



CHAPTER 3

Troubleshooting with Cisco Video Assurance Management Solution 3.1

This chapter contains the following sections:

- [Using the VAMS Dashboards, page 3-1](#)
- [Monitoring VAMS Events with the VAMS Service Dashboard, page 3-3](#)
- [Monitoring with the VAMS Event Views, page 3-9](#)
- [Monitoring ROSA NMS Events, page 3-11](#)
- [Monitoring CMM Events, page 3-16](#)
- [Monitoring VidMon Events, page 3-37](#)
- [Monitoring Video Events, page 3-43](#)
- [Viewing Network Fault Events, page 3-47](#)
- [Troubleshooting with Cisco ANA, page 3-49](#)

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:

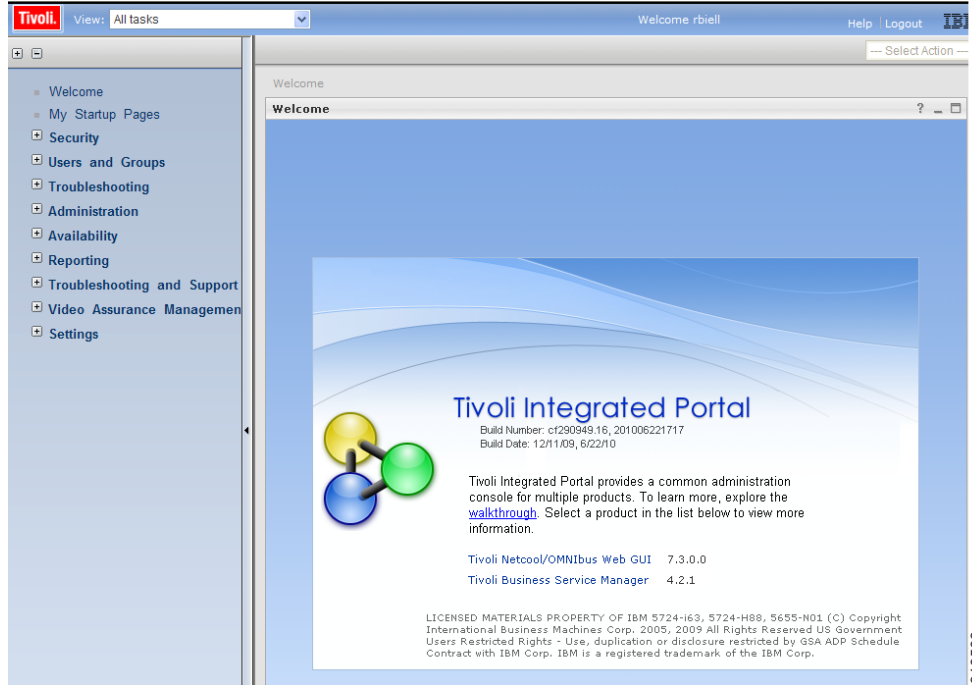
http://www.cisco.com/en/US/products/ps6776/products_user_guide_list.html

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



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

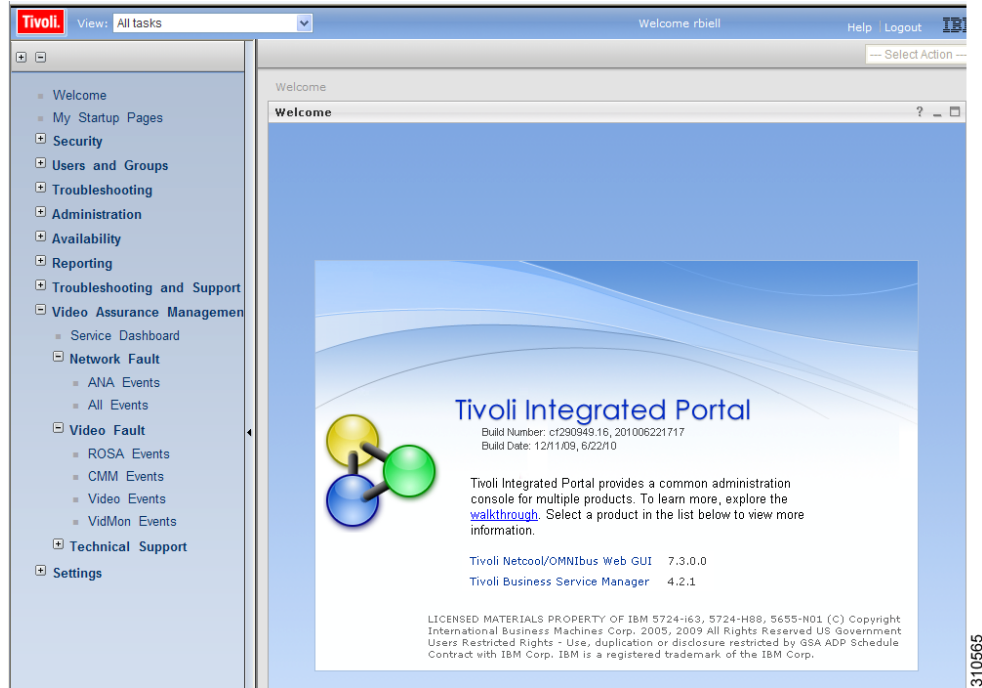
The Video Assurance Management menu appears.

