MTV-FRANCE	0.0
MTV-HITS	0.0
MTV-ROCKS	0.0
NICK	1.0
NICK-AUSTRIA	22.0
NICKELODEON	17.0
NICKELODEON-FRANCE	10.0
RTL-AUSTRIA	1.0
RTL2-AUSTRIA	1.0
SUPER-RTL-A	1.0
TELEMAD-SAT	0.0
TV3-CAT	0.0
VAMS-BBC	10.0
VAMS-CNBC	0.0
VH1	0.0

Status refresh in 48 seconds...

RawEvents_85@NCOMS - Active Event List (10.48.162.174:16316)

Node	BSM_Identity	Summary	AlertKey	C
RHE-1-DCM-1		Service loss at output, Board 2, Port 3, TS 232.4.16.1:5000, Servi...	RHE-1-DCM-1:524396:261150955:2605	R
RHE-1-DCM-1		Service loss at output, Board 2, Port 3, TS 232.4.16.1:5000, Servi...	RHE-1-DCM-1:524396:261150955:2606	R

32 rows inserted, 32 rows updated, and 0 rows deleted. Data Source(s): NCOMS QuickFilter: None Auto refresh in: 50 sec.

  - **IBM Tivoli Impact**—An application that supports the definition of service and network correlations.

    Tivoli Impact custom rules read a description of the CMM address management database for video services from comma-separated value (CSV) address map files and generates meta-events to populate the service map in TBSM.
  - **IBM Tivoli/Netcool/OMNIbus Knowledge Library**—A collection of rules files that are tuned to specific managed objects that send SNMP-based events, such as Cisco networking devices. These rules support a wide range of Cisco system MIBs, including MIBs for specific Cisco devices, protocols, and technologies, as well as syslog messages from a wide range of Cisco devices.

  The combination of Cisco Info Center and Netcool functionality provides:
  - Connectivity between CMM and the ROSA NMS and Cisco Info Center.
  - A “Single Pane of Glass” toolset[1].

[1] Single Pane of Glass—The ability to utilize multiple interconnected tools to monitor, diagnose, and troubleshoot network and video impairments from a single console.

Cisco Info Center includes rules files that define multicast alerts from various sources like probes and routers and also cover unicast addresses and define VoD services in the VAMS Dashboard. The rules files include code that:

- Creates channel services for each of the video channels defined in the MUX definition files for CMM.
- Extracts the multicast group and source information from CMM and video probe alerts and provides the operator with a CMM Multicast Trace option.
- Extracts IP address and channel information from alerts sent by video headend devices and the ROSA NMS and displays enhanced alert information in Cisco Info Center.
- Extracts the source address for unicast VidMon flows and associates the event to the sourcing VOD server in the service tree.
- Allows you to launch CMM to perform troubleshooting and diagnostic analysis from one system instead of looking at several systems.
- Processes ROSA NMS traps, including ETR-290 events.
- Supports ROSA Aggregated Service Status Reflection (ASSR) alerts, including DCM service status and resiliency information. ASSR events indicate the affected services within the alerts sent to CIC. This information is used to to perform the service correlation.

  For more information on ROSA ASSR alerts, see Service Alerts with ASSR support, page 1-20.

- Cisco ANA 3.7.2 to build an abstracted network model through a set of virtual network elements (VNEs).

  Each VNE represents an element in the managed network. Cisco VAMS 3.1 extends the base functions of the Cisco ANA 3.7 VNEs for Cisco 7600 Series routers, Cisco Carrier Routing System (CRS-1) devices, Cisco Catalyst 4948 and 6500 Series switches, ASR 9000 Routers, and Cisco 12000 series routers.

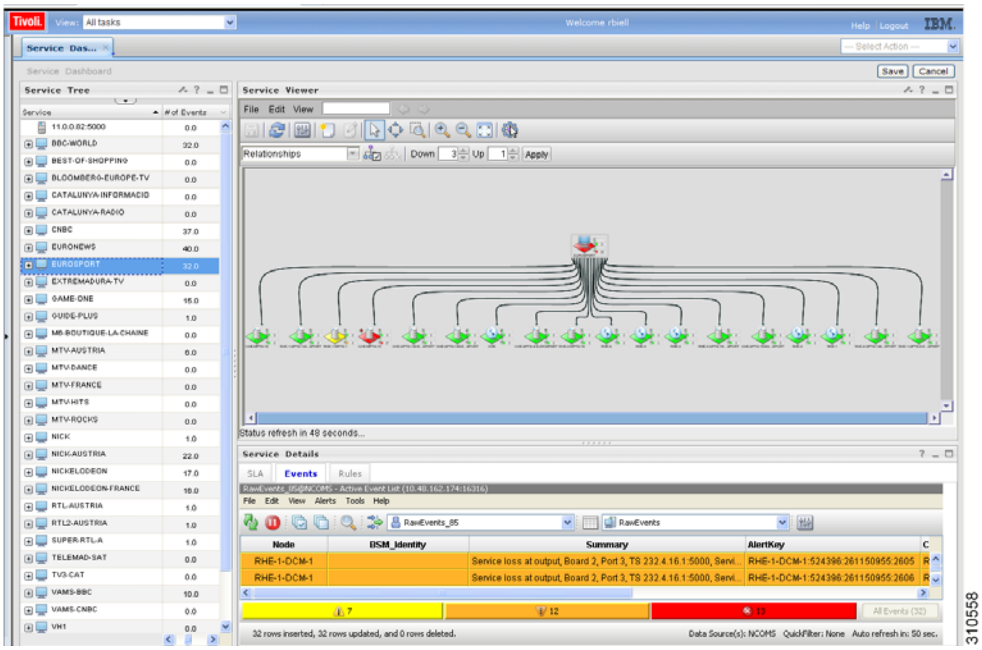
Channel-Based Service Display

Based on data in the configuration files for CMM, TIP/TBSM generates channel services and displays them in service maps on a Service Dashboard. Each channel service represents a video channel defined in the multiplex configuration file for CMM (*muxid.csv*). TIP/TBSM creates a channel when a Multi-Protocol Transport Stream (MPTS) or Single Program Transport Stream (SPTS) is created.

The video streams for the channel may be carried over different multiplexers. In CMM, each multiplex ID (MuxID) configured in CMM is assigned an IP address. In the TIP/TBSM Service Dashboard, the multicast aliases are shown as children of the channel service. Each child service is assigned the name of an IP address alias.

Figure 1-2 shows a high-level service map for the EUROSPORT service in VAMS.

Figure 1-2 High-Level Channel Service View



Service	# of Events
11.0.0.82:5000	0.0
BBC-WORLD	32.0
BEST-OF-SHOPPING	0.0
BLOOMBERG-EUROPE-TV	0.0
CATALUNYA-INFORMACIO	0.0
CATALUNYA-RADIO	0.0
CNBC	37.0
EURONEWS	40.0
EUROSPORT	32.0
EXTREMADURA-TV	0.0
GAME-ONE	15.0
GUIDE-PLUS	1.0
M6-BOUTIQUE-LA-CHAINE	0.0
MTV-AUSTRIA	6.0
MTV-DANCE	0.0
MTV-FRANCE	0.0
MTV-HITS	0.0
MTV-ROCKS	0.0
NICK	1.0
NICK-AUSTRIA	22.0
NICKELODEON	17.0
NICKELODEON-FRANCE	10.0
RTL-AUSTRIA	1.0
RTL2-AUSTRIA	1.0
SUPER-RTL-A	1.0
TELEMAD-SAT	0.0
TV3-CAT	0.0
VAMS-BBC	10.0
VAMS-CNBC	0.0
VH1	0.0

Status refresh in 48 seconds...

RawEvents_85@NCOMS - Active Event List (10.48.162.174:16316)

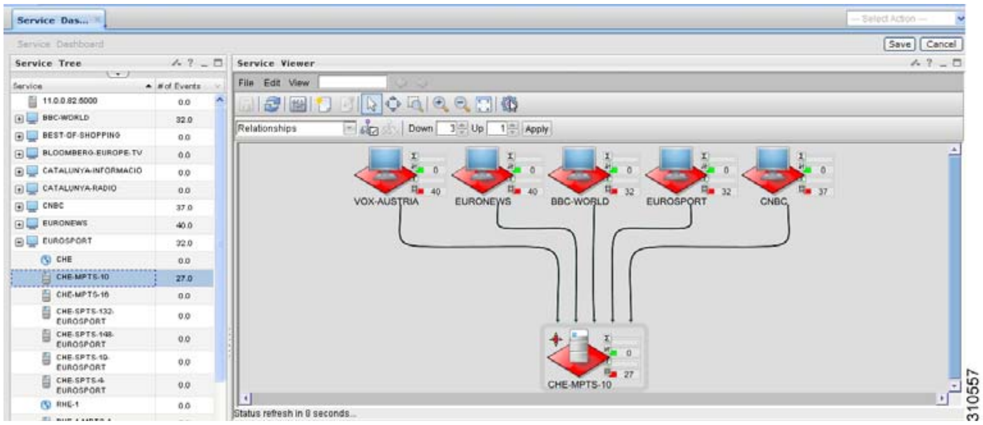
Node	BSM_Identity	Summary	AlertKey	C
RHE-1-DCM-1		Service loss at output, Board 2, Port 3, TS 232.4.16.1:5000, Servi...	RHE-1-DCM-1:524396:261150955:2605	R
RHE-1-DCM-1		Service loss at output, Board 2, Port 3, TS 232.4.16.1:5000, Servi...	RHE-1-DCM-1:524396:261150955:2606	R

32 rows inserted, 32 rows updated, and 0 rows deleted. Data Source(s): NCOMS QuickFilter: None Auto refresh in: 50 sec.

Clicking on a Service Name in the Service Dashboard tree shows all of the video streams associated with the channel. Clicking a specific video stream, for example "CHE-MPTS-10," shows all of the channels transmitted through the video stream.

Figure 1-3 shows the channels for a video stream called "CHE-MPTS10."

Figure 1-3 Channels Associated with a Video Stream



Service	# of Events
11.0.0.82:5000	0.0
BBC-WORLD	32.0
BEST-OF-SHOPPING	0.0
BLOOMBERG-EUROPE-TV	0.0
CATALUNYA-INFORMACIO	0.0
CATALUNYA-RADIO	0.0
CNBC	37.0
EURONEWS	40.0
EUROSPORT	32.0
CHE	0.0
CHE-MPTS-10	27.0
CHE-MPTS-16	0.0
CHE-SPTS-132-EUROSPORT	0.0
CHE-SPTS-148-EUROSPORT	0.0
CHE-SPTS-10-EUROSPORT	0.0
CHE-SPTS-4-EUROSPORT	0.0
RHE-1	0.0

Status refresh in 8 seconds...

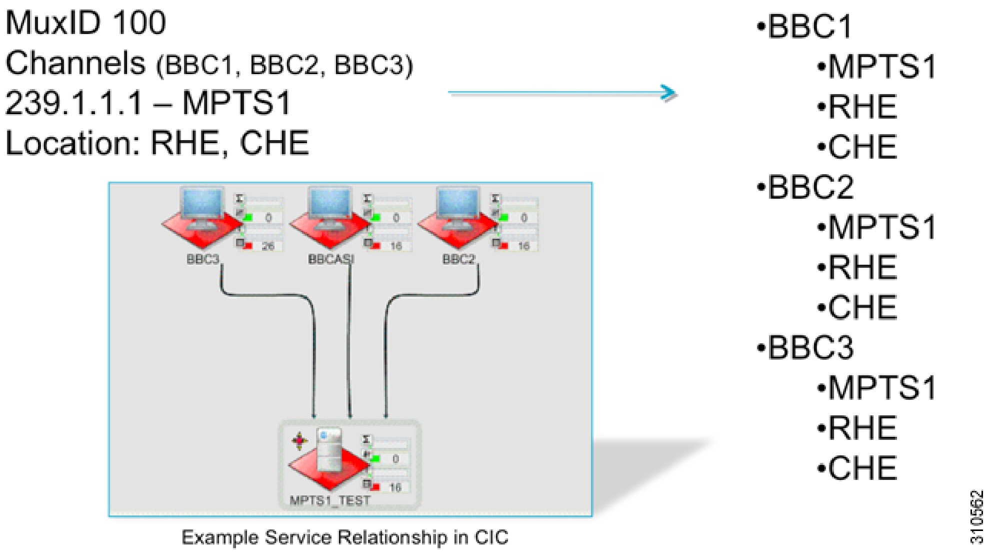
The service channels and MUX IDs are related as follows:

MUX IDs are configured in the multiplex configuration file (*muxid.csv*) in CMM and in Cisco Info Center. The *muxid.csv* file specifies a mux ID and then a broadcast channel that is transmitted over the MUX. The MUX IDs and the CSV file are configured independently of each other.

The CMM and Cisco Info Center *addresses.csv* configuration file specifies the IP address for the MUX. More than one broadcast channel can be assigned to the same MUX.

In addition, Cisco Info Center determines the location for the device, such as regional headend (RHE) or central headend (CHE).

Figure 1-4 Relationship Between Service Channels and IP Address



MuxID 100
Channels (BBC1, BBC2, BBC3)
239.1.1.1 – MPTS1
Location: RHE, CHE

- BBC1
  - MPTS1
  - RHE
  - CHE
- BBC2
  - MPTS1
  - RHE
  - CHE
- BBC3
  - MPTS1
  - RHE
  - CHE

Cisco VAMS 3.1 Network Topology

Cisco VAMS 3.1 monitors events from the entire video network to provide end-to-end video assurance management. Figure 1-5 shows the end-to-end topology of a typical video network.

Figure 1-5 End-to-End Video Network Topology

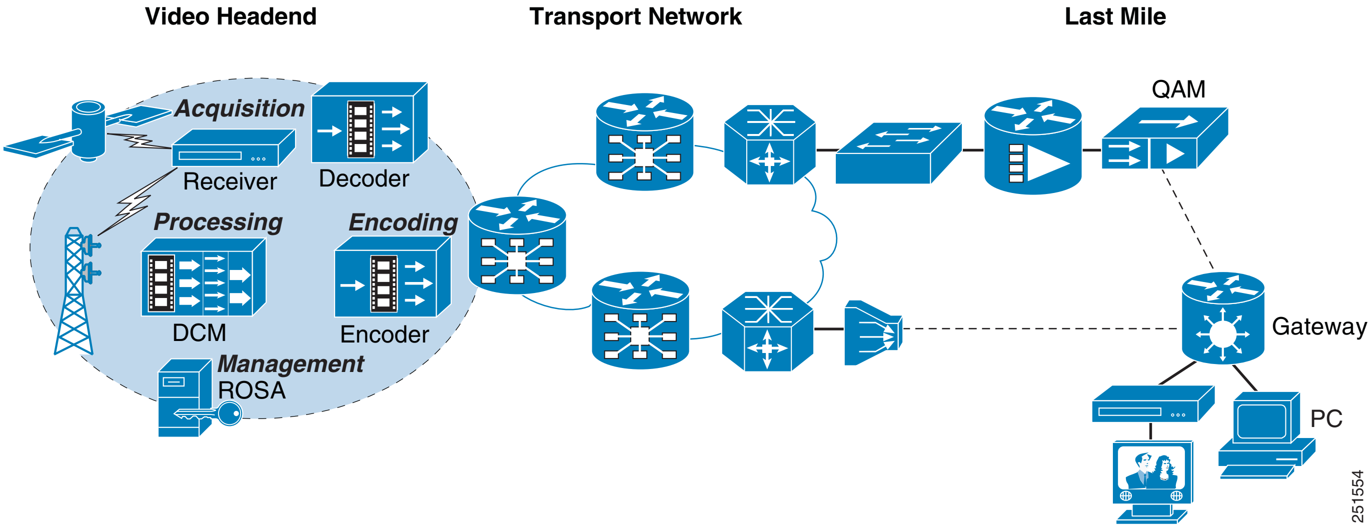


Figure 1-6 shows a Cisco VAMS topology in a video headend environment, and Figure 1-7 shows an example topology in the video transport network.

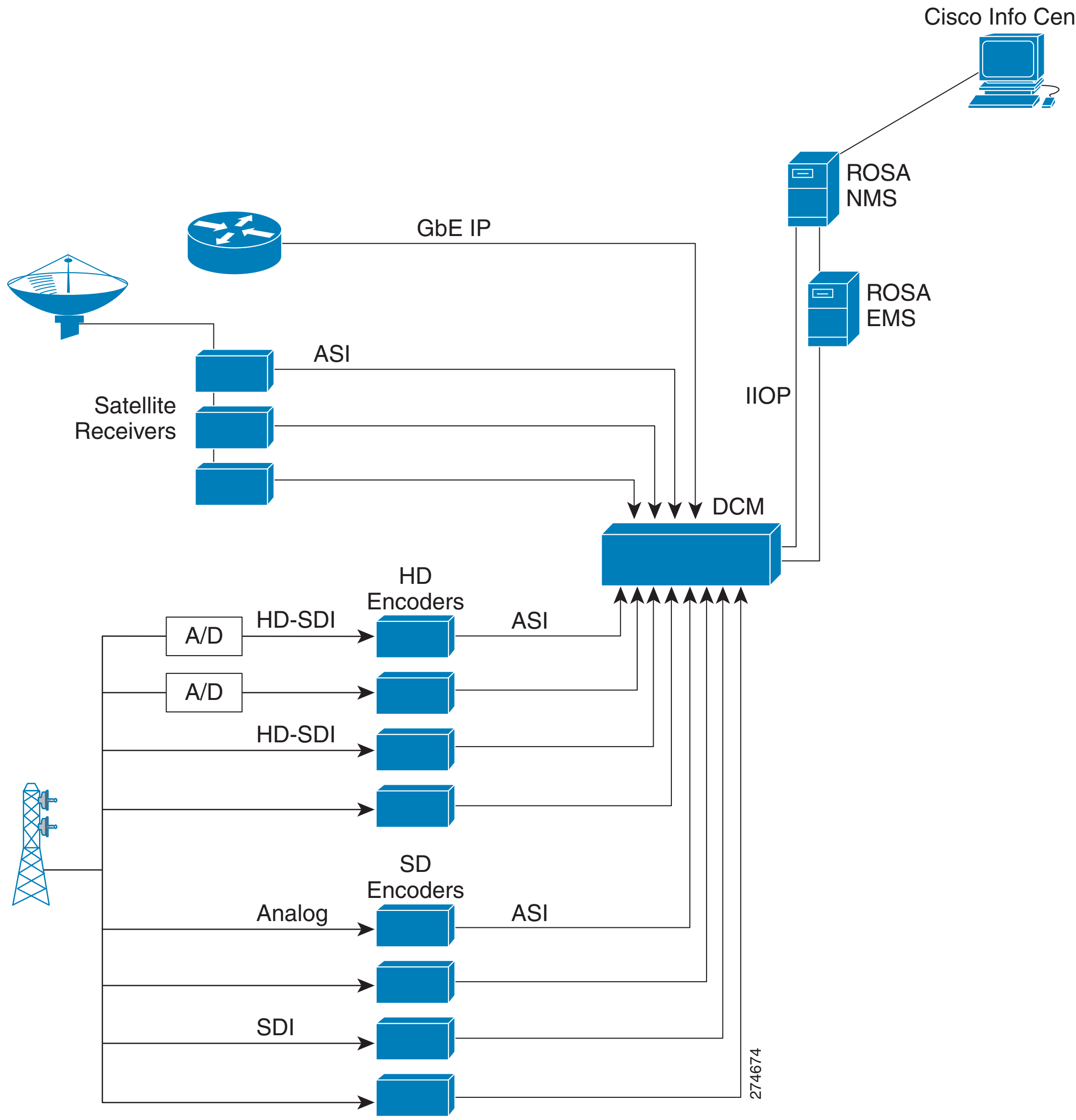
Cisco VAMS monitors devices in the video headend and in the transport network, but does not monitor events in the last mile segment.

Cisco VAMS 3.1 in a Video Headend Environment

In the video headend environment, the Cisco ROSA NMS is the domain manager responsible for monitoring video. The ROSA NMS sends alerts to the Cisco Info Center component of VAMS.

Figure 1-6 shows a Cisco VAMS topology in a video headend environment.

Figure 1-6 Cisco Video Assurance Management Solution 3.1 Components for Video Headend Monitoring



The devices in the video headend perform the following functions.

- **Digital Program Acquisition**—The securing of content from satellite or terrestrial sources and preparation of the content for digital delivery. The acquisition process uses satellite receivers, off-air receivers, and integrated receiver/decoder (IRD) solutions to convert RF streams to digital format including serial digital interface (SDI) and asynchronous serial interface (ASI).

- **Digital Program Storage—**The storage and insertion of additional, non-live broadcast programming like video-on-demand or advertising.
- **Digital Program Distribution**—Includes program preparation and aggregation, modulation, encapsulation and other technical processes to prepare programming for delivery.
- **Digital Program Delivery—**Transport to the receiver devices and set top boxes, which allows subscribers a high quality view of video programming.

The hardware devices in the headend include:

- **Video Encoders**—Video Encoders are used to compress the video into a standard compression technology such as MPEG-2. Digitalization and compression allow for bandwidth saving over the available frequency and enable the delivery of video over low bandwidth environments.
- **Video Rate Shaping (Transrating) and Video Encapsulation Devices**—The video content is typically received at the video headend facility through satellite receivers, off-air, or through a terrestrial route. Since the video streams are typically bundled together as a multiplex from the satellite, they first need to be de-multiplexed and converted to separate video streams. In addition, since these video streams are usually in a variable bit rate (VBR) format, they might need to be rate reduced and rate shaped to get a constant bit rate (CBR). The job of the video rate shaping, also known as transrating, is to convert the video to a constant bit rate while also reducing the video bit rate.

  Video encapsulation is another key component of headend functionality. Encapsulation is important because, although service providers receive video from different sources and in multiple formats, they need to be able to deliver it over their networks as efficiently and cost-effectively as possible. Many providers continue to build out fiber networks; so, while they may want to deliver MPEG-over-ATM today, they are likely to have a migration plan to GbE for the fiber-fed portions of their networks. Some independent telephone companies also have a cable plant in their network, and want to use their headend to upgrade cable customers to digital cable TV, and also deliver video signals through ADSL over their ATM network with the same equipment.
- **Digital Content Manager (DCM)**—The DCM is a critical component of the Video headend topology. The DCM provides these features:
  - Multiplexing/re-multiplexing
  - Transrating, grooming, and rate clamping
  - Statistical multiplexing
  - Digital program insertion
  - Transport service protection
  - Bandwidth analysis
  - Asynchronous serial interface/Internet protocol conversion

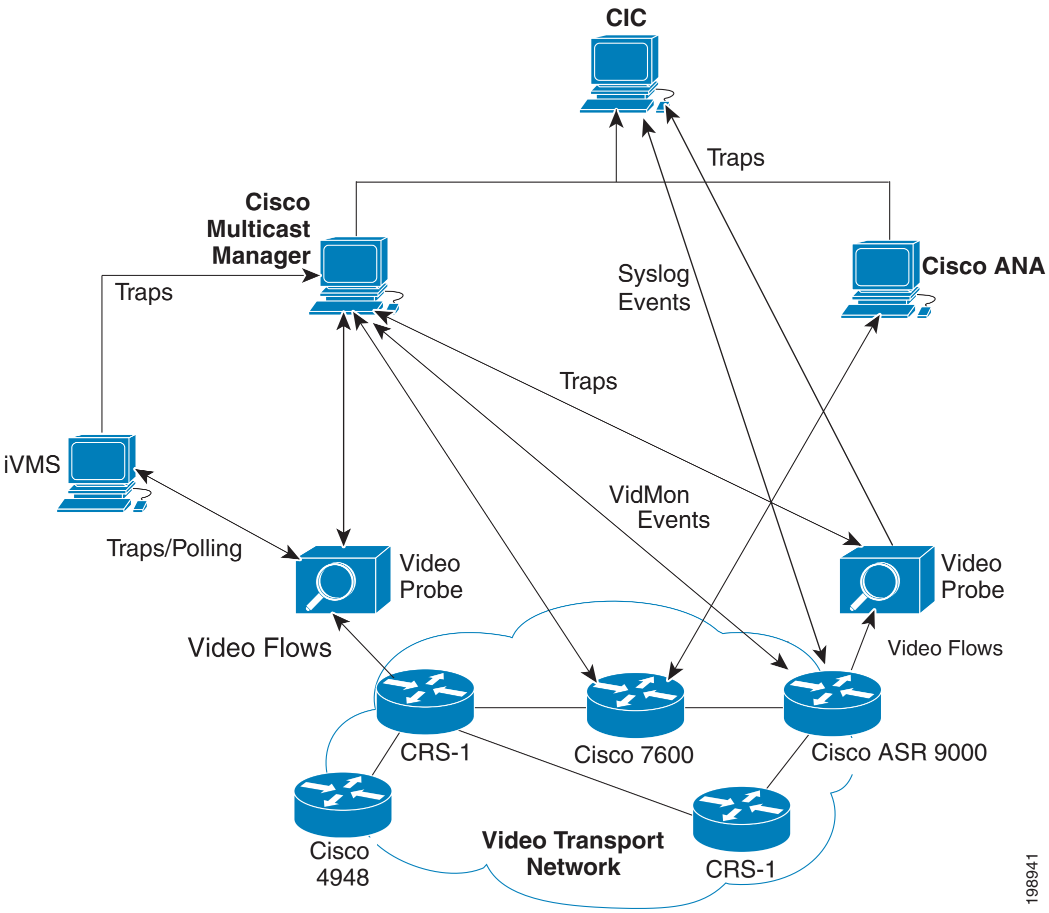
The DCM can export alerts related to these features into the ROSA Management system for video service correlation and association with other events solicited from the IP transport.

In the Cisco VAMS 3.1 environment, the DCM sends events directly to the ROSA NMS, through the Internet Inter-ORB Protocol (IIOP), or indirectly, through the ROSA EMS. The ROSA NMS is configured to relay the events to Cisco Info Center. Cisco Info Center correlates the events from the video headend with events that it receives from the components of the video transport network.

Cisco VAMS in a Video Transport Network

Figure 1-7 shows Cisco VAMS 3.1 in a video transport network.

Figure 1-7 Cisco Video Assurance Management Solution 3.1 Components for Video Transport Monitoring



Cisco VAMS 3.1 monitors video flows by using CMM and video probes, and, if you install Cisco ANA, monitors the network elements (NEs) in the video transport network by using Cisco ANA. The video probes monitor video flows in the video transport network and send events either directly to Cisco Info Center, or send events to Cisco Multicast Manager, which then forwards the events to Cisco Info Center. If installed and configured, ANA sends network topology information and other events to Cisco Info Center.

Cisco Info Center correlates the events that it receives from ANA, the video probes, and Cisco Multicast Manager and generates events that provide more detailed information about the video service. For additional information on Cisco Info Center in the VAMS 3.1 environment, see Cisco Info Center, page 1-23.

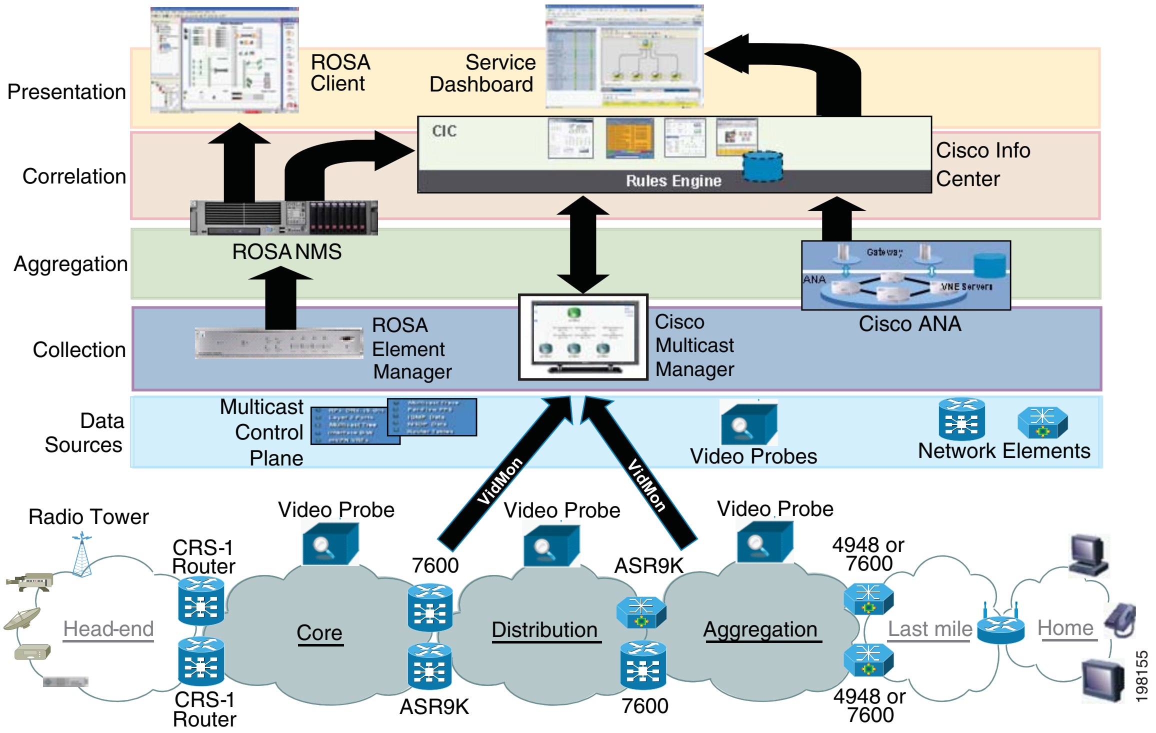
Cisco VAMS Solution Components

The Cisco VAMS 3.1 solution includes the following components:

- Cisco Multicast Manager 3.1.2, page 1-14
- ROSA NMS, page 1-18
- Cisco Info Center, page 1-23
- Cisco ANA 3.7.2, page 1-26
- Third-Party Video Probes, page 1-33

Figure 1-8 shows the components in the VAMS 3.1 architecture.

Figure 1-8 VAMS 3.1 System Architecture



Network Elements in the Video Transport Network

Cisco VAMS 3.1 monitors these network elements (NEs), which form the core of the video transport network (see Figure 1-7 on page 1-9):

- **Cisco 7600 Series Router**—A carrier-class edge router that offers integrated, high-density Ethernet switching, carrier-class Internet Protocol/Multiprotocol Label Switching (IP/MPLS) routing, and 10-Gb/s interfaces.

  Cisco 7600 ES+ line cards on the Cisco 7600 support VidMon as follows:

  - **MDI:MLR Support**—The Cisco 7600 provides Media Loss Rate metrics through a Media Delivery Index (MDI) table.

  - **DF Support**—Delay Factor (DF) metrics are provided through either an MDI or a Constant Bit Rate (CBR) table.
  - **MRV Support**—Media Rate Variation (MRV) metrics are supported through a CBR table.
  - **MDC Support**—Media Discontinuity Counter (MDC) is a measurement of the number of times when a discontinuity occurs in a MPEG TS; therefore MDC indicates the frequency of discontinuities.

- **Cisco ASR 9000 Series Aggregation Services Router**—The Cisco ASR 9000 router is a carrier class routing solution that uses the Cisco IOS-XR operating system, and which includes comprehensive network management capabilities. Combining these elements with a comprehensive set of Ethernet and Multiprotocol Label Switching (MPLS) operations, administration, and maintenance (OAM) capabilities, the Cisco ASR 9000 Series provides an operator-friendly environment.

  The ASR 9000 supports VidMon as follows:

  - **MRV**—Supports MRV metrics through a CBR table.
  - **DF**—Supports DF metrics through a CBR table.

- **Cisco Catalyst 6500 Series Switch**—As the premier intelligent, multilayer modular Cisco switch, the Catalyst 6500 Series delivers secure, converged, end-to-end services, from the wiring closet to the core network, the data center, and the WAN edge.
- **CRS-1**—A carrier routing system that service providers use to deliver data, voice, and video services over a highly available and scalable IP network.
- **Cisco Catalyst 4948 Series Switch**—A low-latency, Layer 2-4 switch that offers performance and reliability for low-density, multi-layer aggregation of high-performance servers and workstations.
- **Video Headend Equipment**—Video headend equipment includes satellite receivers, off-air receivers, integrated receiver/decoder (IRD) solutions, HD encoders, SD encoders, and the DCM.

Note You must equip these NEs with software that enables the NEs to monitor multicast video flows in the network. See the "Solution Component Versions" section on page 1-11, for a list of the required software.

Solution Component Versions

Cisco VAMS 3.1 supports these components and software version levels:

Table 1-1 Solution Components and Version Information

Solution Component	Version Information
Active Network Abstraction (ANA)[1]	3.7.2
Cisco Multicast Manager	3.1.2

Table 1-1 Solution Components and Version Information (continued)

Solution Component	Version Information
ROSA Element Management System	4.2 The ROSA EMS is supported on the following operating systems: • Windows Vista • Microsoft Windows 2000 • Microsoft Windows Server 2003 • Windows XP, Service Pack 2 • Microsoft Windows Vista
ROSA Copernicus NMS	4.2
Digital Content Manager (DCM)	Model D9900 and D9901 with GbE interface card. DCM software V8.7.
Cisco 7600 Series router (7600-SUP720-3BXL with redundant SUP720-3BXL) Line cards include the following Ethernet Services Plus (ES+) line cards: 76-ES+T-4TG,76-ES+T-40G, 7600-ES+4TG3C, 7600-ES+20G3C, and several other versions. Cisco 7600 Series Route Switch Processors (RSPs) 720 with 10 Gigabit Ethernet uplinks include the RSP720-3C-GE and the RSP720-3CXL-10GE.	RLS8
Cisco Catalyst 6500 Series switch	12.2(33)SXI
Cisco Carrier Routing System-1 (CRS-1) Line cards: CRS-MSC, CRS1-SIP-800 (with SPA-8X1GE), 8-10GE	IOS-XR 4.0.1
Cisco Catalyst 4948 Series switch (CAT4948-10GE)	12.2(46)SG
Cisco ASR 9000 router	IOS XR 4.0.1
Cisco Info Center (includes IBM Tivoli Netcool products)[2]	Cisco Info Center, which includes • Tivoli Netcool/OMNIbus ObjectServer - 7.3 • TBSM- 4.2.1 • Netcool/Impact - 5.1.1
IneoQuest iVMS (IneoQuest NMS for IQ probes)	Version 4.02.001.02.29

Table 1-1 Solution Components and Version Information (continued)

Solution Component	Version Information
Bridge Technologies video probes	Version: 3.1.0-26, including the VB260 QAM probe. • VB220—Version 4.2.0-15 • VB250—Version 4.2.0-15 • VB260—Version 4.2.0-15 • VB270—Version 4.2.0-15 • VB280—Version 4.2.0-15
IneoQuest video probes	• Singulus G1-T Media Analyzer, Geminus G1-T Firmware Version: TB6x-3.10a-120109.iqz Software Version: 3.10a • Geminus G10 Firmware Version: Denali-2.1-4a-120109.iqz Software Version 2.14a • Geminus G2x Firmware Version: MAG2X-1.23a-120209.iqz Software Version 1.23a • IQ Media Monitor Firmware Version: MA6x-3.10a -120109.iqz Software Version: 3.10a • Cricket - ASI version Firmware Version: Cricket-A6x-2.10a-120109.iqz Software Version 2.10a • Cricket - MS version Firmware version: Cricket-MS6x-2.11a-120109.iqz Software Version: 2.11a • Cricket - IP version Firmware Version: Cricket-6x-2.10a-120109.iqz Software Version: 2.10a • Cricket - QAM and 8VSB versions Firmware Version: Cricket-Q6x-2.10a-120109.iqz Software Version: 2.10a • Cricket - QAM Plus versions Cricket-DQ-1.4a-120109.iqz Software Version: 1.4a
Mixed Signals video probe **Note** **Reviewers:** Do we support the Mixed Signals prove with VAMS 3.1?	Sentry 136 Digital Content Monitor[3] Sentry Engine Version: PDM (build 1460.84) Sentry Database Version: 3.0.31 Sentry Configuration: TRANSPORT

1. You must purchase base VNEs before installing the VNE extensions. For example, you must acquire the Cisco 7600 series router group VNE license to use the Cisco 7600 VNE extensions.
2. Cisco Info Center is an OEM product that includes the IBM Tivoli Netcool Suite.
3. Cisco VAMS 3.1 does not support carousel-related traps for the Mixed Signals Sentry 136.

Cisco Multicast Manager 3.1.2

This section describes the components of CMM 3.1.2.

CMM is a web-based multicast and video troubleshooting tool that runs on an x86-type computer running Linux or a Sun Microsystems Sun Fire series workstation running Solaris. CMM 3.1.2 has three components: an Event Dashboard, a Devices tab, and a Main Menu.

CMM 3.1.2 uses SNMP MIB polling to monitor devices and traffic in the network. CMM 3.1.2 also provides metrics and alerts, which it then forwards to Cisco Info Center as SNMP traps. Based on the unique requirements of the network environment, the SNMP traps are user-configurable.

CMM 3.1.2 can monitor multicast-specific data such as:

- Rendezvous points (RP)
- Designated routers (DR)
- Multicast traffic (Layer 2 and Layer 3)
- Multicast bandwidth (Layer 2 and Layer 3)
- Layer 3 multicast trees
- Tree Change events
- PPS/BPS per flow monitoring

CMM 3.1.2 monitors video transmission by monitoring:

- Data from video probes
- VidMon data from Cisco 7600 devices and ASR 9000 devices

CMM 3.1.2 also provides detailed diagnostics and a health-check capability.

You use CMM 3.1.2 to set thresholds, generate notifications, and forward them to Cisco Info Center.

See the *User Guide for Cisco Multicast Manager 3.1,* viewable online at:

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

Cisco Multicast Manager 3.1.2 System Requirements

Table 1-2 lists the hardware and software requirements for the CMM 3.1.2.

Table 1-2 Cisco Multicast Manager 3.1 System Requirements

Item	Specifications
Hardware Requirements	
Processor	**AMD Linux** • Dual, Quad, or 6-Core AMD Opteron processor **Linux-Intel** • Xeon Dual or Quad Core (equivalent or better) **Linux CPU Requirements** • Two CPUs with dual core for less than 500 devices • Four CPUs with four cores for more than 500 devices **Solaris-SPARC** • Solaris 10 Cisco Multicast Manager supports the following hardware on Sun Microsystems servers: • Sun Fire V440: Two CPUs with 1.593-GHz UltraSPARC IIIi processors. – Up to four cores for less than 500 devices. – Eight cores for 500 devices or more.
Memory	• 4 GB for less than 500 devices • 8 GB for Large Enterprise

Table 1-2 Cisco Multicast Manager 3.1 System Requirements (continued)

Item	Specifications
Software Requirements	
Operating system	**Linux** • Red Hat Enterprise Linux ES/AS 3 • Red Hat Enterprise Linux ES/AS 4 • Red Hat Enterprise Linux ES/AS 5 Both 32-bit and 64-bit Linux versions are supported. **Solaris** • Solaris 8 • Solaris 9 • Solaris 10 **Note** Solaris x86 is not supported. **VMWare** • ESX Server 3.5 or later
Browser	• Internet Explorer Version 6.0 • Internet Explorer Version 7.0 • Firefox 1.5 or later • Safari 2.0 or later **Note** The browser must have Adobe Flash Player installed.

Cisco Multicast Manager 3.1 Software Components

The CMM 3.1.2 user interface provides three components:

- Event Dashboard, page 1-17
- Devices Tab, page 1-17
- Main Menu, page 1-17

Event Dashboard

The Event Dashboard allows you to:

- View specified categories of events, such as Latest Events, Video Events, S,G Events, Tree Events, and so on
- For S,G events, click on an IP address and run a multicast trace
- From the **Graphs** tab, display performance graphs for a specified S,G, Video Probe, or Vidmon device.

The performance graphs for video probes and Vidmon devices are particularly useful for VAMS users. When you display a video probe graph, you can display a real-time performance graph that shows the performance of a device monitored by a video probe or a Vidmon device.

For a Video Probe graph, you can select:

- **DF**—Delay Factor.
- **MLR**—Media Loss Rate.

For a Vidmon device graph, you can select:

- **DF**—Delay Factor**.**
- **MLR**—Media Loss Rate.
- **MRV**—Media Rate Variation

Devices Tab

The CMM Devices tab displays the multicast devices that are currently being monitored for a specified domain, and allows you to start or restart device polling.

By clicking on the IP address for a device listed on the Devices page, you can log in to the selected device and display the Protocol Independent Multicast (PIM) neighbors, PIM Interface Mode, IGMP information, and Rendezvous Points (RPs) for the selected device.

Main Menu

The CMM Main Menu tab contains menus that launch the main features provided by CMM. By making selections on the Main menu at the left of the display, you can:

- Configure the system by managing domains and setting the global polling configuration.
- Configure polling and run polling reports.
- Discover network devices, including multicast devices, Layer 2 devices, video probes, Vidmon devices, and unicasts devices, and also run multicast traces.
- Display a topology graph of the network.
- Run diagnostics, including video probe status and Vidmon flow status.

- Configure devices, including RP and SSM
- Administer the system, including management of the address management database for your video devices.

For complete hardware and software requirements, see the following:

- *Installation Guide for Cisco Multicast Manager 3.1,* viewable online at:

  http://www.cisco.com/en/US/products/ps6337/prod_installation_guides_list.html
- *User Guide for Cisco Multicast Manager 3.1,* viewable online at:

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

ROSA NMS

The ROSA Copernicus NMS provides monitoring for the DCM and video headend equipment. The ROSA NMS runs on a dedicated hardware device. The ROSA software runs on a client device that you use to access the Copernicus server.

For information on the Copernicus ROSA Network Management Server device, see the data sheet for the ROSA Copernicus NMS at the following location:

http://www.cisco.com/en/US/prod/collateral/video/ps9118/ps9131/product_data_sheet0900aecd806c6a29.pdf

ROSA NMS Client Requirements

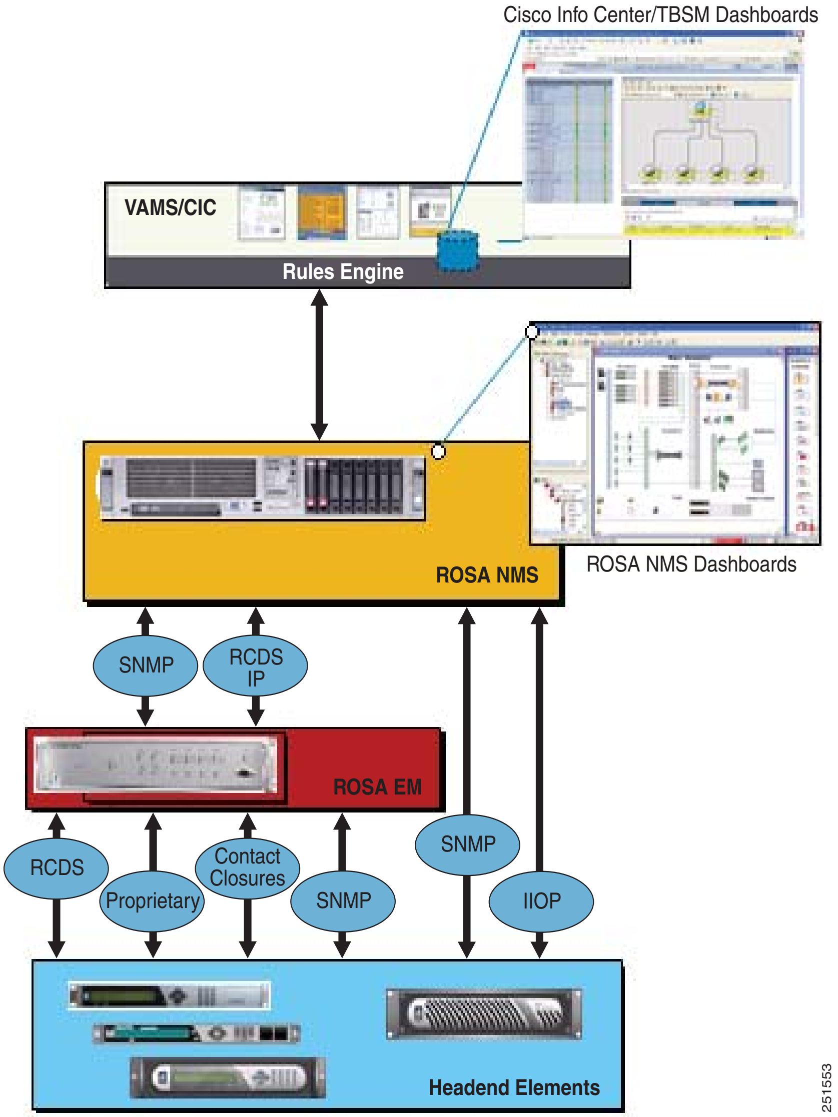
The computer used to run the ROSA NMS client must meet these requirements:

Item	Minimum Requirements	Recommended
Processor	600 Mhz Pentium III compatible or higher	1 Ghz Pentium III compatible or higher
Memory	Minimum 192 MB	512 MB
Free disk space	1 GB	10 GB
Operating System	Windows 2000, Windows Server 2003, Windows XP, Windows Vista	
Web browser	Microsoft Internet Explorer v. 5 or higher	
Serial Ports	One or more serial ports (RS-232 and/or RS-285 if needed)	
Ethernet Adapter	Required	

ROSA NMS Architecture and Process Flow

Figure 1-9 shows the ROSA NMS architecture.

Figure 1-9 ROSA NMS Process Flow



In the VAMS 3.1 architecture, the process flow of alerts is as follows:

1. Data source elements such as the SD and HD encoders and the DCM report events either through the ROSA EMS or directly to the ROSA Copernicus NMS. The events are reported as SNMP traps or as Resource Cataloging and Distribution System (RCDS) IP messages.
2. The ROSA client dashboard allows alerts that are collected from headend devices to be mapped against the reporting hardware and the affected video services.
3. The ROSA NMS uses an SNMP-based northbound interface to send alerts to Cisco Info Center.

Event Categories Reported to Cisco Info Center

The ROSA NMS reports these categories of events to Cisco Info Center:

- Service Alerts
- ETR-290 First Priority Alarms

- Video Transport Events
- Additional Video Quality Measurements

Service Alerts with ASSR support

The ROSA NMS is responsible for monitoring and detecting all categories of service backup events that can occur in the video headend.

When a redundancy scheme is applied to a DCM, the terminology used depends on where the protection is applied. When backup services are applied on the input side of DCM this is called *TS backup*. On output, the term *Service backup* is used.

Upon a service backup cutover, ROSA detects and associates the event with both the hardware and defined video service in the ROSA NMS dashboard. The event is then sent northbound using the `CopMsgNew` structure defined in the ROSA NMS MIB.

ROSA includes a feature called Aggregated Service Status Reflection (ASSR) alerts. ASSR alerts are traps that contains the service name and service location data. Cisco Info Center uses the information in ASSR alerts to identify the geographic location of devices used to transmit a video service that is monitored by VAMS.

Cisco Info Center rules for VAMS 3.1 process the specific alerts from ROSA and the other VAMS components such as CMM, ANA, and video probes. In rules file processing:

- Some alerts are associated through a common multicast association for representation at the VAMS 3.1 Cisco Info Center dashboard.
- For alerts that do not have related multicast data, for example, ASI events in the video headend, Cisco Info Center correlates the event with a service by using the service name provided by the ROSA NMS.

Service alerts include:

- **Service Loss**—For each incoming service, one or more alarms can be defined to trigger a Service Loss alarm. A Transport Stream Loss alarm is triggered when a Service Loss alarm occurs.

  Triggers for a service loss alarm include TS Sync Loss, UDP Stream Loss, Missing in PAT, PMT Error, and PID Error. For a description of these triggers, see ETR-290 First Priority Alarms, page 1-20.
- **Service in Backup (Service Loss)**—This alarm is generated when a service is in backup state triggered by a Service Loss alarm.
- **Service Loss at Output**—This alarm is generated for an outgoing service for which the corresponding incoming service and incoming backup services are in Service Loss state.
- **Service in Backup (TS Loss)**—This alarm is generated when a service is in backup state triggered by a TS Loss alarm.

ETR-290 First Priority Alarms

European Telecommunications Standards Institute 290 (ETR-290) First Priority alarms are defined in the ETR-290 specification. ETR-290 First Priority alarms include:

- **TS Loss**—The first byte of a Transport Stream packet header is the synchronization byte (0x47). A TS Loss error occurs when the synchronization byte in a sequence of at least two Transport Stream packets are not detected.
- **CC Error**—Indicates a discontinuity error in the MPEG TS structure for a particular video program.
- **Sync Byte Error**—The synchronization byte in a Transport Stream packet is not detected. A Transport Stream Loss alarm is also triggered.

- **PAT Error**—Occurs when the PMT reference in the Program Association Table (PAT) for the service is missing. A Service Loss alarm is also triggered.
- **PMT Error**—Occurs when the Program Map Table (PM) for the service is not available within a particular time interval or contains errors. A Service Loss alarm is also triggered.
- **PID Error**—A Packet ID (PID) error occurs when components with PMT reference are not found within a particular time interval. A Service Loss alarm is also triggered.

Video Transport Events

The ROSA NMS generates the following video transport events:

- **UDP Stream Loss**—A Service Loss alarm is triggered when the port of the incoming Transport Stream to which the service belongs no longer detects packets at the corresponding UDP port.
- **Bandwidth Exceeded**—The sum of the services and components within a Transport Stream has exceeded the bit rate that is assigned to the Transport Stream.
- **Destination IP Unresolved**—This alarm is generated when the MAC address for a unicast IP address of an outgoing Transport Stream cannot be resolved.

Additional Video Quality Measurements

The ROSA NMS generates several additional events that measure video quality. These events include:

- **Unreferenced PID Error**—The Transport Stream is permitted to contain only packets with program-specific information (PSI and SI tables), packets with certain PIDs that are reserved in the MPEG-2 standard, and packets that are identified in a Program Map Table (PMT).
- **PMT Section Exceeds 1K**—The PMT section is limited to 1 KB. This alarm occurs if the PMT section exceeds this limit.
- **Missing Forward Error Correction (FEC) Stream**—This alarm is generated if one or both FEC streams are missing for the incoming Transport Stream.
- **Payload Bit Rate Too Low**—This alarm is generated when the bit rate of the payload of an outgoing Transport Stream drops below a configurable threshold.
- **No FEC Licensing Available (Decoding)**—This alarm is generated if no license is available at the arrival of an incoming Transport Stream when the Default Input FEC Settings Mode is set to 1D FEC or 2D FEC. In this case FEC for the corresponding Transport Stream is disabled.
- **No FEC Licensing Available (Encoding)**—This alarm is generated when not enough licenses are available after a reboot if the Default Input FEC Settings Mode is set to 1D FEC or 2D FEC.
- **FEC L/D Error**—This alarm is generated when a Transport Stream enters the device with forward error correction (FEC) scheme L x D > 100.
- **Stuffing Rate Too Low**—This alarm is generated when the bit rate of the stuffing within an outgoing Transport Stream drops below a configurable threshold.
- **Bit Rate Too Variable for CBR Dejitterin**g—This alarm is generated when the bit rate for a transport stream is too variable for constant bit-rate dejittering to be used.

ROSA NMS Service Backup Procedures

The DCM and the ROSA NMS allow you to configure service backup protection for video headend devices. The main categories of service backup protection in the DCM included in the VAMS 3.1 architecture are:

- Service Backup Protection, page 1-22

- Service Loss Notification, page 1-22
- Chassis Protection, page 1-22
- Gigabit Ethernet Port Protection, page 1-22
- ETR-290 Priority 1 Ingress Monitoring, page 1-23

Service Backup Protection

The ROSA NMS is responsible for monitoring and detecting all categories of service backup events that can occur in the video headend. Upon a service backup cutover, ROSA detects the event and associates it with both the hardware and the video service that is defined in the ROSA NMS dashboard. The event is then sent northbound using the `CopMsgNew` structure defined in the ROSA NMS MIB.

Cisco Info Center rules for VAMS 3.1 process specific alerts from ROSA and the other VAMS components, such as CMM, ANA, and video probes. These alerts are combined into a Cisco Info Center alert based on a common multicast association for representation at the Tivoli Business Service Manager (TBSM) dashboard.

Service Loss Notification

Network operators can configure parameters that specify the thresholds applied to video services during acquisition. In the DCM, backup streams can be chosen to replace the primary stream. TS backup results in a single output stream sourced from one of many input streams.

Output service loss is a critical event resulting in complete service disruption from the video headend. ROSA detects this event and associates it with the affected hardware and video service in the ROSA NMS dashboard. The event is also detected in the video transport by other VAMS components as multicast flow loss and potentially multicast state change. Events are summarized at the Cisco Info Center Dashboard based on common multicast information and associated with the affected video service.

Many events can trigger a service loss event, including:

- TSSL (ASI).
- UDP Loss (GbE.)
- First Priority Alarms, for example, missing information in the PAT, PMT, or PID.

All trigger thresholds are configurable (per I/O stream). A template can be configured on a per I/O board basis. A service loss configuration table can be configured in the DCM based on input transport stream (TS) settings.

Chassis Protection

Chassis protection includes:

- ROSA NMS (Copernicus) Protection
- ROSA EM Protection
- Standalone or Heartbeat Loss Monitoring

Gigabit Ethernet Port Protection

Gigabit Ethernet (GbE) port protection consists of (Main/backup), failover based on:

- Link/UDP traffic loss
- ASI port / TS protection
- TS (ASI / IP) protection—Any TS can protect any other TS.

ETR-290 Priority 1 Ingress Monitoring

ETR-290 Priority 1 Ingress Monitoring provides individual service protection by using ETR-290 Priority 1 alarms as triggers. For a list of the ETR-290 Priority 1 alarms, see ETR-290 First Priority Alarms, page 1-20.

Cisco Info Center

Cisco Info Center delivers real-time centralized monitoring and root-cause analysis by integrating the IBM Tivoli/ Netcool components and with Cisco ANA 3.7.2, CMM 3.1.2, and video probe devices.

Cisco Info Center alone provides real-time monitoring, management, and event deduplication[2] or pruning, and helps enterprises and service providers proactively manage their IT infrastructures to ensure the continuous uptime of business services and applications.

The Cisco Info Center/Netcool components comprise:

- IBM Tivoli Netcool/OMNIbus and ObjectServer, page 1-23
- IBM Tivoli Netcool/Impact, page 1-24
- IBM Tivoli Integrated Portal, page 1-24
- IBM Tivoli Business Service Manager, page 1-24
- IBM Tivoli Netcool Probes, page 1-25
- Rules Files, page 1-25

IBM Tivoli Netcool/OMNIbus and ObjectServer

The IBM Tivoli Netcool/OMNIbus service level management (SLM) system collects enterprise-wide event information from several different network data sources, and presents a simplified view of this information to operators and administrators.

This information:

- Assigns information to operators.
- Travels to help desk systems.
- Is logged in a database.
- Replicates on a remote Netcool/OMNIbus system.
- Triggers automatic responses to certain alerts.

Netcool/OMNIbus can also consolidate information from different domain-limited network management platforms in remote locations. By working in conjunction with existing management systems and applications, Netcool/OMNIbus minimizes deployment time; thus, network operators save time in managing the network.

Netcool/OMNIbus tracks alert information in a high-performance, in-memory database, and presents information of interest to you through individually configurable filters and views.

Netcool/OMNIbus automation functions can perform intelligent processing on managed alerts.

The ObjectServer is the in-memory database server at the core of Netcool/OMNIbus. The ObjectServer forwards alert information from external programs, such as probes, monitors, and gateways, stored and managed in database tables, and is visible in the event list.

[2] For a detailed definition, see the Glossary.

For a detailed listing of the Netcool/Omnibus documents, see the *Cisco Info Center 7.3 Documentation Guide and Supplemental License Agreement.* This document is viewable online at:

http://www.cisco.com/en/US/products/sw/netmgtsw/ps996/products_documentation_roadmaps_list.html

IBM Tivoli Netcool/OMNIbus and ObjectServer Requirements

For detailed information on operating system requirements, JRE support, and user interface support for IBM Tivoli Netcool/OMNIbus, see the *Netcool/OMNIbus 7.3 Installation and Deployment Guide,* available online at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.netcool_OMNIbus.doc_7.3.0/omn_pdf_ins_master_73.pdf

IBM Tivoli Netcool/Impact

IBM Tivoli Netcool/Impact is the analysis and correlation engine for the Netcool suite of network management products. IBM Tivoli Netcool/Impact allows you to extensively customize and enhance Netcool/OMNIbus and other Netcool products by adding such functionality as advanced event and business data correlation, event enrichment and event notification. In addition, you can use IBM Tivoli Netcool/Impact to integrate IBM Tivoli Netcool/OMNIbus with a wide variety of third-party software, including databases, messaging systems and network inventory applications.

IBM Tivoli Integrated Portal

The high-level interface for Cisco Video Assurance Management Solution 3.1 is the Tivoli Integrated Portal (TIP) and the Tivoli Business Service Manager (TBSM). TIP allows you to launch TBSM and customized event views for events in the video headend and video transport network.

IBM Tivoli Business Service Manager

IBM Tivoli Business Service Manager (TBSM) delivers technology to visualize and assure the health and performance of critical business services.

TBSM functions include:

- Build business service models.
- Integrate business service status from data sources or event sources including the Netcool/OMNIbus ObjectServer.
- Monitor service outages based on service level agreements.
- Build customized business service views, scorecards, and dashboards.
- Tailor views to different users and roles including service manager, operator, or executive.
- Provide dynamic visualization of key performance indicators (KPIs) and other critical business metrics.
- Provide self-management through monitoring of key components by using IBM Tivoli Monitoring (ITM).

The TBSM tools enable a service model that integrates with the Netcool/OMNIbus ObjectServer alerts, or optionally with the data from a structured query language (SQL) data source. TBSM processes the external data based on the service model data you create in the TBSM database and returns a new or updated TBSM service event to the Netcool/OMNIbus ObjectServer.

TBSM provides a console that allows you to logically link services and business requirements in the service model. The service model provides you with a view on the performance of your business services, second by second.

See the installation, quick start, administrator, service configuration, customizing, and troubleshooting guides for this product, available on the IBM website.

JRE Requirements

Netcool/TBSM version 4.2 requires the Java Runtime Environment (JRE) to be installed on your system.

Netcool/TBSM supports the following JREs:

- JRE 1.5 or 1.6 on Windows platforms
- JRE 1.6 on Linux and Solaris
- IBM JRE 1.6 on AIX platforms

IBM Tivoli Netcool Probes

The IBM Tivoli Netcool Probes connect to an event source, detect and acquire event data, and forward the data to the ObjectServer as alerts. Probes use the logic specified in a rules file to manipulate the event elements before converting them into fields of an alert in the ObjectServer alerts.status table.

Uniquely designed, each probe can acquire event data from a specific source. Probes can also acquire data from any stable data source, including devices, databases, and log files.

Licenses for two probes are included in Cisco CIMS Service Assurance: the Netcool/Tivoli SNMP EMS probe and the Netcool/Tivoli Syslog probe.

The main probe used with Cisco VAMS 3.1 and Cisco Info Center is the MTTrapd (Multi-Threaded) probe, which monitors SNMP traps and events on both UDP and TCP sockets. Using rules defined in the custom rules files for Cisco VAMS 3.1, the MTTrapd probe parses events from the VAMS components and assembles them into enhanced messages that show detailed information about the event and the devices involved in the event.

Cisco VAMS also uses the Netcool/Tivoli Syslog probe to forward syslog events from Cisco devices in the VAMS solution to the Object Server.

Netcool Knowledge Library

IBM Netcool Knowledge Library is a collection of rules files that are tuned to specific managed objects that send SNMP-based events, such as Cisco networking devices. These rules support a wide range of Cisco system MIBs, including MIBs for specific Cisco devices, protocols, and technologies, as well as syslog messages from a wide range of Cisco devices.

Rules Files

Included in Cisco Info Center/Netcool, the rules files enable streamlined communication between the CMM, ROSA NMS, and Cisco ANA components and the Netcool ObjectServer. This functionality includes the decoding of CMM, ROSA NMS, and Cisco ANA trap information pushed up from CMM or Cisco ANA into the ObjectServer database on the Netcool server.

The rules files for VAMS are referred to as VAMS extensions, and you can order them as a separate SKU.

Cisco ANA 3.7.2

This section describes the hardware and software components of Cisco ANA 3.7.2.

Cisco ANA 3.7.2 Hardware Components

Cisco ANA 3.7.2 hardware comprises:

- Cisco ANA Servers, page 1-26
- Cisco ANA Clients, page 1-29

Note The hardware recommendations assume that the Cisco ANA 3.7.2 software will not share the hardware with additional applications.

Cisco ANA Servers

Cisco ANA uses two server types, each performing different activities:

- Cisco ANA Gateway, page 1-26
- Cisco ANA Unit, page 1-27

Cisco ANA Gateway

The Cisco ANA Gateway uses a Sun Fire V490 running Solaris OS 10. It is the gateway through which all clients, including any operations support systems or business support systems (OSS/BSS) applications as well as the Cisco ANA clients, can access the system. The gateway is an extended Cisco ANA unit (see the "Cisco ANA Unit" section on page 1-27). It enforces access control and security for all connections, and manages client sessions. In addition, it functions as a repository for storing configuration, network and system events, and alarms.

Another important function of the gateway is to map network resources to the business context. As a result, Cisco ANA can contain information not directly in the network (such as virtual private networks [VPNs] and subscribers) and display it to northbound applications.

Cisco ANA Gateway Requirements

Table 1-3 lists the hardware and software requirements for the Cisco ANA 3.7.2 gateway.

Table 1-3 Cisco ANA Gateway Requirements

Item	Specifications
Hardware Requirements	
Sun Fire V490	• 4 x at least 1.35-GHz UltraSPARC IV processors. • Minimum 16 GB of memory. • Swap file must be at least twice the size of the installed RAM. • 2 x 73-GB hard disk drives. • 1 x DVD drive.

Table 1-3 Cisco ANA Gateway Requirements (continued)

Item	Specifications
Hardware Requirements	
Software Requirements	
Operating system	• Solaris 10. • Solaris 10 patch cluster release as published by Sun Microsystems on 18 January 2008 or later. • J2SE Solaris 10 patch cluster release as published by Sun Microsystems on 18 January 2008 or later. **Note** For exact patch lists, see the *Cisco ANA Release Notes, 3.7.2* viewable online at: http://www.cisco.com/en/US/products/ps6776/prod_release_notes_list.html
Third-party tools	• Java v1.3.1_08 • Active Perl v5.6
Database	• Customer supplied and installed Oracle 9i Enterprise Edition with partitioning option.

Note Do not use the Cisco ANA 3.7.2 servers (gateway and unit) with any application other than Cisco ANA 3.7.2.

Cisco ANA Unit

The Cisco ANA unit uses a Sun Fire V490 running Solaris OS 10. This unit is a key element of the Cisco ANA system. Networked together, these units create a modular, scalable, and high-performance, distributed knowledge engine. Multiple units cover the entire network as a single complete entity for discovery, assurance, and activation.

Cisco ANA Unit Requirements

Table 1-4 lists the hardware and software requirements for the Cisco ANA 3.7.2 unit.

Table 1-4 Cisco ANA Unit Requirements

Item	Specifications
Hardware Requirements	
Sun Fire V490	• 4 x at least 1.35-GHz UltraSPARC IV processors. • Maximum 16 GB of memory. **Note** CPUs might not use more than 16 GB of memory, even if the hardware has, for example, 32 GB of available memory. All Autonomous Virtual Machine (AVM) and VNE memory must do its calculations as if the unit only has 16 GB of available memory. • 2 x 73-GB hard disk drives. • 1 x DVD drive.
Software Requirements	
Operating system	• Solaris 10. • Solaris 10 patch cluster release as published by Sun Microsystems on 18 January 2008 or later. • J2SE Solaris 10 patch cluster release as published by Sun Microsystems on 18 January 2008 or later. **Note** For exact patch lists, see the *Cisco ANA Release Notes, 3.7.2* viewable online at: http://www.cisco.com/en/US/products/ps6776/prod_release_notes_list.html
Third-party tools	• Java v1.3.1_08 • Active Perl v5.6

Note Do not use the Cisco ANA 3.7.2 servers (gateway and unit) with any application other than Cisco ANA 3.7.2.

Cisco ANA Clients

The Cisco ANA client uses a Wintel platform running a suite of various GUI applications to manage the network. (See the "Cisco ANA Client Software Tools" section on page 1-32.)

Cisco ANA Client Requirements

Table 1-5 lists the hardware and software requirements for the Cisco ANA 3.7.2 client.

Table 1-5 Cisco ANA Client Requirements

Item	Specifications
Hardware Requirements	
Wintel platform	• Pentium IV, 2.66-GHz processor or better • 1 GB RAM • 2 GB of free disk space • 1 DVD drive • 512 MB of free nonvirtual memory
Monitor	• Minimum screen resolution of 1024 x 768 pixels • True color (32-bit) setting
Software Requirements	
Operating system	Microsoft Windows 2000 or Windows XP
Internet Connection	
	Minimum bandwidth of 1.5 MB

Cisco ANA 3.7.2 Software Components

Cisco ANA 3.7.2 provides mediation and abstraction between NEs and OSS applications, and supports fault collection and root-cause analysis for the transport network. Cisco ANA 3.7.2 manages the NEs listed in the "Network Elements in the Video Transport Network" section on page 1-10. The Cisco ANA 3.7.2 features for the Cisco VAMS 3.1 include:

- Soft properties and command builder scripts to extend VNEs for monitoring multicast and video flows.
- Unique VNEs to support the Cisco NEs in the video transport network (Cisco 7600 Series router, Cisco CRS-1, and Catalyst 4948 Series and Catalyst 6500 Series switches).
- Event-handling and threshold-crossing alerts (TCA) for video-affecting conditions.
- New trap and syslog support through event configuration and customization.

Cisco ANA 3.7.2 automatically detects and manages the NEs in its domain, including their physical and logical inventories.

VNEs

Cisco ANA 3.7.2 provides a VNE mediation layer between the managed NEs and the network management applications in Cisco ANA 3.7.2. Generally, a one-to-one correspondence exists between an NE in the managed network and the VNE that depicts it in Cisco ANA 3.7.2. The VNEs collect information from their corresponding NEs for management purposes.

Cisco VAMS 3.1 uses VNEs to represent the solution components in Table 1-6.

Table 1-6 VNEs for the Cisco VAMS 3.1

Solution Component	VNE Description
Cisco 7600 Series routers	7600 VNE[1]
Cisco ASR 9000 routers	ASR 9000 VNE
Cisco Catalyst 6500 Series switch	6500 VNE[1]
Cisco CRS-1	CRS-1 VNE[1]
Cisco Catalyst 4948 Series switches	4948 VNE[1]
Cisco Multicast Manager	Generic Internet Control Message Protocol (ICMP) VNE
IneoQuest Video Probe	Generic Simple Network Management Protocol (SNMP) VNE
Mixed Signals Video Probe	Generic ICMP VNE

[1] Cisco ANA 3.7.2 activation scripts and soft properties created for the Cisco VAMS 3.1 enable the VNE to monitor multicast video flows.

Soft Properties and Threshold-Crossing Alerts

Soft properties are attributes that appear in the inventory of managed VNEs but are not kept in the database. You can configure these properties to poll on a regular basis. You can also configure TCAs to raise events based on preset threshold values. You can associate soft properties with a specific VNE, all instances of a VNE type, or all managed elements.

Configuration Management and Inventory

Cisco ANA 3.7.2 automatically detects managed NEs in the video transport network along with their physical and logical inventories. Cisco ANA 3.7.2 also detects changes in the NEs and automatically synchronizes its archived physical and logical inventories with those changes. Support for traps, syslogs, and polling (SNMP and Telnet) enables this functionality.

Cisco ANA 3.7.2 also supports discovery of the network topology (automatically and manually).

Cisco ANA 3.7.2 monitors and reports interface and operational status for these Cisco NEs in the video transport network:

- Cisco 7600 Series router
- Cisco Catalyst 6500 Series switch
- Cisco ASR 9000 routers
- CRS-1
- Cisco Catalyst 4948 Series switch

This support includes:

- Logical inventory (for example, subinterfaces, VLANs, and routing tables)
- Physical inventory (for example, chassis, cards, and serial numbers)

See the “Network Elements in the Video Transport Network” section on page 1-10, for details about the Cisco NEs.

Fault Management

Cisco ANA 3.7.2 provides fault management for the video transport network:

- Event and Alarm Management, page 1-31
- Polling and CPU Utilization, page 1-31
- GUIs for Fault Management, page 1-31

See the *Cisco ANA User Guide 3.7.2* for a description of the Cisco ANA fault management system, viewable online at:

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

Event and Alarm Management

Cisco ANA 3.7.2 also provides the following event-related features:

- A log of the events.
- Rules-based event processing (for example, to support changing event severities or customize problem descriptions).
- Correlation of events and removal of duplicated events.
- Suppression of events from a particular device or interface.
- Viewing and sorting events (by time and date, severity, or device), switching between multiple event views, and viewing detailed event data.
- Viewing syslog events.

Polling and CPU Utilization

Cisco ANA 3.7.2 monitors CPU utilization of the supported NEs in the Cisco VAMS 3.1. For more information about ANA polling and its interaction with the CPU utilization of managed NEs, see the *Cisco ANA User Guide, 3.7.2,* viewable online at:

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

Cisco ANA 3.7.2 also supports ICMP to verify that supported NEs are reachable. The ANA VNEs send the ICMP packets to the NEs at a designated rate. You specify the polling rate when you define the VNEs for the Cisco VAMS 3.1.

For more information about ICMP polling, see the *Cisco ANA User Guide, 3.7.2,* viewable online at:

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

Cisco ANA 3.7.2 also provides dynamic, on-demand polling of specific object identifiers (OIDs) by using the ANA Command Builder, a tool which you use to create and run activation scripts.

See the *Cisco ANA Command Builder User Guide 3.7.2,* viewable online at:

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

GUIs for Fault Management

Cisco ANA 3.7.2 provides GUIs that show NE:

- Status information on the components that this solution supports. (See the "Network Elements in the Video Transport Network" section on page 1-10, for descriptions of the supported NEs.)
- Events, including severity levels and timestamps.
- Cisco ANA Network Vision and Cisco ANA Event Vision are the software tools that provide these GUIs.

Security Management

Cisco ANA 3.7.2 provides user identification and authentication for accessing the Cisco ANA 3.7.2 to perform configuration and fault management tasks on the supported NEs. For more information about security information in Cisco ANA 3.7.2, see the *Cisco ANA Administrator Guide, 3.7.2*, viewable online at:

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

Multicast and Video Management

Cisco ANA 3.7.2 provides these multicast and video metrics:

- **PIM Alarms**—Cisco ANA creates alarms for events related to Protocol Independent Multicast (PIM) status changes. The video transport network uses PIM to build a video-specific multicast topology. Therefore, PIM alarms are important for monitoring the status of the solution.
- **Multicast Routes**—Cisco ANA uses a VNE soft property to display the number of multicast routes in the device (Cisco 7600 Series router, Cisco CRS-1, or Cisco Catalyst 4948 Series switch). Cisco ANA NetworkVision displays the number of multicast routes on the selected device.

Cisco ANA uses the Event MIB to monitor changes in the number of multicast routes. When the number of multicast routes changes, indicating a possible problem in the video flow, the Event MIB sends an SNMP trap. Cisco ANA receives the trap and creates an event in the Cisco ANA EventVision.

- **Non-RPF Drops**—Cisco ANA monitors non-Reverse Path Forwarding (non-RPF) drops on each multicast stream. Non-RPF packets, also called RPF failure packets, are RPF packets transmitted backwards, against the flow from the source. Multicast streams include video and non-video streams. If the number of non-RPF drops on a multicast stream exceeds five drops during a polling period, the device sends an SNMP notification. The Cisco ANA 3.7.2 receives the notification and generates an alarm. The Cisco ANA 3.7.2 correlates subsequent alarms and generates subalarms.

Cisco ANA Client Software Tools

Cisco ANA 3.7.2 includes several applications built on top of the virtual network as the mediation layer.

Cisco ANA 3.7.2 applications include:

- **Cisco ANA Manage**—You use the Cisco ANA Manage tool to add, delete, or modify the Cisco NEs in the Layer 2 transport sections of multicast video networks. The administrator configures and controls the Cisco ANA with this GUI tool. The Cisco ANA Manage tool interacts with the Cisco ANA Registry to query and modify configuration information.

  See the *Cisco ANA Administrator Guide 3.7.2,* viewable online at:

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

- **Cisco ANA NetworkVision**—You use the Cisco ANA NetworkVision tool (the main GUI for Cisco ANA 3.7.2) to view the network inventory and topology. Cisco ANA NetworkVision displays events, while the mediation layer collects information from the NEs and displays the objects in a topology map. Cisco ANA NetworkVision also displays status and event information (including severities and timestamps) for these supported NEs.

  Network administrators and anyone else responsible for the management, fulfillment, planning, and assurance of the integrity of network resources can use the Cisco NetworkVision tool. See the *Cisco ANA User Guide 3.7.2,* viewable online at:

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

- **Cisco ANA EventVision**—You use the Cisco ANA EventVision tool (a GUI for browsing the events in the system) to view and manage alarms, traps, syslogs, provisioning, and system and security events. Monitoring the Cisco ANA EventVision helps predict and identify the sources of network problems, which might prevent future problems.

  See the *Cisco ANA EventVision User Guide 3.7.2,* viewable online at:

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

Third-Party Video Probes

Cisco VAMS 3.1 supports several third-party probes including the Bridge Technologies, IneoQuest, and Mixed Signals video probes. You can add these video quality monitoring probes to key points in the transport network. Functionally, these probes detect impairments and validate the integrity of the Moving Pictures Expert Group (MPEG) transport stream, which carries video.

The video probes communicate with the Cisco VAMS components as follows:

- By sending traps to ROSA.
- CMM uses SNMP polling to retrieve MDI statistics from video probes.
- When you are viewing a video probe event forwarded by these probes, you can launch CMM diagnostics directly from the Cisco Info Center interface.

Cisco VAMS 3.1 receives events from the probes based on thresholds that you configure in the video probes or in CMM. Cisco VAMS 3.1 associates probe events with a severity level in Cisco Info Center.

Note IneoQuest probes are polled directly by the CMM 3.1.2 application.

See the video probe guides for VAMS 3.1, which are listed in the *Documentation Guide for Cisco Video Assurance Manager, 3.1*, available online at:

http://www.cisco.com/en/US/products/ps9518/products_documentation_roadmaps_list.html

Cisco Advanced Services Support for VAMS

Cisco Advanced Services provides services such as technical application support, network application integration support and network optimization support for the VAMS solution.

Using the Cisco Lifecycle Services approach, Cisco and its partners provide a broad portfolio of services that address all aspects of deploying, operating, and optimizing your network to help increase business value and return on investment.

This section describes:

- Cisco Lifecycle Approach, page 1-34
- Prepare Phase, page 1-34
- Plan Phase, page 1-35
- Design Phase, page 1-35
- Implement Phase, page 1-36

For detailed information on Cisco Advanced Services support for video services, go to the following URL:

http://www.cisco.com/en/US/products/ps9908/serv_group_home.html

For detailed information on Advanced Services support for network management, go to the following URL:

http://www.cisco.com/en/US/products/ps6835/serv_group_home.html

For a detailed description of Cisco Advanced Services support for VAMS 3.1, see the *Video Assurance Monitoring Delivery Cisco Advanced Services* document at the following URL (TBD):

Cisco Lifecycle Approach

Cisco takes a Lifecycle approach for deploying and operating network management systems. This approach helps companies to accelerate their success with advanced technologies and to improve their network's business value and return on investment.

Table 1-7 lists each phase in the product lifecycle and describes the type of support that Advanced Services and other consulting groups at Cisco provide.

Table 1-7 Cisco Life Cycle Mapping

Lifecycle Stage	Services	Organization
Prepare	Establishing a technology vision and high-level conceptual architecture	Presales/Advisory/ Advanced Services
Plan	Properly assessing the existing environment to determine whether it can support the new technologies and services	Advanced Services
Design	Designing a system that meets business and technical requirements	Advanced Services
Implement	Integrating the new solution without disrupting the network or creating points of vulnerability	Advanced Services
Operate	Maintaining network health through day-to-day operations	Advanced Services Technical Services
Optimize	Achieving operational excellence by adapting the architecture, operation, and performance of the network to ever changing business goals	Technical Services

Prepare Phase

In the prepare phase of the VAMS lifecycle, a company establishes business requirements and a corresponding management technology vision. The company develops a technology strategy and identifies the technologies that can best support its growth plans. After the financial and business value of migrating to a particular advanced technology solution has been assessed, the company establishes a high-level, conceptual architecture for the proposed system and validates features and functionality documented in the high-level design through proof-of-concept testing. The customer can choose to perform all or some of the activities in house or use Cisco Services.

Cisco Advanced Services can provide services to deploy a turnkey VAMS solution, ranging from a base probeless solution with CMM only to a full solution with probes with ANA, ROSA, and Cisco Info Center integration. The solution complexity scales based on the n, ROSA and Cisco Info Center will increase the complexity of the integration. Probes can be added to any offering whether base or a full integration with ANA and Cisco Info Center.

Additional features can also be added on in later phases.

Services Provided

- Customer requirements document (CRD) and CRD response
- Current Video Service Operations Assessment document
- High Level Design Document
- Proof of concept (POC) of the solution, and POC lab execution report
- Statement of work (SOW) and quotation

Plan Phase

In the plan phase of the lifecycle, the organization tries to make sure that adequate resources are available to manage the technology deployment project from planning through design and implementation. A project plan is created to help manage the tasks, risk, problems, responsibilities, critical milestones, and resources required to implement VAMS solution into the production network.

Services Provided

- Data collection of channel-lineup, ad-zone, and multicast addresses for the video flows (Base offering, CMM only). A spreadsheet summarizing the collected data.
- Data collection regarding MPEG probes parameters and associated alarm thresholds. (probes only).
- Data collection regarding ROSA-managed devices.
- Data collection regarding ANA managed nodes and alarm thresholds (ANA only).
- Data collection regarding VAMS Cisco Info Center-specific data. (CIC).
- Gaps and recommendation to gaps document.
- VAMS program and project management: Aligns with the scope, cost, and resource parameters in the original business requirements established during the prepare phase.
- An overall project management plan (PMP).
- VAMS site readiness report.

Design Phase

During the design phase of the VAM lifecycle, Cisco validates the proposed high level design and develops a low level design to the specified customer requirements and data. During the design phase, Cisco Network Consulting Engineers create a variety of plans and documents to guide activities such as configuring, deploying, and commissioning the proposed system.

Services Provided

- VAMS design development (CMM, probes, ANA and/or Cisco Info Center) and associated Low-Level Design (LLD) documents.

- VAMS test plan development (CMM, probes, ANA, and/or Cisco Info Center).
- VAMS implementation plan.
- VAMS design validation and review.
- Probes placement methodology.
- Network management for probes.
- Probe configuration.
- Specific configuration for ROSA.
- Probe network management plan.
- ANA-plug in configuration for VAMS (ANA).
- Specific configuration for Cisco Info Center.

Implement Phase

In the Implementation phase, Cisco Advanced Services integrates systems without disrupting the existing network or creating points of vulnerability. Cisco configures and integrates system components, and installs, configures, tests, and commissions the VAMS system. After installation, Cisco validates that its operational network is working as intended, validates system operations, and works to close gaps in staff skills

Services Provided

- Site readiness review.
- CMM installation and configuration.
- Discovery of the multicast devices.
- Configuration, testing, and adjustment of critical flows and multicast thresholds.
- Configuration, testing, and implementation of MPEG thresholds (probes only). Customer performs physical installation of probes.
- Implementation and configuration of the ANA VAMS plug-in (ANA only)
- Implementation of Cisco Info Center plug-in (Cisco Info Center only).
- Test plan execution.
- CMM cases.
- Probes cases.
- ROSA test cases
- ANA VAMS-plug in cases.
- Cisco Info Center-plug in cases.
- AS build documents and support for on-site knowledge transfer.

CHAPTER 2

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

This chapter contains the following sections:

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.

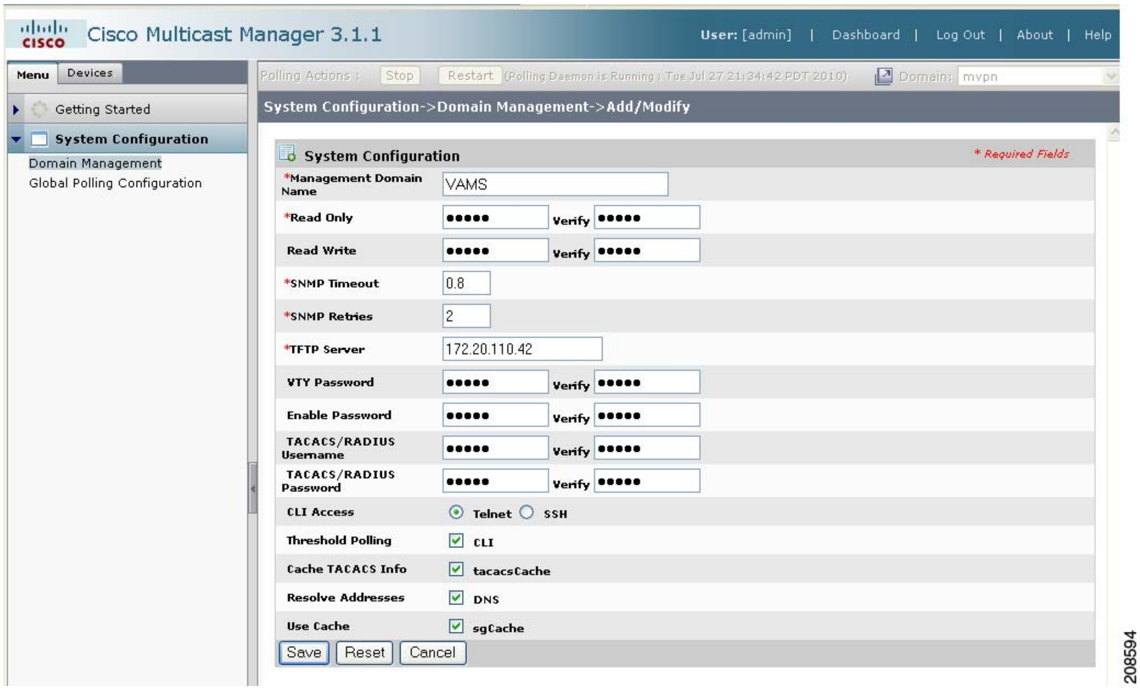
Step 4 Click the **Add** button and from the drop-down list, choose **By Domain.**

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
Getting Started
System Configuration
Domain Management
Global Polling Configuration
208594

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

Domain: mvpn

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		

Save Reset Cancel

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.

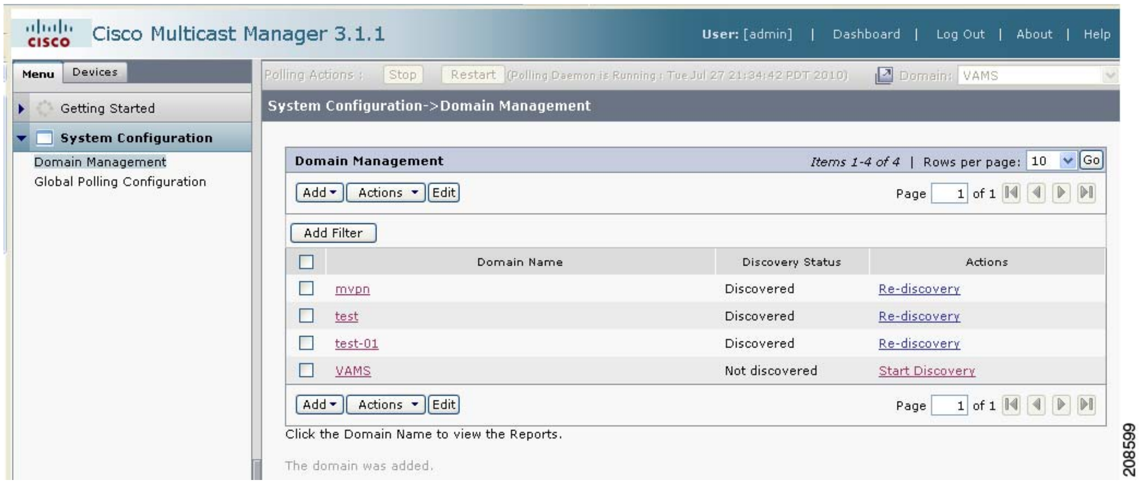
- Specify the remaining settings as described in "Creating a Domain" in the "System Configuration" chapter of the *User Guide for Cisco Multicast Manager, 3.1* at the following location:

  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



Cisco Multicast Manager 3.1.1

User: [admin] | Dashboard | Log Out | About | Help

Polling Actions : Stop Restart (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 Go

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

Click the Domain Name to view the Reports.

The domain was added.