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

**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

The screenshot shows the Tivoli Service Dashboard interface. On the left is the 'Service Tree' with a list of services and their event counts. The 'Service Viewer' on the right shows a service map for the selected service, 'EUROSPORT'. Below the map is the 'Service Details' window, which contains a table of active events. The table has the following data:

Node	BSM_Identity	Summary	AlertKey
RHE-1-DCM-1		Service loss at output, Board 2, Port 3, TS 232.4.16.1.5000, Sent.	RHE-1-DCM-1.524396.2611.50955.2605
RHE-1-DCM-1		Service loss at output, Board 2, Port 3, TS 232.4.16.1.5000, Sent.	RHE-1-DCM-1.524396.2611.50955.2608



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

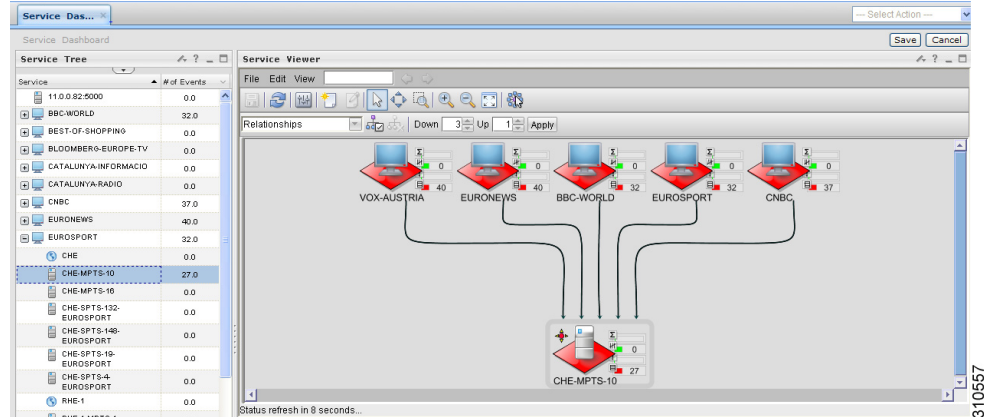


Note You can sort the service tree by clicking on either the **State** or **Events** column head.

- 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, click 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



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**.

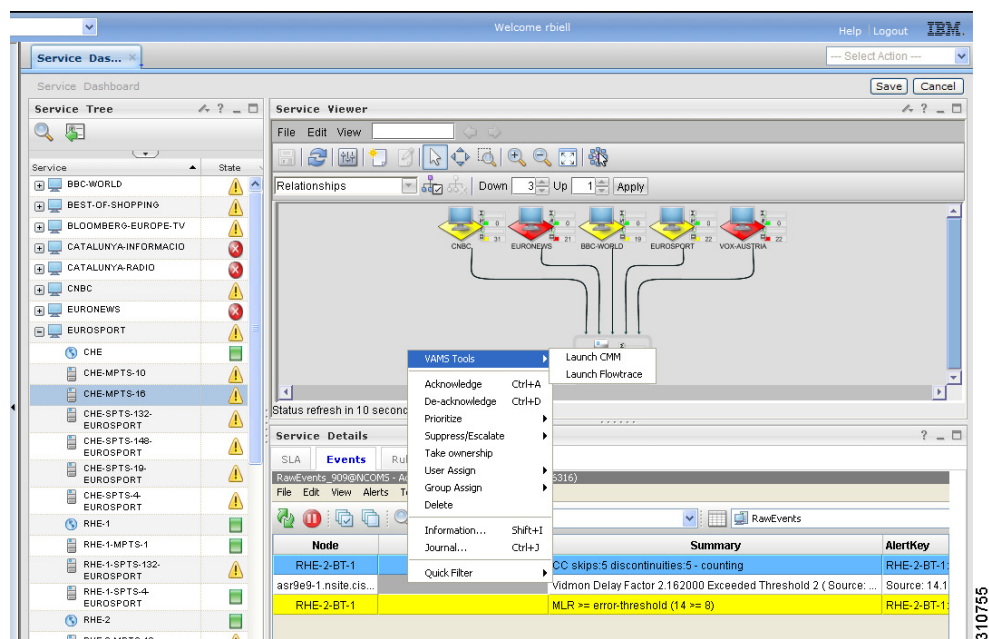


Note

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



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:

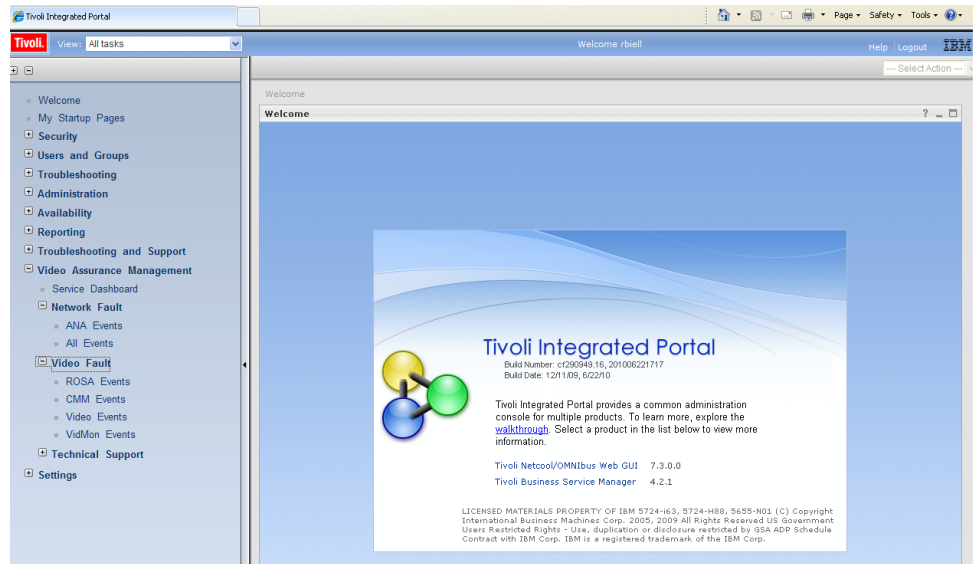
- Step 1** Log in to IBM TIP/TBSM.
The main TBSM window appears.
- Step 2** Click the plus sign (+) next to **Video Assurance Management**.
The Video Assurance Management menu appears.