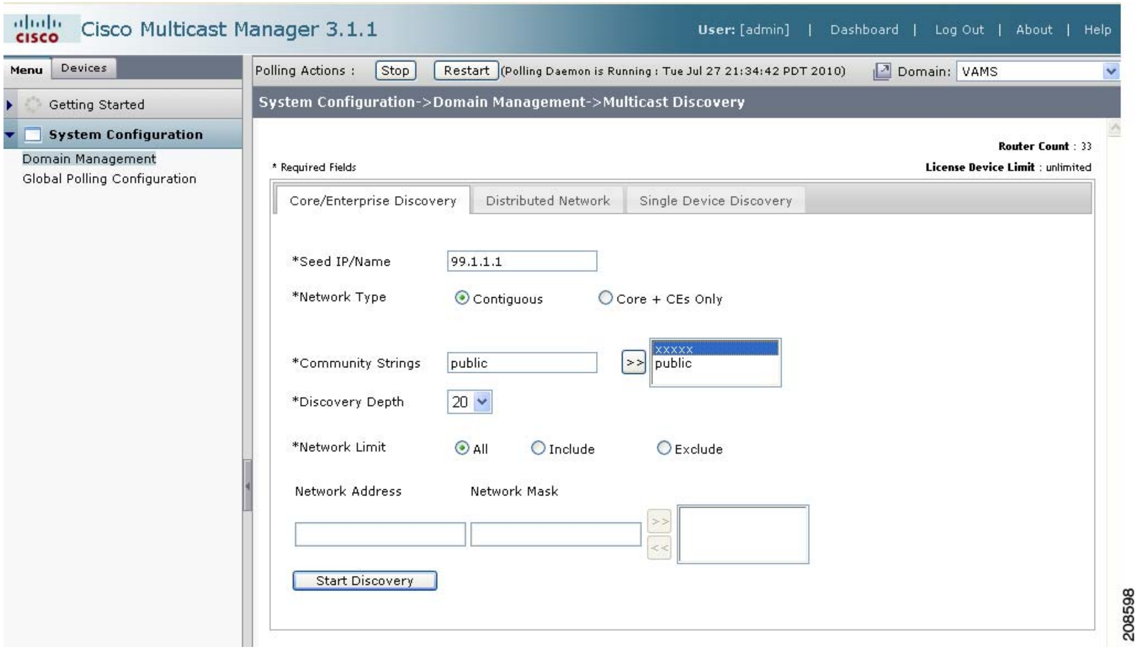
Discovering Devices to Monitor

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



Cisco Multicast Manager 3.1.1

User: [admin] | Dashboard | Log Out | About | Help

Polling Actions : Stop Restart (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

Core/Enterprise Discovery | Distributed Network | Single Device Discovery

*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

Start Discovery

Step 2 Enter values as follows:

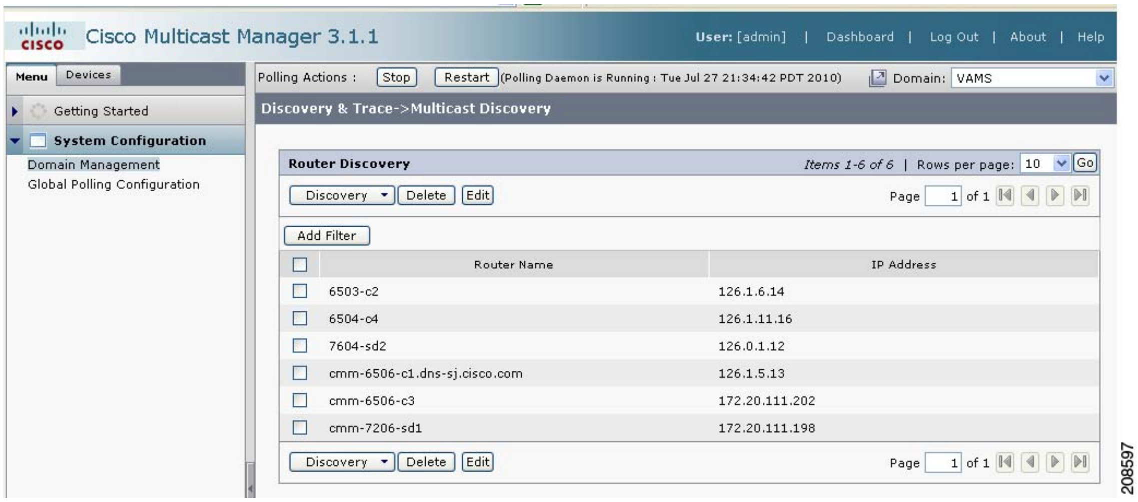
- In the Seed/IP/Name field, enter the IP address or hostname of any device in the domain.
- In the Community Strings field, enter *public* and click the right arrow to move it to the list of community strings.
- From the drop-down list in the Discovery Depth field, select the number of hops to discover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

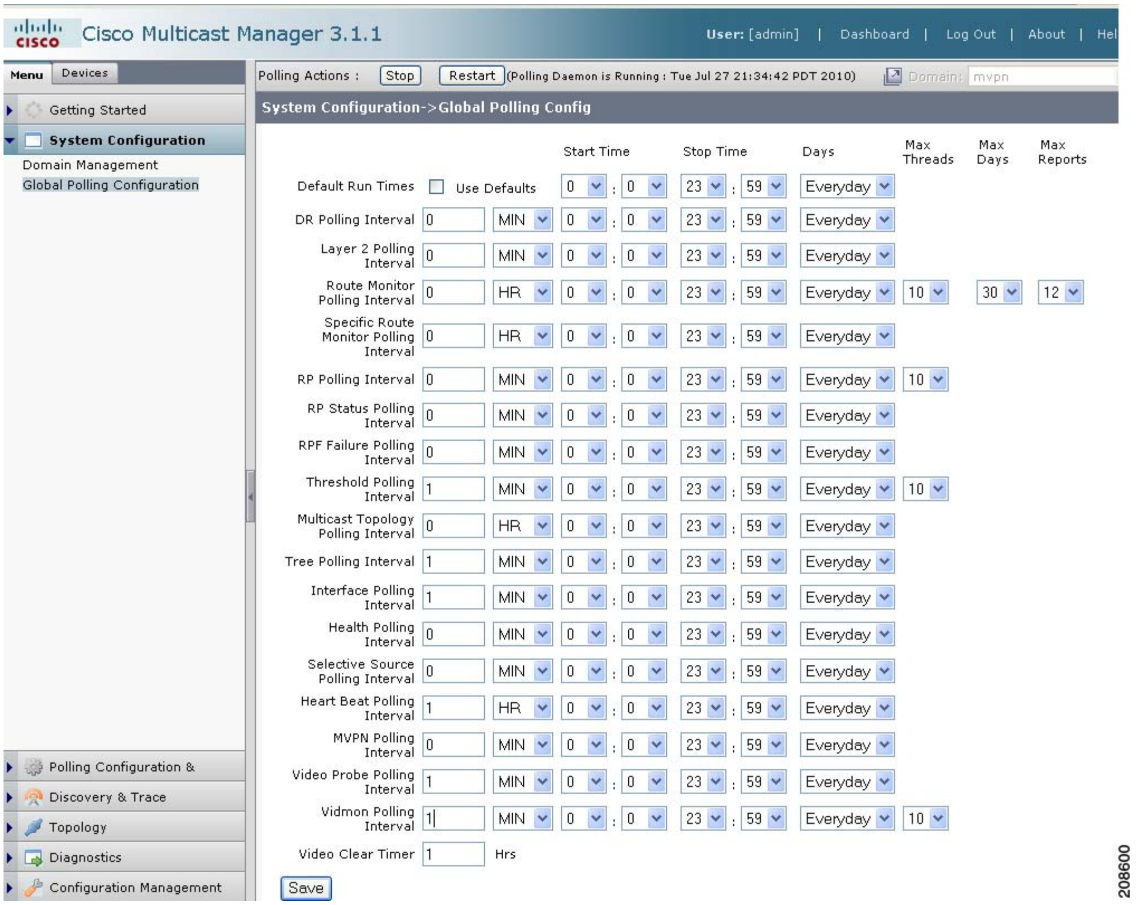
- The IP address of the CIC server, for northbound forwarding of SNMP traps

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						

Save

Step 2 Configure the following Global Polling intervals:

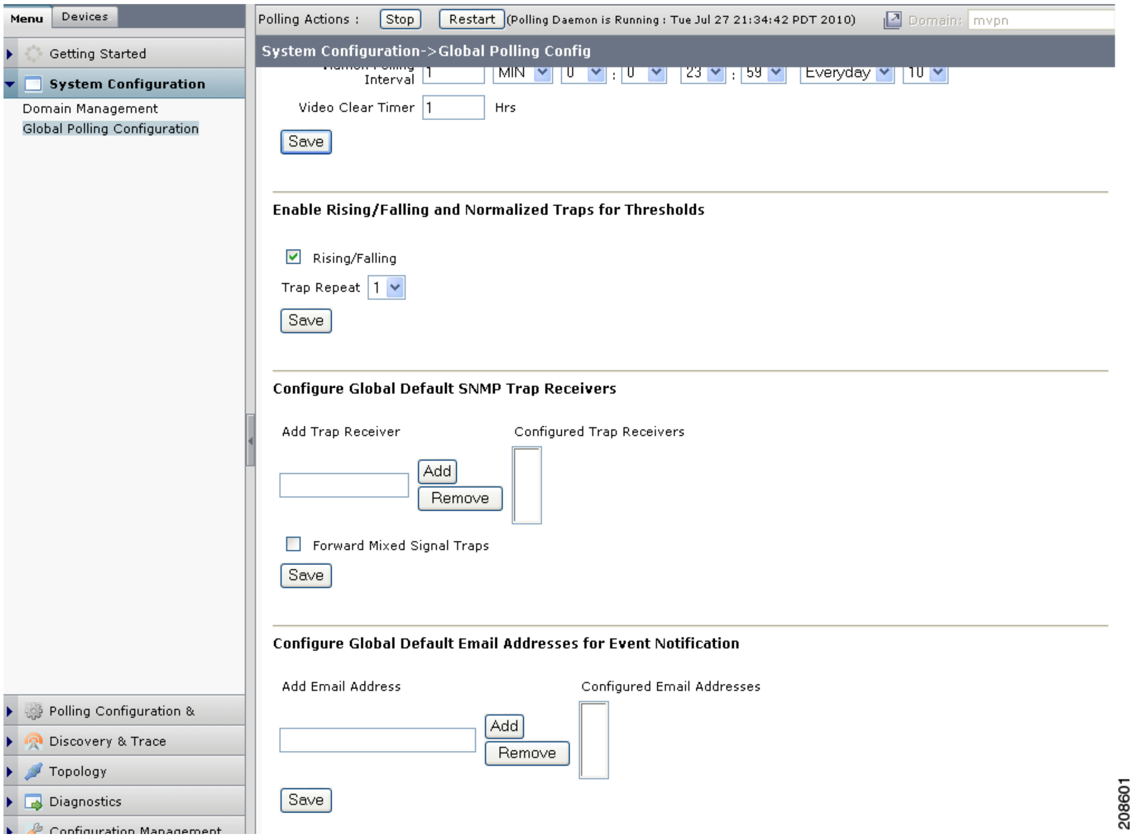
- Threshold Polling Interval
- Tree Polling Interval
- Heart Beat Polling Interval
- Video Probe Polling Interval

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

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

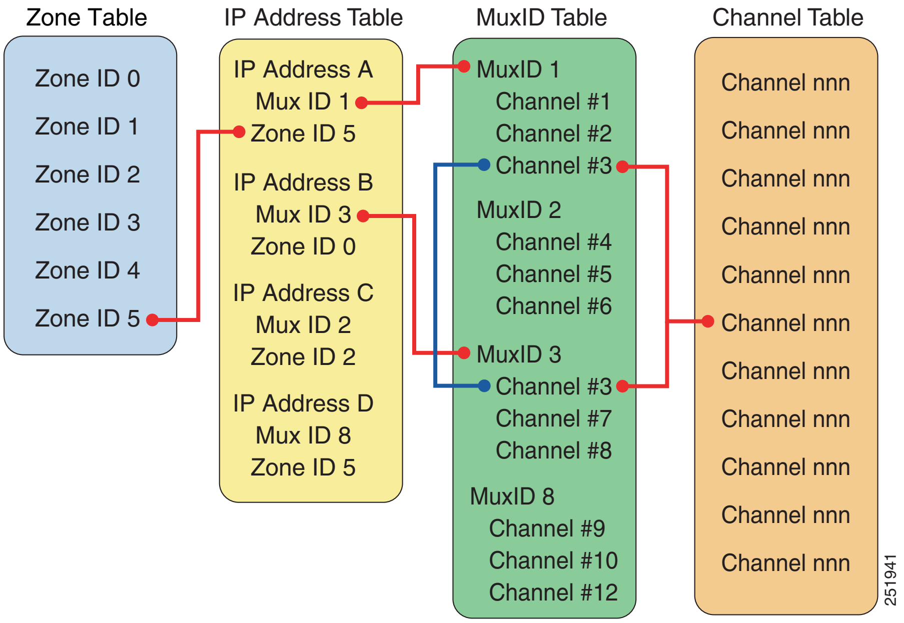
Note Ensure that you configure the CMM databases before you install and configure Cisco Info Center. During Cisco Info Center installation, you must place CSV files containing the database information into a directory used for CIC installation and which is accessible to the *customize_vams.sh* script.

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:

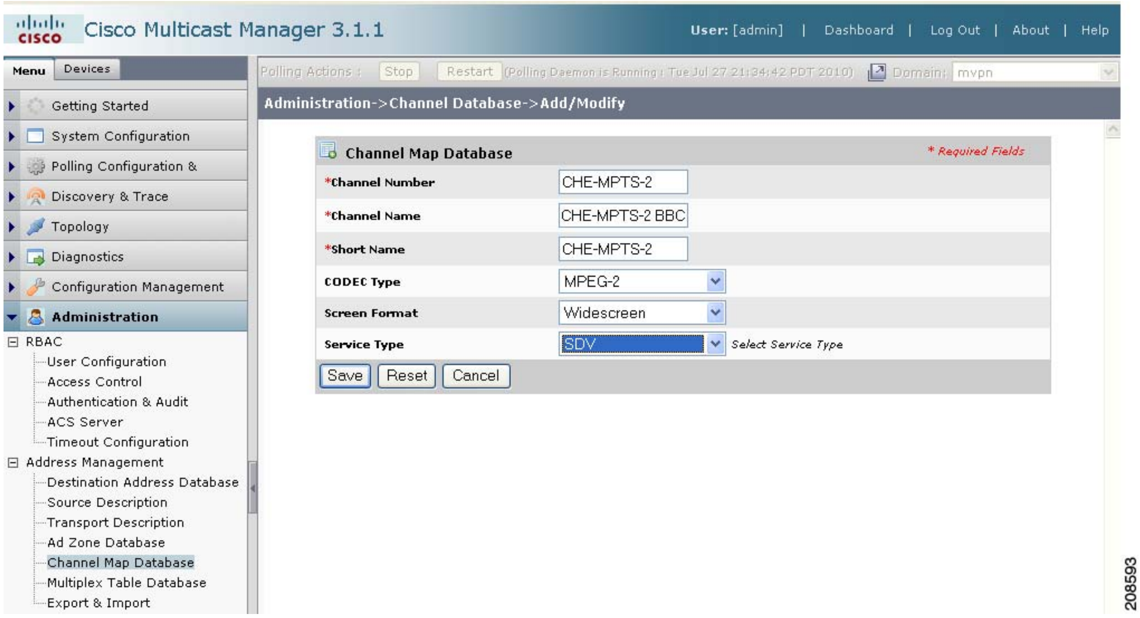
Step 1 From the CMM main menu, choose **Administration > Address Management > Channel Map Database**.

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



Administration->Channel Database->Add/Modify

Channel Map Database — * Required Fields

*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 — Select Service Type

Save Reset Cancel

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**.

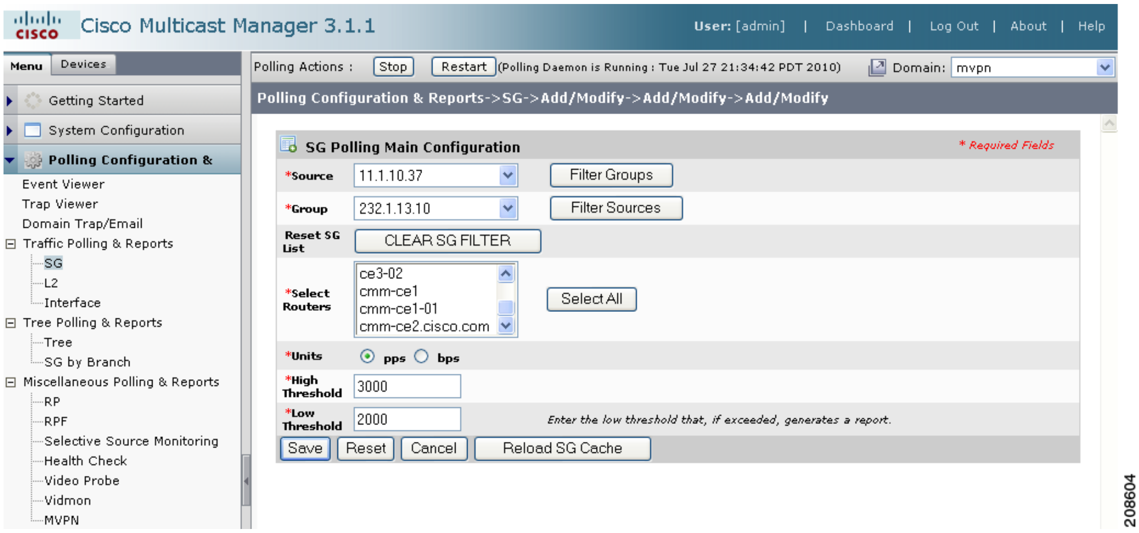
The SG Configurations page opens.

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)

*Source: 11.1.10.37

*Group: 232.1.13.10

*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.

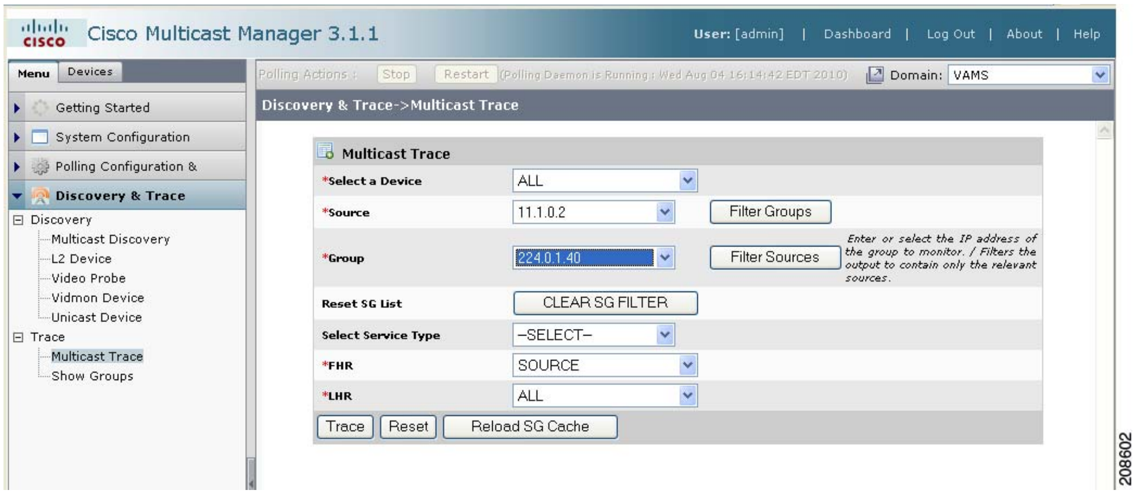
To configure tree polling, you must first create a trace file by drawing a multicast tree and saving it.

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



Multicast Trace

*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

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:

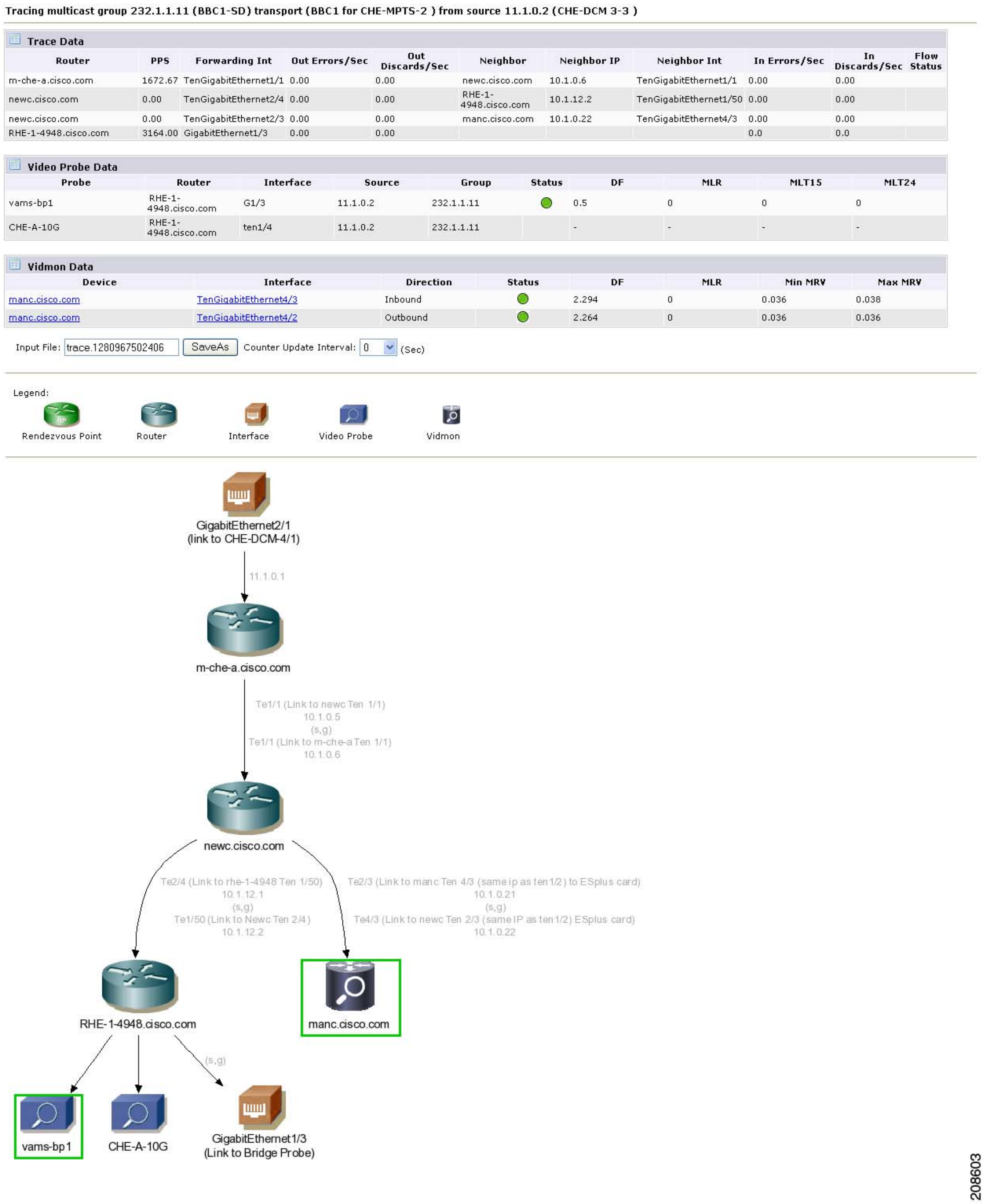
http://www.cisco.com/en/US/docs/net_mgmt/cisco_multicast_manager/3.1/user/guide/cmm_dt.html#wp1054116

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.**

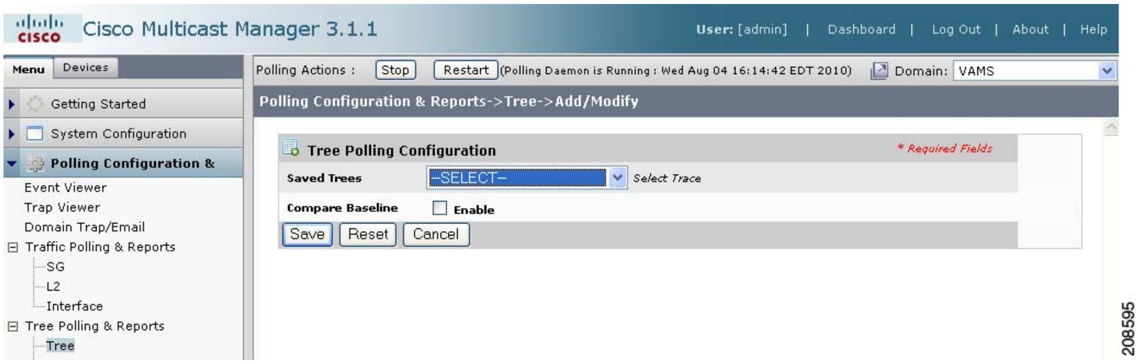
The Tree Report page opens.

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 Actions : Stop Restart (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.

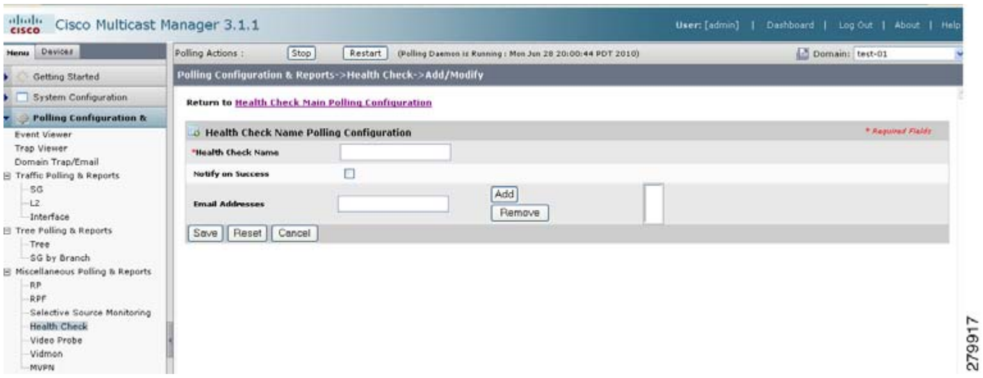
Step 2 Click **Config Health Check Polling**.

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



Cisco Multicast Manager 3.1.1

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

Domain: test-01

Polling Configuration & Reports->Health Check->Add/Modify

Return to Health Check Main Polling Configuration

Health Check Name Polling Configuration

* Required Fields

*Health Check Name

Notify on Success □

Email Addresses

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.**

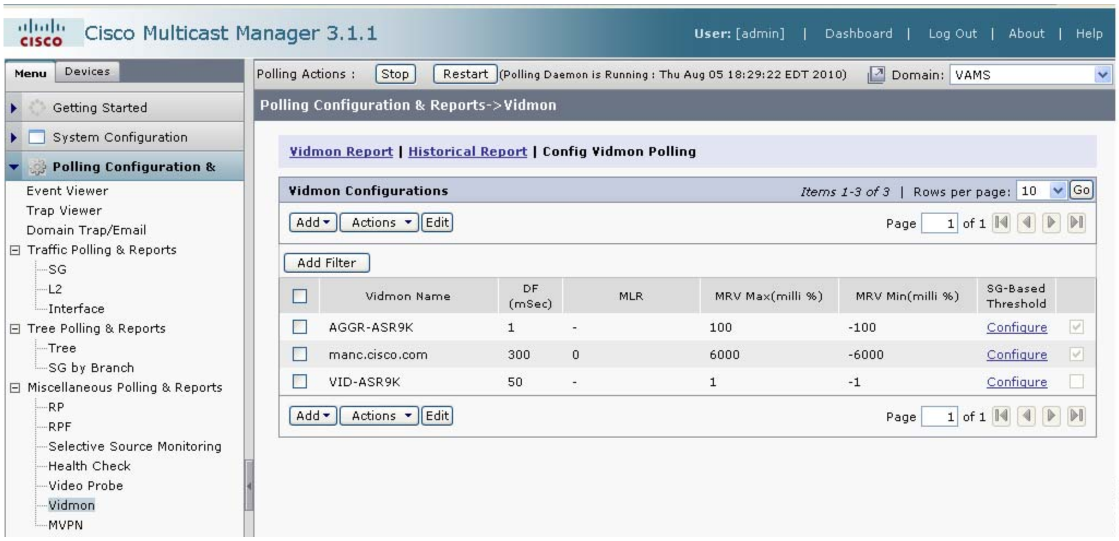
Step 3 Select **Vidmon**.

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)

Polling Configuration & Reports->Vidmon

Vidmon Configurations — *Items 1-3 of 3* | Rows per page: 10 — Page 1 of 1

□	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:

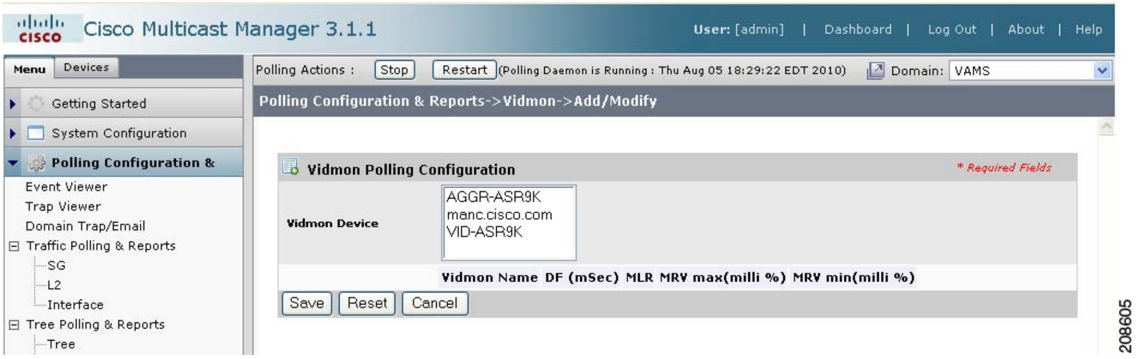
- To add a new configuration using the CMM interface, click the **Add** button, and from the drop-down list, select **By Vidmon**.
- To add a VidMon configuration by importing a text file, click the **Add** button and from the drop-down list, select **By Import**.

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

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.

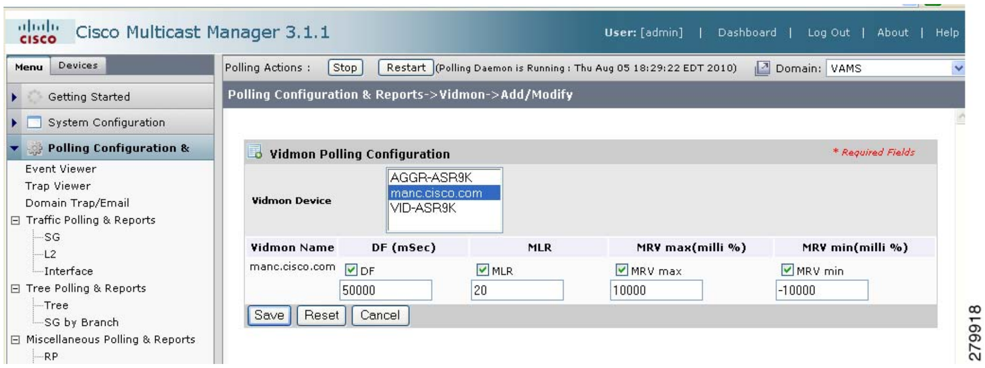
Step 8 To configure polling for a device, check the check box next to the configuration option for the device.

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

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.

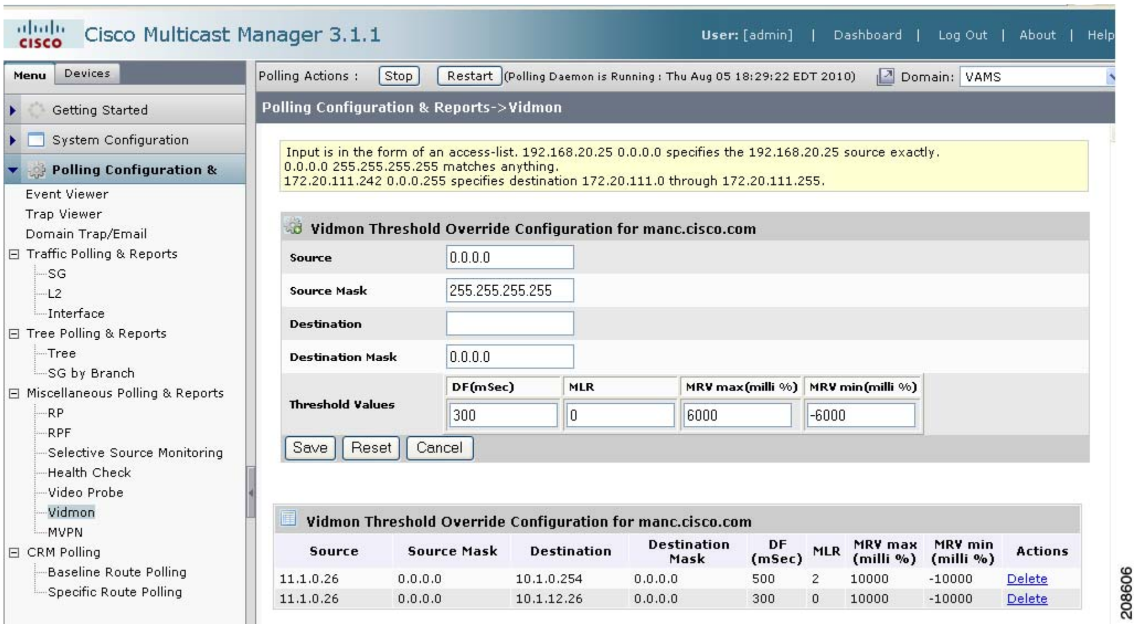
After you have saved the device-level VidMon threshold configuration, you can configure individual thresholds for the flows on the device.

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)

Domain: VAMS

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.

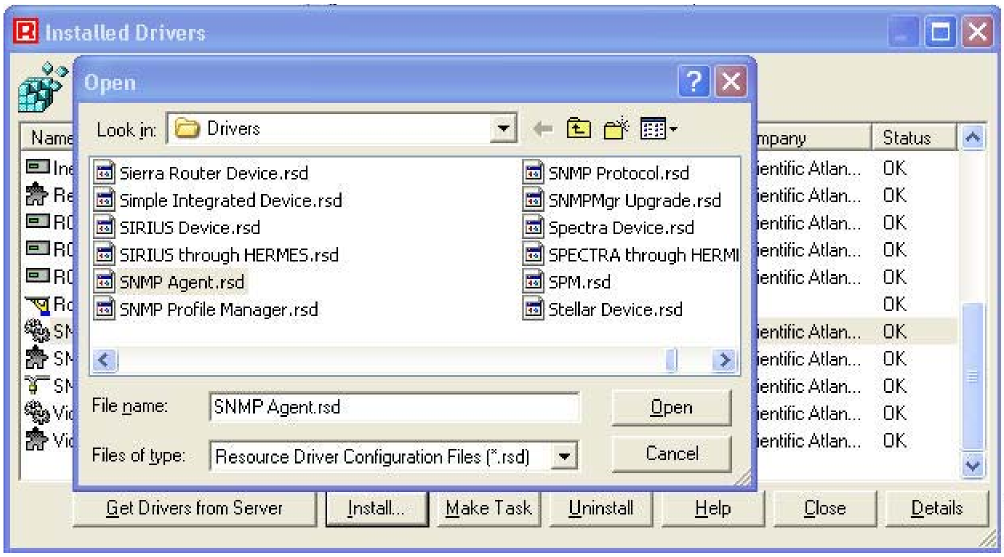
Step 3 Select **Config > Drivers.**

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



Look in: Drivers

Sierra Router Device.rsd
Simple Integrated Device.rsd
SIRIUS Device.rsd
SIRIUS through HERMES.rsd
SNMP Agent.rsd
SNMP Profile Manager.rsd
SNMP Protocol.rsd
SNMPMgr Upgrade.rsd
Spectra Device.rsd
SPECTRA through HERMI
SPM.rsd
Stellar Device.rsd

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**.

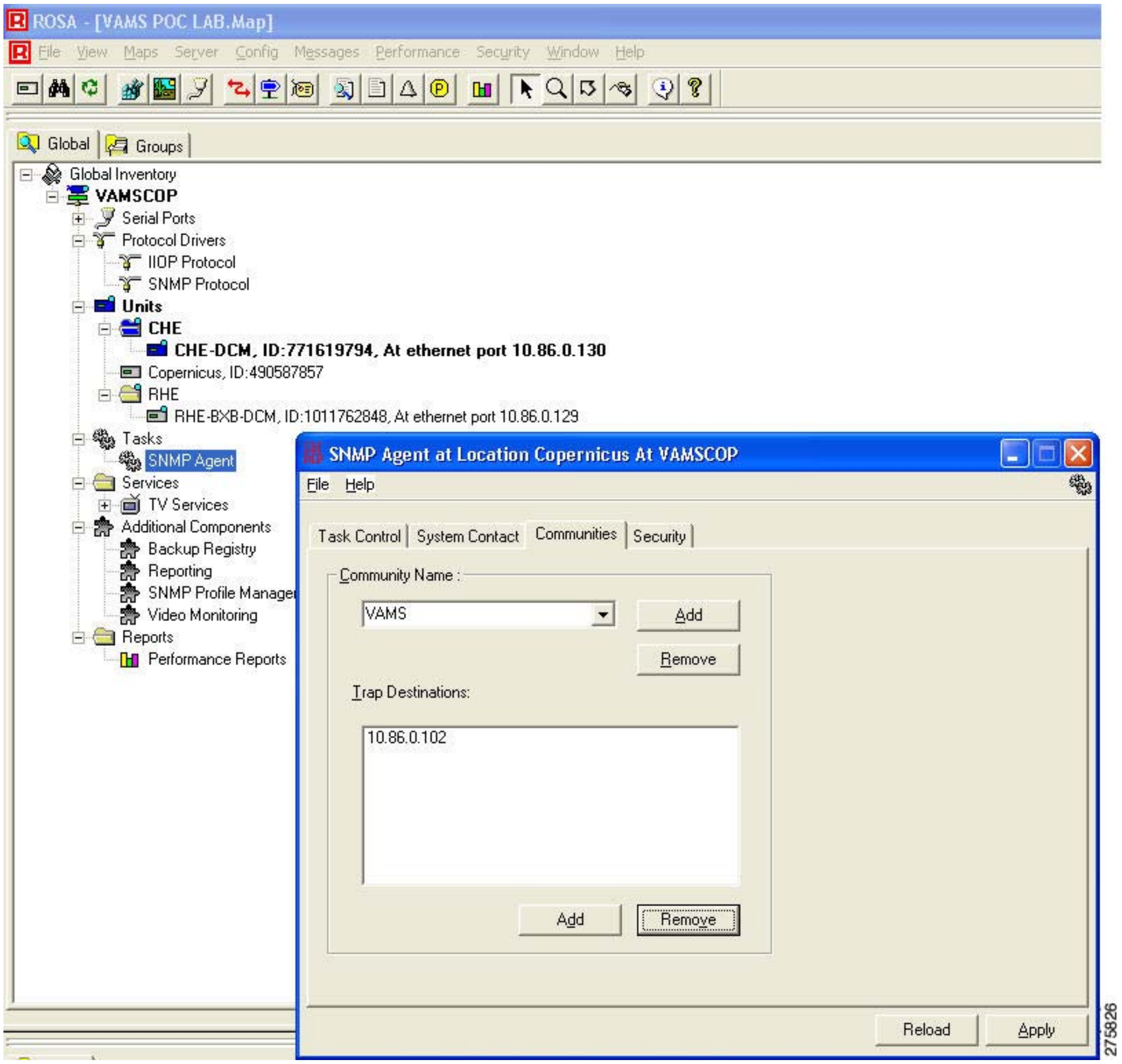
Step 3 From the pull-down menu for the task, select Properties.

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.

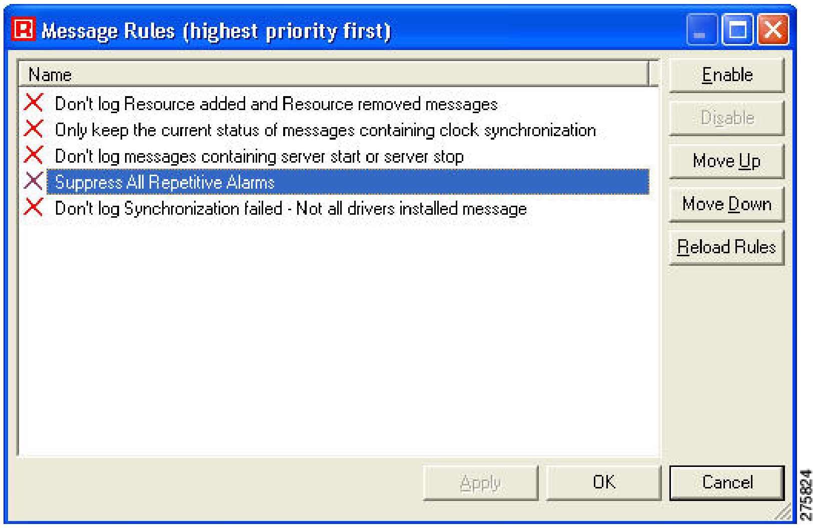
Disabling the Repetitive Alarm Distribution Rule

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



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.

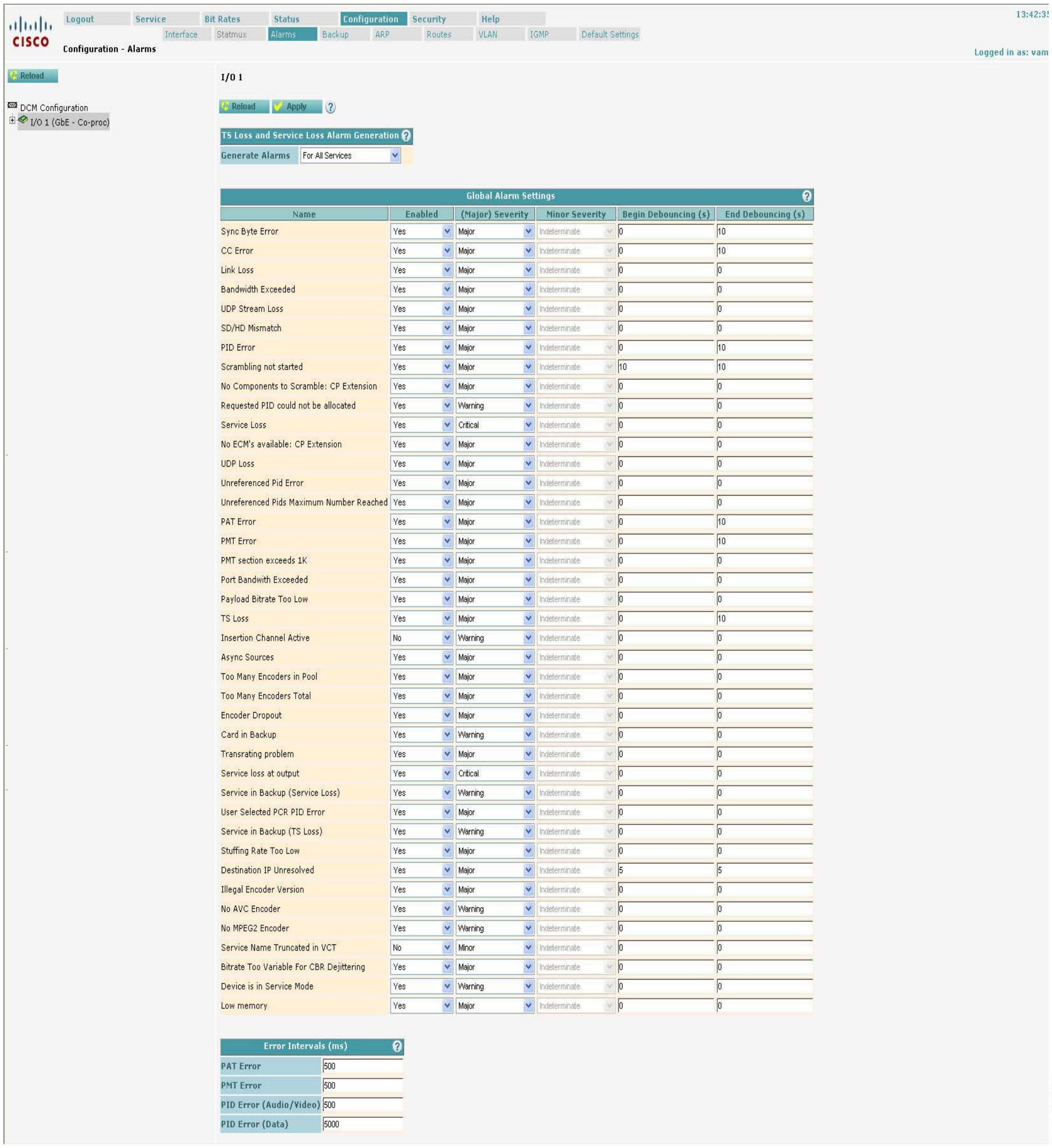
Step 2 In the DCM configuration tree, double-click on the interface card for which alarm settings must be configured.

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



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.

CHAPTER 3

Troubleshooting with Cisco Video Assurance Management Solution 3.1

This chapter contains the following sections:

Using the VAMS Dashboards

The VAMS components provide operational dashboards that give you a top-down view of video network events. Cisco VAMS 3.1 provides:

- The TIP/TBSM Dashboard
- The Video Assurance Management Dashboard
- Cisco Multicast Manager
- The ROSA NMS
- Cisco ANA

TIP/TBSM Dashboard

The high-level interface for Cisco Video Assurance Management Solution 3.1 is the Tivoli Integrated Portal (TIP) and the Tivoli Business Service Manager (TBSM). TIP allows you to launch TBSM and customized event views for events in the video headend and video transport network.

From the TIP dashboard, you can view all of the tasks provided with TIP/TBSM, or select specific tasks provided for the VAMS application. You can select:

- **Tivoli Netcool/OMNIbus Web GUI**—A web-based application that processes network events from one or more data sources and presents event data to TIP/TBSM users in various graphical formats.
- **Tivoli Business Service Manager**—Provides real-time service dashboards for the Cisco Info Center applications.
- **Video Assurance Management Dashboard**—A customized dashboard for the Cisco VAMS product.

These tasks are selectable from the drop-down list in the View menu at the top of the TIP dashboard.

Video Assurance Management Dashboard

The TIP/TBSM dashboard provides a menu for the Video Assurance Dashboard. The Video Assurance Dashboard provides a view of all of the video services in your network that includes:

- A Service Availability directory that lists video services and associated devices.
- A Service Dashboard that includes:
  - A Service Tree that shows a directory map of the devices in your video network.
  - A Service Viewer that shows a topology map of the devices providing the service.
  - A Service Details window that provides an event list showing the events for the selected service.
- Custom event views that show Video Fault event views and Network Fault event:
  - The Video Fault event views include ROSA events, CMM events, Video Events, and VidMon events.
  - The Network Fault event views include ANA events and a view that shows all events.

The TIP/TBSM event lists show Cisco Info Center events that combine alerts received from all of the components of VAMS 3.1 and present them in a consolidated event based on processing rules specified in Cisco Info Center rules files.

You can launch the CMM home page from any CMM event with a right-click. You can also launch a CMM flow trace with a right-click from any event that includes a Multicast Group Address and a Source IP address. Currently, Digital Content Manager (DCM) events do not contain a Source IP address, so only CMM cross-launch is available for DCM events.

Figure 6-4 on page 6-7 shows the VAMS Service Dashboard. Figure 6-7 shows the custom events menu.

For information on how to use the VAMS Service Dashboard and the custom event views to manage video events, see:

- Monitoring ROSA NMS Events, page 6-12
- Monitoring CMM Events, page 6-22
- Monitoring VidMon Events, page 6-35
- Monitoring Video Events, page 6-37
- Viewing Network Fault Events, page 6-35

For information on using ANA to troubleshoot video events, see Troubleshooting with Cisco ANA, page 6-43

Cisco Multicast Manager

Cisco Multicast Manager provides a monitoring interface that allows you to monitor and manage video devices, including VidMon devices and monitoring for video probes. For information on the Cisco Multicast Manager interface, see the *User Guide for Cisco Multicast Manager 3.1*, viewable online at:

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

ROSA NMS

The ROSA NMS provides a user interface for monitoring and configuring the Digital Content Manager (DCM) and associated video headend devices. For information on using the ROSA NMS, see 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.

Cisco ANA

Cisco Active Network Abstraction provides several applications for viewing network topology and events. For information on the Cisco ANA components, see the user guides for Cisco ANA, viewable online at:

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

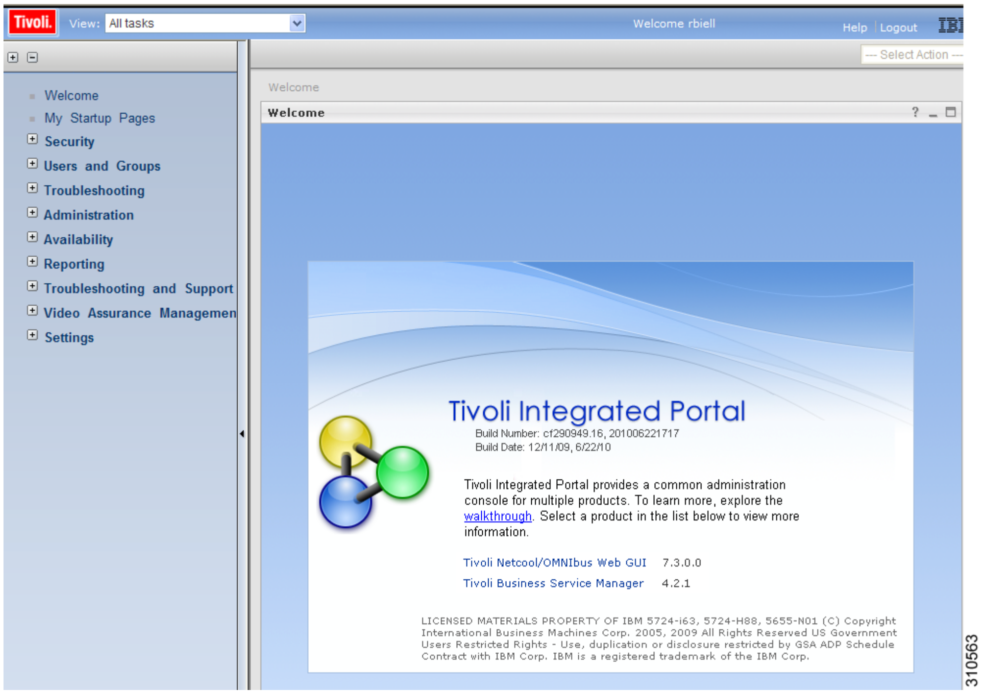
Monitoring VAMS Events with the VAMS Service Dashboard

To monitor VAMS events for video services:

Step 1 Log in to IBM Tivoli Integrated Portal (TIP).