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



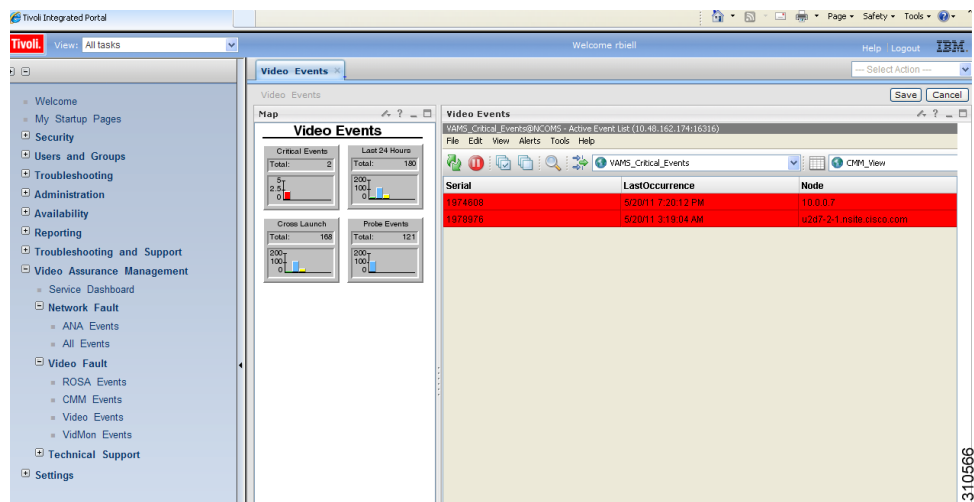
Step 5 To View a specific category of events, click the event selection. For example, click **Video Events**.

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



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.

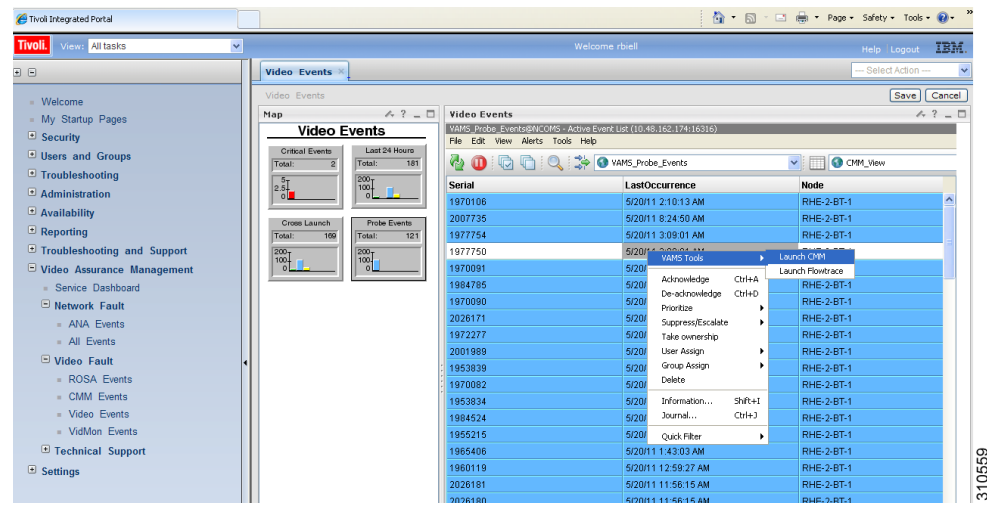


Note

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



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 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

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

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:

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

The screenshot shows the IBM TIP/TBSM Service Dashboard. On the left is a navigation pane with categories like 'Welcome', 'Security', 'Users and Groups', 'Troubleshooting', 'Administration', 'Availability', 'Reporting', 'Troubleshooting and Support', and 'Video Assurance Management'. The main area is divided into 'Service Tree' and 'Service Viewer'. The 'Service Tree' lists various services with their status and event counts. The 'Service Viewer' displays a network diagram with nodes like 'CHE', 'RHE', and 'VOR-AUSTRIA'. Below the diagram is a 'Service Details' section with a table of events.

Id	Node	Count	Last Occurrence	Summary
1254	RHE-1-DCM-1	1	1308656298	Service: Launch DCM
1312	RHE-1-DCM-1	1	1308656298	UDP S
1251	RHE-1-DCM-1	1	1308656298	Service: Acknowledge
1248	RHE-1-DCM-1	1	1308656298	Service: De-acknowledge
1298	RHE-2-BT-1	1	1308656301	No bug
1244	RHE-1-DCM-1	1	1308656298	Service: Prioritize
1292	RHE-1-DCM-1	1	1308656301	Service: Suppress/Escalate

**Note**

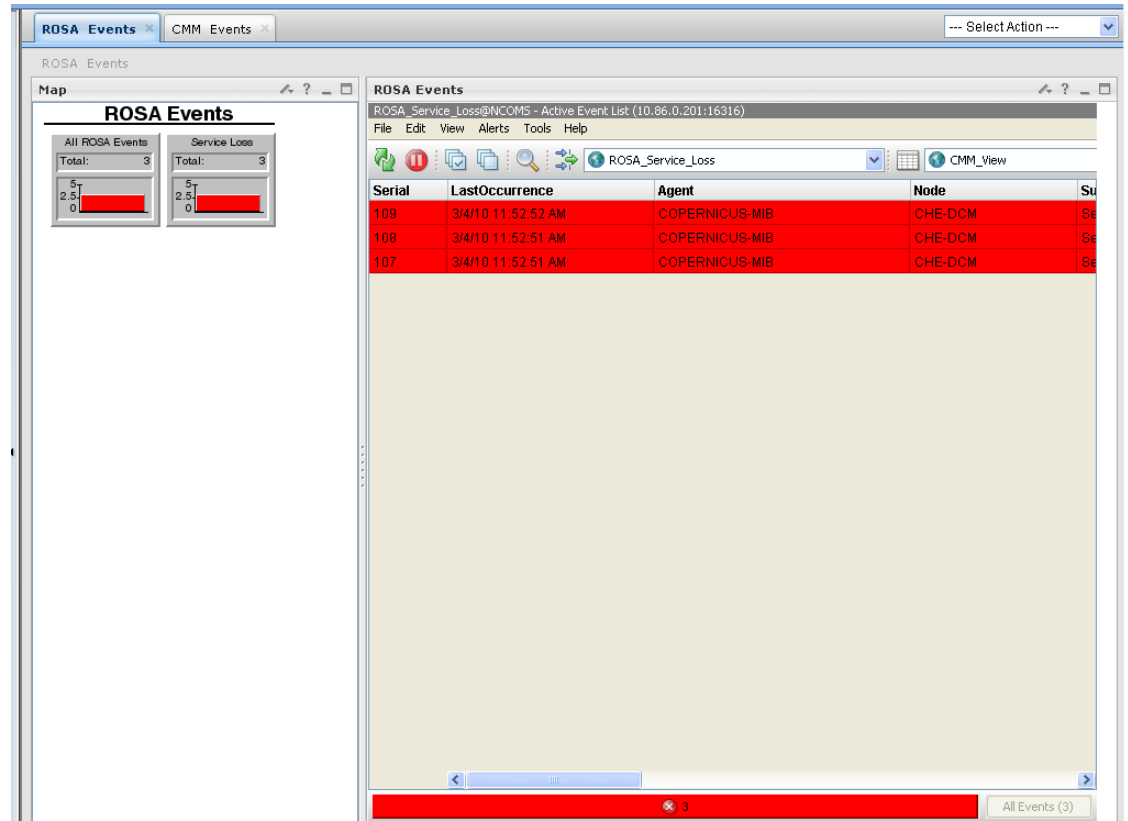
In this example, the event highlighted in grey has been right-clicked to bring up the cross-launch menu. The cross-launch is based on the information in the event that has been selected above, which is highlighted in white.