The TIP start page appears, as shown in Figure 3-1.

Figure 3-1 TBSM Main Window



Tivoli Integrated Portal

Build Number: cf290949.16, 201006221717
Build Date: 12/11/09, 6/22/10

Tivoli Integrated Portal provides a common administration console for multiple products. To learn more, explore the walkthrough. Select a product in the list below to view more information.

Tivoli Netcool/OMNIbus Web GUI	7.3.0.0
Tivoli Business Service Manager	4.2.1

LICENSED MATERIALS PROPERTY OF IBM 5724-i63, 5724-H88, 5655-N01 (C) Copyright International Business Machines Corp. 2005, 2009 All Rights Reserved US Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp. IBM is a registered trademark of the IBM Corp.

Step 2 Click the plus sign (+) next to **Video Assurance Management**.

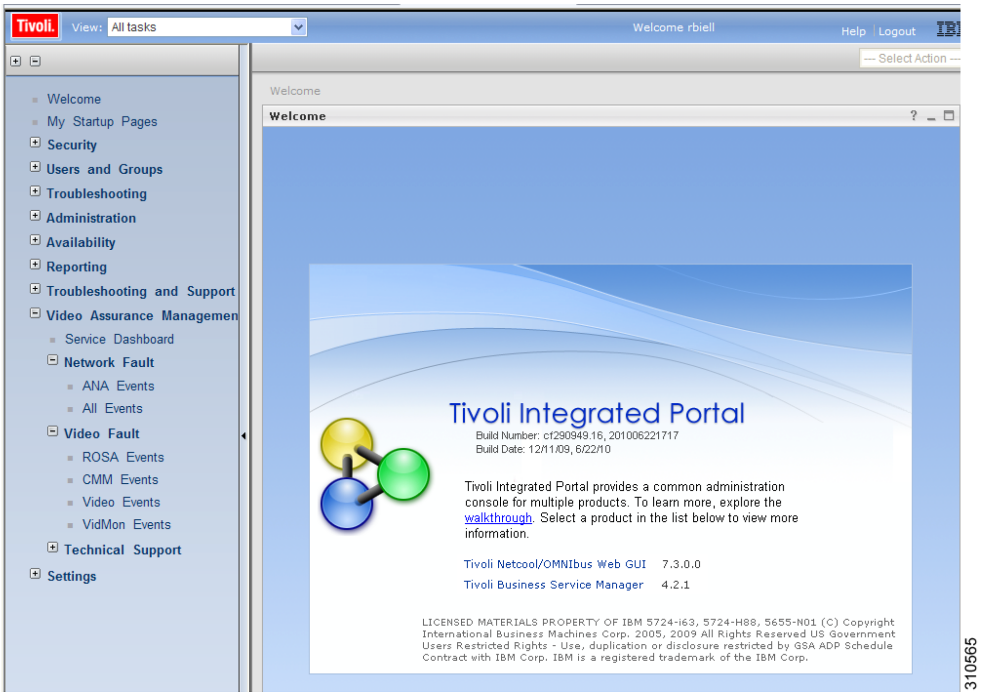
The Video Assurance Management menu appears.

Step 3 Click the plus sign (+) next to **Video Fault**.

Step 4 Click the plus sign (+) next to **Network Fault**.

The TIP display now shows all of the Video Assurance Management menu items, as shown in Figure 3-2.

Figure 3-2 Video Assurance Management Menu



Build Number: cf290949.16, 201006221717
Build Date: 12/11/09, 6/22/10

Tivoli Integrated Portal provides a common administration console for multiple products. To learn more, explore the walkthrough. Select a product in the list below to view more information.

Tivoli Netcool/OMNIbus Web GUI 7.3.0.0
Tivoli Business Service Manager 4.2.1

LICENSED MATERIALS PROPERTY OF IBM 5724-i63, 5724-H88, 5655-N01 (C) Copyright International Business Machines Corp. 2005, 2009 All Rights Reserved US Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp. IBM is a registered trademark of the IBM Corp.

Step 5 Click **Service Dashboard**.

The Service Dashboard appears:

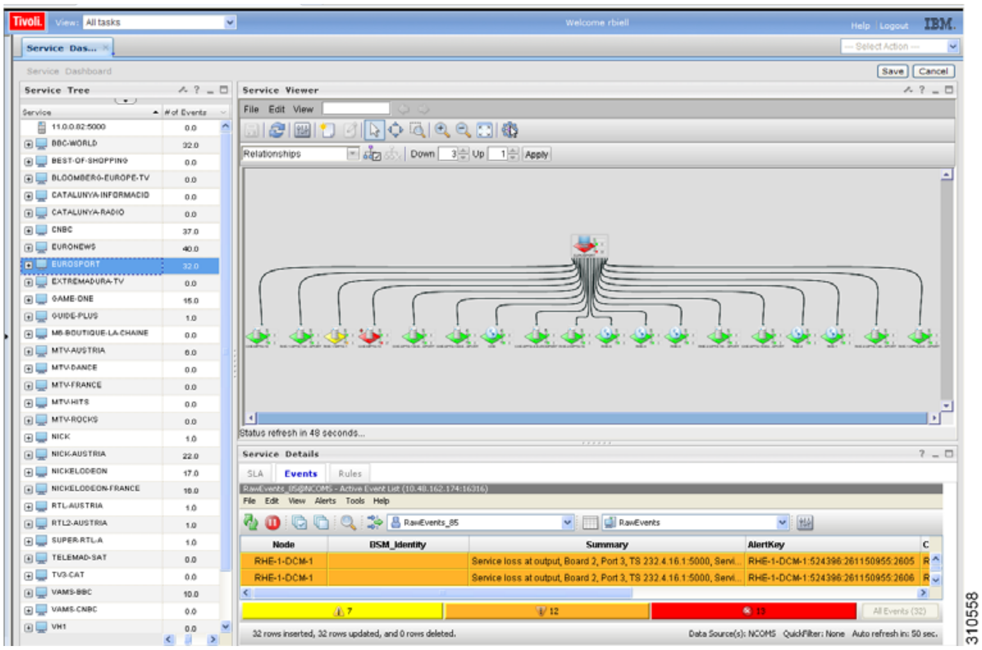
- The Service Tree shows a list of the configured video services in your network.

Step 6 Left-click on a channel service on the Service Tree directory browser at the left of the page

- The Service Viewer shows a network topology map of the currently selected channel service
- The Service Details window shows an event list for the events associated with the currently selected service.

Figure 3-3 shows a Service Map for a channel service called *EUROSPORT*.

Figure 3-3 Service Tree and Service Map



Service	# of Events
11.0.0.82:5000	0.0
BBC-WORLD	32.0
BEST-OF-SHOPPING	0.0
BLOOMBERG-EUROPE-TV	0.0
CATALUNYA-INFORMACIO	0.0
CATALUNYA-RADIO	0.0
CNBC	37.0
EURONEWS	40.0
EUROSPORT	32.0
EXTREMADURA-TV	0.0
GAME-ONE	15.0
GUIDE-PLUS	1.0
M6-BOUTIQUE-LA-CHAINE	0.0
MTV-AUSTRIA	6.0
MTV-DANCE	0.0
MTV-FRANCE	0.0
MTV-HITS	0.0
MTV-ROCKS	0.0
NICK	1.0
NICK-AUSTRIA	22.0
NICKELODEON	17.0
NICKELODEON-FRANCE	10.0
RTL-AUSTRIA	1.0
RTL2-AUSTRIA	1.0
SUPER-RTL-A	1.0
TELEMAD-SAT	0.0
TV3-CAT	0.0
VAMS-BBC	10.0
VAMS-CNBC	0.0
VH1	0.0

Status refresh in 48 seconds...

Node	BSM_Identity	Summary	AlertKey	C
RHE-1-DCM-1		Service loss at output, Board 2, Port 3, TS 232.4.16.1:5000, Servi...	RHE-1-DCM-1:524396:261150955:2605	R
RHE-1-DCM-1		Service loss at output, Board 2, Port 3, TS 232.4.16.1:5000, Servi...	RHE-1-DCM-1:524396:261150955:2606	R

32 rows inserted, 32 rows updated, and 0 rows deleted.

Data Source(s): NCOMS QuickFilter: None Auto refresh in: 50 sec.

Note Until you select a service, the Service Viewer and the Service Details window are empty.

Note You can sort the service tree by clicking on either the **State** or **Events** column head.

Step 7 To view an event in the Service Details area, expand the Service Details area.

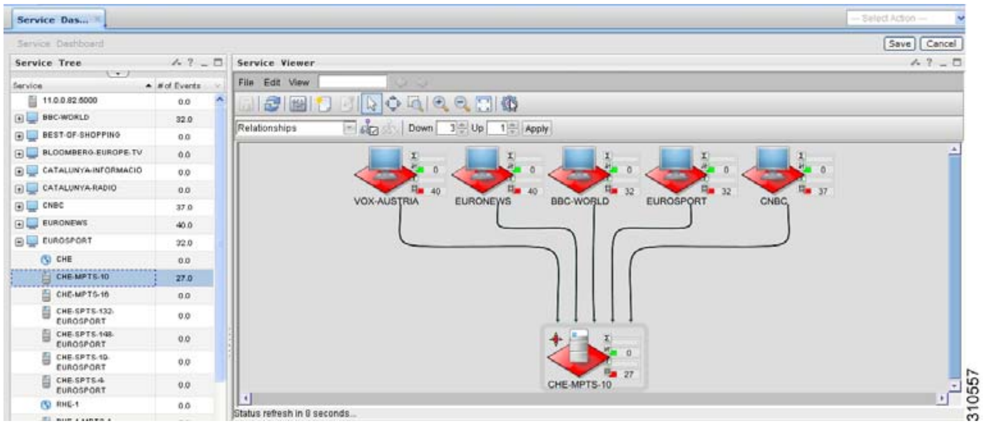
Step 8 To view details on an event, select the event and right-click.

Step 9 To expand the Service Tree for a service, click the plus sign (+) next to the service.

Step 10 To show a service view for a specific device providing the channel service, slick on the device in the service tree.

Figure 6-4 shows the service map for the *CHE-MPTS-10* in the EUROSPORT channel service.

Figure 3-4 Service Viewer and Service Details Window



Service	# of Events
11.0.0.82.6000	0.0
BBC-WORLD	32.0
BEST-OF-SHOPPING	0.0
BLOOMBERG-EUROPE-TV	0.0
CATALUNYA-INFORMACIO	0.0
CATALUNYA-RADIO	0.0
CNBC	37.0
EURONEWS	40.0
EUROSPORT	32.0
CHE	0.0
CHE-MPTS-10	27.0
CHE-MPTS-16	0.0
CHE-SPTS-132-EUROSPORT	0.0
CHE-SPTS-148-EUROSPORT	0.0
CHE-SPTS-10-EUROSPORT	0.0
CHE-SPTS-4-EUROSPORT	0.0
RHE-1	0.0

Relationships Down 3 Up 1

Status refresh in 0 seconds...

The Service Tree for CHE-MPTS-10 shows all of the channel services that are transmitted using this device.

In the Service Viewer:

- Green indicates that there is no alarm or a cleared alarm for the service.
- All other colors are service alarms for the service:
  - Red indicates the existence of critical alarms.
  - Yellow indicates the existence of minor alarms.

Step 11 To sort the events in the Service Tree by Severity, click **State** in the Service Tree area.

Clicking **State** changes the sort order between ascending order by severity and descending order. To see the highest severity events, and any fault events, sort the list to show the highest severity events first.

Step 12 To view the details of an event:

a. Expand the Service Details area for the device.

b. Double-click on the row for the event.

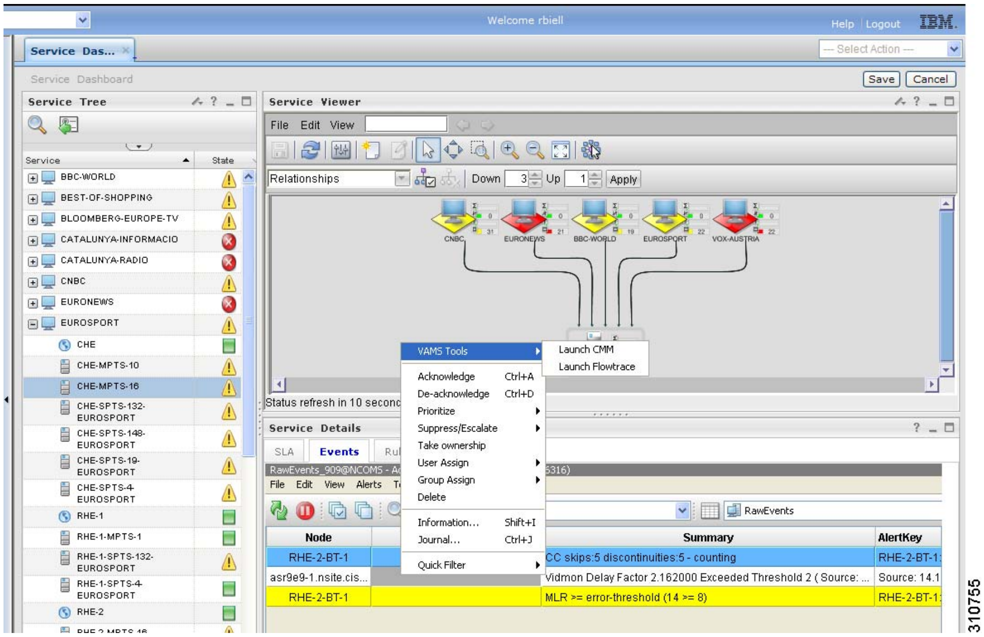
A table giving detailed field information for the event appears.

Step 13 For a CMM event, to launch the CMM application, first left-click on a CMM event to select it, then right-click the event, and from the Alerts Menu, choose **VAMS Tools > Launch CMM**.

Note For a CMM event, you can launch a real-time CMM flow trace or launch the CMM Latest Events page for further troubleshooting. It is possible to have one or more CMM servers available to launch to. The example in Figure 3-5 shows two regional CMM servers reporting events to a single Cisco Info Center server.

Figure 3-5 shows the menu selections for starting CMM.

Figure 3-5 Launching CMM from a TBSM Event List



Service	State
BBC-WORLD	⚠
BEST-OF-SHOPPING	⚠
BLOOMBERG-EUROPE-TV	⚠
CATALUNYA-INFORMACIO	✖
CATALUNYA-RADIO	✖
CNBC	⚠
EURONEWS	✖
EUROSPORT	⚠
CHE	🟩
CHE-MPTS-10	⚠
CHE-MPTS-16	⚠
CHE-SPTS-132-EUROSPORT	⚠
CHE-SPTS-148-EUROSPORT	⚠
CHE-SPTS-19-EUROSPORT	⚠
CHE-SPTS-4-EUROSPORT	⚠
RHE-1	🟩
RHE-1-MPTS-1	🟩
RHE-1-SPTS-132-EUROSPORT	⚠
RHE-1-SPTS-4-EUROSPORT	🟩
RHE-2	🟩

Node		Summary	AlertKey
RHE-2-BT-1		CC skips:5 discontinuities:5 - counting	RHE-2-BT-1:
asr9e9-1.nsite.cis...		Vidmon Delay Factor 2.162000 Exceeded Threshold 2 (Source: ...	Source: 14.1
RHE-2-BT-1		MLR >= error-threshold (14 >= 8)	RHE-2-BT-1:

The CMM application starts.

For additional information on the Tivoli TBSM application, and information on how to adjust and customize the TBSM window, see the IBM Tivoli TBSM documentation at the following URL:

http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.tivoli.itbsm.doc/tbsm42custom.pdf

Monitoring with the VAMS Event Views

The Video Assurance Management Dashboard provides custom event views that you can use to view events related to the specific VAMS components.

The following event views are provided:

- **Video Fault**—Provides event views for video services, including:
  - **ROSA Events**—Shows events from the Cisco ROSA application

    See Viewing Events in the ROSA Event Views, page 6-21.
  - **CMM Events**—Shows events from CMM.

    See Viewing Events in the CMM Event View, page 6-34.
  - **Video Events**—Shows events from video probes.

    See Viewing Events in the Video Events View, page 6-38.
  - **VidMon Events**—Shows IOS video monitoring events from VidMon devices.

    See Viewing Events in the VidMon Event Views, page 6-36.
- **Network Fault**—Includes events from Cisco ANA and from all network devices, including:
  - **ANA Events**—Shows events from Cisco ANA.
  - **All Events**—Shows all network fault events.

    See Viewing Events in the ANA Event Views, page 6-40 and Viewing All Events, page 6-41.

To access the VAMS event views:

Step 1 Log in to IBM TIP/TBSM.

The main TBSM window appears.

Step 2 Click the plus sign (+) next to **Video Assurance Management**.

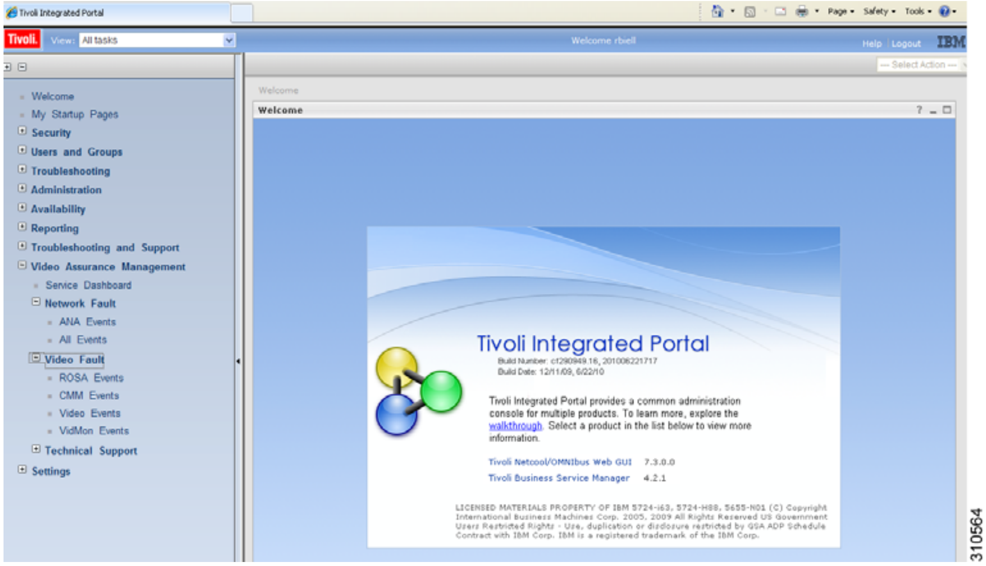
The Video Assurance Management menu appears.

Step 3 Click the plus sign (+) next to **Video Fault**.

Step 4 Click the plus sign (+) next to **Network Fault**.

The TIP display now shows all of the Video Assurance Management menu items, as shown in Figure 3-6.

Figure 3-6 Video Assurance Management Menu



Tivoli Integrated Portal

Build Number: cf290949.16, 201006221717
Build Date: 12/11/09, 6/22/10

Tivoli Integrated Portal provides a common administration console for multiple products. To learn more, explore the walkthrough. Select a product in the list below to view more information.

Tivoli Netcool/OMNIbus Web GUI	7.3.0.0
Tivoli Business Service Manager	4.2.1

LICENSED MATERIALS PROPERTY OF IBM 5724-i63, 5724-H88, 5655-N01 (C) Copyright International Business Machines Corp. 2005, 2009 All Rights Reserved US Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp. IBM is a registered trademark of the IBM Corp.

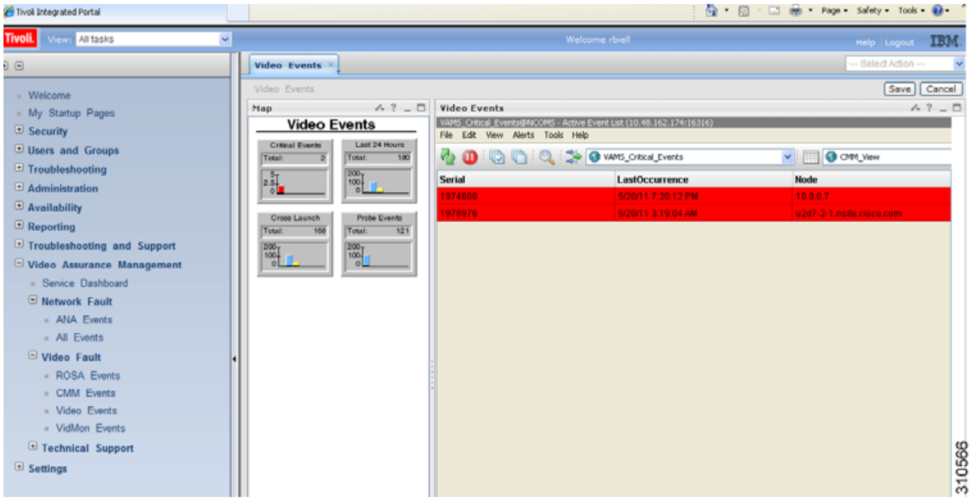
Step 5 To View a specific category of events, click the event selection. For example, click **Video Events**.

The Events Views page for the selected event category appears and shows monitor boxes for each category within the general event category

Step 6 Click on a monitor box for a type of event, for example, click on Critical events.

Figure 3-7 shows the event view for Critical Events (Video Events).

Figure 3-7 Video Events Views



VAMS_Critical_Events@NCOMS - Active Event List (10.48.162.174:16316)

Serial	LastOccurrence	Node
1974608	5/20/11 7:20:12 PM	10.0.0.7
1978976	5/20/11 3:19:04 AM	u2d7-2-1.nsite.cisco.com

The left part of the display shows monitor boxes for the selected event type. Each monitor box shows a bar graph indicating the number events in each severity level for the event category.

The Video Events views include:

- **Critical Events**—Shows high severity events.
- **Last 24 Hours Events**—Shows video event for the last 24 hours.
- **Cross Launch Events**—Shows events indicating a video probe has been started.
- **Probe Events**—Shows events from video probes.

Step 7 To view the details of an event, double-click on the row for the event.

A table giving detailed field information for the event appears.

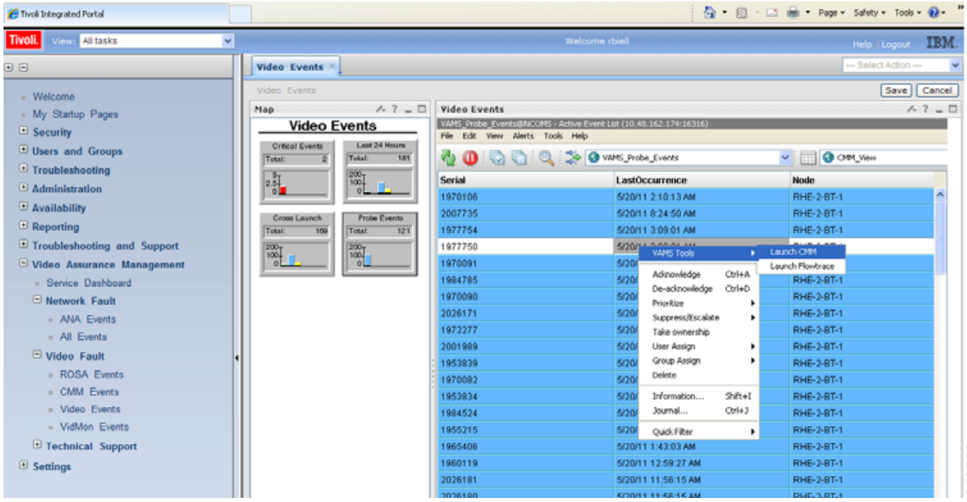
Step 8 To launch the CMM application, first left-click an event to select it, then right-click the event, and from the Alerts Menu, choose **VAMS Tools > Launch CMM** or choose **VAMS Tools > Launch Flowtrace.**

You can launch a real-time CMM flow trace or you can launch the CMM Latest Events page for further troubleshooting.

Note It is possible to have one or more CMM servers available to launch to. The example in Figure 3-8 shows two regional CMM servers reporting events to a single Cisco Info Center server.

Figure 3-8 shows the menu selections for starting CMM.

Figure 3-8 Launching CMM from an Event Item



Serial	LastOccurrence	Node
1970106	5/20/11 2:10:13 AM	RHE-2-BT-1
2007735	5/20/11 8:24:50 AM	RHE-2-BT-1
1977754	5/20/11 3:09:01 AM	RHE-2-BT-1
1977750	5/20/	
1970091	5/20/	
1984785	5/20/	RHE-2-BT-1
1970090	5/20/	RHE-2-BT-1
2026171	5/20/	RHE-2-BT-1
1972277	5/20/	RHE-2-BT-1
2001989	5/20/	RHE-2-BT-1
1953839	5/20/	RHE-2-BT-1
1970082	5/20/	RHE-2-BT-1
1953834	5/20/	RHE-2-BT-1
1984524	5/20/	RHE-2-BT-1
1955215	5/20/	RHE-2-BT-1
1965406	5/20/11 1:43:03 AM	RHE-2-BT-1
1960119	5/20/11 12:59:27 AM	RHE-2-BT-1
2026181	5/20/11 11:56:15 AM	RHE-2-BT-1
2026180	5/20/11 11:56:15 AM	RHE-2-BT-1

Monitoring ROSA NMS Events

This section describes:

- Summary of ROSA NMS Events, page 6-12
- Viewing ROSA Alerts in the Service Dashboard, page 3-12
- Viewing Events in the ROSA Event Views, page 6-21

Summary of ROSA NMS Events

VAMS 3.1 allows you to monitor a variety of events from components in the video headend. These events are collected by the ROSA NMS and forwarded to Cisco Info Center. Cisco Info Center correlates the events with additional alerts received from the video network and consolidates the information into one alert.

You can view the following categories of alerts in TBSM:

- **All ROSA Events**—Shows all ROSA events.
- **Service Loss Events**—Shows service loss events.,

Viewing ROSA Alerts in the Service Dashboard

By using the VAMS Service Dashboard you can view service alerts. Service alerts indicate the loss of a video service. Cisco VAMS reports four types of service alert:

- **Service Loss**—For each incoming service, one or more alarms can be defined to trigger a Service Loss alarm. A Transport Stream Loss alarm is triggered when a Service Loss alarm occurs.
- **Service in Backup (Service Loss)**—This alarm is generated when a service is in backup state triggered by a Service Loss alarm.
- **Service Loss at Output**—This alarm is generated for an outgoing service for which the corresponding incoming service and incoming backup services are in Service Loss state.
- **Service in Backup (TS Loss)—**This alarm is generated when a service is in backup state triggered by a TS Loss alarm.

Viewing a Service Loss Event

To monitor Service Loss events with Cisco Info Center, bring up an event list using Cisco Info Center/TBSM:

Step 1 Log in to TIP/TBSM.

Step 2 On the Video Assurance Management menu, click **Service Dashboard**.

The Service Dashboard appears.

The Service Tree shows a list of the configured video services in your network.

Step 3 Left-click on a a service on the Service Tree directory browser at the left of the page

- The Service Viewer shows a service map for the elected service.
- The Service Details window shows an event list for the service.

Step 4 To see the devices associated with the selected video service, click on the plus sign (+) next to the service name.

The devices in the service topology are listed in the Service Tree directory.

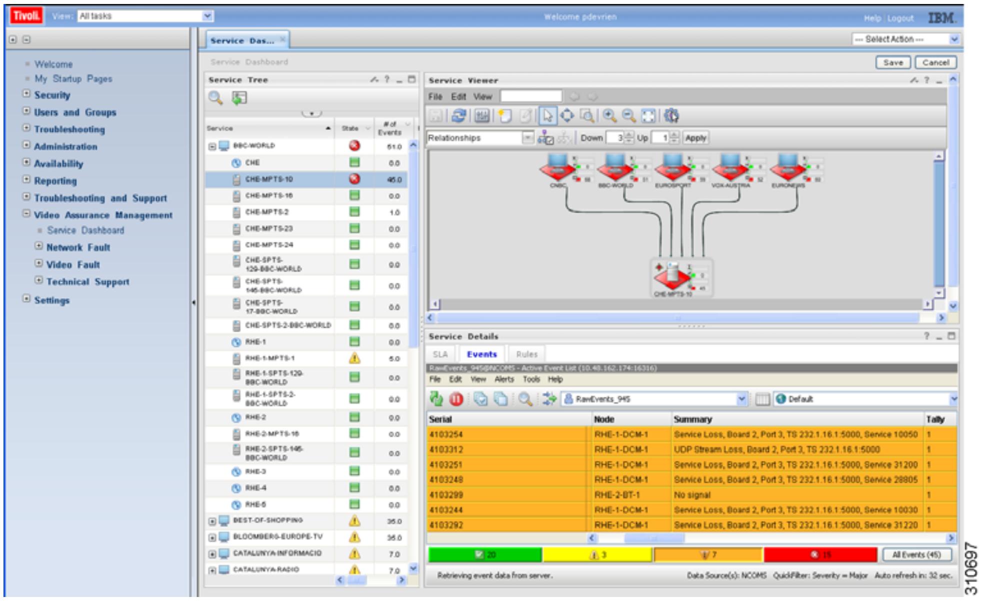
Step 5 Click on a device to see the service map for the device.

The Service Viewer shows a service map for the service. If there are faults, such as service loss alarms, the device is highlighted in red. In the event list in the Service Details area, fault events are highlighted in red.

The Service Viewer displays the network topology and the Service Details window shows an event list for the service.

Figure 3-9 shows a Cisco Info Center/TBSM display that includes a Service Loss event and associated events.

Figure 3-9 Viewing a Service Loss Event



Service	State	# of Events
BBC-WORLD	✕	51.0
CHE	🟩	0.0
CHE-MPTS-10	✕	45.0
CHE-MPTS-16	🟩	0.0
CHE-MPTS-2	🟩	1.0
CHE-MPTS-23	🟩	0.0
CHE-MPTS-24	🟩	0.0
CHE-SPTS-129-BBC-WORLD	🟩	0.0
CHE-SPTS-145-BBC-WORLD	🟩	0.0
CHE-SPTS-17-BBC-WORLD	🟩	0.0
CHE-SPTS-2-BBC-WORLD	🟩	0.0
RHE-1	🟩	0.0
RHE-1-MPTS-1	⚠	5.0
RHE-1-SPTS-129-BBC-WORLD	🟩	0.0
RHE-1-SPTS-2-BBC-WORLD	🟩	0.0
RHE-2	🟩	0.0
RHE-2-MPTS-16	🟩	0.0
RHE-2-SPTS-145-BBC-WORLD	🟩	0.0
RHE-3	🟩	0.0
RHE-4	🟩	0.0
RHE-5	🟩	0.0
BEST-OF-SHOPPING	⚠	35.0
BLOOMBERG-EUROPE-TV	⚠	35.0
CATALUNYA-INFORMACIO	⚠	7.0
CATALUNYA-RADIO	⚠	7.0

Serial	Node	Summary	Tally
4103254	RHE-1-DCM-1	Service Loss, Board 2, Port 3, TS 232.1.16.1:5000, Service 10050	1
4103312	RHE-1-DCM-1	UDP Stream Loss, Board 2, Port 3, TS 232.1.16.1:5000	1
4103251	RHE-1-DCM-1	Service Loss, Board 2, Port 3, TS 232.1.16.1:5000, Service 31200	1
4103248	RHE-1-DCM-1	Service Loss, Board 2, Port 3, TS 232.1.16.1:5000, Service 28805	1
4103299	RHE-2-BT-1	No signal	1
4103244	RHE-1-DCM-1	Service Loss, Board 2, Port 3, TS 232.1.16.1:5000, Service 10030	1
4103292	RHE-1-DCM-1	Service Loss, Board 2, Port 3, TS 232.1.16.1:5000, Service 31220	1

Retrieving event data from server.

Data Source(s): NCOMS QuickFilter: Severity = Major Auto refresh in: 32 sec.

The Service Loss Event summary indicates:

- **Board Number**—The board on which the service loss occurred on the indicated device.
- **Port Number**—The port number on which the video stream was transmitted.
- **TS**—A number identifying the Transport Stream affected by the service loss.
- **IP Address**—The IP address of the port.

Additional Events Related to the Service Loss

The TBSM event list shown in Figure 3-9 indicates several additional events related to the service loss.

- **UDP Stream Loss**—A Service Loss alarm is triggered when the port of the incoming Transport Stream to which the service belongs no longer detects packets at the corresponding UDP port.
- **No signal**—There has been no UDP packet for the predefined period of time (default 1 second).

When a service loss occurs, you might see additional ETR-290 First Priority events related to the service loss; for example, you might see a CC error event indicating a discontinuity error in the MPEG TS structure for a program transmitted in the TS.

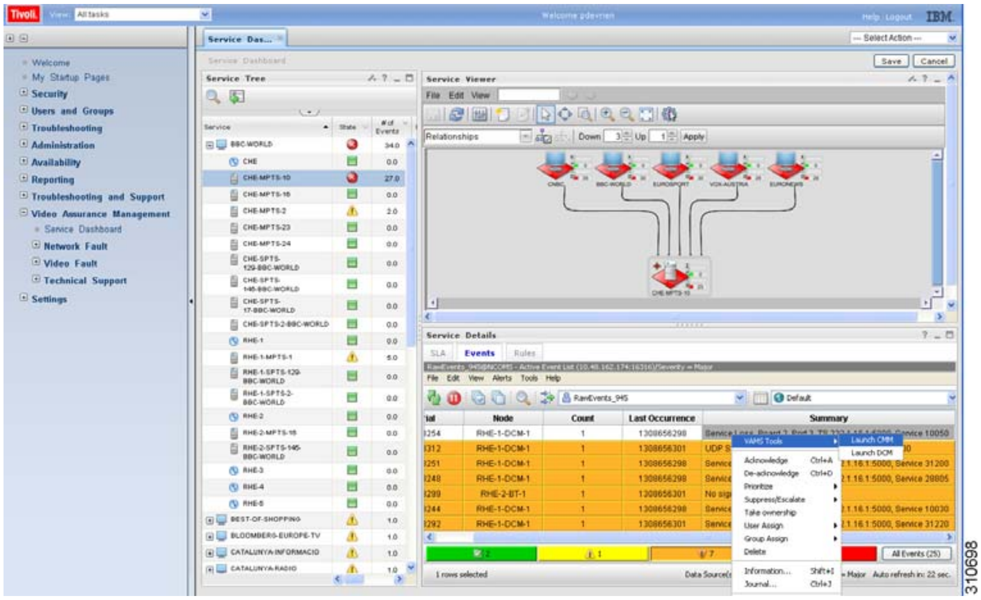
Step 6 To launch Cisco Multicast Manager to view additional monitoring information related to the service loss event:

a. Right-click on the event in the event list.

b. From the pull-down menu, choose **VAMS Tools > Launch CMM**.

Figure 3-10 shows how to launch CMM to view additional monitoring information for service events.

Figure 3-10 Launching CMM for Service Events



ial	Node	Count	Last Occurrence	Summary
254	RHE-1-DCM-1	1	1308656298	Service Loss, Board 2, Port 3, TS 232.1.16.1:5000, Service 10050
312	RHE-1-DCM-1	1	1308656301	UDP S
251	RHE-1-DCM-1	1	1308656298	Service 2.1.16.1:5000, Service 31200
248	RHE-1-DCM-1	1	1308656298	Service 2.1.16.1:5000, Service 28805
299	RHE-2-BT-1	1	1308656301	No sig
244	RHE-1-DCM-1	1	1308656298	Service 2.1.16.1:5000, Service 10030
292	RHE-1-DCM-1	1	1308656301	Service 2.1.16.1:5000, Service 31220

Note In this example, the event highlighted in grey has been right-clicked to bring up the cross-launch menu. The cross-launch is based on the information in the event that has been selected above, which is highlighted in white.

Viewing Events in the ROSA Event Views

To view the custom event views for ROSA events:

Step 1 Log in to IBM TIP/TBSM.

The main TBSM window appears.

Step 2 Click the plus sign (+) next to **Video Assurance Management**.

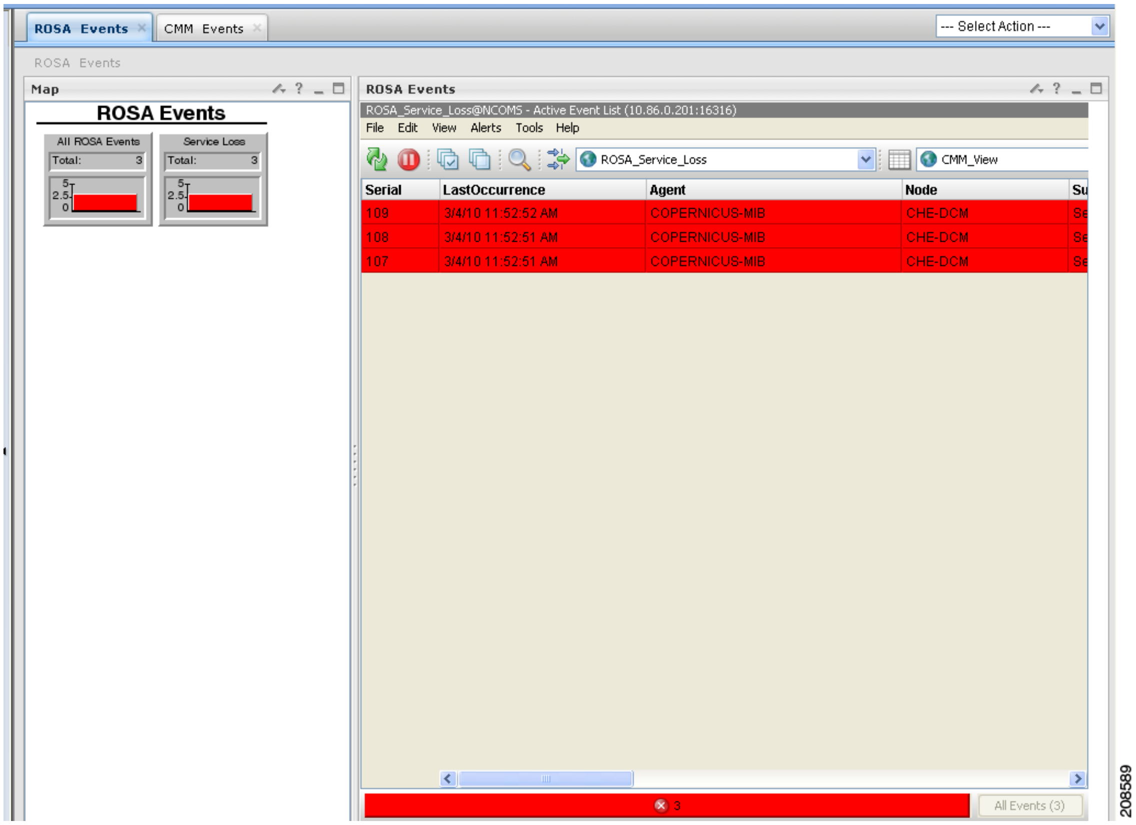
The Video Assurance Management menu appears.

Step 3 Click the plus sign (+) next to **Video Fault**.

Step 4 Click **ROSA Events**.

The Events Views page for ROSA events appears. Figure 3-11 shows the event views for ROSA Events.

Figure 3-11 ROSA Events Views



ROSA_Service_Loss@NCOMS - Active Event List (10.86.0.201:16316)

Serial	LastOccurrence	Agent	Node	Su
109	3/4/10 11:52:52 AM	COPERNICUS-MIB	CHE-DCM	Se
108	3/4/10 11:52:51 AM	COPERNICUS-MIB	CHE-DCM	Se
107	3/4/10 11:52:51 AM	COPERNICUS-MIB	CHE-DCM	Se

The left part of the display shows monitor boxes for the selected event type. Each monitor box shows a bar graph indicating the number events in each severity level for the event category.

The ROSA Events views include:

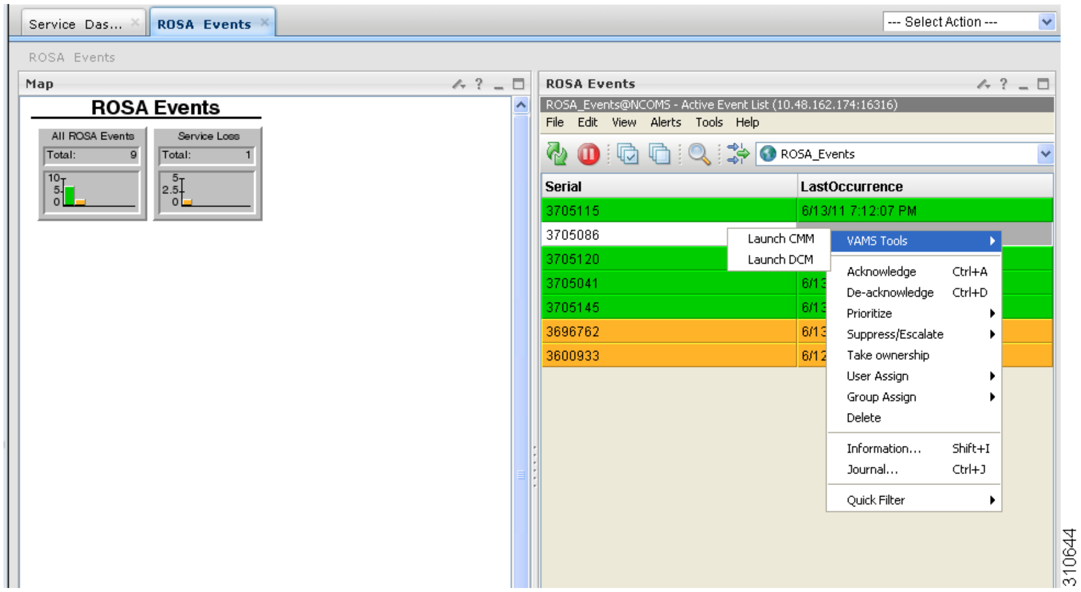
- **All ROSA Events**—Includes events with a severity level of critical
- **Service Loss**—Shows service loss events.

Step 5 To view the details of an event, double-click on the row for the event.

A table giving detailed field information for the event appears.

Step 6 For an event from a Digital Content Manager (DCM) event, to launch the DCM GUI, first left-click on a CMM event to select it, then right-click the event, and from the Alerts Menu, choose **VAMS Tools > Launch DCM**, as shown in Figure 3-12.

Figure 3-12 Launching the DCM GUI from a DCM Event



Serial	LastOccurrence
3705115	6/13/11 7:12:07 PM
3705086	
3705120	
3705041	6/13
3705145	6/13
3696762	6/13
3600933	6/12

.

Monitoring CMM Events

This section describes:

- Advanced Troubleshooting with the Service Dashboard and CMM, page 6-22
- Viewing Events in the CMM Event View, page 6-34

Advanced Troubleshooting with the Service Dashboard and CMM

CMM provides a diagnostics tool that gives you a multicast global view and a router-specific view of your network. CIC events that you can view using TBSM allow you to see additional details about the network.