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



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:

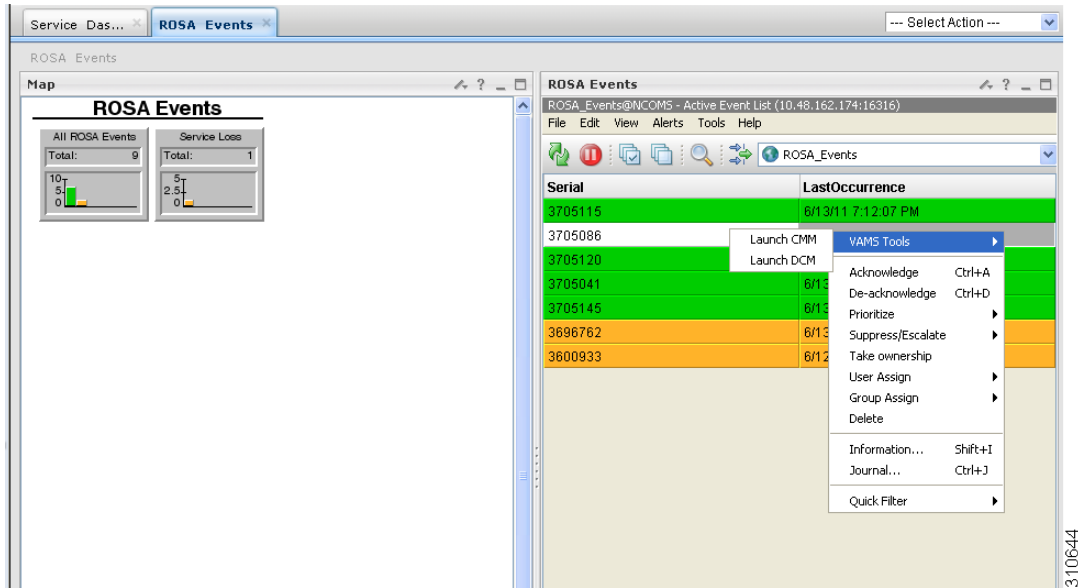
- **All ROSA Events**—Includes events with a severity level of critical
- **Service Loss**—Shows service loss events.

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



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 <i>User Guide for Cisco Multicast Manager, 3.1</i> 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 <i>User Guide for Cisco Multicast Manager, 3.1</i> 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 <i>User Guide for Cisco Multicast Manager, 3.1</i> 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 <i>User Guide for Cisco Multicast Manager, 3.1</i> 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 <i>User Guide for Cisco Multicast Manager, 3.1</i> 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 <i>User Guide for Cisco Multicast Manager, 3.1</i> 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: <ul style="list-style-type: none"> • Monitoring Multicast Tree Changes (Tree Polling), page 6-23 • “Tree Reports” in the <i>User Guide for Cisco Multicast Manager 3.1</i> 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: <ul style="list-style-type: none"> • Performing Health Checks, page 6-30 • The “Health Check” section in the <i>User Guide for Cisco Multicast Manager 3.1</i> 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)

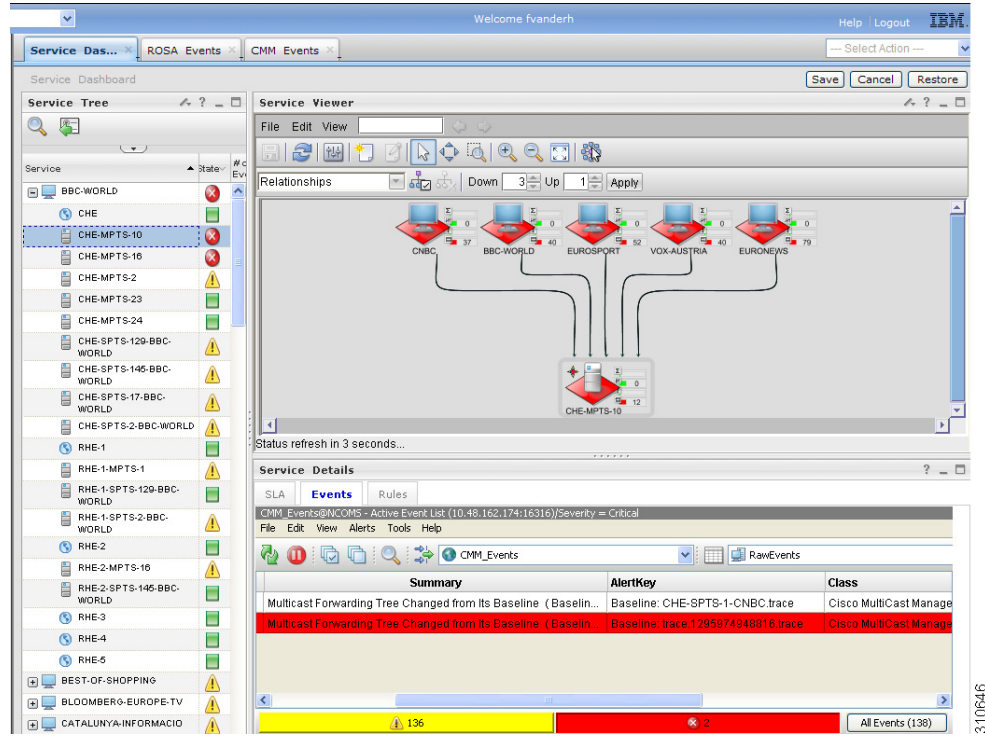
You can monitor multicast tree changes with Cisco Multicast Manager and receive the alert in Cisco Info Center. From Cisco Info Center you can then launch CMM for advanced troubleshooting of the tree changes.

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 and 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.

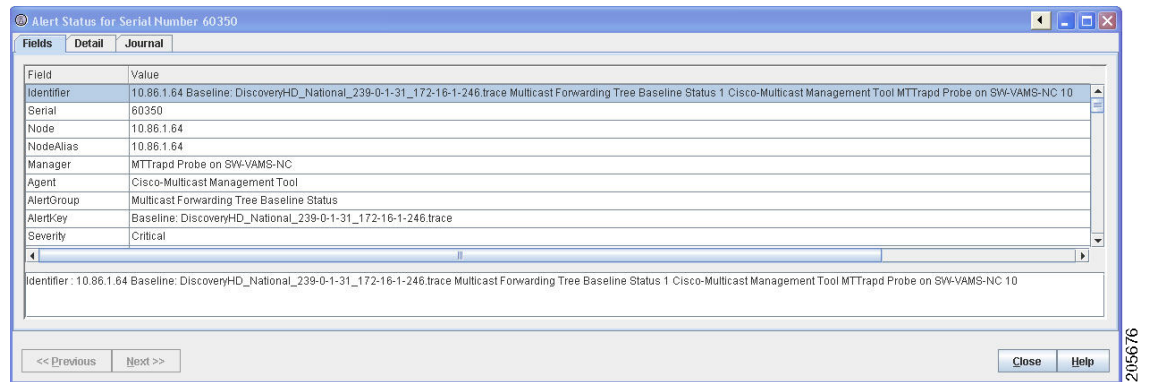
Figure 3-13 Viewing a Tree Change Event in TBSM



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



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:

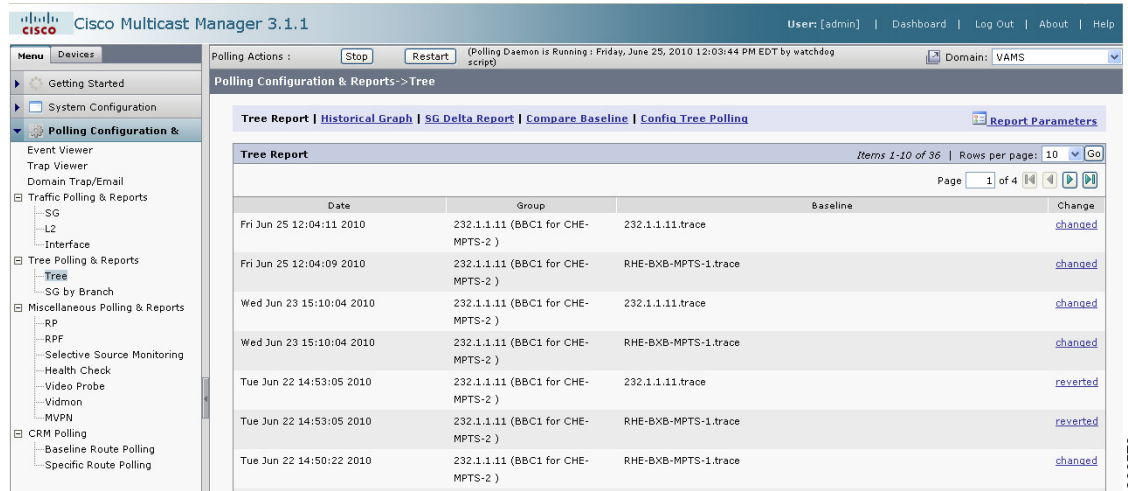
- Step 1** If you are in the TBSM/Cisco Info Center interface, highlight an event, and then from the Alerts Menu, choose **VAMS Tools > Launch CMM**.

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*

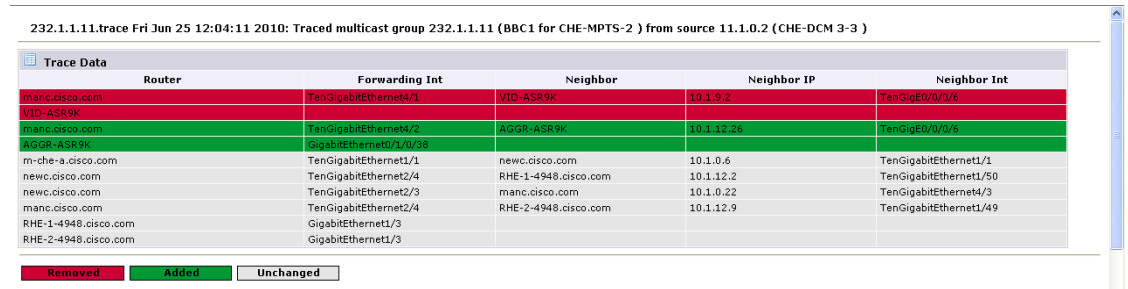


The Tree Change Report page shows a list of Multicast Tree Change reports.