Table 3-1 lists important areas of the CMM that you can use to troubleshoot a multicast video distribution network using Cisco VAMS:

Table 3-1 Cisco Multicast Manager

Troubleshooting Area	Task and Reference
Viewing network status	View the status of all devices in the current multicast domain. See "The Devices Tab" in the *User Guide for Cisco Multicast Manager, 3.1* at: http://www.cisco.com/en/US/docs/net_mgmt/cisco_multicast_manager/3.1/user/guide/cmm_diag.html#wp1054772
Viewing RP status	View all routers in the database, their RPs, and the active groups. See "RP Summary" in the *User Guide for Cisco Multicast Manager, 3.1* at: http://www.cisco.com/en/US/docs/net_mgmt/cisco_multicast_manager/3.1/user/guide/cmm_diag.html#wp1054769
IGMP diagnostics	View the interfaces that have joined a particular group. See "IGMP Diagnostics" in the *User Guide for Cisco Multicast Manager, 3.1* at: http://www.cisco.com/en/US/docs/net_mgmt/cisco_multicast_manager/3.1/user/guide/cmm_diag.html#wp1054775
Layer 2 switches	View Layer 2 multicast information and host IPs. The table shows, from a Layer 2 perspective, which multicast groups are being forwarded out which interfaces. See "L2 Diagnostics" in the *User Guide for Cisco Multicast Manager, 3.1* at: http://www.cisco.com/en/US/docs/net_mgmt/cisco_multicast_manager/3.1/user/guide/cmm_diag.html#wp1054764
Cisco 6500/7600 troubleshooting	Gather accurate packet-forwarding statistics and other information. See "6500/7600 Troubleshooting" in the *User Guide for Cisco Multicast Manager, 3.1* at: http://www.cisco.com/en/US/docs/net_mgmt/cisco_multicast_manager/3.1/user/guide/cmm_diag.html#wp1058009
Top-20 video flows	View the top-20 video flows. The top-20 video flows are dynamically updated at every polling interval. See "Cisco Multicast Manager Dashboard" in the *User Guide for Cisco Multicast Manager, 3.1* at: http://www.cisco.com/en/US/docs/net_mgmt/cisco_multicast_manager/3.1/user/guide/cmm_gs.html#wp1239864
Video probe status	View diagnostic information about video probes and the flows that they are monitoring. See Monitoring Video Probe Status with CMM, page 3-29.
VidMon flow status	View VidMon flows, VidMon reports view historical graphs of VidMon performance, and view real-time graphs showing VidMon performance. See Monitoring VidMon Status with CMM, page 3-31.
Video Flow Tracing	Video flows can be traced through the network. All routers participating in the transport of the multicast flow are listed. A graphical representation of the flow path is provided which includes IneoQuest probes and their status for a given flow. See Monitoring Video Probe Status with CMM, page 3-29.
PPS/BPS Threshold Monitoring	PPS/BPS threshold monitoring allows you to set and monitor thresholds on Cisco routers and switches for high or low BPS or PPS rates on a per flow basis. See Monitoring Multicast Tree Changes (Tree Polling), page 6-23 for details on PPS/BPS threshold monitoring.

Table 3-1 Cisco Multicast Manager (continued)

Troubleshooting Area	Task and Reference
Monitoring Multicast Tree Changes (Tree Polling)	View changes to multicast trees, which might affect video quality immediately, or at some time in the future. Tree polling allows you to monitor the multicast distribution tree of a video service and receive an alert when changes to the distribution tree occur. See: • Monitoring Multicast Tree Changes (Tree Polling), page 6-23 • "Tree Reports" 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#wp1096257
Health Checks	You can perform health checks to check and report on the critical components of your network. For example, you can check on the status of Rendezvous Points (RPs), Multicast Source Discovery Protocol (MSDP) peering, the presence of sources and groups, and the status of multicast trees. See: • Performing Health Checks, page 6-30 • The "Health Check" section 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_diag.html#wp1054777
Monitoring IP Multicast Heartbeat	You can configure IP multicast heartbeat monitoring on Cisco routers and switches to verify that data is flowing on the monitored multicast flow(s). See Monitoring IP Multicast Heartbeat, page 6-27.

Monitoring Multicast Tree Changes (Tree Polling)

You can monitor multicast tree changes with Cisco Multicast Manager and receive the alert in Cisco Info Center. From Cisco Info Center you can then launch CMM for advanced troubleshooting of the tree changes.

Monitoring Multicast Tree Changes with Cisco Info Center

To monitor multicast tree changes with Cisco Info Center, bring up an event list using Cisco Info Center/TBSM:

Step 1 From the service tree directory browser at the left of the Cisco Info Center/TBSM display, click on a service.

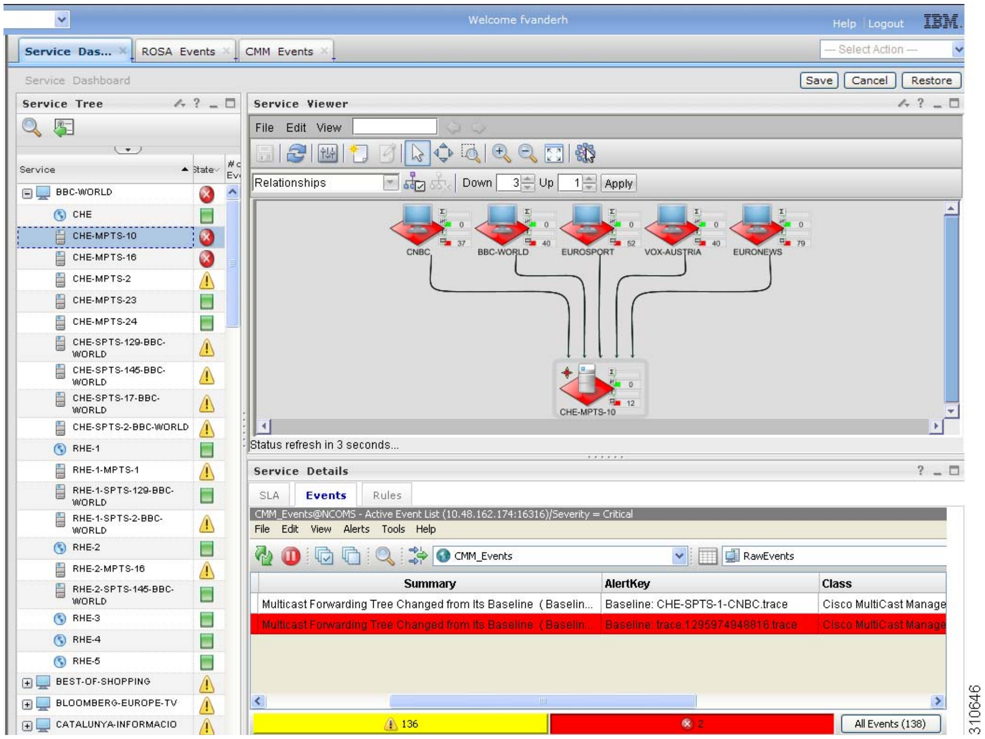
The service tree for the selected service appears.

Step 2 Click on a specific device address.

The Service Viewer displays the network topology an the Service Details window shows an event list for the service.

Figure 3-13 shows a Cisco Info Center/TBSM display and an event indicating that a Multicast Forwarding Tree has changed from its baseline.

Figure 3-13 Viewing a Tree Change Event in TBSM



Status refresh in 3 seconds...

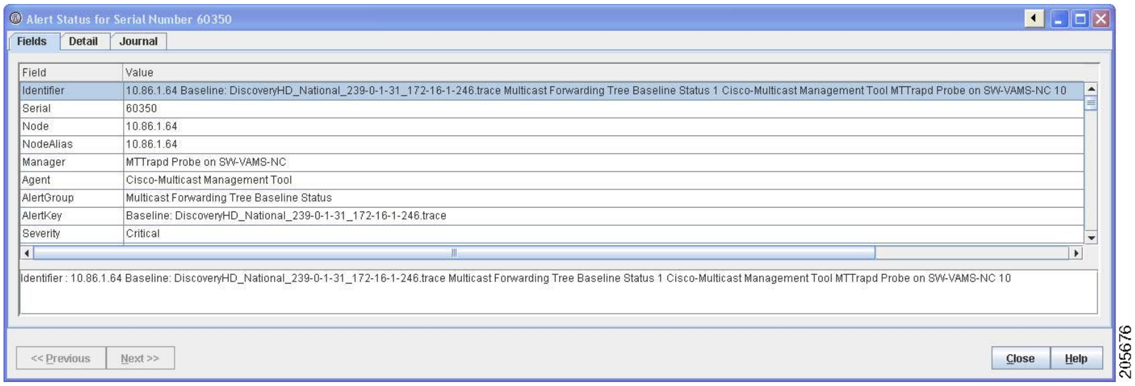
CMM_Events@NCOMS - Active Event List (10.48.162.174:16316)/Severity = Critical

Summary	AlertKey	Class
Multicast Forwarding Tree Changed from Its Baseline (Baselin...	Baseline: CHE-SPTS-1-CNBC.trace	Cisco MultiCast Manage
Multicast Forwarding Tree Changed from Its Baseline (Baselin...	Baseline: trace.1295974948816.trace	Cisco MultiCast Manage

Step 3 To view the details of an event, double-click on the row for the event.

A table giving detailed field information for the tree change event appears. Figure 3-14 shows a sample Alerts Status page with tree change event details.

Figure 3-14 Detailed Tree Change Event Information



Field	Value
Identifier	10.86.1.64 Baseline: DiscoveryHD_National_239-0-1-31_172-16-1-246.trace Multicast Forwarding Tree Baseline Status 1 Cisco-Multicast Management Tool MTTrapd Probe on SW-VAMS-NC 10
Serial	60350
Node	10.86.1.64
NodeAlias	10.86.1.64
Manager	MTTrapd Probe on SW-VAMS-NC
Agent	Cisco-Multicast Management Tool
AlertGroup	Multicast Forwarding Tree Baseline Status
AlertKey	Baseline: DiscoveryHD_National_239-0-1-31_172-16-1-246.trace
Severity	Critical

Identifier : 10.86.1.64 Baseline: DiscoveryHD_National_239-0-1-31_172-16-1-246.trace Multicast Forwarding Tree Baseline Status 1 Cisco-Multicast Management Tool MTTrapd Probe on SW-VAMS-NC 10

Step 4 To launch the CMM application and monitor additional information about the tree change event, highlight an event, and then from the Alerts Menu, choose **VAMS Tools > Launch CMM**.

Step 5 Go to the Monitoring Multicast Tree Changes with CMM, page 3-20 for information on monitoring tree change events with CMM.

Monitoring Multicast Tree Changes with CMM

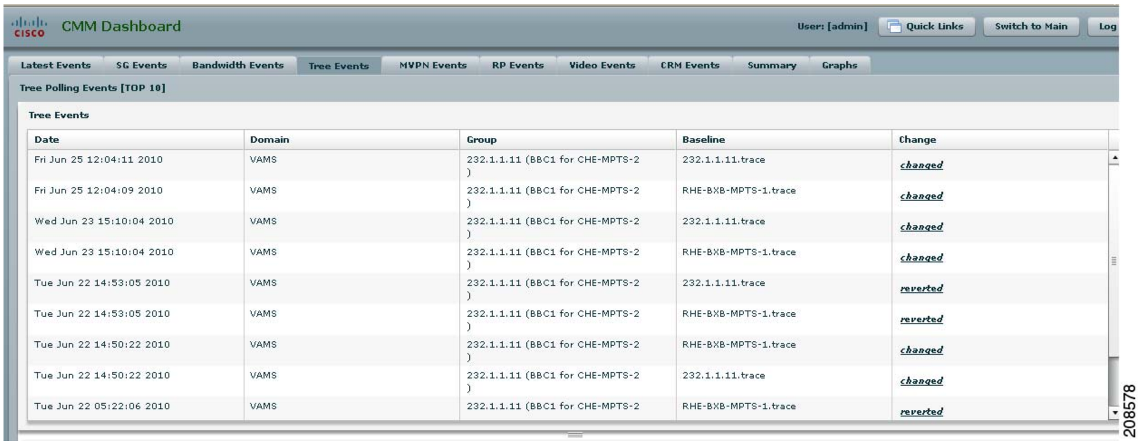
Using CMM, you can:

- View the latest tree change events.
- View a Tree Changed Report that shows details about the changes in the tree

When you launch CMM from TBSM/Cisco Info Center, the CMM Latest Events list appears.

To view Tree Change events, click the **Tree Events** tab. Figure 3-15 shows a Latest Events list from CMM that includes tree change events.

Figure 3-15 CMM Tree Change Events



Date	Domain	Group	Baseline	Change
Fri Jun 25 12:04:11 2010	VAMS	232.1.1.11 (BBC1 for CHE-MPTS-2)	232.1.1.11.trace	changed
Fri Jun 25 12:04:09 2010	VAMS	232.1.1.11 (BBC1 for CHE-MPTS-2)	RHE-BXB-MPTS-1.trace	changed
Wed Jun 23 15:10:04 2010	VAMS	232.1.1.11 (BBC1 for CHE-MPTS-2)	232.1.1.11.trace	changed
Wed Jun 23 15:10:04 2010	VAMS	232.1.1.11 (BBC1 for CHE-MPTS-2)	RHE-BXB-MPTS-1.trace	changed
Tue Jun 22 14:53:05 2010	VAMS	232.1.1.11 (BBC1 for CHE-MPTS-2)	232.1.1.11.trace	reverted
Tue Jun 22 14:53:05 2010	VAMS	232.1.1.11 (BBC1 for CHE-MPTS-2)	RHE-BXB-MPTS-1.trace	reverted
Tue Jun 22 14:50:22 2010	VAMS	232.1.1.11 (BBC1 for CHE-MPTS-2)	RHE-BXB-MPTS-1.trace	changed
Tue Jun 22 14:50:22 2010	VAMS	232.1.1.11 (BBC1 for CHE-MPTS-2)	232.1.1.11.trace	changed
Tue Jun 22 05:22:06 2010	VAMS	232.1.1.11 (BBC1 for CHE-MPTS-2	RHE-BXB-MPTS-1.trace	reverted

The event list in the figure shows two events:

- The first event to come in is a Tree Changed event indicating that a tree has been changed.

  The Tree Changed event indicates the name of the trace file that was used as the baseline to compare the current distribution tree against. The format of the trace filename shown in the event is the same format that you use to specify the trace filename when during Tree Polling configuration for the domain.

  The trace filename has this format:

  ```
  <channel name>_<ad zone>_<Mcast-Group>_<source-IP>
  ```

  where *channel_name* is the name of the channel, *ad_zone* is the name of the Ad zone, *Mcast-Group* is the address of the multicast group, and source-IP is the IP address of the source. For example:

  ```
  PBS_National_232-0-1-32_12-101-2-18
  ```

- The second event to come in is a Tree Reverted event that indicates that the tree reverted back to its previous state. This trap has the same format as the Tree Changed event (indicates the filename of the trace file was used as the baseline to compare against).

Viewing a Tree Changed Report

To view a Tree Changed Report:

Step 1 If you are in the TBSM/Cisco Info Center interface, highlight an event, and then from the Alerts Menu, choose **VAMS Tools > Launch CMM**.

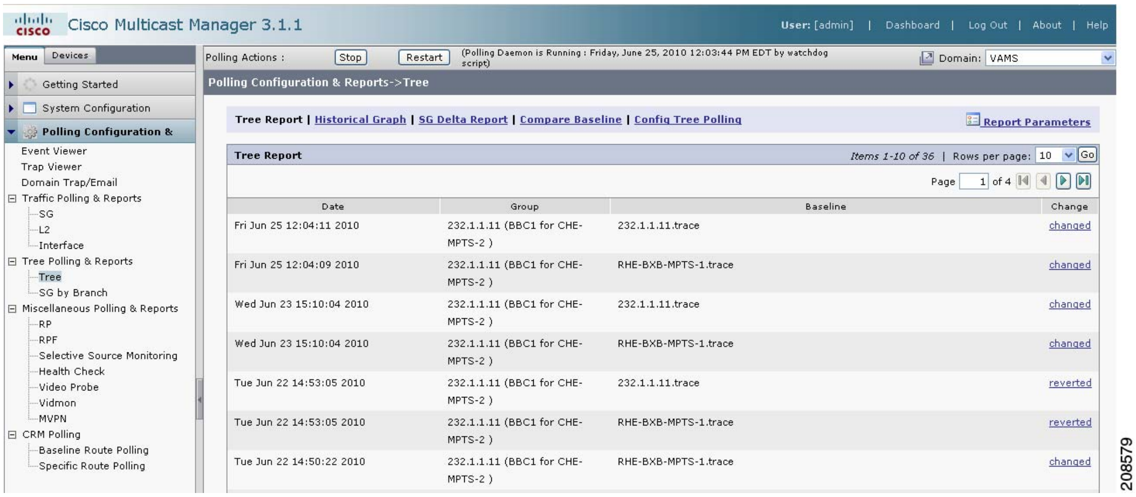
The CMM Latest Events page appears.

Step 2 Click the **Switch to Main** button.

Step 3 From the CMM Main Menu, select **Polling Configuration & Reports > Tree Polling & Reports> Tree**.

The Multicast Tree Report page appears, as shown in Figure 3-16.

Figure 3-16 Selecting a Tree Change Report



(Polling Daemon is Running : Friday, June 25, 2010 12:03:44 PM EDT by watchdog script)

Polling Configuration & Reports->Tree

Tree Report *Items 1-10 of 36*

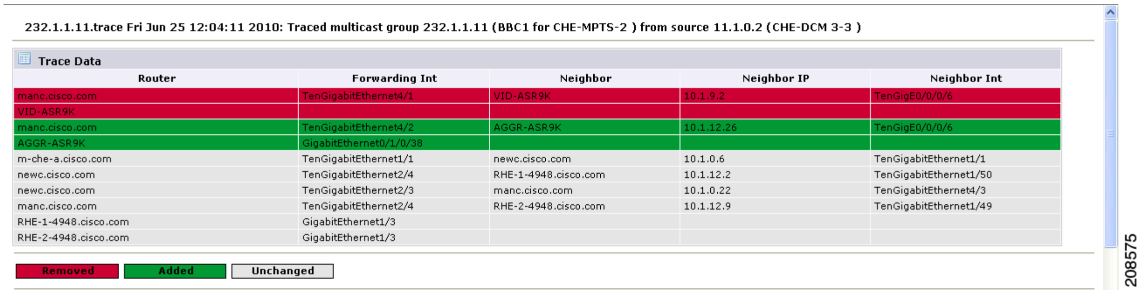
Date	Group	Baseline	Change
Fri Jun 25 12:04:11 2010	232.1.1.11 (BBC1 for CHE-MPTS-2)	232.1.1.11.trace	changed
Fri Jun 25 12:04:09 2010	232.1.1.11 (BBC1 for CHE-MPTS-2)	RHE-BXB-MPTS-1.trace	changed
Wed Jun 23 15:10:04 2010	232.1.1.11 (BBC1 for CHE-MPTS-2)	232.1.1.11.trace	changed
Wed Jun 23 15:10:04 2010	232.1.1.11 (BBC1 for CHE-MPTS-2)	RHE-BXB-MPTS-1.trace	changed
Tue Jun 22 14:53:05 2010	232.1.1.11 (BBC1 for CHE-MPTS-2)	232.1.1.11.trace	reverted
Tue Jun 22 14:53:05 2010	232.1.1.11 (BBC1 for CHE-MPTS-2)	RHE-BXB-MPTS-1.trace	reverted
Tue Jun 22 14:50:22 2010	232.1.1.11 (BBC1 for CHE-MPTS-2)	RHE-BXB-MPTS-1.trace	changed

The Tree Change Report page shows a list of Multicast Tree Change reports.

Step 4 Click a **changed** link to view a Tree Changed Report.

The selected Tree Changed Report appears, as shown in Figure 3-17.

Figure 3-17 Multicast Tree Change Report



232.1.1.11.trace Fri Jun 25 12:04:11 2010: Traced multicast group 232.1.1.11 (BBC1 for CHE-MPTS-2) from source 11.1.0.2 (CHE-DCM 3-3)

Trace Data

Router	Forwarding Int	Neighbor	Neighbor IP	Neighbor Int
manc.cisco.com	TenGigabitEthernet4/1	VID-ASR9K	10.1.9.2	TenGigE0/0/0/6
VID-ASR9K				
manc.cisco.com	TenGigabitEthernet4/2	AGGR-ASR9K	10.1.12.26	TenGigE0/0/0/6
AGGR-ASR9K	GigabitEthernet0/1/0/38			
m-che-a.cisco.com	TenGigabitEthernet1/1	newc.cisco.com	10.1.0.6	TenGigabitEthernet1/1
newc.cisco.com	TenGigabitEthernet2/4	RHE-1-4948.cisco.com	10.1.12.2	TenGigabitEthernet1/50
newc.cisco.com	TenGigabitEthernet2/3	manc.cisco.com	10.1.0.22	TenGigabitEthernet4/3
manc.cisco.com	TenGigabitEthernet2/4	RHE-2-4948.cisco.com	10.1.12.9	TenGigabitEthernet1/49
RHE-1-4948.cisco.com	GigabitEthernet1/3			
RHE-2-4948.cisco.com	GigabitEthernet1/3			

The report shows:

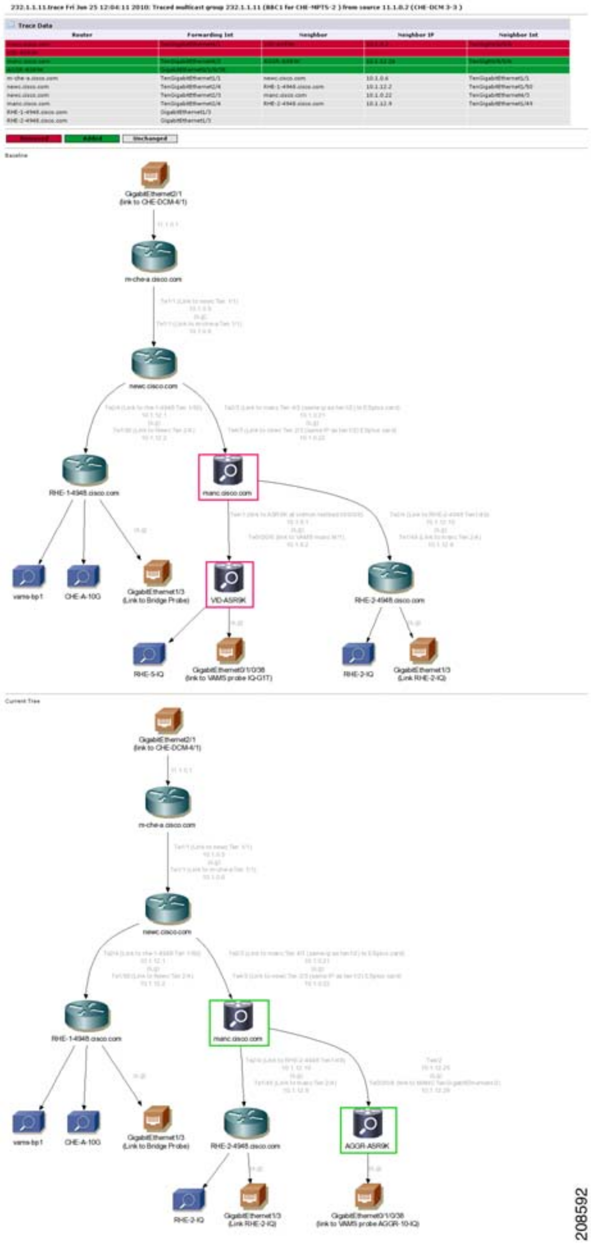
- A table containing detailed information about the routers and interfaces in the tree
- The baseline tree.
- The current tree (changed tree).

Routers and interfaces that are no longer part of the multicast tree are highlighted in red. Routers and interfaces that have been added to the distribution tree are highlighted in green.

Step 5 If you want to view a Tree Reverted report, click the **reverted** link next to a report name.

A Tree Reverted report shows the baseline distribution tree in tabular and in graphical format. Figure 3-18 shows a sample Tree Changed Report.

Figure 3-18 Tree Changed Report



232.1.1.11.trace Fri Jun 25 12:04:11 2010: Traced multicast group 232.1.1.11 (BBC1 for CHE-MPTS-2) from source 11.1.0.2 (CHE-DCM 3-3)

Trace Data

Router	Forwarding Int	Neighbor	Neighbor IP	Neighbor Int
[illegible]	TenGigabitEthernet4/1	VID-ASR9K	[illegible]	[illegible]
VID-ASR9K				
manc.cisco.com	TenGigabitEthernet4/2	AGGR-ASR9K	[illegible]	[illegible]
AGGR-ASR9K	GigabitEthernet0/1/0/38			
m-che-a.cisco.com	TenGigabitEthernet1/1	newc.cisco.com	10.1.0.6	TenGigabitEthernet1/1
newc.cisco.com	TenGigabitEthernet2/4	RHE-1-4948.cisco.com	10.1.12.2	TenGigabitEthernet1/50
newc.cisco.com	TenGigabitEthernet2/3	manc.cisco.com	10.1.0.22	TenGigabitEthernet4/3
manc.cisco.com	TenGigabitEthernet2/4	RHE-2-4948.cisco.com	10.1.12.9	TenGigabitEthernet1/49
RHE-1-4948.cisco.com	GigabitEthernet1/3			
RHE-2-4948.cisco.com	GigabitEthernet1/3			

Removed
Added
Unchanged
Baseline
GigabitEthernet2/1 (link to CHE-DCM-4/1)
m-che-a.cisco.com
newc.cisco.com
RHE-1-4948.cisco.com
manc.cisco.com
vams-bp1
CHE-A-10G
GigabitEthernet1/3 (Link to Bridge Probe)
VID-ASR9K
RHE-2-4948.cisco.com
RHE-5-IQ
GigabitEthernet0/1/0/38 (link to VAMS probe IQ-G1T)
RHE-2-IQ
GigabitEthernet1/3 (Link RHE-2-IQ)
Current Tree
GigabitEthernet2/1 (link to CHE-DCM-4/1)
m-che-a.cisco.com
newc.cisco.com
RHE-1-4948.cisco.com
manc.cisco.com
vams-bp1
CHE-A-10G
GigabitEthernet1/3 (Link to Bridge Probe)
RHE-2-4948.cisco.com
AGGR-ASR9K
RHE-2-IQ
GigabitEthernet1/3 (Link RHE-2-IQ)
GigabitEthernet0/1/0/38 (link to VAMS probe AGGR-10-IQ)
208592

Monitoring IP Multicast Heartbeat

You can monitor the multicast data plane of multicast video flows on Cisco routers and switches that utilize the IP Multicast Heartbeat feature to confirm that the routers and switches are receiving the monitored multicast video flows. You can view heartbeat events with Cisco Info Center, and from Cisco Info Center, launch CMM for advanced troubleshooting of the heartbeat events.

Monitoring Heartbeat Events with Cisco Info Center/TBSM

To view heartbeat events in TIP/TBSM:

Step 1 From the service tree directory browser at the left of the TBSM display, click on a service.

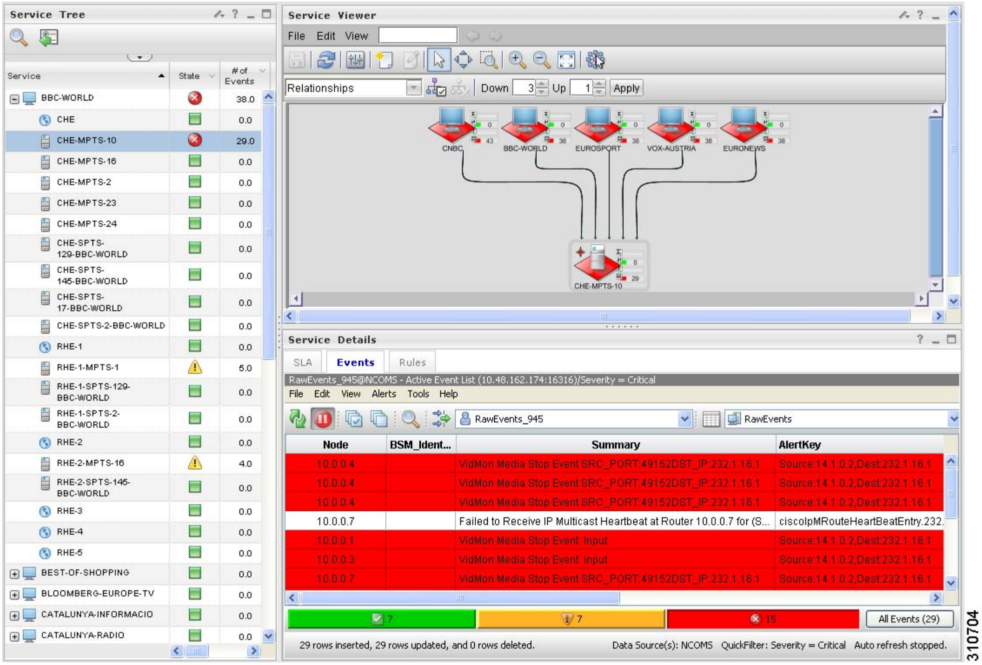
The service tree for the selected service appears.

Step 2 Click on a specific device address.

The Service Viewer displays the network topology and the Service Details window shows an event list for the service.

Figure 3-19 shows a TBSM display with a heartbeat event (Failed to Receive IP Multicast Heartbeat event) from a Cisco 7606 router.

Figure 3-19 Viewing a Heartbeat Event in TBSM



Service	State	# of Events
BBC-WORLD	☒	38.0
CHE	🟩	0.0
CHE-MPTS-10	☒	29.0
CHE-MPTS-16	🟩	0.0
CHE-MPTS-2	🟩	0.0
CHE-MPTS-23	🟩	0.0
CHE-MPTS-24	🟩	0.0
CHE-SPTS-129-BBC-WORLD	🟩	0.0
CHE-SPTS-145-BBC-WORLD	🟩	0.0
CHE-SPTS-17-BBC-WORLD	🟩	0.0
CHE-SPTS-2-BBC-WORLD	🟩	0.0
RHE-1	🟩	0.0
RHE-1-MPTS-1	⚠	5.0
RHE-1-SPTS-129-BBC-WORLD	🟩	0.0
RHE-1-SPTS-2-BBC-WORLD	🟩	0.0
RHE-2	🟩	0.0
RHE-2-MPTS-16	⚠	4.0
RHE-2-SPTS-145-BBC-WORLD	🟩	0.0
RHE-3	🟩	0.0
RHE-4	🟩	0.0
RHE-5	🟩	0.0
BEST-OF-SHOPPING	🟩	0.0
BLOOMBERG-EUROPE-TV	🟩	0.0
CATALUNYA-INFORMACIO	🟩	0.0
CATALUNYA-RADIO	🟩	0.0

RawEvents_945@NCOMS - Active Event List (10.48.162.174:16316)/Severity = Critical

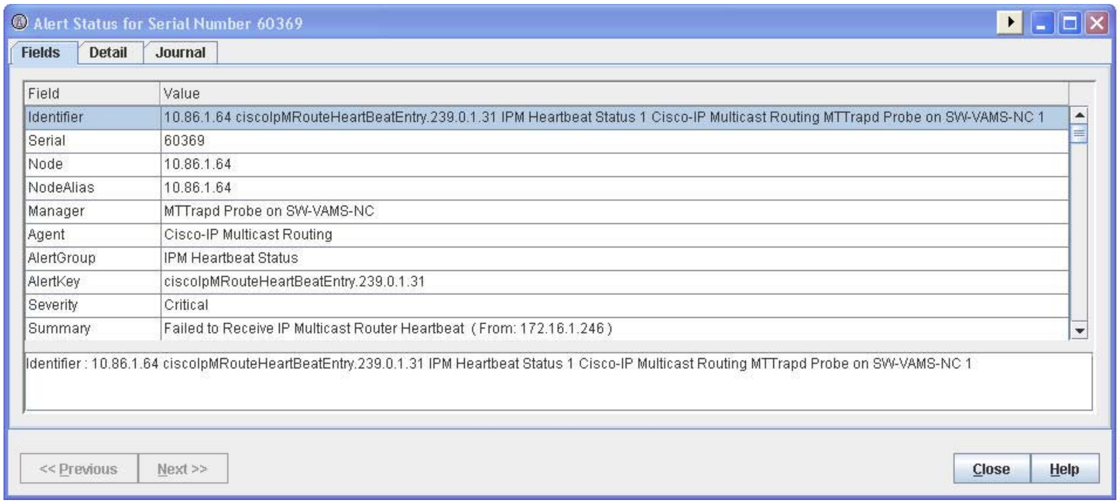
Node	BSM_Ident...	Summary	AlertKey
10.0.0.4		VidMon Media Stop Event SRC_PORT:49152DST_IP:232.1.16.1	Source:14.1.0.2,Dest:232.1.16.1
10.0.0.4		VidMon Media Stop Event SRC_PORT:49152DST_IP:232.1.16.1	Source:14.1.0.2,Dest:232.1.16.1
10.0.0.4		VidMon Media Stop Event SRC_PORT:49152DST_IP:232.1.16.1	Source:14.1.0.2,Dest:232.1.16.1
10.0.0.7		Failed to Receive IP Multicast Heartbeat at Router 10.0.0.7 for (S...	ciscoIpMRouteHeartBeatEntry.232.
10.0.0.1		VidMon Media Stop Event Input	Source:14.1.0.2,Dest:232.1.16.1
10.0.0.3		VidMon Media Stop Event Input	Source:14.1.0.2,Dest:232.1.16.1
10.0.0.7		VidMon Media Stop Event SRC_PORT:49152DST_IP:232.1.16.1	Source:14.1.0.2,Dest:232.1.16.1

29 rows inserted, 29 rows updated, and 0 rows deleted. Data Source(s): NCOMS QuickFilter: Severity = Critical Auto refresh stopped.

Step 3 To view additional details about the event, double click on the event in the event list display.

Figure 3-20 shows a sample Alerts Status page with heartbeat event details.

Figure 3-20 TBSM: Viewing Heartbeat Event Details



Field	Value
Identifier	10.86.1.64 ciscoIpMRouteHeartBeatEntry.239.0.1.31 IPM Heartbeat Status 1 Cisco-IP Multicast Routing MTTrapd Probe on SW-VAMS-NC 1
Serial	60369
Node	10.86.1.64
NodeAlias	10.86.1.64
Manager	MTTrapd Probe on SW-VAMS-NC
Agent	Cisco-IP Multicast Routing
AlertGroup	IPM Heartbeat Status
AlertKey	ciscoIpMRouteHeartBeatEntry.239.0.1.31
Severity	Critical
Summary	Failed to Receive IP Multicast Router Heartbeat (From: 172.16.1.246)

Identifier : 10.86.1.64 ciscoIpMRouteHeartBeatEntry.239.0.1.31 IPM Heartbeat Status 1 Cisco-IP Multicast Routing MTTrapd Probe on SW-VAMS-NC 1

The event summary for the service details includes the baseline trace filename, which includes the Service Name, Ad Zone, Multicast Group, and Source Address.

Step 4 To launch the CMM application and monitor additional information about the heartbeat event, left-click an event to select it, then right-click the event, and from the Alerts Menu, choose **VAMS Tools > Launch CMM**.

Step 5 Go to Monitoring Heartbeat Events with CMM, page 6-29 for information on monitoring heartbeat events with CMM.

Monitoring Heartbeat Events with CMM

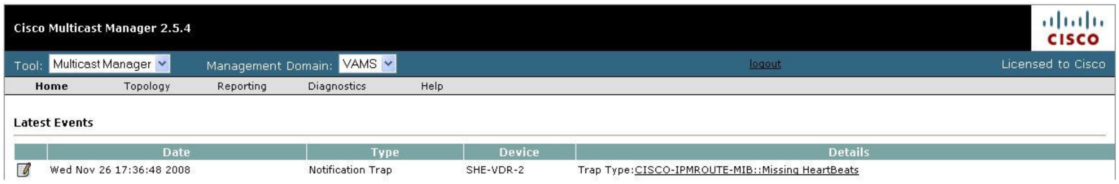
To view IP Multicast heartbeat events with CMM:

Step 1 If you are in the TBSM/Cisco Info Center interface, highlight an event, and then from the Alerts Menu, choose **VAMS Tools > Launch CMM**.

The CMM home page shows the Latest Events list, which includes any heartbeat events that have come in.

Figure 3-21 shows a Latest Events list with a heartbeat event.

Figure 3-21 Viewing a Heartbeat Event in CMM



Tool: Multicast Manager

Management Domain: VAMS

Latest Events

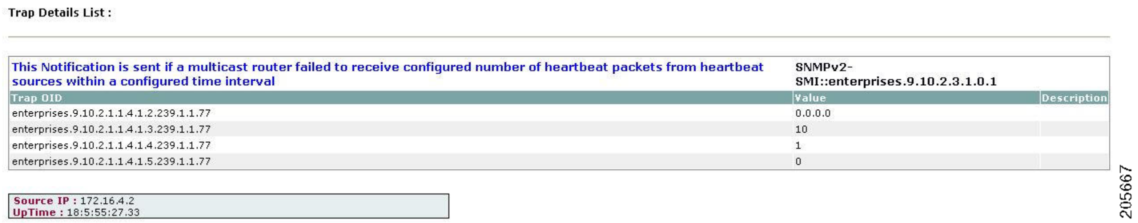
	Date	Type	Device	Details
	Wed Nov 26 17:36:48 2008	Notification Trap	SHE-VDR-2	Trap Type:CISCO-IPMROUTE-MIB::Missing HeartBeats

The heartbeat event includes the name of the SNMP MIB used to forward the event and the name of the event; however, CMM 3.1 does not indicate the name of the Multicast Group or the Channel Name on the Latest Events page for heartbeat events.

Step 2 To view additional information about the heartbeat event click the URL link in the Details column.

A Trap Details list appears for the heartbeat event, as shown in Figure 3-22.

Figure 3-22 Trap Details List for a Heartbeat Event



Trap Details List :

This Notification is sent if a multicast router failed to receive configured number of heartbeat packets from heartbeat sources within a configured time interval	SNMPv2-SMI::enterprises.9.10.2.3.1.0.1	
Trap OID	Value	Description
enterprises.9.10.2.1.1.4.1.2.239.1.1.77	0.0.0.0	
enterprises.9.10.2.1.1.4.1.3.239.1.1.77	10	
enterprises.9.10.2.1.1.4.1.4.239.1.1.77	1	
enterprises.9.10.2.1.1.4.1.5.239.1.1.77	0	

Source IP : 172.16.4.2
UpTime : 18:5:55:27.33

The Trap Details list displays the full description of the heartbeat event, the SNMP version used to generate the event, and the OIDs from the reporting router.

The last four octets of the OID indicate the Multicast Group. The Source IP address at the bottom of the Trap Details page is the IP address of the reporting router.

Step 3 To determine the video service affected by the event, select **Diagnostics > Show All Groups** and find the corresponding Multicast Group in the list that matches the heartbeat event. Note that Cisco Info Center/TBSM parses the heartbeat event to and matches the Multicast Group to the corresponding video service directly.

Performing Health Checks

Using the Health Check page, you can run a health check on a multicast domain.

To run a health check:

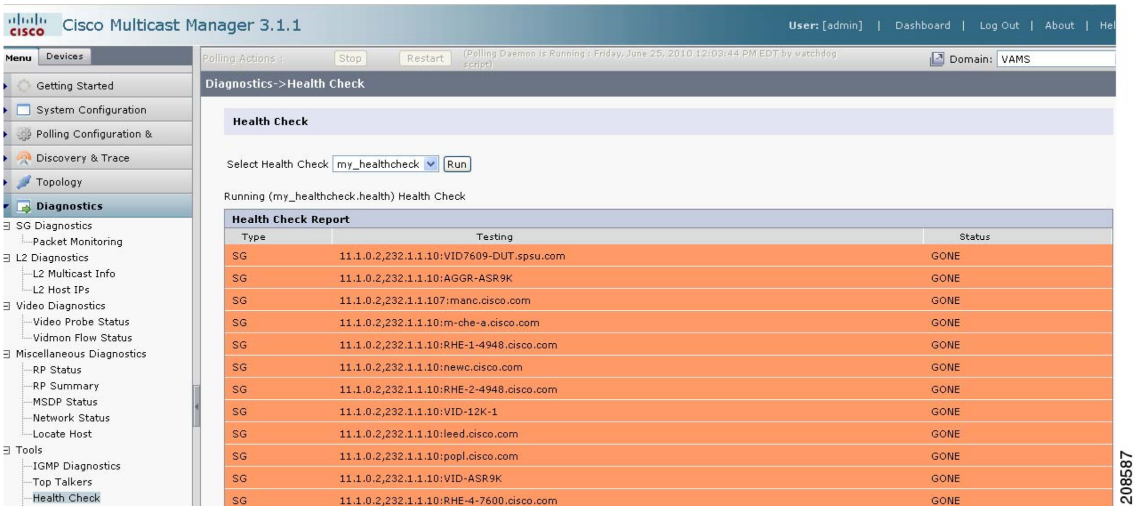
Step 1 On the Multicast Manager tool, select **Diagnostics** > **Health Check**.

The Select Health Check page appears.

Step 2 Select a health check from the list of health checks and click **Run**.

Figure 3-23 shows a sample health check display.

Figure 3-23 Health Check



(Polling Daemon is Running : Friday, June 25, 2010 12:03:44 PM EDT by watchdog script)

Domain: VAMS

Diagnostics->Health Check

Health Check

Select Health Check: my_healthcheck

Running (my_healthcheck.health) Health Check

Health Check Report

Type	Testing	Status
SG	11.1.0.2,232.1.1.10:VID7609-DUT.spsu.com	GONE
SG	11.1.0.2,232.1.1.10:AGGR-ASR9K	GONE
SG	11.1.0.2,232.1.1.107:manc.cisco.com	GONE
SG	11.1.0.2,232.1.1.10:m-che-a.cisco.com	GONE
SG	11.1.0.2,232.1.1.10:RHE-1-4948.cisco.com	GONE
SG	11.1.0.2,232.1.1.10:newc.cisco.com	GONE
SG	11.1.0.2,232.1.1.10:RHE-2-4948.cisco.com	GONE
SG	11.1.0.2,232.1.1.10:VID-12K-1	GONE
SG	11.1.0.2,232.1.1.10:leed.cisco.com	GONE
SG	11.1.0.2,232.1.1.10:popl.cisco.com	GONE
SG	11.1.0.2,232.1.1.10:VID-ASR9K	GONE
SG	11.1.0.2,232.1.1.10:RHE-4-7600.cisco.com	GONE

The color of the displayed text on the Health Check display indicates the status of the monitored condition:

- White = normal
- Red = error condition

Monitoring PPS/BPS Thresholds

When a PPS/BPS threshold is exceeded or fails to reach a minimum value, an event is generated and the event is displayed in Cisco Info Center event lists. From the event list, you can launch CMM to view enhanced monitoring information about the threshold event.

Monitoring PPS/BPS Thresholds in the Service Dashboard

To view PPS/BPS threshold events in the TBSM Service Dashboard:

Step 1 From the service tree directory browser at the left of the TBSM display, click on a service.

The service tree for the selected service appears.

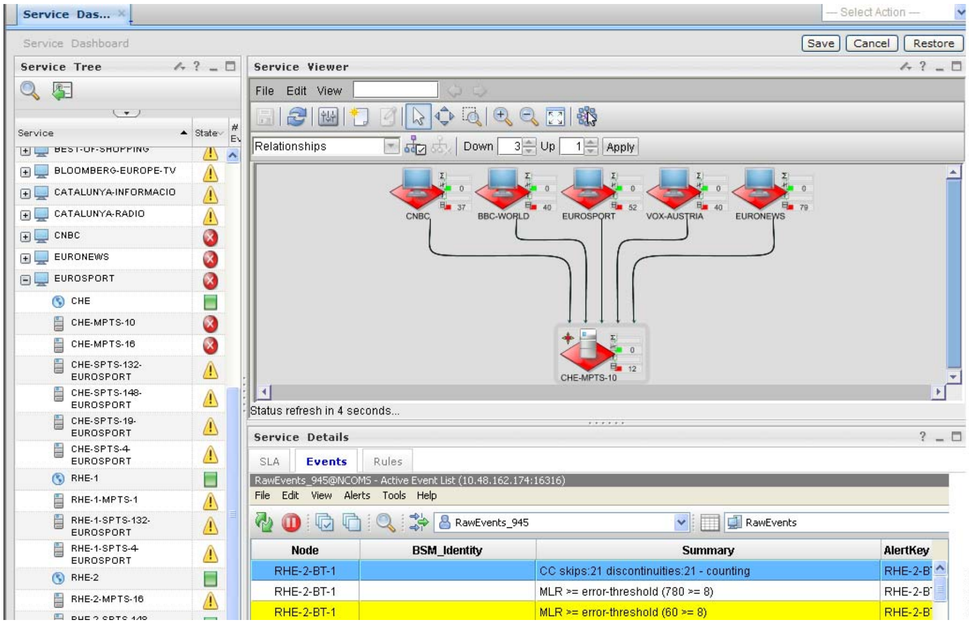
Step 2 Click on a specific device address.

The Service Viewer displays the network topology and the Service Details window shows an event list for the service.

Figure 3-24 shows a Service Dashboard with threshold events indicating that a Layer 3 multicast PPS rate is below the configured threshold level.

Related VidMon events show that VidMon delay thresholds in the service tree for the VidMon TS have been exceeded.

Figure 3-24 Viewing a Threshold Event in TBSM



Service	State
BEST-OF-SHOPPING	⚠
BLOOMBERG-EUROPE-TV	⚠
CATALUNYA-INFORMACIO	⚠
CATALUNYA-RADIO	⚠
CNBC	✖
EURONEWS	✖
EUROSPORT	✖
CHE	🟩
CHE-MPTS-10	✖
CHE-MPTS-16	✖
CHE-SPTS-132-EUROSPORT	⚠
CHE-SPTS-148-EUROSPORT	⚠
CHE-SPTS-19-EUROSPORT	⚠
CHE-SPTS-4-EUROSPORT	⚠
RHE-1	🟩
RHE-1-MPTS-1	⚠
RHE-1-SPTS-132-EUROSPORT	⚠
RHE-1-SPTS-4-EUROSPORT	⚠
RHE-2	🟩
RHE-2-MPTS-16	⚠
RHE-2-SPTS-148	

Status refresh in 4 seconds...

RawEvents_945@NCOMS - Active Event List (10.48.162.174:16316)

File Edit View Alerts Tools Help

RawEvents_945 RawEvents

Node	BSM_Identity	Summary	AlertKey
RHE-2-BT-1		CC skips:21 discontinuities:21 - counting	RHE-2-B
RHE-2-BT-1		MLR >= error-threshold (780 >= 8)	RHE-2-B
RHE-2-BT-1		MLR >= error-threshold (60 >= 8)	RHE-2-B

The event summary for threshold events includes the measured value and the configured threshold.

Step 3 To view additional details about the event, double-click on the event in the event list.

Step 4 To launch the CMM application and monitor additional information about the threshold events, highlight an event, and then from the Alerts Menu, choose **VAMS Tools > Launch CMM**.

Step 5 Go to Monitoring Threshold Events with CMM, page 3-27 for information on monitoring threshold events with CMM.

Monitoring Threshold Events with CMM

To view threshold events with CMM:

Step 1 If you are in the TBSM/Cisco Info Center interface, highlight an event, and then from the Alerts Menu, choose **VAMS Tools > Launch CMM**.

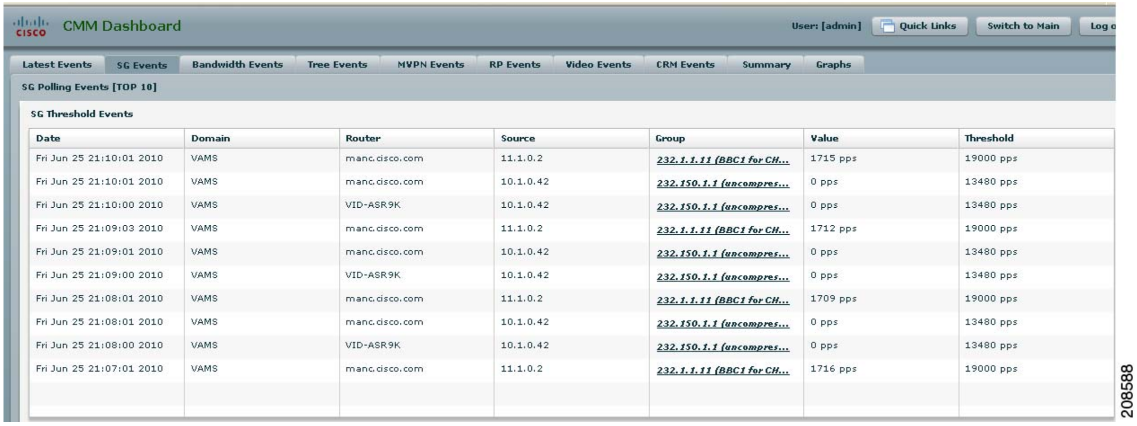
The CMM home page shows the Latest Events list.

Step 2 Click **SG Events**.

Step 3 The SG Events page appears, which includes any BPS/PPS threshold events that have come in.

Figure 3-25 shows a SG Events page with BPS/PPS threshold events.

Figure 3-25 Viewing BPS/PPS Threshold Events in CMM



SG Polling Events [TOP 10]

SG Threshold Events

Date	Domain	Router	Source	Group	Value	Threshold
Fri Jun 25 21:10:01 2010	VAMS	manc.cisco.com	11.1.0.2	232.1.1.11 (BBC1 for CH...	1715 pps	19000 pps
Fri Jun 25 21:10:01 2010	VAMS	manc.cisco.com	10.1.0.42	232.150.1.1 (uncompres...	0 pps	13480 pps
Fri Jun 25 21:10:00 2010	VAMS	VID-ASR9K	10.1.0.42	232.150.1.1 (uncompres...	0 pps	13480 pps
Fri Jun 25 21:09:03 2010	VAMS	manc.cisco.com	11.1.0.2	232.1.1.11 (BBC1 for CH...	1712 pps	19000 pps
Fri Jun 25 21:09:01 2010	VAMS	manc.cisco.com	10.1.0.42	232.150.1.1 (uncompres...	0 pps	13480 pps
Fri Jun 25 21:09:00 2010	VAMS	VID-ASR9K	10.1.0.42	232.150.1.1 (uncompres...	0 pps	13480 pps
Fri Jun 25 21:08:01 2010	VAMS	manc.cisco.com	11.1.0.2	232.1.1.11 (BBC1 for CH...	1709 pps	19000 pps
Fri Jun 25 21:08:01 2010	VAMS	manc.cisco.com	10.1.0.42	232.150.1.1 (uncompres...	0 pps	13480 pps
Fri Jun 25 21:08:00 2010	VAMS	VID-ASR9K	10.1.0.42	232.150.1.1 (uncompres...	0 pps	13480 pps
Fri Jun 25 21:07:01 2010	VAMS	manc.cisco.com	11.1.0.2	232.1.1.11 (BBC1 for CH...	1716 pps	19000 pps

The Value column for BPS/PPS threshold events includes the measured value and the Threshold field indicates the configured threshold.

Note CMM 3.1 does not reflect the BPS/PPS flow status on CMM flow traces, as it does for video probe status. Therefore, you will have to manually correlate the devices reporting BPS/PPS events from either Cisco Info Center/TBSM or the CMM Latest Events page, to the CMM flow trace, to isolate where in the distribution tree the problem is occurring.

Running Threshold Reports

CMM provides two threshold reports that you can use to monitor threshold events:

- S, G Threshold Report—Shows threshold events for a specified source and group.
- Layer 2 PPS Threshold Report—Shows threshold events for a specified port on a specified switch.

To run an S, G Threshold report:

Step 1 In the CMM Multicast Manager tool, click **Reporting**.

Step 2 Select **S, G Threshold Report**.

A list of groups appears.

Step 3 Select a group from the list and then click **Report**.

CMM displays an S,G Threshold Report listing any events that have occurred in the last 24 hours.

To run a Layer 2 PPS Threshold report:

Step 1 In the CMM Multicast Manager tool, click **Reporting**.

Step 2 Select **Layer 2 PPS Threshold Report**.

A list of groups appears.

Step 3 Select a group from the list and then click **Report**.

CMM displays a Layer 2 PPS Threshold Report listing any events that have occurred in the last 24 hours.

Monitoring Video Probe Status with CMM

Using CMM, you can:

- View video probe flows.

  See Viewing Video Probe Flows, page 3-29.

- View Video Probe Reports

  See Viewing Video Probe Reports, page 3-29.

- View a historical graph of video probe performance

  See Viewing a Historical Graph of Video Probe Performance, page 3-30.

- View a graph of video probe performance

  See Viewing Video Probe Performance Graphs, page 3-31.

Viewing Video Probe Flows

To view video probe status:

Step 1 Right-click on a CMM event and from the Alerts Menu, choose **VAMS Tools > Launch CMM**.

Step 2 From the Cisco Multicast Manager menu, select **Diagnostics.**

Step 3 Select **Video Diagnostics**.

Step 4 Select **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 a status indicator for the probe.

For detailed information, see 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_diag.html#wp1061409

Viewing Video Probe Reports

To view video probe reports in CMM:

Step 1 Right-click on a CMM event and from the Alerts Menu, choose **VAMS Tools > Launch CMM**.

Step 2 From the Multicast Manager menu, select **Polling Configuration & Reports**.

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

Step 4 Select **Video Probe**.

For additional information, see “Video Probe Report” 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_pc.html#wp1074979

Viewing a Historical Graph of Video Probe Performance

Cisco Multicast Manager 3.1 allows you to view a historical graph showing performance of a specified video probe over time.

To view a historical graph of video probe performance:

Step 1 Right-click on a CMM event and from the Alerts Menu, choose **VAMS Tools > Launch CMM**.

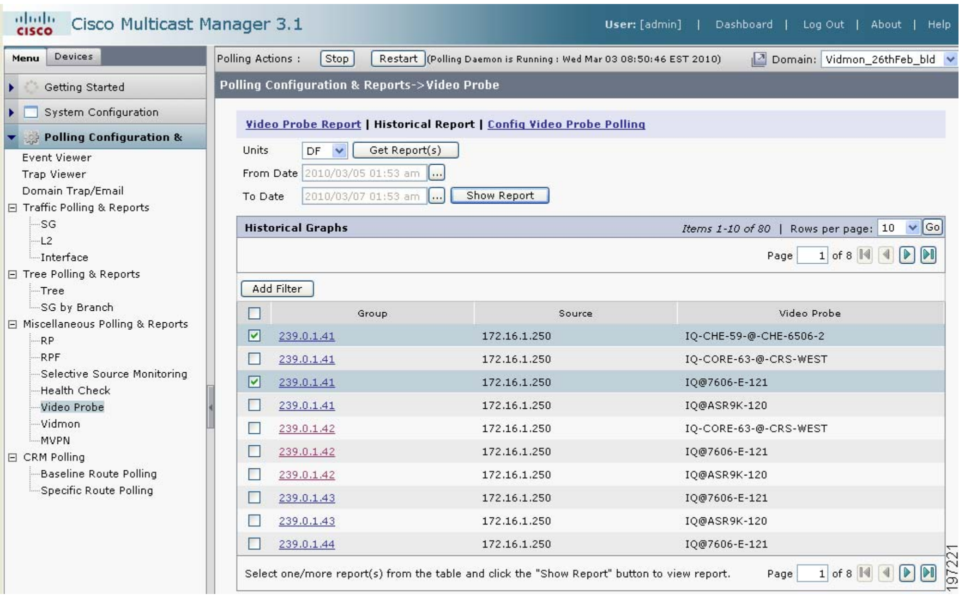
Step 2 From the Multicast Manager menu, select **Polling Configuration & Reports**.

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

Step 4 Select **Video Probe**.

Step 5 Select **Historical Report**. The Historical Graphs page for video probe reports appears, as shown in Figure 3-26.

Figure 3-26 Historical Graphs Page for Video Probes



(Polling Daemon is Running : Wed Mar 03 08:50:46 EST 2010)

Domain: Vidmon_26thFeb_bld

Units: DF

From Date: 2010/03/05 01:53 am

To Date: 2010/03/07 01:53 am

Historical Graphs — *Items 1-10 of 80* | Rows per page: 10

Page 1 of 8

□	Group	Source	Video Probe
☑	239.0.1.41	172.16.1.250	IQ-CHE-59-@-CHE-6506-2
□	239.0.1.41	172.16.1.250	IQ-CORE-63-@-CRS-WEST
☑	239.0.1.41	172.16.1.250	IQ@7606-E-121
□	239.0.1.41	172.16.1.250	IQ@ASR9K-120
□	239.0.1.42	172.16.1.250	IQ-CORE-63-@-CRS-WEST
□	239.0.1.42	172.16.1.250	IQ@7606-E-121
□	239.0.1.42	172.16.1.250	IQ@ASR9K-120
□	239.0.1.43	172.16.1.250	IQ@7606-E-121
□	239.0.1.43	172.16.1.250	IQ@ASR9K-120
□	239.0.1.44	172.16.1.250	IQ@7606-E-121

Select one/more report(s) from the table and click the "Show Report" button to view report. Page 1 of 8

Step 6 From the drop-down list in the **Units** field, select the units for the report:

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

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

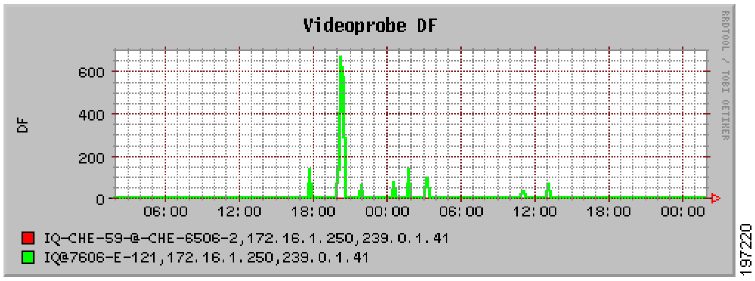
Step 8 Click the calendar item (...) for **To Date** and from the calendar that appears, select the To Date,

Step 9 On the list of Video Probes, check the check boxes for up to three video probes.

Step 10 Click the **Show Report** button.

A graph showing the statistics for the selected video probes appears, as shown in Figure 3-27.

Figure 3-27 Historical Report Showing DF for Two Video Probes



Viewing Video Probe Performance Graphs

From the CMM Event Dashboard, you can view a graph showing real-time DF or MLR for a specified video probe.

To view a video probe performance graph:

Step 1 Right-click on a CMM event and from the Alerts Menu, choose **VAMS Tools > Launch CMM**.

Step 2 From the CMM Dashboard, click the **Graphs** tab.

For detailed information, see “Viewing Performance Graphs from the Dashboard” 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_gs.html#wp1253283

Monitoring VidMon Status with CMM

Using CMM, you can:

- View VidMon Flows

  See Viewing VidMon Flows, page 3-32.

- View Vidmon reports

  See Viewing VidMon Reports, page 3-34.

- View historical graphs of VidMon performance

  See Viewing VidMon Historical Reports, page 3-34.

- View a graph of video probe performance

  See Viewing VidMon Performance Graphs, page 3-35.

Viewing VidMon Flows

To view VidMon flows from CMM:

Step 1 Right-click on a CMM event and from the Alerts Menu, choose **VAMS Tools > Launch CMM**.

Step 2 From the Cisco Multicast Manager menu, select **Diagnostics.**

Step 3 Select **Video Diagnostics**.

Step 4 Select **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 5 To view more detailed status for the interfaces on the Vidmon device, click a device name on the Video Flow Status page.

The Vidmon Flows Status page appears. The Vidmon Flows Status page shows the status of the current video flow on each interface on the device.

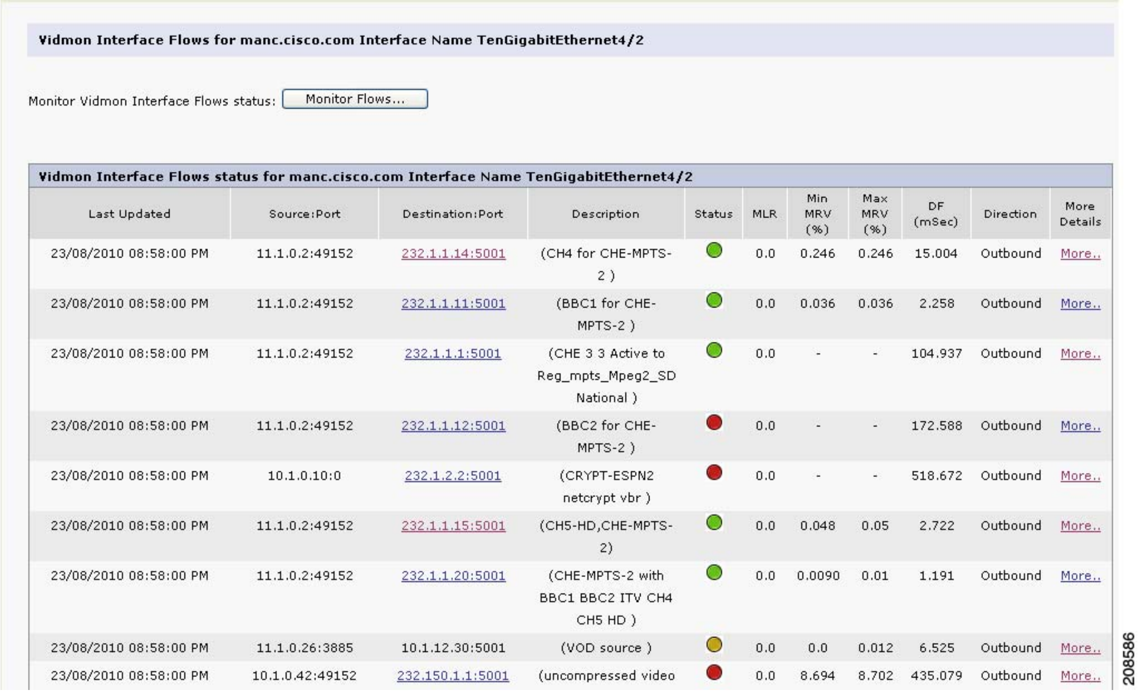
Step 6 To view detailed statistics on the current video flow on the interface, click on an interface name in the list.

The Vidmon Interface Flows page appears. The Vidmon Interface Flows page shows detailed statistics for the current flows on the interface.

To refresh monitoring data, click the **Monitor Flows** button.

Figure 3-28 shows the Vidmon Interface Flows page.

Figure 3-28 Vidmon Interface Flows Page



Vidmon Interface Flows for manc.cisco.com Interface Name TenGigabitEthernet4/2

Monitor Vidmon Interface Flows status: Monitor Flows...

Vidmon Interface Flows status for manc.cisco.com Interface Name TenGigabitEthernet4/2

Last Updated	Source:Port	Destination:Port	Description	Status	MLR	Min MRV (%)	Max MRV (%)	DF (mSec)	Direction	More Details
23/08/2010 08:58:00 PM	11.1.0.2:49152	232.1.1.14:5001	(CH4 for CHE-MPTS-2)	🟢	0.0	0.246	0.246	15.004	Outbound	More..
23/08/2010 08:58:00 PM	11.1.0.2:49152	232.1.1.11:5001	(BBC1 for CHE-MPTS-2)	🟢	0.0	0.036	0.036	2.258	Outbound	More..
23/08/2010 08:58:00 PM	11.1.0.2:49152	232.1.1.1:5001	(CHE 3 3 Active to Reg_mpts_Mpeg2_SD National)	🟢	0.0	-	-	104.937	Outbound	More..
23/08/2010 08:58:00 PM	11.1.0.2:49152	232.1.1.12:5001	(BBC2 for CHE-MPTS-2)	🔴	0.0	-	-	172.588	Outbound	More..
23/08/2010 08:58:00 PM	10.1.0.10:0	232.1.2.2:5001	(CRYPT-ESPN2 netcrypt vbr)	🔴	0.0	-	-	518.672	Outbound	More..
23/08/2010 08:58:00 PM	11.1.0.2:49152	232.1.1.15:5001	(CH5-HD,CHE-MPTS-2)	🟢	0.0	0.048	0.05	2.722	Outbound	More..
23/08/2010 08:58:00 PM	11.1.0.2:49152	232.1.1.20:5001	(CHE-MPTS-2 with BBC1 BBC2 ITV CH4 CH5 HD)	🟢	0.0	0.0090	0.01	1.191	Outbound	More..
23/08/2010 08:58:00 PM	11.1.0.26:3885	10.1.12.30:5001	(VOD source)	🟡	0.0	0.0	0.012	6.525	Outbound	More..
23/08/2010 08:58:00 PM	10.1.0.42:49152	232.150.1.1:5001	(uncompressed video	🔴	0.0	8.694	8.702	435.079	Outbound	More..

208586

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).

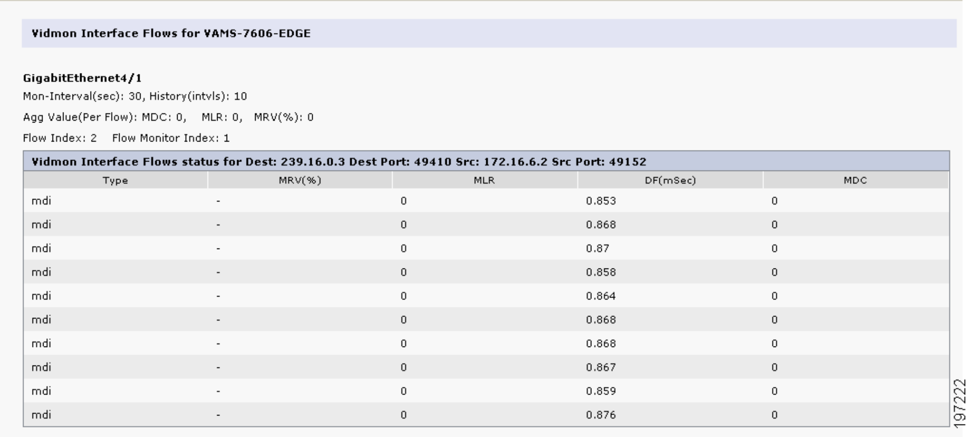
Step 7 To clear yellow indicators, click the **Clear** button.

Step 8 To perform a multicast trace for the flow, click on the IP address of the Destination Port for the flow.

Step 9 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 3-29.

Figure 3-29 Vidmon Interface Flows Page for a 76xx Device



Vidmon Interface Flows for VAMS-7606-EDGE

GigabitEthernet4/1
Mon-Interval(sec): 30, History(intvls): 10
Agg Value(Per Flow): MDC: 0, MLR: 0, MRV(%): 0
Flow Index: 2 Flow Monitor Index: 1

Vidmon Interface Flows status for Dest: 239.16.0.3 Dest Port: 49410 Src: 172.16.6.2 Src Port: 49152

Type	MRV(%)	MLR	DF(mSec)	MDC
mdi	-	0	0.853	0
mdi	-	0	0.868	0
mdi	-	0	0.87	0
mdi	-	0	0.858	0
mdi	-	0	0.864	0
mdi	-	0	0.868	0
mdi	-	0	0.868	0
mdi	-	0	0.867	0
mdi	-	0	0.859	0
mdi	-	0	0.876	0

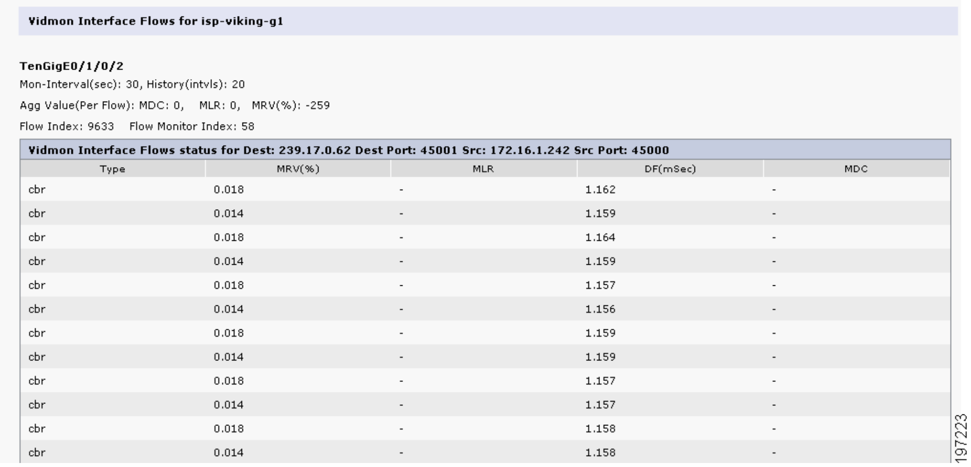
The Vidmon Interface Flows Page shown in Figure 3-29 indicates flow information for a Cisco 76xx device.

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 3-30 shows a Vidmon Interface Flows page for an ASR 9000 device.

Figure 3-30 Vidmon Interface Flows Page for an ASR 9000 Device.



Vidmon Interface Flows for isp-viking-g1

TenGigE0/1/0/2

Mon-Interval(sec): 30, History(intvls): 20

Agg Value(Per Flow): MDC: 0, MLR: 0, MRV(%): -259

Flow Index: 9633 Flow Monitor Index: 58

Vidmon Interface Flows status for Dest: 239.17.0.62 Dest Port: 45001 Src: 172.16.1.242 Src Port: 45000

Type	MRV(%)	MLR	DF(mSec)	MDC
cbr	0.018	-	1.162	-
cbr	0.014	-	1.159	-
cbr	0.018	-	1.164	-
cbr	0.014	-	1.159	-
cbr	0.018	-	1.157	-
cbr	0.014	-	1.156	-
cbr	0.018	-	1.159	-
cbr	0.014	-	1.159	-
cbr	0.018	-	1.157	-
cbr	0.014	-	1.157	-
cbr	0.018	-	1.158	-
cbr	0.014	-	1.158	-

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.

Viewing VidMon Reports

To view VidMon reports in CMM:

Step 1 Right-click on a CMM event and from the Alerts Menu, choose **VAMS Tools > Launch CMM**.

Step 2 From the Multicast Manager menu, select **Polling Configuration & Reports**.

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

Step 4 Select **VidMon**.

For additional information, see "Viewing a VidMon Report" 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_pc.html#wp1116936

Viewing VidMon Historical Reports

To view a historical graph of VidMon performance in CMM:

Step 1 Right-click on a CMM event and from the Alerts Menu, choose **VAMS Tools > Launch CMM**.

Step 2 From the Multicast Manager menu, select **Polling Configuration & Reports**.

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

Step 4 Select **Vidmon**.

Step 5 Select **Historical Report**. The Historical Graphs page for video probe reports appears.

Step 6 From the drop-down list in the **Units** field, select the units for the report:

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

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

Step 8 Click the calendar item (...) for **To Date** and from the calendar that appears, select the To Date,

Step 9 On the list of interfaces on Vidmon devices, check the check boxes for up to three interfaces.

Step 10 Click the **Show Report** button.

A graph showing the statistics for the selected Vidmon devices appears.

Viewing VidMon Performance Graphs

From the CMM Event Dashboard, you can view a graph showing real-time DF, MLR, or MRV for a specified VidMon device.

To view a VidMon performance graph:

Step 1 Right-click on a CMM event and from the Alerts Menu, choose **VAMS Tools > Launch CMM**.

Step 2 From the CMM Dashboard, click the **Graphs** tab.

For detailed information, see “Viewing Performance Graphs from the Dashboard” 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_gs.html#wp1253283

Viewing Events in the CMM Event View

To view the custom CMM event views:

Step 1 Log in to IBM TIP/TBSM.

The main TBSM window appears.

Step 2 Click the plus sign (+) next to **Video Assurance Management**.

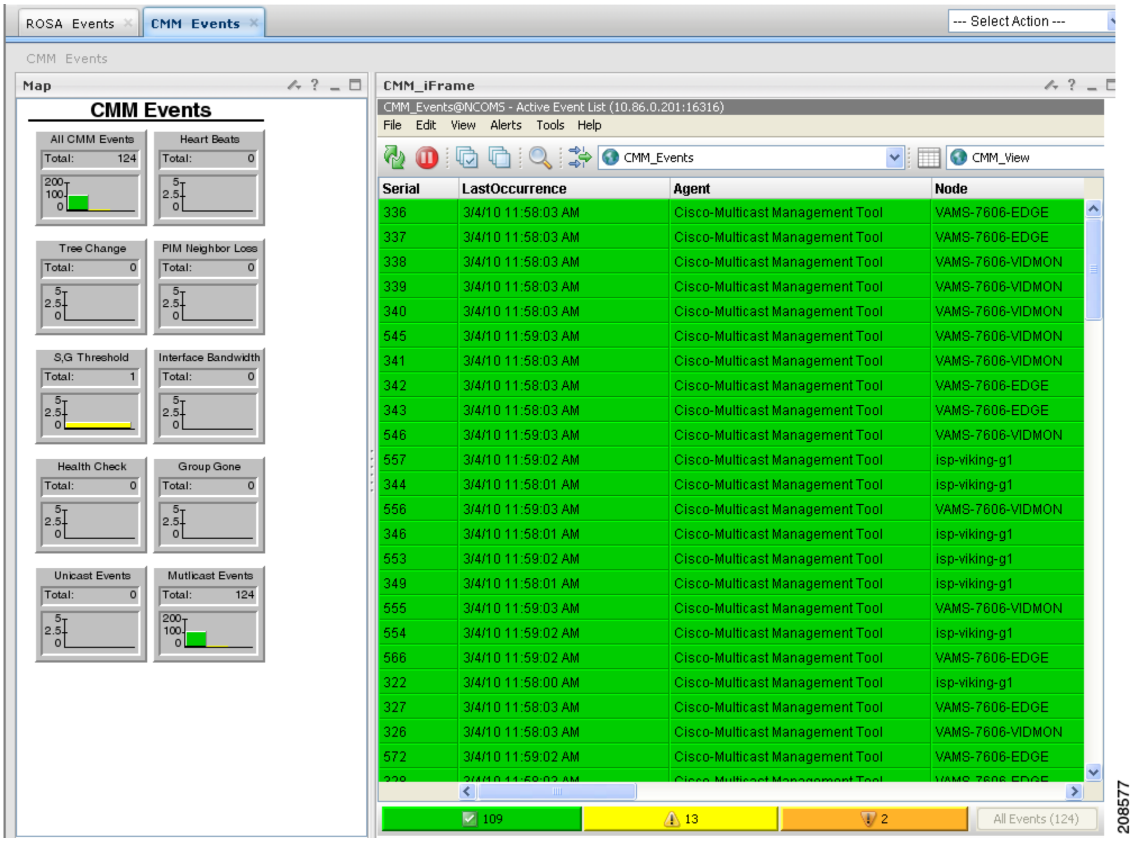
The Video Assurance Management menu appears.

Step 3 Click the plus sign (+) next to **Video Fault**.

Step 4 Click **CMM Events**.

The Events Views page for the CMM events appears. Figure 3-31 shows the event views for CMM Events.

Figure 3-31 CMM Events Views



CMM_Events@NCOMS - Active Event List (10.86.0.201:16316)

Serial	LastOccurrence	Agent	Node
336	3/4/10 11:58:03 AM	Cisco-Multicast Management Tool	VAMS-7606-EDGE
337	3/4/10 11:58:03 AM	Cisco-Multicast Management Tool	VAMS-7606-EDGE
338	3/4/10 11:58:03 AM	Cisco-Multicast Management Tool	VAMS-7606-VIDMON
339	3/4/10 11:58:03 AM	Cisco-Multicast Management Tool	VAMS-7606-VIDMON
340	3/4/10 11:58:03 AM	Cisco-Multicast Management Tool	VAMS-7606-VIDMON
545	3/4/10 11:59:03 AM	Cisco-Multicast Management Tool	VAMS-7606-VIDMON
341	3/4/10 11:58:03 AM	Cisco-Multicast Management Tool	VAMS-7606-VIDMON
342	3/4/10 11:58:03 AM	Cisco-Multicast Management Tool	VAMS-7606-EDGE
343	3/4/10 11:58:03 AM	Cisco-Multicast Management Tool	VAMS-7606-EDGE
546	3/4/10 11:59:03 AM	Cisco-Multicast Management Tool	VAMS-7606-VIDMON
557	3/4/10 11:59:02 AM	Cisco-Multicast Management Tool	isp-viking-g1
344	3/4/10 11:58:01 AM	Cisco-Multicast Management Tool	isp-viking-g1
556	3/4/10 11:59:03 AM	Cisco-Multicast Management Tool	VAMS-7606-VIDMON
346	3/4/10 11:58:01 AM	Cisco-Multicast Management Tool	isp-viking-g1
553	3/4/10 11:59:02 AM	Cisco-Multicast Management Tool	isp-viking-g1
349	3/4/10 11:58:01 AM	Cisco-Multicast Management Tool	isp-viking-g1
555	3/4/10 11:59:03 AM	Cisco-Multicast Management Tool	VAMS-7606-VIDMON
554	3/4/10 11:59:02 AM	Cisco-Multicast Management Tool	isp-viking-g1
566	3/4/10 11:59:02 AM	Cisco-Multicast Management Tool	VAMS-7606-EDGE
322	3/4/10 11:58:00 AM	Cisco-Multicast Management Tool	isp-viking-g1
327	3/4/10 11:58:03 AM	Cisco-Multicast Management Tool	VAMS-7606-EDGE
326	3/4/10 11:58:03 AM	Cisco-Multicast Management Tool	VAMS-7606-VIDMON
572	3/4/10 11:59:02 AM	Cisco-Multicast Management Tool	VAMS-7606-EDGE

The left part of the display shows monitor boxes for the selected event type. Each monitor box shows a bar graph indicating the number events in each severity level for the event category.

The CMM Events views include:

- **All CMM Events**—Shows all CMM events.
- **Heart Beats**—Shows heartbeat events from CMM.
- **Tree Change**—Shows tree change events.
- **PIM Neighbor Loss**—Shows events from video probes.
- **S,G Threshold**—Shows S,G threshold events (above threshold and below threshold events)
- **Interface Bandwidth**—Shows events indicating a video probe has been started.
- **Health Check**—Shows events from video probes.
- **Group Gone**—Shows video events for the last 24 hours,
- **Unicast Events**—Shows events indicating a video probe has been started.
- **Multicast Events**—Shows events from video probes.

Step 5 To see the events in a CMM event view, click the monitor box for the event class.

For example, click the monitor box for S,G Threshold events to see all S,G Threshold events from CMM.

Step 6 To view the details of an event, double-click on the row for the event.

A table giving detailed field information for the event appears.

Step 7 To troubleshoot the event in CMM, right-click the event, and from the Alerts menu, choose **VAMS Tools > Launch CMM**.

Monitoring VidMon Events

This section describes:

- Monitoring VidMon Events in the Service Dashboard, page 6-35
- Viewing Events in the VidMon Event Views, page 6-36

Monitoring VidMon Events in the Service Dashboard

To monitor VidMon events in the service dashboard:

Step 1 On the Video Assurance Management menu, click **Service Dashboard**.

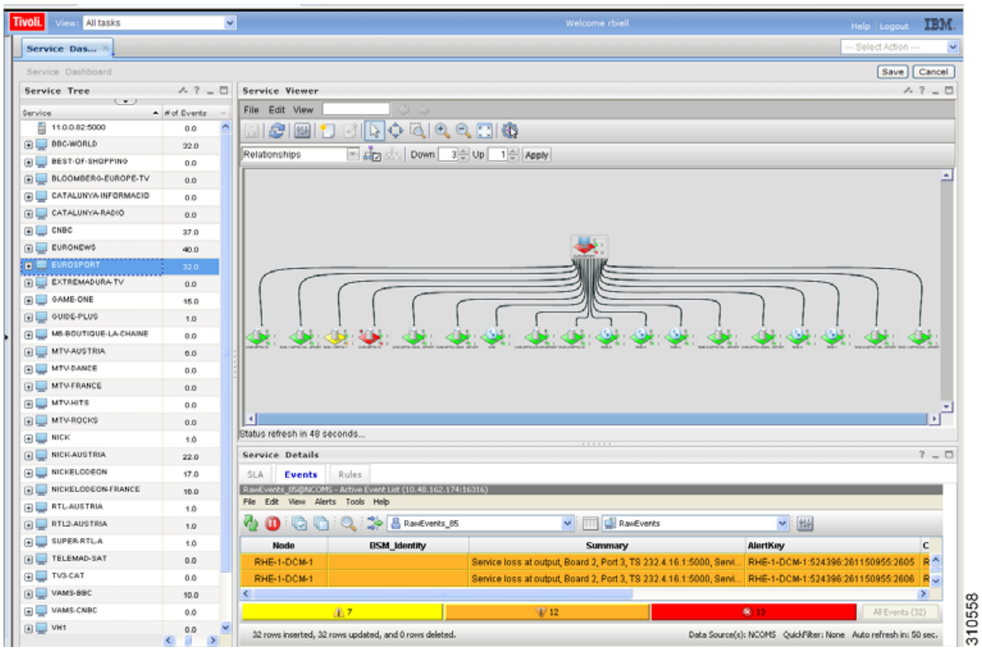
The Service Dashboard appears, and the Service Tree shows a list of the configured video services in your network.

Step 2 Left-click on a a service on the Service Tree directory browser at the left of the page

- The Service Viewer shows a service map for the elected service.
- The Service Details window shows an event list for the service.

Figure 3-32 shows the Service Tree, Service Viewer, and Service Details window for a channel service called *EUROSPORT*.

Figure 3-32 Service Dashboard for a High Level Service



Service	# of Events
11.0.0.82:5000	0.0
BBC-WORLD	32.0
BEST-OF-SHOPPING	0.0
BLOOMBERG-EUROPE-TV	0.0
CATALUNYA-INFORMACIO	0.0
CATALUNYA-RADIO	0.0
CNBC	37.0
EURONEWS	40.0
EUROSPORT	32.0
EXTREMADURA-TV	0.0
GAME-ONE	15.0
GUIDE-PLUS	1.0
M6-BOUTIQUE-LA-CHAINE	0.0
MTV-AUSTRIA	6.0
MTV-DANCE	0.0
MTV-FRANCE	0.0
MTV-HITS	0.0
MTV-ROCKS	0.0
NICK	1.0
NICK-AUSTRIA	22.0
NICKELODEON	17.0
NICKELODEON-FRANCE	10.0
RTL-AUSTRIA	1.0
RTL2-AUSTRIA	1.0
SUPER-RTL-A	1.0
TELEMAD-SAT	0.0
TV3-CAT	0.0
VAMS-BBC	10.0
VAMS-CNBC	0.0
VH1	0.0

Status refresh in 48 seconds...

Node	BSM_Identity	Summary	AlertKey	C
RHE-1-DCM-1		Service loss at output, Board 2, Port 3, TS 232.4.16.1:5000, Servi...	RHE-1-DCM-1:524396:261150955:2605	R
RHE-1-DCM-1		Service loss at output, Board 2, Port 3, TS 232.4.16.1:5000, Servi...	RHE-1-DCM-1:524396:261150955:2606	R

32 rows inserted, 32 rows updated, and 0 rows deleted.   Data Source(s): NCOMS QuickFilter: None Auto refresh in: 50 sec.

Step 3 To see the devices associated with the selected video service, click on the plus sign (+) next to the service name.

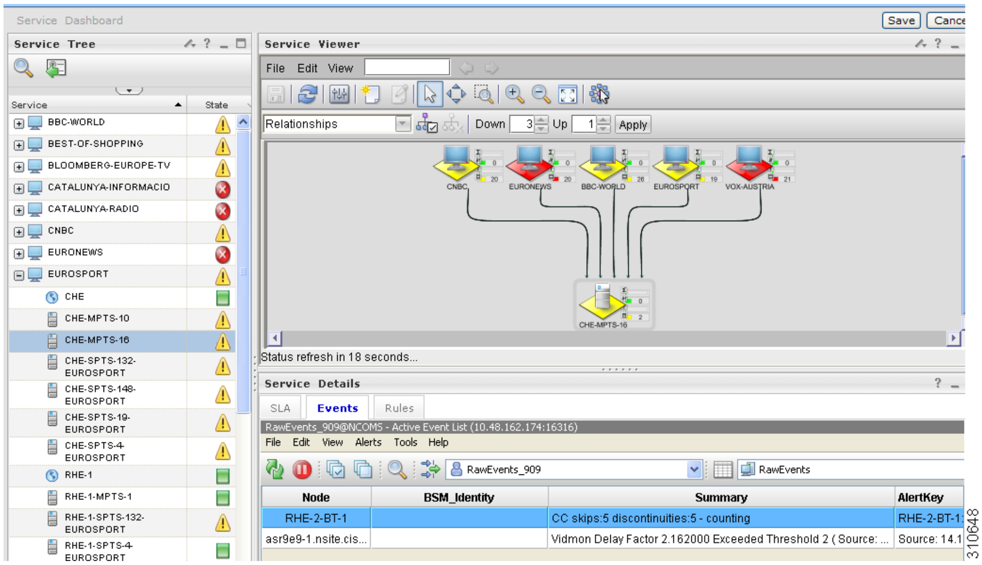
The devices in the service topology are listed in the Service Tree directory.

Step 4 Click on a device or service component to see the service map for the device or component.

The Service Viewer shows a service map for the device. If there are faults, such as VidMon alarms, the device is highlighted in red or in yellow. In the event list in the Service Details area, fault events are highlighted in yellow or red.

Figure 3-33 shows a Service Map and fault events for a device called *CHE-MPTS-16* that is associated with the *EUROSPORT* channel service.

Figure 3-33 Viewing VidMon Events in the Service Dashboard



Service	State
BBC-WORLD	⚠
BEST-OF-SHOPPING	⚠
BLOOMBERG-EUROPE-TV	⚠
CATALUNYA-INFORMACIO	☒
CATALUNYA-RADIO	☒
CNBC	⚠
EURONEWS	☒
EUROSPORT	⚠
CHE	🟩
CHE-MPTS-10	⚠
CHE-MPTS-16	⚠
CHE-SPTS-132-EUROSPORT	⚠
CHE-SPTS-148-EUROSPORT	⚠
CHE-SPTS-19-EUROSPORT	⚠
CHE-SPTS-4-EUROSPORT	⚠
RHE-1	🟩
RHE-1-MPTS-1	🟩
RHE-1-SPTS-132-EUROSPORT	⚠
RHE-1-SPTS-4-EUROSPORT	🟩

Status refresh in 18 seconds...

RawEvents_909@NCOMS - Active Event List (10.48.162.174:16316)

Node	BSM_Identity	Summary	AlertKey
RHE-2-BT-1		CC skips:5 discontinuities:5 - counting	RHE-2-BT-1:
asr9e9-1.nsite.cis...		Vidmon Delay Factor 2.162000 Exceeded Threshold 2 (Source: ...	Source: 14.1

The event list shown in Figure 3-32 shows the following VidMon event:

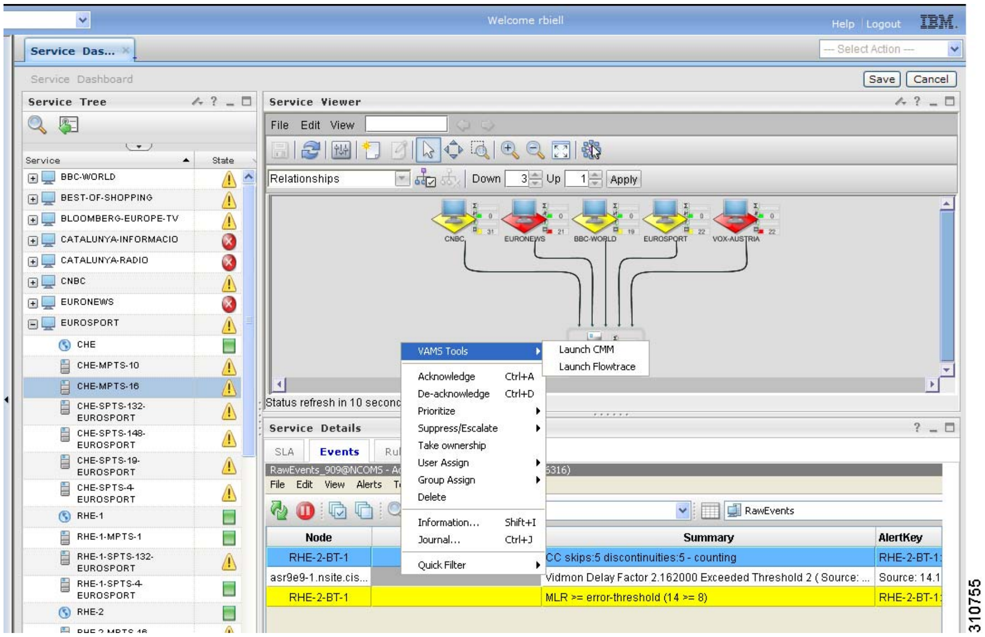
Vidmon Delay Factor Exceeded Threshold—SNMP trap generated by CMM indicating that a VidMon DF threshold has been exceeded on a Cisco 9000 device used to transport the MPTS stream.

Step 5 To view details about an event, highlight the event and right click on it.

Step 6 To launch CMM to troubleshoot the event, right-click on the event and choose **VAMS Tools > Launch CMM** or **VAMS Tools > Launch Flowtrace**.

Figure 3-34 shows the menu selections for launching CMM.

Figure 3-34 Launching CMM to Troubleshoot a VidMon Event



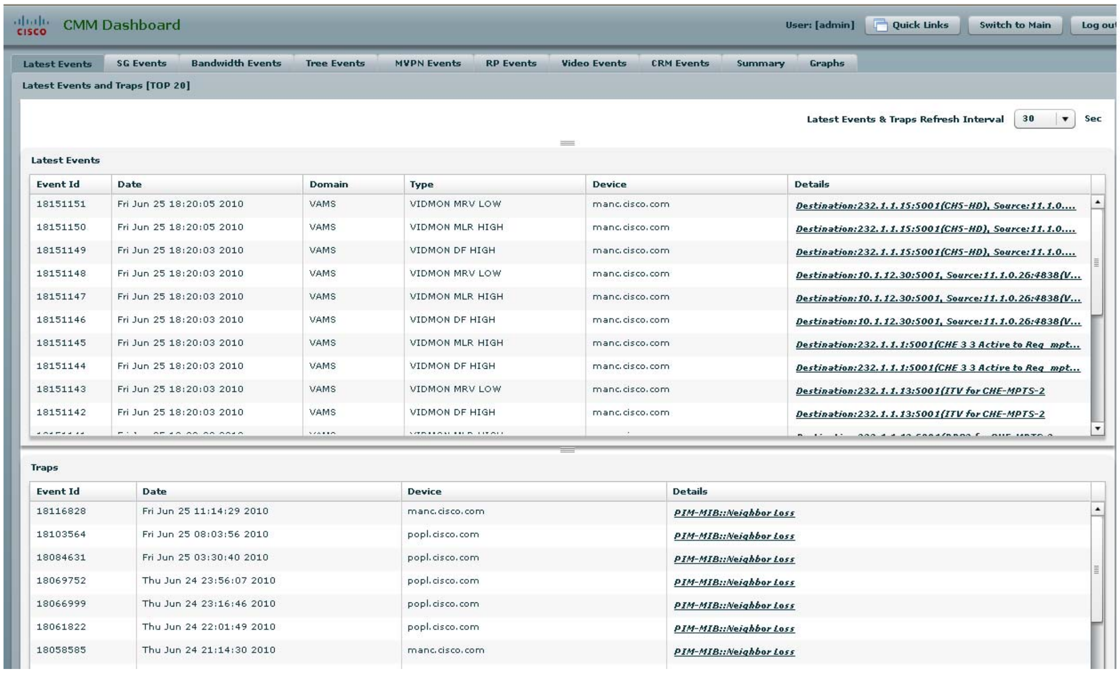
Node	Summary	AlertKey
RHE-2-BT-1	CC skips:5 discontinuities:5 - counting	RHE-2-BT-1
asr9e9-1.nsite.cis...	Vidmon Delay Factor 2.162000 Exceeded Threshold 2 (Source: ...	Source: 14.1
RHE-2-BT-1	MLR >= error-threshold (14 >= 8)	RHE-2-BT-1

The CMM login screen appears.