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*



The report shows:

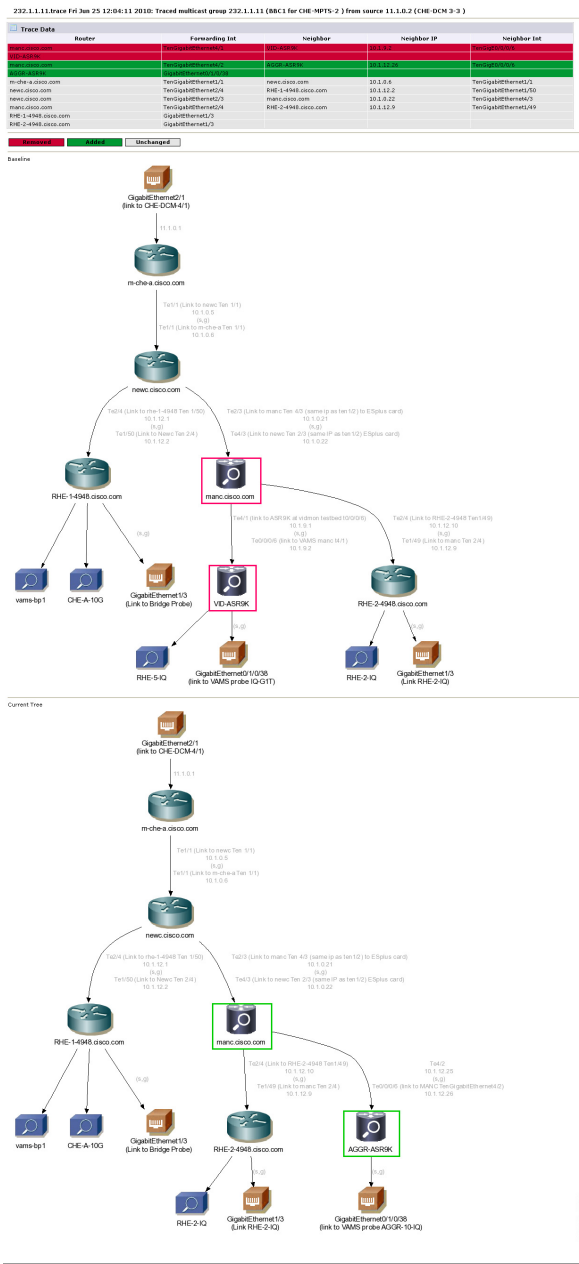
- A table containing detailed information about the routers and interfaces in the tree
- The baseline tree.
- The current tree (changed tree).

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



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

The screenshot displays the Cisco TBSM interface. On the left is the 'Service Tree' with a list of services and their states. The 'Service Viewer' in the center shows a network topology with nodes like CHBC, BBC-WORLD, EUROSPORT, VOX-AUSTRIA, and EURONEWS connected to CHE-MPTS-10. The 'Service Details' window at the bottom right shows a list of events for 'RawEvents_945'. The event list is as follows:

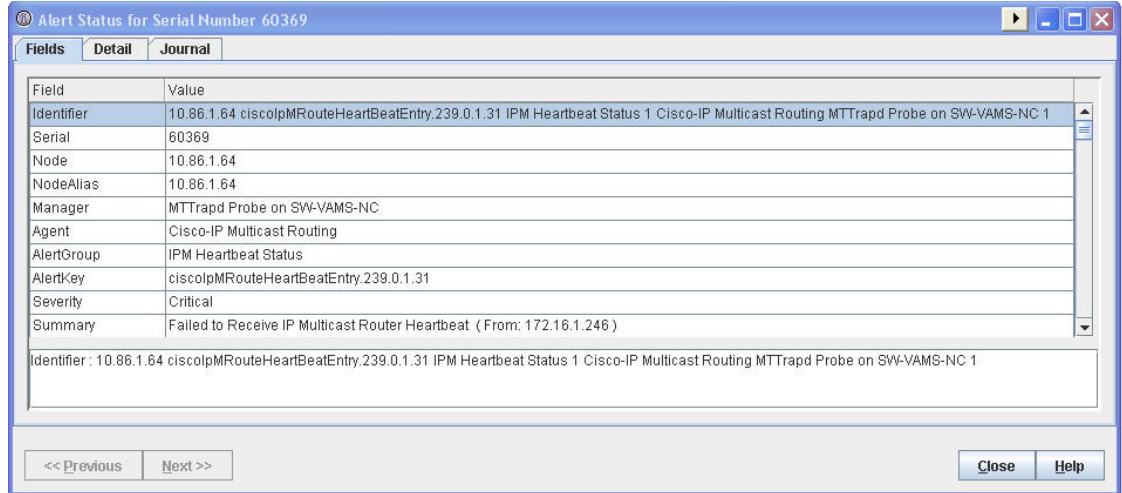
Node	BSM Ident...	Summary	AlertKey
10.0.0.4		ViolMon Media Stop Event SRC_PORT 49152DST_IP:232.1.18.1	Source:14.1.0.2, Dest:232.1.18.1
10.0.0.4		ViolMon Media Stop Event SRC_PORT 49152DST_IP:232.1.18.1	Source:14.1.0.2, Dest:232.1.18.1
10.0.0.4		ViolMon Media Stop Event SRC_PORT 49152DST_IP:232.1.18.1	Source:14.1.0.2, Dest:232.1.18.1
10.0.0.7		Failed to Receive IP Multicast Heartbeat at Router 10.0.0.7 for (S...	ciscoipMRouteHeartBeatEntry.232
10.0.0.1		ViolMon Media Stop Event Input	Source:14.1.0.2, Dest:232.1.18.1
10.0.0.3		ViolMon Media Stop Event Input	Source:14.1.0.2, Dest:232.1.18.1
10.0.0.7		ViolMon Media Stop Event SRC_PORT 49152DST_IP:232.1.18.1	Source:14.1.0.2, Dest:232.1.18.1

At the bottom of the event list, it shows '29 rows inserted, 29 rows updated, and 0 rows deleted.' and '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.

310704

Figure 3-20 TBSM: Viewing Heartbeat Event Details

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.