Step 7 Log in to CMM.

The CMM Dashboard appears, shown in Figure 3-35.

Figure 3-35 CMM Dashboard Showing Video Flows


CISCO CMM Dashboard
User: [admin] Quick Links Switch to Main Log out
Latest Events SG Events Bandwidth Events Tree Events MVPN Events RP Events Video Events CRM Events Summary Graphs
Latest Events and Traps [TOP 20]
Latest Events & Traps Refresh Interval 30 Sec
208576

Latest Events

Event Id	Date	Domain	Type	Device	Details
18151151	Fri Jun 25 18:20:05 2010	VAMS	VIDMON MRV LOW	manc.cisco.com	Destination:232.1.1.15:5001(CH5-HD), Source:11.1.0....
18151150	Fri Jun 25 18:20:05 2010	VAMS	VIDMON MLR HIGH	manc.cisco.com	Destination:232.1.1.15:5001(CH5-HD), Source:11.1.0....
18151149	Fri Jun 25 18:20:03 2010	VAMS	VIDMON DF HIGH	manc.cisco.com	Destination:232.1.1.15:5001(CH5-HD), Source:11.1.0....
18151148	Fri Jun 25 18:20:03 2010	VAMS	VIDMON MRV LOW	manc.cisco.com	Destination:10.1.12.30:5001, Source:11.1.0.26:4838(V...
18151147	Fri Jun 25 18:20:03 2010	VAMS	VIDMON MLR HIGH	manc.cisco.com	Destination:10.1.12.30:5001, Source:11.1.0.26:4838(V...
18151146	Fri Jun 25 18:20:03 2010	VAMS	VIDMON DF HIGH	manc.cisco.com	Destination:10.1.12.30:5001, Source:11.1.0.26:4838(V...
18151145	Fri Jun 25 18:20:03 2010	VAMS	VIDMON MLR HIGH	manc.cisco.com	Destination:232.1.1.1:5001(CHE 3 3 Active to Req mpt...
18151144	Fri Jun 25 18:20:03 2010	VAMS	VIDMON DF HIGH	manc.cisco.com	Destination:232.1.1.1:5001(CHE 3 3 Active to Req mpt...
18151143	Fri Jun 25 18:20:03 2010	VAMS	VIDMON MRV LOW	manc.cisco.com	Destination:232.1.1.13:5001(ITV for CHE-MPTS-2
18151142	Fri Jun 25 18:20:03 2010	VAMS	VIDMON DF HIGH	manc.cisco.com	Destination:232.1.1.13:5001(ITV for CHE-MPTS-2

Traps

Event Id	Date	Device	Details
18116828	Fri Jun 25 11:14:29 2010	manc.cisco.com	PIM-MIB::Neighbor Loss
18103564	Fri Jun 25 08:03:56 2010	popl.cisco.com	PIM-MIB::Neighbor Loss
18084631	Fri Jun 25 03:30:40 2010	popl.cisco.com	PIM-MIB::Neighbor Loss
18069752	Thu Jun 24 23:56:07 2010	popl.cisco.com	PIM-MIB::Neighbor Loss
18066999	Thu Jun 24 23:16:46 2010	popl.cisco.com	PIM-MIB::Neighbor Loss
18061822	Thu Jun 24 22:01:49 2010	popl.cisco.com	PIM-MIB::Neighbor Loss
18058585	Thu Jun 24 21:14:30 2010	manc.cisco.com	PIM-MIB::Neighbor Loss

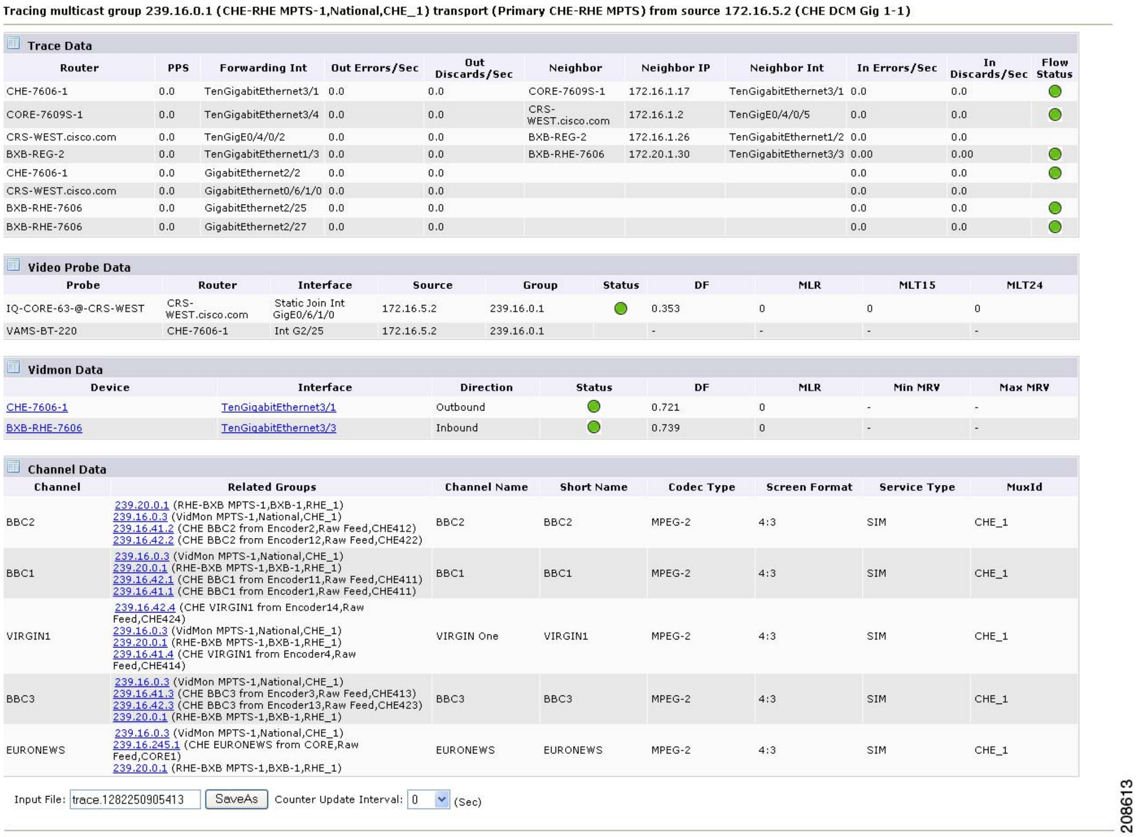
Step 8 From the CMM Dashboard:

- To launch a trace for the flow, locate the entry for the fault indicated in the TIP/TBSM message, for example, the DF high event on BBC2, and then click on the underlined link for the flow.
- To perform other troubleshooting tasks, click the Switch to Main button and then go to the appropriate CMM menu and task to perform a task.

If you click on a link to trace a flow, CMM launches a multicast trace for the flow and a multicast trace for the flow appears.

The top part of the Multicast Trace page presents a trace table, as shown in Figure 3-36. The bottom part of the page shows a topology map of the devices involved in the trace, as shown in Figure 3-36.

Figure 3-36 CMM Multicast Flow Trace: Trace Data Table



Tracing multicast group 239.16.0.1 (CHE-RHE MPTS-1,National,CHE_1) transport (Primary CHE-RHE MPTS) from source 172.16.5.2 (CHE DCM Gig 1-1)

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
CHE-7606-1	0.0	TenGigabitEthernet3/1	0.0	0.0	CORE-7609S-1	172.16.1.17	TenGigabitEthernet3/1	0.0	0.0	●
CORE-7609S-1	0.0	TenGigabitEthernet3/4	0.0	0.0	CRS-WEST.cisco.com	172.16.1.2	TenGigE0/4/0/5	0.0	0.0	●
CRS-WEST.cisco.com	0.0	TenGigE0/4/0/2	0.0	0.0	BXB-REG-2	172.16.1.26	TenGigabitEthernet1/2	0.0	0.0	
BXB-REG-2	0.0	TenGigabitEthernet1/3	0.0	0.0	BXB-RHE-7606	172.20.1.30	TenGigabitEthernet3/3	0.00	0.00	●
CHE-7606-1	0.0	GigabitEthernet2/2	0.0	0.0				0.0	0.0	●
CRS-WEST.cisco.com	0.0	GigabitEthernet0/6/1/0	0.0	0.0				0.0	0.0	
BXB-RHE-7606	0.0	GigabitEthernet2/25	0.0	0.0				0.0	0.0	●
BXB-RHE-7606	0.0	GigabitEthernet2/27	0.0	0.0				0.0	0.0	●

Video Probe Data

Probe	Router	Interface	Source	Group	Status	DF	MLR	MLT15	MLT24
IQ-CORE-63-@-CRS-WEST	CRS-WEST.cisco.com	Static Join Int GigE0/6/1/0	172.16.5.2	239.16.0.1	●	0.353	0	0	0
VAMS-BT-220	CHE-7606-1	Int G2/25	172.16.5.2	239.16.0.1		-	-	-	-

Vidmon Data

Device	Interface	Direction	Status	DF	MLR	Min MRV	Max MRV
CHE-7606-1	TenGigabitEthernet3/1	Outbound	●	0.721	0	-	-
BXB-RHE-7606	TenGigabitEthernet3/3	Inbound	●	0.739	0	-	-

Channel Data

Channel	Related Groups	Channel Name	Short Name	Codec Type	Screen Format	Service Type	MuxId
BBC2	239.20.0.1 (RHE-BXB MPTS-1,BXB-1,RHE_1) 239.16.0.3 (VidMon MPTS-1,National,CHE_1) 239.16.41.2 (CHE BBC2 from Encoder2,Raw Feed,CHE412) 239.16.42.2 (CHE BBC2 from Encoder12,Raw Feed,CHE422)	BBC2	BBC2	MPEG-2	4:3	SIM	CHE_1
BBC1	239.16.0.3 (VidMon MPTS-1,National,CHE_1) 239.20.0.1 (RHE-BXB MPTS-1,BXB-1,RHE_1) 239.16.42.1 (CHE BBC1 from Encoder11,Raw Feed,CHE411) 239.16.41.1 (CHE BBC1 from Encoder1,Raw Feed,CHE411)	BBC1	BBC1	MPEG-2	4:3	SIM	CHE_1
VIRGIN1	239.16.42.4 (CHE VIRGIN1 from Encoder14,Raw Feed,CHE424) 239.16.0.3 (VidMon MPTS-1,National,CHE_1) 239.20.0.1 (RHE-BXB MPTS-1,BXB-1,RHE_1) 239.16.41.4 (CHE VIRGIN1 from Encoder4,Raw Feed,CHE414)	VIRGIN One	VIRGIN1	MPEG-2	4:3	SIM	CHE_1
BBC3	239.16.0.3 (VidMon MPTS-1,National,CHE_1) 239.16.41.3 (CHE BBC3 from Encoder3,Raw Feed,CHE413) 239.16.42.3 (CHE BBC3 from Encoder13,Raw Feed,CHE423) 239.20.0.1 (RHE-BXB MPTS-1,BXB-1,RHE_1)	BBC3	BBC3	MPEG-2	4:3	SIM	CHE_1
EURONEWS	239.16.0.3 (VidMon MPTS-1,National,CHE_1) 239.16.245.1 (CHE EURONEWS from CORE,Raw Feed,CORE1) 239.20.0.1 (RHE-BXB MPTS-1,BXB-1,RHE_1)	EURONEWS	EURONEWS	MPEG-2	4:3	SIM	CHE_1

Input File: trace.1282250905413 Counter Update Interval: 0 (Sec)

The trace data shown in Figure 3-36 shows the following information:

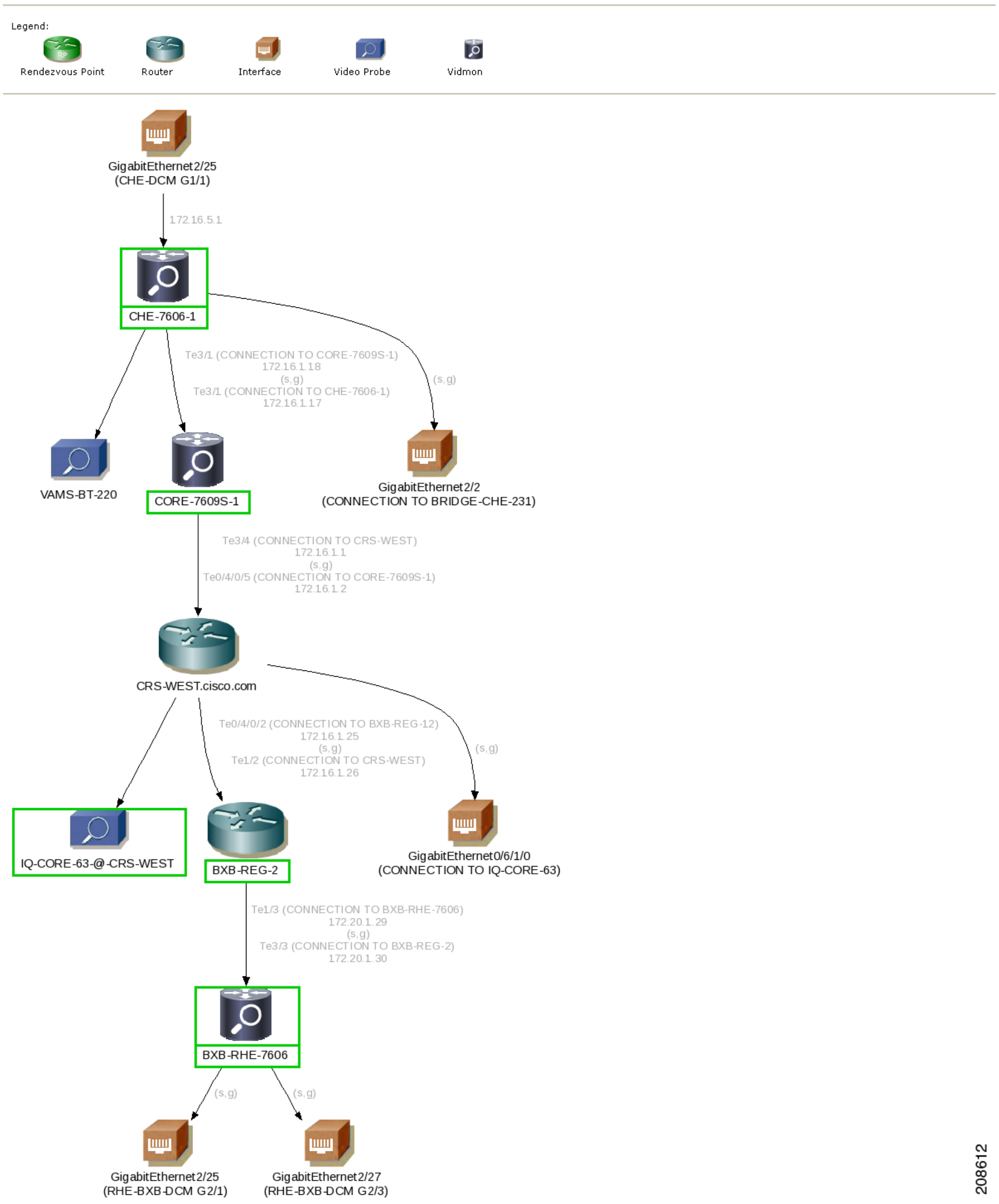
- **Flow Description**—The flow description at the top of the page indicates the unicast Group, Channel Name, Transport Description, Source IP and Source description, as configured in the CMM for the flow.
- **Trace Data Table**—Lists the routers, interfaces, and PIM neighbors that transport the multicast flow.
- **Video Probe Data Table**—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**—Lists all 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**—Displays 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.

The bottom of the trace display shows a topology map of the devices involved in the flow, as shown in Figure 3-37.

Figure 3-37 CMM Multicast Flow Trace: Topology Map



Viewing Events in the VidMon Event Views

To view custom VidMon event views:

Step 1 From the Video Assurance Management menu, click the plus sign (+) next to **Video Assurance Management**.

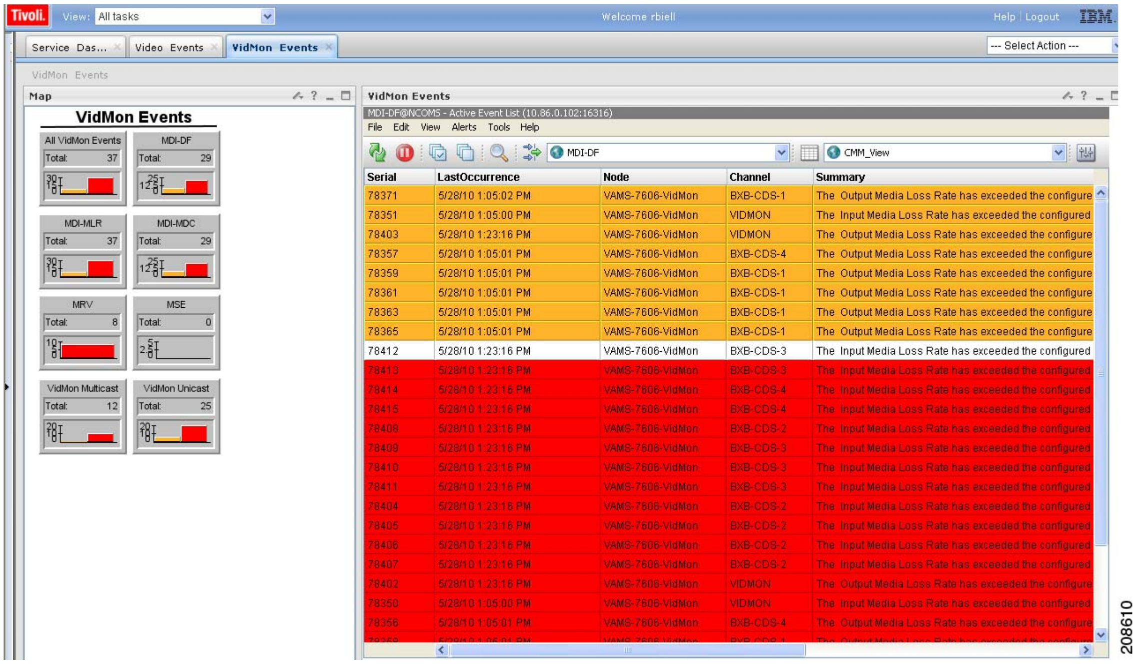
The Video Assurance Management menu appears.

Step 2 Click the plus sign (+) next to **Video Fault**.

Step 3 Click **VidMon Events**.

The Events Views page for the VidMon events appears. Figure 3-38 shows the event views for Video Events.

Figure 3-38 VidMon Events Views



Serial	LastOccurrence	Node	Channel	Summary
78371	5/28/10 1:05:02 PM	VAMS-7606-VidMon	BXB-CDS-1	The Output Media Loss Rate has exceeded the configure
78351	5/28/10 1:05:00 PM	VAMS-7606-VidMon	VIDMON	The Input Media Loss Rate has exceeded the configured
78403	5/28/10 1:23:16 PM	VAMS-7606-VidMon	VIDMON	The Output Media Loss Rate has exceeded the configure
78357	5/28/10 1:05:01 PM	VAMS-7606-VidMon	BXB-CDS-4	The Output Media Loss Rate has exceeded the configure
78359	5/28/10 1:05:01 PM	VAMS-7606-VidMon	BXB-CDS-1	The Output Media Loss Rate has exceeded the configure
78361	5/28/10 1:05:01 PM	VAMS-7606-VidMon	BXB-CDS-1	The Output Media Loss Rate has exceeded the configure
78363	5/28/10 1:05:01 PM	VAMS-7606-VidMon	BXB-CDS-1	The Output Media Loss Rate has exceeded the configure
78365	5/28/10 1:05:01 PM	VAMS-7606-VidMon	BXB-CDS-1	The Output Media Loss Rate has exceeded the configure
78412	5/28/10 1:23:16 PM	VAMS-7606-VidMon	BXB-CDS-3	The Input Media Loss Rate has exceeded the configured
78413	5/28/10 1:23:16 PM	VAMS-7606-VidMon	BXB-CDS-3	The Input Media Loss Rate has exceeded the configured
78414	5/28/10 1:23:16 PM	VAMS-7606-VidMon	BXB-CDS-4	The Input Media Loss Rate has exceeded the configured
78415	5/28/10 1:23:16 PM	VAMS-7606-VidMon	BXB-CDS-4	The Input Media Loss Rate has exceeded the configured
78408	5/28/10 1:23:16 PM	VAMS-7606-VidMon	BXB-CDS-2	The Input Media Loss Rate has exceeded the configured
78409	5/28/10 1:23:16 PM	VAMS-7606-VidMon	BXB-CDS-3	The Input Media Loss Rate has exceeded the configured
78410	5/28/10 1:23:16 PM	VAMS-7606-VidMon	BXB-CDS-3	The Input Media Loss Rate has exceeded the configured
78411	5/28/10 1:23:16 PM	VAMS-7606-VidMon	BXB-CDS-3	The Input Media Loss Rate has exceeded the configured
78404	5/28/10 1:23:16 PM	VAMS-7606-VidMon	BXB-CDS-2	The Input Media Loss Rate has exceeded the configured
78405	5/28/10 1:23:16 PM	VAMS-7606-VidMon	BXB-CDS-2	The Input Media Loss Rate has exceeded the configured
78406	5/28/10 1:23:16 PM	VAMS-7606-VidMon	BXB-CDS-2	The Input Media Loss Rate has exceeded the configured
78407	5/28/10 1:23:16 PM	VAMS-7606-VidMon	BXB-CDS-2	The Input Media Loss Rate has exceeded the configured
78402	5/28/10 1:23:16 PM	VAMS-7606-VidMon	VIDMON	The Output Media Loss Rate has exceeded the configure
78350	5/28/10 1:05:00 PM	VAMS-7606-VidMon	VIDMON	The Input Media Loss Rate has exceeded the configured
78356	5/28/10 1:05:01 PM	VAMS-7606-VidMon	BXB-CDS-4	The Output Media Loss Rate has exceeded the configure

The left part of the display shows monitor boxes for the selected event type. Each monitor box shows a bar graph indicating the number events in each severity level for the event category.

The CMM Events views include:

- **All VidMon Events**—Shows all VidMon events.
- **MDI-DF**—Shows Delay Factor (DF) events.
- **MDI-MLR**—Shows Media Loss Rate (MLR) events.
- **MDI-MDC**—Shows Media Discontinuity Counter (MDC) events.
- **MRV**—Shows Media Rate Variation (MRV) events.
- **MSE**—Shows Media Stop Events (MSE).
- **VidMon Multicast**—Shows VidMon events from multicast VidMon flows.
- **VidMon Unicast**—Shows VidMon events from unicast VidMon flows.

Step 4 To see the events in a CMM event view, click the monitor box for the event class.

For example, click the monitor box for **MDI-DF** to see DF events.

Step 5 To view the details of an event, double-click on the row for the event.

A table giving detailed field information for the event appears.

Step 6 To troubleshoot the event in CMM, right-click the event, and from the Alerts menu, choose **VAMS Tools > Launch CMM** or choose **VAMS Tools > Launch Flowtrace**.

Step 7 To view the details of an event, double-click on the row for the event.

A table giving detailed field information for the event appears.

Monitoring Video Events

This section describes:

- Monitoring Video Events in the Service Dashboard, page 6-38
- Viewing Events in the Video Events View, page 6-38

Monitoring Video Events in the Service Dashboard

Video events are events sent to TIP/TNSM from a video probe that is monitored by CMM. To view video events in the service dashboard.

Step 1 On the Video Assurance Management menu, click **Service Dashboard**.

The Service Dashboard appears:

The Service Tree shows a list of the configured video services in your network.

Step 2 Left-click on a a service on the Service Tree directory browser at the left of the page

- The Service Viewer shows a service map for the elected service.
- The Service Details window shows an event list for the service.

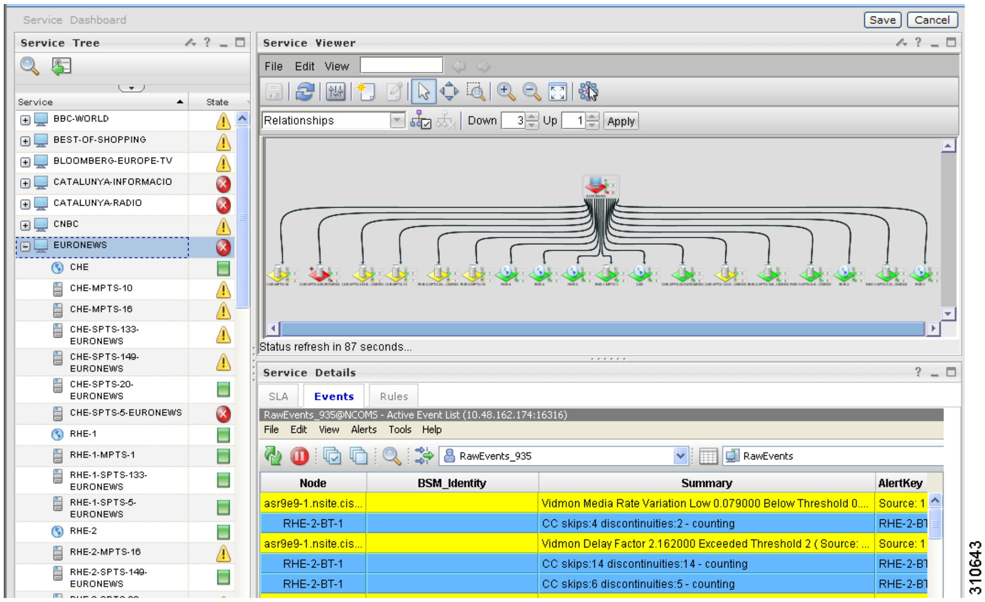
The devices in the service topology are listed in the Service Tree directory.

Step 3 Click on a device or service component to see the service map for the device.

The Service Viewer shows a service map for the service. If there are faults, such as video alarms, the device is highlighted in red. In the event list in the Service Details area, fault events are highlighted in red.

Figure 3-39 shows the Service Tree, Service Viewer, and Service Details window for a service called *EURONEWS*.

Figure 3-39 Service Dashboard for a High Level Service



Service	State
BBC-WORLD	⚠
BEST-OF-SHOPPING	⚠
BLOOMBERG-EUROPE-TV	⚠
CATALUNYA-INFORMACIO	☒
CATALUNYA-RADIO	☒
CNBC	⚠
EURONEWS	☒
CHE	🟩
CHE-MPTS-10	⚠
CHE-MPTS-16	⚠
CHE-SPTS-133-EURONEWS	⚠
CHE-SPTS-149-EURONEWS	⚠
CHE-SPTS-20-EURONEWS	🟩
CHE-SPTS-5-EURONEWS	☒
RHE-1	🟩
RHE-1-MPTS-1	🟩
RHE-1-SPTS-133-EURONEWS	🟩
RHE-1-SPTS-5-EURONEWS	🟩
RHE-2	🟩
RHE-2-MPTS-16	⚠
RHE-2-SPTS-149-EURONEWS	🟩

Status refresh in 87 seconds...

RawEvents_935@NCOMS - Active Event List (10.48.162.174:16316)

Node	BSM_Identity	Summary	AlertKey
asr9e9-1.nsite.cis...		Vidmon Media Rate Variation Low 0.079000 Below Threshold 0....	Source: 1
RHE-2-BT-1		CC skips:4 discontinuities:2 - counting	RHE-2-BT
asr9e9-1.nsite.cis...		Vidmon Delay Factor 2.162000 Exceeded Threshold 2 (Source: ...	Source: 1
RHE-2-BT-1		CC skips:14 discontinuities:14 - counting	RHE-2-BT
RHE-2-BT-1		CC skips:6 discontinuities:5 - counting	RHE-2-BT

Step 4 To see the devices associated with the selected video service, click on the plus sign (+) next to the service name.

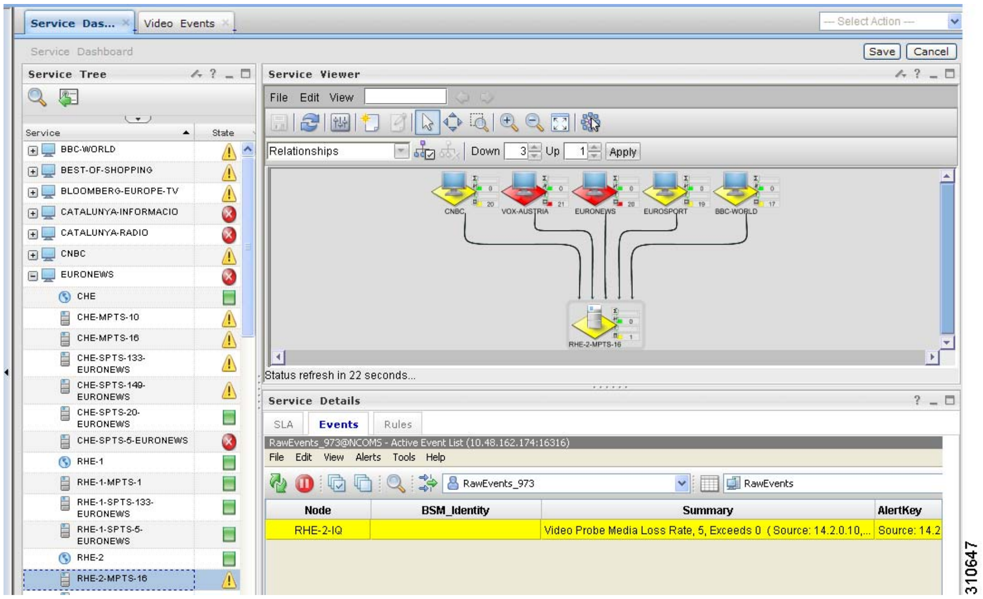
The devices in the service topology are listed in the Service Tree directory.

Step 5 Click on a device or service component, such as a channel associated with a video service, to see the service map for the device.

The Service Viewer shows a service map for the device. If there are faults, such as VidMon alarms, the device is highlighted in red or in yellow. In the event list in the Service Details area, fault events are highlighted in red.

Figure 3-40 shows a Service Map and fault events for a stream called *RHE-2-MPTS-16,* which is associated with the *EURONEWS* service and four other channel services.

Figure 3-40 Viewing VidMon Events in the Service Dashboard



Status refresh in 22 seconds...

RawEvents_973@NCOMS - Active Event List (10.48.162.174:16316)

Node	BSM_Identity	Summary	AlertKey
RHE-2-IQ		Video Probe Media Loss Rate, 5, Exceeds 0 (Source: 14.2.0.10,...	Source: 14.2

The event list shown in Figure 3-40 shows the following event from a video events from a BridgeTech video probe:

Vidmon Probe Media Loss Rate Exceeds 0—Video probe event generated by an IQ probe monitored by CMM when the media loss rate (MLR) on a monitored device exceeds a threshold.

Step 6 To view details about an event, highlight the event and right click on it.

Step 7 To launch CMM to troubleshoot the event, right click on the event and choose **VAMS Tools > Launch CMM** or **VAMS Tools > Launch Flowtrace**.

The CMM login screen appears.

Step 8 Log in to CMM and go to the appropriate menu to troubleshoot the event.

Viewing Events in the Video Events View

To view custom video event views:

Step 1 From the Video Assurance Management menu, click the plus sign (+) next to **Video Assurance Management**.

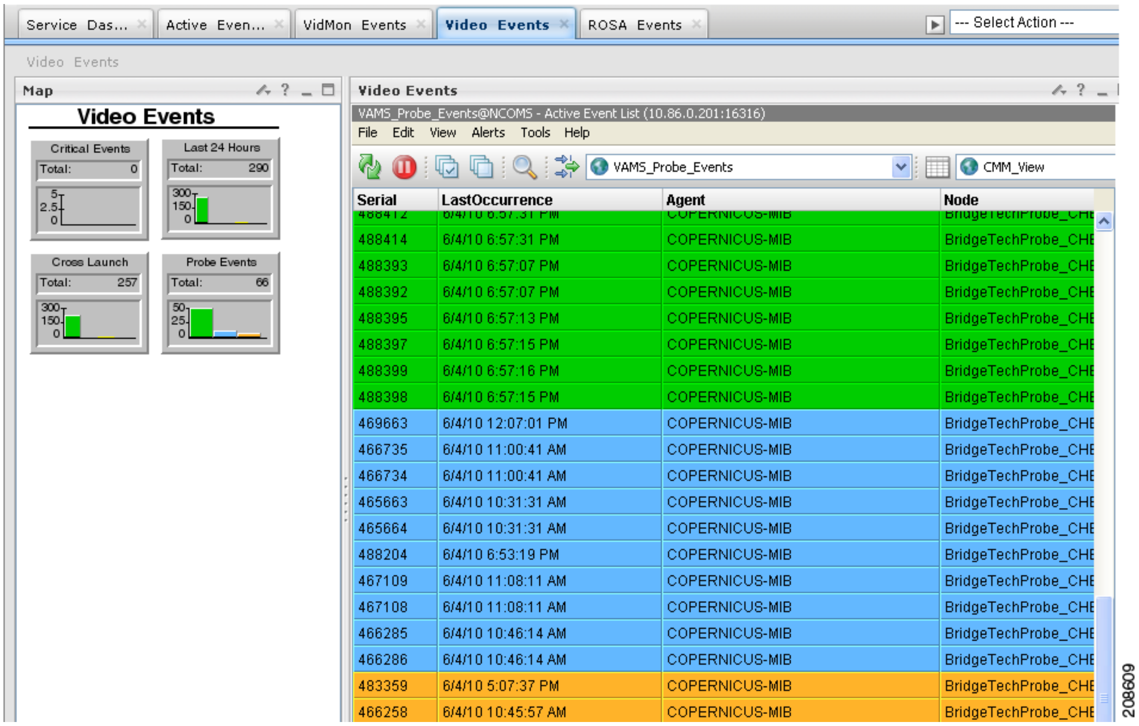
The Video Assurance Management menu appears.

Step 2 Click the plus sign (+) next to **Video Fault**.

Step 3 Click **Video Events**.

The Events Views page for the VidMon events appears. Figure 3-41 shows the event views for Video Events.

Figure 3-41 Video Events Views



Serial	LastOccurrence	Agent	Node
488412	6/4/10 6:57:31 PM	COPERNICUS-MIB	BridgeTechProbe_CHE
488414	6/4/10 6:57:31 PM	COPERNICUS-MIB	BridgeTechProbe_CHE
488393	6/4/10 6:57:07 PM	COPERNICUS-MIB	BridgeTechProbe_CHE
488392	6/4/10 6:57:07 PM	COPERNICUS-MIB	BridgeTechProbe_CHE
488395	6/4/10 6:57:13 PM	COPERNICUS-MIB	BridgeTechProbe_CHE
488397	6/4/10 6:57:15 PM	COPERNICUS-MIB	BridgeTechProbe_CHE
488399	6/4/10 6:57:16 PM	COPERNICUS-MIB	BridgeTechProbe_CHE
488398	6/4/10 6:57:15 PM	COPERNICUS-MIB	BridgeTechProbe_CHE
469663	6/4/10 12:07:01 PM	COPERNICUS-MIB	BridgeTechProbe_CHE
466735	6/4/10 11:00:41 AM	COPERNICUS-MIB	BridgeTechProbe_CHE
466734	6/4/10 11:00:41 AM	COPERNICUS-MIB	BridgeTechProbe_CHE
465663	6/4/10 10:31:31 AM	COPERNICUS-MIB	BridgeTechProbe_CHE
465664	6/4/10 10:31:31 AM	COPERNICUS-MIB	BridgeTechProbe_CHE
488204	6/4/10 6:53:19 PM	COPERNICUS-MIB	BridgeTechProbe_CHE
467109	6/4/10 11:08:11 AM	COPERNICUS-MIB	BridgeTechProbe_CHE
467108	6/4/10 11:08:11 AM	COPERNICUS-MIB	BridgeTechProbe_CHE
466285	6/4/10 10:46:14 AM	COPERNICUS-MIB	BridgeTechProbe_CHE
466286	6/4/10 10:46:14 AM	COPERNICUS-MIB	BridgeTechProbe_CHE
483359	6/4/10 5:07:37 PM	COPERNICUS-MIB	BridgeTechProbe_CHE
466258	6/4/10 10:45:57 AM	COPERNICUS-MIB	BridgeTechProbe_CHE

The left part of the display shows monitor boxes for the selected event type. Each monitor box shows a bar graph indicating the number events in each severity level for the event category.

The Video Events views include:

- **Critical Events**—Includes events with a severity level of critical
- **Last 24 Hours**—Shows video events for the last 24 hours,
- **Cross Launch Events**—Shows events indicating a video probe has been started.
- **Probe Events**—Shows events from video probes.

Step 4 To see the events in a video event view, click the monitor box for the event class.

For example, click the monitor box for **Probe Events** to see video probe events.

Step 5 To view the details of an event, double-click on the row for the event.

A table giving detailed field information for the event appears.

Step 6 To troubleshoot the event in CMM, right-click the event, and from the Alerts menu, choose **VAMS Tools > Launch CMM** or choose **VAMS Tools > Launch Flowtrace**.

Step 7 To view the details of an event, double-click on the row for the event.

A table giving detailed field information for the event appears.

Step 8 To view the details of an event, double-click on the row for the event.

A table giving detailed field information for the event appears.

Viewing Network Fault Events

This section describes how to view network fault events.

Viewing Events in the ANA Event Views

Step 1 Log in to IBM TIP/TBSM.

The main TBSM window appears.

Step 2 Click the plus sign (+) next to **Video Assurance Management**.

The Video Assurance Management menu appears.

Step 3 Click the plus sign (+) next to **Network Fault**.

The Network Fault menu appears.

Step 4 Click **ANA Events**.

The Events Views page for ANA events appears.

The left part of the display shows monitor boxes for the selected event type. Each monitor box shows a bar graph indicating the number events in each severity level for the event category.

The ANA Events views include:

- **All Events**—Shows all ANA events.
- **ANA Tickets**—Shows ANA tickets.
- **Status Events**—ANA status events.

Step 5 To see the events in a video event view, click the monitor box for the event class.

For example, click the monitor box for **ANA Tickets** to see ANA ticket events.

Step 6 To view the details of an event, double-click on the row for the event.

A table giving detailed field information for the event appears.

.

Viewing All Events

Step 1 Log in to IBM TIP/TBSM.

The main TBSM window appears.

Step 2 Click the plus sign (+) next to **Video Assurance Management**.

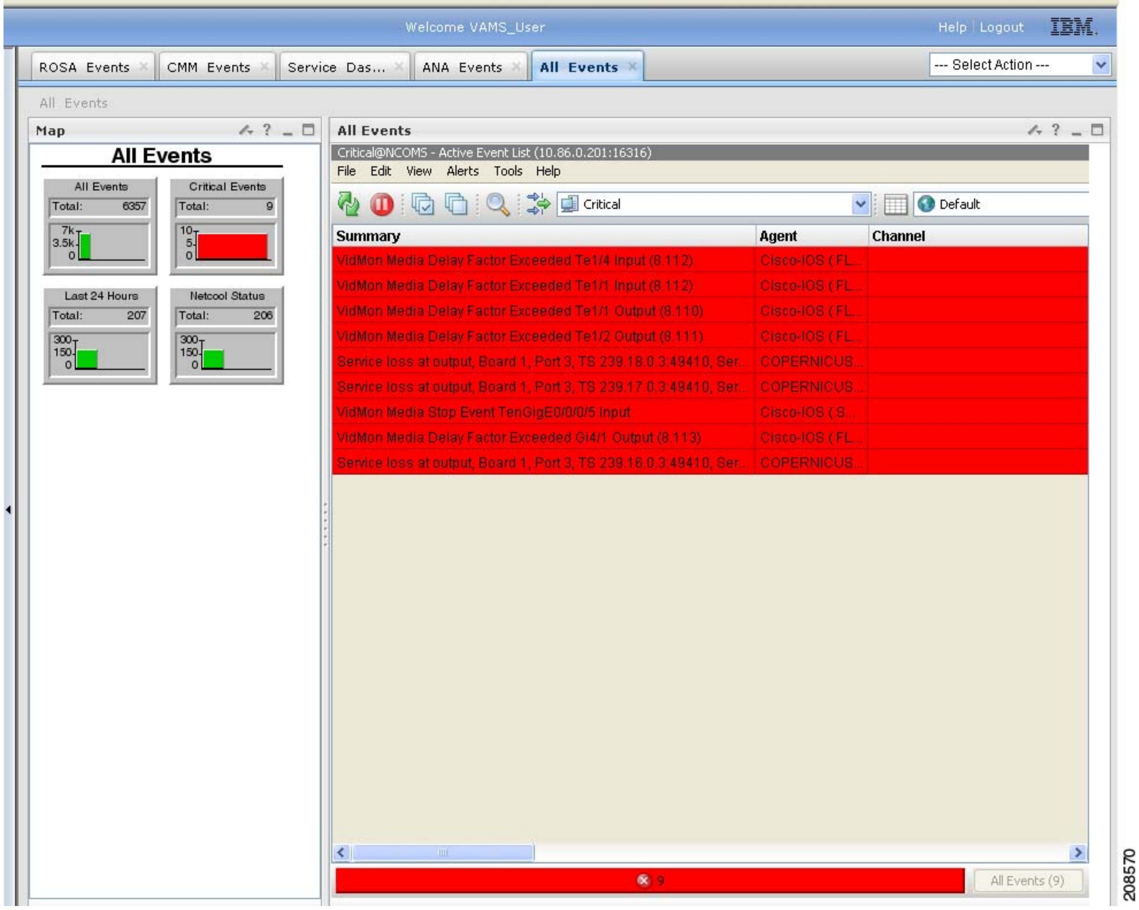
Step 3 Click the plus sign (+) next to **Network Fault**.

The Network Fault menu appears.

Step 4 Click **All Events**.

The Events Views page for all events appears. Figure 3-42 shows the event views for all events.

Figure 3-42 All Events Views



All Events — Total: 6357

Critical Events — Total: 9

Last 24 Hours — Total: 207

Netcool Status — Total: 206

Critical@NCOMS - Active Event List (10.86.0.201:16316)

Summary	Agent	Channel
VidMon Media Delay Factor Exceeded Te1/4 Input (8.112)	Cisco-IOS (FL...	
VidMon Media Delay Factor Exceeded Te1/1 Input (8.112)	Cisco-IOS (FL...	
VidMon Media Delay Factor Exceeded Te1/1 Output (8.110)	Cisco-IOS (FL...	
VidMon Media Delay Factor Exceeded Te1/2 Output (8.111)	Cisco-IOS (FL...	
Service loss at output, Board 1, Port 3, TS 239.18.0.3:49410, Ser...	COPERNICUS...	
Service loss at output, Board 1, Port 3, TS 239.17.0.3:49410, Ser...	COPERNICUS...	
VidMon Media Stop Event TenGigE0/0/0/5 Input	Cisco-IOS (S...	
VidMon Media Delay Factor Exceeded Gi4/1 Output (8.113)	Cisco-IOS (FL...	
Service loss at output, Board 1, Port 3, TS 239.16.0.3:49410, Ser...	COPERNICUS...	

The left part of the display shows monitor boxes for the selected event type. Each monitor box shows a bar graph indicating the number events in each severity level for the event category.

The All Events views include:

- **All Events**—Includes all network events.
- **Critical Events**—Includes events with a severity level of critical.
- **Last 24 Hours**—Shows network events for the last 24 hours,
- **Netcool Status**—Shows Netcool Probewatch events, events indicating that a process has connected from a Netcool device, and so on.

Step 5 To see the events in a specific event view, click the monitor box for the event class.

For example, click the monitor box for **Netcool Status** to see Netcool status events.

Step 6 To view the details of an event, double-click on the row for the event.

A table giving detailed field information for the event appears.

Step 7 To troubleshoot the event in CMM, right-click the event, and from the Alerts menu, choose **VAMS Tools > Launch CMM** or choose **VAMS Tools > Launch Flowtrace**.

Step 8 To view the details of an event, double-click on the row for the event.

A table giving detailed field information for the event appears.

.

Troubleshooting with Cisco ANA

Troubleshooting with Cisco ANA requires an understanding of the Cisco ANA fault-management system. You should also understand how to use ANA NetworkVision and ANA EventVision.

This section contains:

- Fault Management, page 3-49
- ANA NetworkVision, page 3-50
- ANA EventVision, page 3-50

Fault Management

Table 3-2 highlights important aspects of the fault management system in Cisco ANA.

Table 3-2 Cisco ANA Fault Management

Troubleshooting Area	Description and Reference
Fault detection and isolation	Describes: • How the various VNEs use reachability to check connectivity with the NEs. • Basic alarm sources that indicate problems in the network. • What happens when a VNE with associated open alarms shuts down. • The integrity service tests that run on the gateway and the units. For detailed information about working with fault detection and isolation, see the *Cisco Active Network Abstraction User Guide, 3.7,* viewable online at: http://www.cisco.com/en/US/docs/net_mgmt/active_network_abstraction/3.7/user/guide/User_Guide_3_7.html
Casualty correlation and root-cause analysis	Describes: • Enabling or disabling port-down, port-up, link-down, and link-up alarms. • The root-cause correlation concept. • The root-cause alarm and weights concepts. • Correlation by flow and correlation by key. For detailed information about working with casualty correlation and root-cause analysis, see the *Cisco Active Network Abstraction User Guide, 3.7,* viewable online at: http://www.cisco.com/en/US/docs/net_mgmt/active_network_abstraction/3.7/user/guide/User_Guide_3_7.html
Advanced correlation scenarios	Describes alarms that use advanced correlation logic on top of the root cause analysis flow. For detailed information about working with advanced correlation scenarios, see the *Cisco Active Network Abstraction User Guide, 3.7,* viewable online at: http://www.cisco.com/en/US/docs/net_mgmt/active_network_abstraction/3.7/user/guide/User_Guide_3_7.html

ANA NetworkVision

Network administrators use Cisco ANA NetworkVision to manage, fulfill, plan, and assure the integrity of network resources. Table 3-3 lists important aspects of using Cisco ANA NetworkVision for troubleshooting.

Table 3-3 Cisco ANA NetworkVision

Troubleshooting Area	Description and Reference
Working with ANA tickets	Cisco ANA NetworkVision: • Correlates alarms, and enables you to view tickets and ticket properties, including correlated alarms, active alarms, and alarm history. • Describes ticket management and the different ways in which a ticket displays in the ticket pane, depending on the status or severity of the alarm. For detailed information about working with tickets, see the *Cisco Active Network Abstraction User Guide, 3.7,* viewable online at: http://www.cisco.com/en/US/docs/net_mgmt/active_network_abstraction/3.7/user/guide/User_Guide_3_7.html
Working with ANA PathTracer	You use the Cisco ANA PathTracer to view a network path between two network objects in packet-switched networks such as Ethernet and IP. For detailed information about working with the Cisco ANA PathTracer, see the *Cisco Active Network Abstraction User Guide, 3.7,* viewable online at: http://www.cisco.com/en/US/docs/net_mgmt/active_network_abstraction/3.7/user/guide/User_Guide_3_7.html

ANA EventVision

You use Cisco ANA EventVision to view, filter, and display the properties of specific events. Table 3-4 lists important aspects of using Cisco ANA EventVision for troubleshooting.

Table 3-4 Cisco ANA EventVision

Troubleshooting Area	Description and Reference
Viewing events	Events appear in different event categories in the ANA EventVision. For detailed information about displaying events, see the *Cisco Active Network Abstraction User Guide, 3.7,* viewable online at: http://www.cisco.com/en/US/docs/net_mgmt/active_network_abstraction/3.7/user/guide/User_Guide_3_7.html
Working with EventVision	For detailed information about working with EventVision, see the *Cisco Active Network Abstraction User Guide, 3.7,* viewable online at: http://www.cisco.com/en/US/docs/net_mgmt/active_network_abstraction/3.7/user/guide/User_Guide_3_7.html

APPENDIX A

Trap Definitions

Cisco VAMS 3.1 supports traps (alarms) for:

- CMM, page A-1
- ROSA NMS Events, page A-3
- Cisco 7600, Catalyst 6500, CRS-1, and Catalyst 4948 Devices, page A-4
- Bridge Technologies Video Probe, page A-4
- IneoQuest Video Probe, page A-5
- Mixed Signals Video Probe, page A-6

CMM

Alarm Message Text[1]	Severity
The Layer 3 multicast bandwidth percentage on an interface has exceeded the percentage threshold.	Minor
The designated router for an interface has been detected.	Warning
One or more parameters of a multicast route entry has changed.	Warning
The rendezvous point did not respond to a *sysUpTime* poll.	Information
The Layer 3 multicast b/s rate for a (source, group) has exceeded the high b/s rate threshold.	Minor
The application has rediscovered a router.	Information
The rendezvous point responded to a *sysUpTime* poll.	Information
The designated router for an interface has been removed.	Major
That a health check has detected one or more failures.	Minor
The Layer 3 multicast bandwidth percentage on an interface has exceeded the percentage threshold.	Information
The Layer 3 multicast Reverse Path Forwarding (RPF) failures for a (source, group) that is now being measured at a value above the low threshold.	Minor
The unicast or multicast routing table has changed compared to the initial baseline.	Information
The video probe media loss rate (MLR) for a video flow has exceeded the configured threshold.	Major

Alarm Message Text[1] (continued)	Severity
The multicast group limit exceeded the configured threshold on the rendezvous point.	Minor
A Layer 2 port multicast p/s low threshold is exceeded.	Minor
The Layer 3 multicast b/s rate for a (source, group) has exceeded the low b/s rate threshold.	Minor
A rendezvous point that did not respond to a poll.	Information
The Layer 3 multicast p/s rate for a (source, group) has exceeded the set threshold when measured between the routers on a multicast forwarding tree.	Warning
A (source, group) no longer exists on the router.	Major
One or more parameters of a unicast route entry has changed.	Information
A multicast forwarding tree that has reverted to its baseline.	Warning
The Layer 3 multicast b/s rate for a (source, group) has exceeded the high b/s rate threshold.	Cleared
The multicast p/s rate for the aggregate multicast traffic on a Layer 2 port, which is now being measured at a value between the high and low p/s rate thresholds.	Cleared
A (source, group) has been removed from the rendezvous point since the poll.	Major
Notification that the video probe delay factor (DF) for a video flow has exceeded the configured threshold.	Major
A (source, group) has been added to the rendezvous point since the last poll.	Information
A Layer 2 port multicast p/s high threshold is exceeded.	Minor
The multicast bandwidth percentage for the aggregate multicast traffic on an interface is now at a value lower than the high threshold.	Cleared
The Layer 3 multicast p/s rate for a (source, group) that is now being measured at a value between the high and low p/s rate thresholds.	Cleared
A multicast group that has more than a single source sending to it.	Major
A multicast forwarding tree that has changed from its baseline.	Critical
The Layer 3 multicast p/s rate for a (source, group) has exceeded the high p/s rate threshold.	Minor
The Layer 3 multicast p/s rate for a (source, group) has exceeded the low p/s rate threshold.	Minor
The designated router for an interface has changed.	Warning
A multicast sender on the default multicast distribution tree (MDT) for a particular VPN routing/forwarding (VRF) instance has been removed.	Warning
A VRF on a multicast VPN (MVPN) Provider Edge (PE) router has been removed.	Warning
A default MDT address for a VRF has been configured on a PE that does not match the configuration on the rest of the PEs.	Warning
The number interfaces associated with a VRF on an MVPN PE has changed.	Warning
A VRF on an MVPN PE has been added.	Warning
A new multicast sender on the default MDT for a particular VRF has been detected.	Warning
The number of VRFs configured on an MVPN PE has changed.	Warning

[1] See the Glossary for abbreviations used in alarm message text.

ROSA NMS Events

Alarm Message Text[1]	Severity
Service Loss, Board *xx*, Port *yy*, TS *nnn.nnn.nnn.nnn*:, Service *z*: sssss where *xx* represents the board number, *yy* represents the port number, *nnn.nnn.nnn.nnn* indicates the IP multicast address for the Transport Stream, *z* represents the service number, and *sssss* represents the UDP port number.	Major
Service Loss at output, Board *xx*, Port *yy*, TS *nnn.nnn.nnn.nnn*:, Service *z*: sssss where *xx* represents the board number, *yy* represents the port number, *nnn.nnn.nnn.nnn* indicates the IP multicast address for the Transport Stream, *z* represents the service number, and *sssss* represents the UDP port number.	Major
Service in Backup (Service Loss), Board *xx*, Port *yy*, TS *nnn.nnn.nnn.nnn*:, Service *z*: sssss where *xx* represents the board number, *yy* represents the port number, *nnn.nnn.nnn.nnn* indicates the IP multicast address for the Transport Stream, *z* represents the service number, and *sssss* represents the UDP port number.	Major
PID Error, Board *xx*, Port *yy*, TS *nnn.nnn.nnn.nnn*:sssss where *xx* represents the board number, *yy* represents the port number, *nnn.nnn.nnn.nnn* indicates the IP multicast address for the Transport Stream, and *sssss* represents the UDP port number.	Major
TS Loss, Board *xx*, Port *yy*, TS *nnn.nnn.nnn.nnn*:, Service *z* where *xx* represents the board number, *yy* represents the port number, *nnn.nnn.nnn.nnn* indicates the IP multicast address for the Transport Stream, and *z* represents the service number.	Major
UDP Stream Loss, Board *xx*, Port *yy*, TS *nnn.nnn.nnn.nnn*:sssss, Service z where *xx* represents the board number, *yy* represents the port number, *nnn.nnn.nnn.nnn* indicates the IP multicast address for the Transport Stream, *sssss* represents the UDP port number, and *z* represents the service number	Major
CC Error, Board *xx*, Port *yy*, TS *nnn.nnn.nnn.nnn*:sssss, where *xx* represents the board number, *yy* represents the port number, *nnn.nnn.nnn.nnn* indicates the IP multicast address for the Transport Stream, and *sssss* represents the UDP port number.	Major

[1] See the Glossary for abbreviations used in alarm message text.

Cisco 7600, Catalyst 6500, CRS-1, and Catalyst 4948 Devices

Alarm Text Message [1]	Severity
PIM Neighbor loss	Major
PIM Interface down	Major
PIM Interface up	Clear
The number of multicast routes changed.	Information
The number of non-RPF drops exceeded threshold.	Minor

[1] See the Glossary for abbreviations used in alarm message text.

Bridge Technologies Video Probe

Ethernet Alarms

Alarm Message Text [1]	Severity
No signal: There has been no UDP packet for the predefined period of time (default 1 second)	Major
RTP duplicates: Number of duplicate IP packets (only if RTP)	Warning
RTP packet drop: Number of dropped IP packets (only if RTP headers are present)	Error
RTP out of order: Out-of-order IP-packet detections (requires RTP)	Warning
CC skips: Number of lost Transport Stream packets	Warning
MDI-DF >= err-thresh: The MDI Delay Factor exceeds the error-threshold	Error
MDI-DF >= warn-thresh: The MDI Delay Factor exceeds the warning-threshold	Warning
MDI-MLR>= err-thresh: The MDI Media Loss Rate exceeds the error-threshold	Error
MDI-MLR>= warn-thresh: The MDI Media Loss Rate exceeds the warning-threshold	Warning
TTL changed: The Time-to-Live field is changing	Error
TOS changed: The Type-Of-Service field is changing	Error
Multiple mcast sources: There are multiple multicast sources	Error

[1] See Glossary for abbreviations used in alarm message text.

ETR (290) Alarms

Alarm Message Text [1]	Severity
TS Sync: No TS Sync	Major
Sync byte: Sync byte error	Major
PAT: Program Allocation Table error	Major

Continuity: Continuity counter error	Major
PMT: Program Map Table error	Major
PID: Pid is missing	Major
Transport: Transport stream error indicator is set	Major
CRC: Table checksum error	Major
PCR: Program Map table error	Major
PCR accuracy	Major
PTS: Presentation Time Stamp error	Major
CAT: Conditional Access Table error	Major
NIT: Network Information Table error	Major
SI Rep Rate: Wrong repetition rate for SI table	Major
Buffer: Buffer error	Major
Unref PID: Pid is unreferenced	Major
SDT: Service Description Table error	Major
EIT: Event Information Table error	Major
RST: Running Status Table error	Major
TDT: Time Data Table error	Major
CA System: CA System error	Major
Pid checks: Pid check error	Major
Service checks: Service check error	Major
Interface checks: Input interface error	Major

[1] See Glossary for abbreviations used in alarm message text.

SYS (System) Events

Alarm Message Text [1]	Severity
Critical system errors: Enable this to view all critical system errors	Fatal
System errors: Enable this to view all system errors	Major
System info: Enable this to view system information messages	OK

[1] See Glossary for abbreviations used in alarm message text.

IneoQuest Video Probe

Alarm Message Text [1]	Severity
The network utilization on the primary port exceeds the threshold value.	Minor
User feedback event.	Information
The delay factor threshold crossover is detected.	Minor

Alarm Message Text [1] (continued)	Severity
A stream was lost for a period defined in the outage.	Major
A 15-minute monitored metric threshold crossover is detected.	Information
The Bit-Rate for a stream exceeds the threshold value.	Warning
The maximum RTP media loss period threshold crossover is detected.	Minor
A system fault condition occurred.	Minor
Software or config download.	Information
This trap is sent when link is lost.	Major
This event is sent every 15-Min to indicate the completion of an interval of system statistics.	Information
The PID bitrate threshold is crossed for a PID selected from the video characteristic template.	Minor
This trap is sent when the media loss threshold crossover is detected.	Minor
The minimum loss distance threshold crossover is detected.	Minor
The media loss threshold crossover is detected.	Minor
The multicast IGMP join time threshold crossover is detected.	Information
The stream alarms limit is reached for a 15-Minute period.	Information
The media link is established.	Information
A new flow has been detected by the system.	Information
The bit rate for a stream exceeds the threshold value.	Minor
A stream was lost for a period defined in the outage.	Major
The Minimum Bit-Rate threshold is crossed.	Warning
The ZAP time threshold crossover is detected.	Information

[1] See Glossary for abbreviations used in alarm message text.

Mixed Signals Video Probe

Alarm Message Text [1]	Severity
Table bit rate	Warning
Table detect	Warning
Table cycle time	Warning
PID bit rate	Warning
PID detect	Warning
PID discontinuity	Minor
PID audio silence	Minor
PID video freeze	Minor
PID table bit rate	Warning
PID table detect	Warning

Alarm Message Text [1] (continued)	Severity
PID table cycle time	Warning
Program bit rate	Warning
Program detect	Warning
Program discontinuity	Warning
Program audio silence	Warning
Program video freeze	Warning
Program PCR interval	Warning
Program PCR jitter	Warning
Program table PMT bit rate	Warning
Program table PMT detect	Warning
Program table PMT cycle time	Warning
DSM-CC DII bit rate	Warning
DSM-CC DII detect	Warning
DSM-CC DII cycle time	Warning
DSM-CC DC bit rate	Warning
DSM-CC DC detect	Warning
DSM-CC DC cycle time	Warning
Carousel bit rate	Warning
Carousel source file add-delete	Warning
Carousel source DSM-CC DII bit rate	Warning
Carousel source DSM-CC DII detect	Warning
Carousel source DSM-CC DII cycle time	Warning
Carousel source DSM-CC DC bit rate	Warning
Carousel source DSM-CC DC detect	Warning
Carousel source DSM-CC DC cycle time	Warning
Carousel file bit rate	Warning
Carousel file detect	Warning
Carousel file cycle time	Warning
Carousel file change	Warning
Port IP arrival interval	Warning
Port delay factor	Warning

[1] See Glossary for abbreviations used in alarm message text.

APPENDIX B

End User License Agreement Supplement

END USER LICENSE AGREEMENT SUPPLEMENT FOR CISCO SYSTEMS NETWORK MANAGEMENT SOFTWARE: Cisco Video Assurance Management Solution Software

Dear Customer,

This End User License Agreement Supplement ("Supplement") contains additional terms and conditions for the Software Product licensed under the End User License Agreement ("EULA") between you and Cisco (collectively, the "Agreement"). Capitalized terms used in this Supplement but not defined will have the meanings assigned to them in the EULA. To the extent that there is a conflict between the terms and conditions of the EULA and this Supplement, the terms and conditions of this Supplement will take precedence.

In addition to the limitations set forth in the EULA on your access and use of the Software, you agree to comply at all times with the terms and conditions provided in this Supplement, including any restrictions on access and use of the Software. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT (COLLECTIVELY, "CUSTOMER") TO THE AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE (INCLUDING ANY UNOPENED CD PACKAGE AND ANY WRITTEN MATERIALS) FOR A FULL REFUND, OR, IF THE SOFTWARE AND WRITTEN MATERIALS ARE SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM CISCO OR AN AUTHORIZED CISCO RESELLER, AND APPLIES ONLY IF YOU ARE THE ORIGINAL END USER PURCHASER.

For purposes of the SEULA, the Product name and the Product description you have ordered is one or more of the product SKUs for the VAMS component products.

For purposes of this Supplement, the following definitions will apply:

"Cisco Video Assurance Management Solution" is software licensed to manage the assurance of video in a network environment. The Software is licensed per device managed.

ADDITIONAL LICENSE RESTRICTIONS

- Installation and Use. The Software components are provided to Customer solely to install, update, supplement, or replace existing functionality of the applicable Network Management Software product.

Cisco Video Assurance Management Software is licensed and deployed such that it may be loaded on multiple processors. Customers must purchase software licenses for each device family to be managed in the Customer's environment.

- Customer may install and use following Software components:
  - Cisco Video Assurance Management Solution - Video extensions to 4948 (G2) VNE license: Customer may install and run the Software on unlimited number of processors in the Customer's network environment, subject to a limitation on the number of 4948 devices managed that equals the number of ANA Group 2 licenses purchased from Cisco and in effect.
  - Cisco Video Assurance Management Solution - Video extensions to 7600 (G3) VNE license: Customer may install and run the Software on unlimited number of processors in the Customer's network environment subject to a limitation on the number of 7600 devices managed that equals the number of ANA Group 3 licenses purchased from Cisco and in effect.
  - Cisco Video Assurance Management Solution - Video extensions to CRS-1 (G5) VNE license: Customer may install and run the Software on unlimited number of processors in the Customer's network environment, subject to a limitation on the number CRS-1(G5) devices managed that equals the number of ANA Group 5 licenses purchased from Cisco and in effect.
  - Cisco Video Assurance Management Solution - Video extensions to CRS-1 (G6) VNE license: Customer may install and run the Software on unlimited number of processors in the Customer's network environment, subject to a limitation on the number of CRS-1(G6) devices managed that equals the number of ANA Group 6 licenses purchased from Cisco and in effect.
  - Cisco Video Assurance Management Solution - Cisco Multicast Manager VNE license: Customer may install and run the Software on unlimited number of processors in the Customer's network environment to enable ANA to interface with Cisco Multicast Manager installations in the Customer's network environment.
  - Cisco Video Assurance Management Solution - IneoQuest Video Probe VNE license: Customer may install and run the Software on unlimited number of processors in the Customer's network environment, subject to a limitation on the number of IneoQuest probe devices managed that equals the number of IneoQuest licenses purchased from Cisco and in effect.
  - Cisco Video Assurance Management Solution - Mixed Signals Video Probe VNE license: Customer may install and run the Software on unlimited number of processors in the Customer's network environment, subject to a limitation on the number of Mixed Signals probe devices managed that equals the number of Mixed Signals licenses purchased from Cisco and in effect.
  - Cisco Video Assurance Management Solution - Tektronix Video Probe VNE license: Customer may install and run the Software on unlimited number of processors in the Customer's network environment, subject to a limitation on the number Tektronix probe devices managed that equals the number of Tektronix Video Probe licenses purchased from Cisco and in effect.
- Other license restrictions on software:
  - Cisco Video Assurance Management Solution - IneoQuest Video Probe license: Each license permits the Customer to manage one IneoQuest probe device.
  - Cisco Video Assurance Management Solution - Mixed Signals Video Probe RTU license: Each license permits the Customer to manage one Mixed Signals probe device.
  - Cisco Video Assurance Management Solution - Tektronix Video Probe license: Each license permits the Customer to manage one Tektronix probe device.
  - Reproduction and Distribution. Customer may not reproduce nor distribute Software.

DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS

Please see the Cisco Systems, Inc. End User License Agreement

GLOSSARY

A

Access privilege In computer security, the process of ensuring that only authorized users can access the resources of a computer system in authorized ways.

Activation script A command script that Cisco ANA applies to one or more VNEs to extend their configurations. You use Cisco ANA Command Builder to create activation scripts. The Cisco Video Assurance Management Solution runs an IPTV activation script on its VNEs.

Alarm An audible or visual signal at a device, such as a display station or printer, that is used to notify the user that a predefined condition exists.

Alarm Thresholding A mechanism by which Cisco ANA constantly monitors selected soft properties and generates an alarm every time they cross a user-defined threshold or violate a condition. See also Soft Properties.

ANA Active Network Abstraction. A Cisco resource management solution designed with a fully distributed OSS mediation platform which abstracts the network, its topology and its capabilities from the physical elements.

ANA EventVision ANA EventVision is a GUI application that serves as a browser for viewing and retrieving detailed information about the different types of system events and tickets that are generated within the Cisco ANA system. Monitoring EventVision helps predict and identify the sources of system problems, which assists in preventing future problems.

ANA Manage ANA Manage is a GUI tool in Cisco ANA that performs various system administration activities for simple system control.

Active Network Abstraction See ANA.

ANA NetworkVision ANA NetworkVision is the primary GUI for Cisco ANA. It is a surveillance tool providing total visibility for multi-vendor, multi-tier, multi-technology networks. It also supports fault and configuration functionality.

ANA NetworkVision supports the creation of multiple network maps to represent specific network views. Views can cover specific network segments, customer networks, or any other mix of network elements desired. Once the maps have been created, they are available for all connecting clients (with support for fine grained access privileges).

ASI Asynchronous serial interface.

ASR 9000 A Cisco carrier class routing solution that uses the Cisco IOS operating system, and which includes comprehensive network management capabilities, and a comprehensive set of Ethernet and Multiprotocol Label Switching (MPLS) operations, administration, and maintenance (OAM) capabilities. The ASR 9000 supports Cisco Video Monitoring VidMon capabilities.

Authentication In computer security, (1) verification of the identity of a user or the user's eligibility to access an object; (2) verification that a message has not been altered or corrupted; (3) a process that is used to verify the user of an information system or of protected resources.

Authorization In computer security, (1) the right granted to a user to communicate with or make use of a computer system; (2) the process of granting a user either complete or restricted access to an object, resource, or function.

Automation In IBM Tivoli/OMNIbus, the ObjectServer can respond automatically to specified alerts.

Autonomous Virtual Machine See AVM.

AVM Autonomous Virtual Machine. Java processes that provide the necessary distribution support platform for executing and monitoring multiple VNEs.

B

back-office The internal operations of an organization that are not accessible or visible to the general public.

back up To copy information to another location to ensure against loss of data. Contrast with restore.

C

Carrier Routing System-1 See CRS-1

Cisco 7600 A carrier-class edge router that offers integrated, high-density Ethernet switching, carrier-class Internet Protocol/Multiprotocol Label Switching (IP/MPLS) routing, and 10-Gb/s interfaces.Cisco 7600 ES+ line cards on the Cisco 7600 support VidMon.

Cisco Info Center Cisco Info Center is a service level management (SLM) system that collects enterprise-wide event information from many different network data sources and presents a simplified view of the event information to operators and administrators. Cisco Info Center is provided with the Cisco VAMS Solution, and includes the Object Server, Netcool Web GUI, Nckl, and Tivoli/Netcool Impact.

Cisco Multicast Manager A web-based network management application that simplifies the holistic discovery, visualization, monitoring, and troubleshooting of multicast networks. CMM is applicable to multiple system operators that use multicast to transport video over IP.

Configuration The machines, devices, and programs that make up a system, subsystem, or network.

CPU Central Processing Unit.

CRC Cyclic Redundancy Check. Error-checking technique in which the frame recipient calculates a remainder by dividing frame contents by a prime binary divisor and compares the calculated remainder to a value stored in the frame by the sending node.

CRS-1 Carrier Routing System-1. A Cisco large-scale core router for carrier networks.

Cyclic Redundancy Check See CRC.

D

DCM See Digital Content Manager.

Deduplication Deduplication (also known as record linkage) is a task of finding the same (duplicate) entry in multiple files. You use deduplication when merging two or more data sets. Deduplication is a useful tool when performing data mining tasks, where the data originated from different sources or different organizations.

Delay Factor See DF.

Deploy To place files or install software into an operational environment.

Designated Router See DR.

Device Any non-client, non-server part of a network managed by Tivoli software, including, but not limited to, cable set-top boxes and other pervasive devices.

DF Delay Factor. A time value indicating the amount of data that buffers must contain to eliminate jitter.

Digital Content Manager Cisco Digital Content Manager (DCM). A Cisco multiplexing appliance that allows processing of a high number of MPEG video streams and supports advanced MPEG processing functions such as content re-compression to lower bit rates, open loop statistical multiplexing, digital program insertion and scrambling.

Digital Storage Media - Command and Control See DSM-CC.

Digital Subscriber Line Access Multiplexer See DSLAM.

Digital Video Broadcast See DVB.

Discovery The automatic detection of a topology change, such as finding new and deleted nodes or links within a network topology, or such as finding storage resources and devices within a network that are not yet being monitored.

Domain A logical grouping of resources in a network for the purpose of common management and administration.

Domain name In the Internet suite of protocols, a name of a host system. A domain name consists of a sequence of subnames that are separated by a delimiter character. For example, Cisco.com.

DR Designated Router. A router in a multiaccess network that designates the originate network link advertisements and establishes adjacencies with all routers in the network.

Drools rules engine Drools rules engine is a general-purpose expert-system generator and combines rule-based techniques and object-oriented programming. It also provides a customizable mechanism to add decision support and data flow control functions to business applications.

Drools rules engine is based on an object-oriented paradigm and uses user-defined rules to perform pattern matching on different conditions. The rules are written in a Java-like syntax, and are organized into source files (known as a rule files), which are plain ASCII files.

DSLAM Digital Subscriber Line Access Multiplexer. A device that connects many digital subscriber lines to a network by multiplexing the DSL traffic onto one or more network trunk lines.

DSM-CC Digital Storage Media - Command and Control. A toolkit for developing control channels associated with MPEG-1 and MPEG-2 streams.

DVB Digital Video Broadcast. A European standard for digital television.

E

EMS Element Management System. A system that manages a network of elements.

Element Management System See EMS.

ETR-290 European Telecommunications Standards Institute Technical Report 290 (ETR-290), *Digital Video Broadcasting (DVB): Measurement Guidelines for DVB Systems* is a report produced by the European Broadcasting Union (EBU) that provides guidelines for measurements of video transmission and quality in DVB satellite, cable and terrestrial and related digital television systems, including Moving Picture Experts Group (MPEG)-2 transmission.

ETR-290 First Priority Alarms

Alarms that indicate that ETSI indicators listed in Table 5.2.1 in the ETR-290 specification—First priority: necessary for de-codability (basic monitoring)—are activated. These indicators indicate that a video transport stream (TS) is not decodable. The ETR-290 First Priority alarms include:

- **TS Loss**—The first byte of a Transport Stream packet header is the synchronization byte (0x47). A TS Loss error occurs when the synchronization byte in a sequence of at least two Transport Stream packets are not detected.
- **CC Error**—Indicates a discontinuity error in the MPEG TS structure for a particular video program.
- **Sync Byte Error**—The synchronization byte in a Transport Stream packet is not detected. A Transport Stream Loss alarm is also triggered.
- **PAT Error**—Occurs when the PMT reference in the Program Association Table (PAT) for the service is missing. A Service Loss alarm is also triggered.
- **PMT Error**—Occurs when the Program Map Table (PM) for the service is not available within a particular time interval or contains errors. A Service Loss alarm is also triggered.
- **PID Error**—A Packet ID (PID) error occurs when components with PMT reference are not found within a particular time interval. A Service Loss alarm is also triggered.

Event

Any significant change in the state of a system resource, network resource, or network application. An event can be generated for a problem, for the resolution of a problem, or for the successful completion of a task.

F

Field

The building block of which objects are composed. A field is characterized by a field name, a data type (integer, Boolean, character string, or enumerated value), and a set of flags that describe how the field is treated. A field can contain data only when it is associated with an object.

G

Gateway

In the IP community, an older term referring to a routing device. Today, the term *router* is used to describe nodes that perform this function, and *gateway* refers to a special-purpose device that performs an application layer conversion of information from one protocol stack to another.

H

HDD

Hard disk drive.

Health check

A report that shows the values over time of one or more metrics, which can be selected from one or more schemas, for one or more components. Typically, a health check shows time-delineated, diagnostic data that shows the fluctuation of key indicators.

Heartbeat Monitoring

See IP Multicast Heartbeat Monitoring.

Host A computer that is connected to a network (such as the Internet or an Systems Network Architecture [SNA] network) and provides an access point to the network. Also, depending on the environment, the host may provide centralized control of the network. The host can be a client, a server, or both a client and a server simultaneously.

HFC Hybrid Fiber-Coaxial. Technology being developed by the cable TV industry to provide two-way, high-speed data access to the home by using a combination of fiber optics and traditional coaxial cable.

Hybrid Fiber-Coaxial See HFC.

I

IBM Tivoli Network Services Manager See TBSM.

iVMS IP Video Management System (iVMS) from Ineoquest Technologies has been added to CMM 2.5 to provide real-time alerts to allow for rapid fault isolation of customer impacting video events.

ICMP Internet Control Message Protocol. Network layer Internet protocol that reports errors and provides other information relevant to IP packet processing. Documented in RFC 792.

IGMP Internet Group Management Protocol. Used by IP hosts to report their multicast group memberships to an adjacent multicast router.

Impact A component of the Cisco Info Center application, IBM/Tivoli Netcool/Impact provides a common platform for data access that circumvents organizational boundaries. In the Cisco VAMS environment, Netcool/Impact collects data from devices and applications used in the video headend and video transport network and correlates the data into events that are tailored to the IP Multicast video processing environment.

Internet Control Message Protocol See ICMP.

Internet Group Management Protocol See IGMP.

Internet Protocol Television See IPT.

Internet Service Monitors See ISM.

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. When the configured threshold for a heartbeat has been exceeded, the router sends an SNMP trap, which Cisco Info Center receives. This is useful to confirm that the traffic stream is active. From Tivoli Business Service Manager, you can monitor heartbeat events to confirm that the routers and switches are receiving the monitored multicast video flows.

IPTV Internet Protocol Television. Video transport over IP.

IPTV extensions Configurations that extend the capabilities of the VNEs to include functions that are unique to the Cisco Video Assurance Management Solution. These extensions are applied to supported VNEs with an activation script.

IP Video Management System See iVMS.

IRD Integrated receiver/decoder.

ISM Internet Service Monitors. A collection of software components that monitors the status and performance of Internet services such as e-mail, Dynamic Host Configuration Protocol (DHCP), Domain Name Service (DNS), and Remote Authentication Dial-In User Service (RADIUS). To assist CIC users in integrating CIC with ISM, CIC includes utilities you can run after installing CIC and ISM. These utilities customize the ISM installation to function more smoothly with CIC.

J

Java EventLists See JEL.

JEL Java EventLists. Java EventLists use passive software probes to collect network events from a wide variety of management environments. Then, JEL distributes color-coded views (output from the Netcool/OMNIbus ObjectServer memory-resident SQL data repository) of networked services to operators who monitor service levels. When combined, the topology displays and Java EventLists are updated in real time, giving managers a collaborative network management environment.

M

Management Information Base See MIB.

Map A named collection of objects, symbols, submaps, and their relationships, all of which represent the network topology. See topology.

MDI:MLR Media Delivery Index:Media Loss Rate. A video metric that measures: (1) Magnitude of lost MPEG frames and (2) Per MPEG PID loss using Continuity Counter field

MDI:MLR is derived by summarizing the total missing MPEG frames for a given reporting period for a given PID (program

MDI:MRV Media Delivery Index:Media Loss Rate. A video metric that measures (1) Magnitude of lost MPEG frames (2) Per MPEG PID loss using Continuity Counter field.

MDI:MLR is derived by summarizing the total missing MPEG frames for a given reporting period for a given program ID (PID).

MDT Multicast Distribution Tree. A distribution tree that controls the path that IP multicast traffic takes through the network to deliver traffic to all receivers. The two basic types of multicast distribution trees are source trees and shared trees.

Media Delivery Index See MDI:MLR.

Media Loss Rate See MLR.

Media Rate Variation See MRV.

MIB Management Information Base. Network management protocol, such as SNMP, uses and maintains a database of network management information. The value of a MIB object can be changed or retrieved by using SNMP commands, usually through a GUI network management system.

MLR Media Loss Rate. The number of lost or out-of-order media packets per second.

Motion Picture Experts Group See MPEG.

MPEG Motion Picture Experts Group. Standard for compressing video. MPEG1 is a bit stream standard for compressed video and audio optimized to fit into a bandwidth of 1.5 Mb/s. Intended for higher quality video-on-demand applications, MPEG2 runs at data rates between 4 and 9 Mb/s. Intended for 64-kb/s connections, MPEG4 is a low-bit-rate compression algorithm.

MPLS Multiprotocol Label Switching. Switching method that forwards IP traffic by using a label. This label instructs the routers and the switches in the network where to forward the packets based on preestablished IP routing information.

MTTrapd probe The Cisco MTTrapd (Multi-Threaded) probe is the main probe used with Cisco Info Center in the Cisco VAMS environment. The MTTrapd probe monitors SNMP traps and events on both UDP and TCP sockets.

MUXId Multiplex ID. A table that describes video channels transmitted in multicast video flows.

MVPN Multicast VPN.

Multicast Distribution Tree See MDT.

Multicast VPN See MVPN.

Multiprotocol Label Switching See MPLS.

N

NE Network Element. A user-named physical component or device existing in the network.

Netcool Knowledge Library Also known as NcKL, IBM Netcool Knowledge Library is a collection of rules files that are tuned to specific managed objects that send SNMP-based events, such as Cisco networking devices. These rules support a wide range of Cisco system MIBs, including MIBs for specific Cisco devices, protocols, and technologies, as well as syslog messages from a wide range of Cisco devices.

Network Element See NE.

Network Time Protocol See NTP.

NTP Network Time Protocol. Protocol built on top of TCP that ensures accurate local time-keeping with reference to radio and atomic clocks located on the Internet. This protocol is capable of synchronizing distributed clocks in milliseconds over long time periods.

O

Object Identifier See OID.

Object Server The Object Server is the database server at the core of Cisco Info Center, where all events are stored and managed. The Object Server consolidates events such as faults, alarms, and warning messages collected by probes from various management environments. The in-memory database is optimized to handle large volumes of events, which is essential for networks where thousands of events may arrive each second.

OID Object Identifier. Values are defined in specific MIB modules. The Event MIB allows a user or an NMS to watch over specified objects and to set event triggers based on existence, threshold, and boolean tests. An event occurs when a trigger is fired; this means that a specified test on an object returns a value of true. To create a trigger, a user or an NMS configures a trigger entry in the mteTriggerTable of the Event MIB. This trigger entry specifies the OID of the object to be watched. For each trigger entry type, corresponding tables (existence, threshold, and boolean tables) are populated with the information required for carrying out the test. The MIB can be configured so that when triggers are activated (fired) either an SNMP Set is performed, a notification is sent out to the interested host, or both.

Operations Support Systems/Business Support Systems See OSS/BSS.

OSS/BSS Operations Support Systems/Business Support Systems. Operations support systems (OSS) and business support systems are a set of programs that help a communications service provider monitor, control, analyze, and manage a telephone or computer network.

P

Packet ID See PID.

Packets per second See PPS.

PAT Program Association Table. A table that lists the PIDs that are associated with the PMTs in the transport stream.

PCR Program Clock Reference. A clock reference on a program PID that helps to present programs on time and at the right speed.

PE Provider Edge. A router at the edge of a network service provider area.

PID Packet ID. The ID of a packet in a transport stream.

PIM Protocol Independent Multicast. Multicast routing architecture that allows the addition of IP multicast routing on existing IP networks. PIM is a unicast routing protocol which is independent and can be operated in two modes: dense and sparse.

PMT Program Map Table. A table that provides information about a program on a video transport stream. The PMT lists the PIDs of the streams associated with the program.

Polling (1) The process whereby stations are invited, one at a time, to transmit. The polling process usually involves the sequential interrogation of several data stations. (2) In network management, the process by which a manager interrogates one or more managed nodes at regular intervals. (3) The process by which databases are interrogated at regular intervals to determine if data needs to be transmitted.

PPS Packets per second.

Presentation Time Stamp See PTS.

Probe In the Cisco Info Center architecture, a probe is an application that acquires data from network devices and forwards it to the Object Server. A probe is a are non-intrusive software listeners that identifies and collects SNMP MIB and non-SNMP events and data. See Mttrapd probe.

Program Association Table See PAT.

Program Clock Reference See PCR.

Program Map Table See PMT.

Protocol Independent Multicast See PIM.

Provider Edge See PE.

Provision To provide, deploy, and track a service or component.

Provisioning The process of setting up and maintaining a user's access to a system.

PTS Presentation Time Stamp. The time stamp when a video or audio frame must be presented to the user.

Q

QAM Quadratrue Amplitude Modulation. Method for encoding digital data in an analog signal in which each combination of phase and amplitude represents one of sixteen four-bit patterns. Also refers to devices that encode digital cable channels for transmission over cable.

Quadrature Amplitude Modulation See QAM.

QoS Quality of Service. Measure of performance for a transmission system that reflects its transmission quality and service availability.

Quality of Service See QoS.

R

RDBMS Relational Database Management System. A collection of hardware and software that organizes and provides access to a relational database.

Realtime Transport Protocol See RTP.

Registry The data store that contains access and configuration information for users, systems, and software.

Relational database A database that can be perceived as a set of tables and manipulated in accordance with the relational model of data.

Relational database management system See RDBMS.

Rendezvous Point See RP.

Reverse Path Forwarding See RPF.

Root-cause analysis The process of determining the actual cause of a network problem. For example, when a device on a network cannot be reached, it might be because of a problem with the device or a problem with a network component that is used to reach that device.

ROSA EMS The ROSA EMS is a hardware and software platform that allows network operators to monitor the video headend using a web browser client. The ROSA EMS:

- Polls the devices that it manages and reports any problems that occur as SNMP alarms.

- If configured to perform backup protection, automatically indicates predefined backup schemes that reroute signals and activate and configure standby devices within seconds of a device failure.

- Can pass alarms to the ROSA NMS.

ROSA NMS A Cisco network management system for video that runs on dedicated hardware platform with preloaded ROSA NMS software or as a client application that runs on Microsoft Windows 2000, Microsoft Windows XP, Microsoft Windows Vista, or Microsoft Windows Server 2003 and communicates with the ROSA NMS Server.

The ROSA NMS manages Telco, CATV, HFC networks, Multichannel Multipoint Distribution System (MMDS) sites, satellite uplinks, and broadcast stations in accordance with basic telecom network management principle. In the Cisco VAMS Solution, the ROSA NMS sends SNMP traps to Cisco Info Center, which are viewable using TBSM.

RP Rendezvous Point. Router specified in PIM sparse mode implementations to track membership in multicast groups and to forward messages to known multicast group addresses.

RPF Reverse Path Forwarding. Multicasting technique in which a multicast datagram is forwarded out of all but the receiving interface if the receiving interface is the one used to forward unicast datagrams to the source of the multicast datagram. Non-RPF packets, also called RPF failure packets, are RPF packets that have been transmitted backwards, against the flow from the source.

RTP Realtime Transport Protocol. IP transport protocol that provides media-specific time stamp data for real-time flows.

Rule A set of logical statements that enable the event server to recognize relationships among events and to execute automated responses accordingly. See also event.

Run time The time period during which a computer program is executing. A run-time environment is an execution environment.

S

Schema The set of statements, expressed in a data definition language, that completely describe the structure of a database. In a relational database, the schema defines the tables, the fields in each table, and the relationships between fields and tables.

SDI Serial digital interface.

Secure sockets layer See SSL.

Service provider Any company that provides services for a fee to its customers, such as telecommunication companies, application service providers, enterprise IT, and Internet service providers (ISPs). These fee services include application provisioning, application hosting, service level agreement management, and others.

Service Dashboard The VAMS Service Dashboard provides a view of services in the video network that includes a Service Tree showing a hierarchical view of the services, a Service Viewer that shows a topology map of the devices involved in the selected service, and an event list for the service.

Service Details window The area of the VAMS Service Dashboard that shows a detailed event list for the service.

Service Tree The area of the VAMS Service Dashboard that shows a hierarchical tree diagram of the video services in the network.

Service Viewer The area of the VAMS Service Dashboard that shows a topology view of the selected service.

Set-top box See STB.

SHE Super Head End. Network location for live feeds for the broadcast video service. This site contains the real-time encoders used for the broadcast video service, along with the asset distribution systems for on-demand services. This site may also contain back-office systems such as the subscriber database. The SHE typically resides in the core of the transport network.

Simple Network Management Protocol

See SNMP.

SNMP

Simple Network Management Protocol. Network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

Soft Properties

Cisco ANA offers the soft properties mechanism to enable user-configurable extensions of device modeling, which can cover any unsupported MIB variable. This mechanism enables adding new monitored NE properties in runtime to the default set of supported properties.

Every soft property is implemented through a set of definitions that determine how to retrieve, parse and display a certain MIB variable from the NE. The definition process is done through a simple GUI utility, and does not require system restart. Soft properties are retrieved from the NE by using SNMP, or Telnet/SSH.

See also Alarm Thresholding.

SSL

Secure sockets layer. A security protocol that provides communication privacy. SSL enables client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery.

STB

Set-top box. A set-top box (STB) or set-top unit (STU) is a device that connects to a television and an external source of signal, turning the signal into content which is then displayed on the television screen.

Structured Query Language

See SQL.

SQL

Structured Query Language. A database computer language designed for the retrieval and management of data in relational database management systems (RDBMS), database schema creation and modification, and database object access control management.

SQL is a standard interactive and programming language for querying and modifying data and managing databases. Although SQL is both an ANSI and an ISO standard, many database products support SQL with proprietary extensions to the standard language. The core of SQL is formed by a command language that allows the retrieval, insertion, updating, and deletion of data, and performing management and administrative functions.

Super Head End

See SHE.

T

TBSM

IBM Tivoli Business and Services Manager (TBSM) is an application that integrates the Cisco Info Center product with the IBM Tivoli/Netcool network management application and allows Tivoli to manage a Cisco Info Center installation. TBSM provides a service dashboard and visualization tool that you can use to view service trees for multicast video networks and view events sent to by TBSM the components of the Cisco VAMS Solution.

TCA

Threshold Crossing Alert. A system message that alerts the operator when a provisionable threshold has been crossed.

Threshold

A customizable value for defining the acceptable tolerance limits (maximum, minimum, or reference limit) for an application resource or system resource. When the measured value of the resource is greater than the maximum value, less than the minimum value, or equal to the reference value, an exception is raised.

Threshold Crossing Alert

See TCA.

TIP

The high-level interface for Cisco Video Assurance Management Solution 3.1 is the Tivoli Integrated Portal (TIP) and the Tivoli Business Service Manager (TBSM). TIP allows you to launch TBSM and customized event views for events in the video headend and video transport network.

Tivoli Integrated Portal

See TIP.

Topology

Physical arrangement of network nodes and media within an enterprise networking structure.

Transrating

See Video Rate Shaping.

V

VHO

Video Hub Office. Network location of the video server complex, which includes the video sources for on-demand services and real-time encoders for local television stations. A VHO typically serves a metropolitan area of between 100,000 and 1,000,000 homes.

Video Hub Office

See VHO.

Video Rate Shaping

Video rate shaping, also known as transrating, is a process that converts video to a constant bit rate while also reducing the video bit rate.

Video Switching Office

See VSO.

Virtual Network Element

See VNE.

Virtual Private Network

See VPN.

VNE

Virtual Network Element. A virtual representation of a single network element as a modeled component. VNEs all communicate with each other to present ANA-based applications with a single, common device abstraction for network element discovery, configuration, status collection, fault analysis and other basic network functions. VNEs can be extended to support new application functionality.

VPN

Virtual Private Network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses tunneling to encrypt all information at the IP level.

VPN routing/forwarding

See VRF.

VRF VPN routing/forwarding. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table.

VSO Video Switching Office. VSOs house aggregation routers that aggregate traffic from subscriber homes.

Z

ZAP Zone Announcement Protocol. A multicast protocol for discovering the multicast administrative scope zones that are relevant at a particular location. See RFC 2776.

Zone Announcement Protocol See ZAP.

INDEX