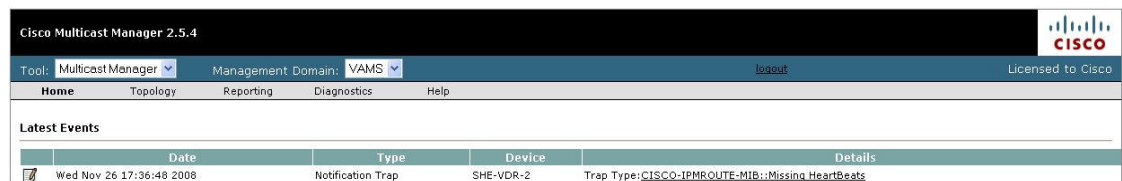
Monitoring Heartbeat Events with CMM

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

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 :

Trap OID	Value	Description
This Notification is sent if a multicast router failed to receive configured number of heartbeat packets from heartbeat sources within a configured time interval		
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	

SNMPv2-SMI::enterprises.9.10.2.3.1.0.1

Source IP : 172.16.4.2
UpTime : 18:55:27.33

2105667

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

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

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.

310756

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

Date	Domain	Router	Source	Group	Value	Threshold
Fri Jun 25 21:10:01 2010	VAMS	man.cisco.com	11.1.0.2	232.1.1.1 (BBCI for CH...	1715 pps	19000 pps
Fri Jun 25 21:10:01 2010	VAMS	man.cisco.com	10.1.0.42	232.150.1.1 (uncompress...	0 pps	13480 pps
Fri Jun 25 21:10:00 2010	VAMS	VID-ASR9K	10.1.0.42	232.150.1.1 (uncompress...	0 pps	13480 pps
Fri Jun 25 21:09:03 2010	VAMS	man.cisco.com	11.1.0.2	232.1.1.1 (BBCI for CH...	1712 pps	19000 pps
Fri Jun 25 21:09:01 2010	VAMS	man.cisco.com	10.1.0.42	232.150.1.1 (uncompress...	0 pps	13480 pps
Fri Jun 25 21:09:00 2010	VAMS	VID-ASR9K	10.1.0.42	232.150.1.1 (uncompress...	0 pps	13480 pps
Fri Jun 25 21:08:01 2010	VAMS	man.cisco.com	11.1.0.2	232.1.1.1 (BBCI for CH...	1709 pps	19000 pps
Fri Jun 25 21:08:01 2010	VAMS	man.cisco.com	10.1.0.42	232.150.1.1 (uncompress...	0 pps	13480 pps
Fri Jun 25 21:08:00 2010	VAMS	VID-ASR9K	10.1.0.42	232.150.1.1 (uncompress...	0 pps	13480 pps
Fri Jun 25 21:07:01 2010	VAMS	man.cisco.com	11.1.0.2	232.1.1.1 (BBCI 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

The screenshot shows the Cisco Multicast Manager 3.1 interface. The left sidebar contains a navigation menu with 'Polling Configuration & Reports' expanded to 'Video Probe'. The main content area is titled 'Polling Configuration & Reports -> Video Probe' and includes a 'Video Probe Report | Historical Report | Config Video Probe Polling' section. Below this, there are controls for 'Units' (set to 'DF'), 'From Date' (2010/03/05 01:53 am), and 'To Date' (2010/03/07 01:53 am). A 'Show Report' button is visible. The 'Historical Graphs' section shows a table with 8 rows of data. The first three rows are selected, and the 'Show Report' button is highlighted.

Group	Source	Video Probe
<input checked="" type="checkbox"/> 239.0.1.41	172.16.1.250	IQ-CHE-59-@-CHE-6506-2
<input checked="" type="checkbox"/> 239.0.1.41	172.16.1.250	IQ-CORE-63-@-CRS-WEST
<input checked="" type="checkbox"/> 239.0.1.41	172.16.1.250	IQ@7606-E-121
<input type="checkbox"/> 239.0.1.41	172.16.1.250	IQ@ASR9K-120
<input type="checkbox"/> 239.0.1.42	172.16.1.250	IQ-CORE-63-@-CRS-WEST
<input type="checkbox"/> 239.0.1.42	172.16.1.250	IQ@7606-E-121
<input type="checkbox"/> 239.0.1.42	172.16.1.250	IQ@ASR9K-120
<input type="checkbox"/> 239.0.1.43	172.16.1.250	IQ@7606-E-121
<input type="checkbox"/> 239.0.1.43	172.16.1.250	IQ@ASR9K-120
<input type="checkbox"/> 239.0.1.44	172.16.1.250	IQ@7606-E-121

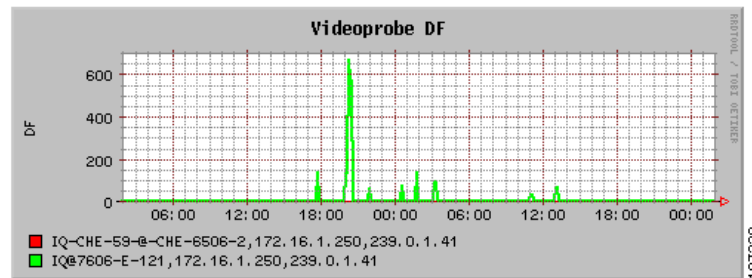
- Step 6** From the drop-down list in the **Units** field, select the units for the report:

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

- Step 7** Click the calendar item (...) for **From Date** 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: <input type="button" value="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-ESP2 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..

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 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	0
mdi	-	0	0.868	0	0
mdi	-	0	0.87	0	0
mdi	-	0	0.858	0	0
mdi	-	0	0.864	0	0
mdi	-	0	0.868	0	0
mdi	-	0	0.868	0	0
mdi	-	0	0.867	0	0
mdi	-	0	0.859	0	0
mdi	-	0	0.876	0	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(intvl): 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 Date** 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**.

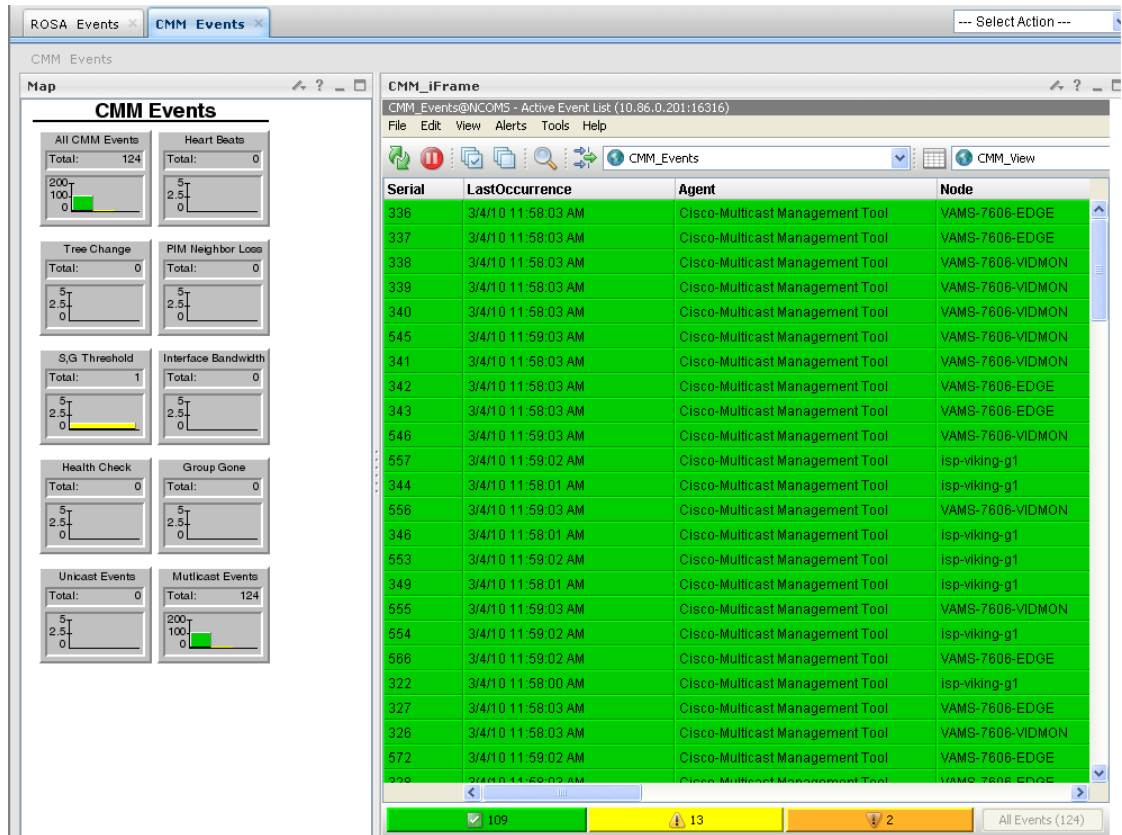
The Video Assurance Management menu appears.

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



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 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

Node	BSM_Identity	Summary	AlertWay	C
RHE-1-DCM-1		Service loss at output, Board 2, Port 3, TS 232.4.16.1.5000, Ser...	RHE-1-DCM-1.524398.261150955.2605	
RHE-1-DCM-1		Service loss at output, Board 2, Port 3, TS 232.4.16.1.5000, Ser...	RHE-1-DCM-1.524398.261150955.2606	

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

310558

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

The screenshot shows the Service Dashboard interface. On the left is the Service Tree, and on the right is the Service Viewer. The Service Tree lists services like BEST-OF-SHOPPING, BLOOMBERG-EUROPE-TV, and EUROSPORT, with CHE-MPTS-16 selected. The Service Viewer shows a service map with nodes like CHE-MPTS-16, EUROSPORT, and others. Below the map, the Service Details section shows a table of events.

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:

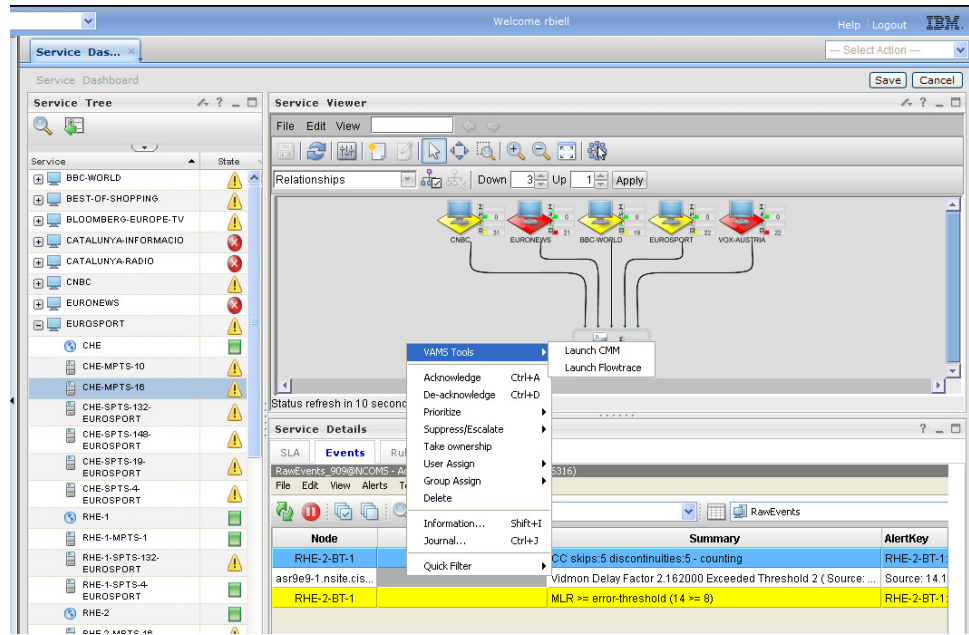
Vidmon Delay Factor Exceeded Threshold—SNMP trap generated by CMM indicating that a VidMon DF threshold has been exceeded on a Cisco 9000 device used to transport the MPTS stream.

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

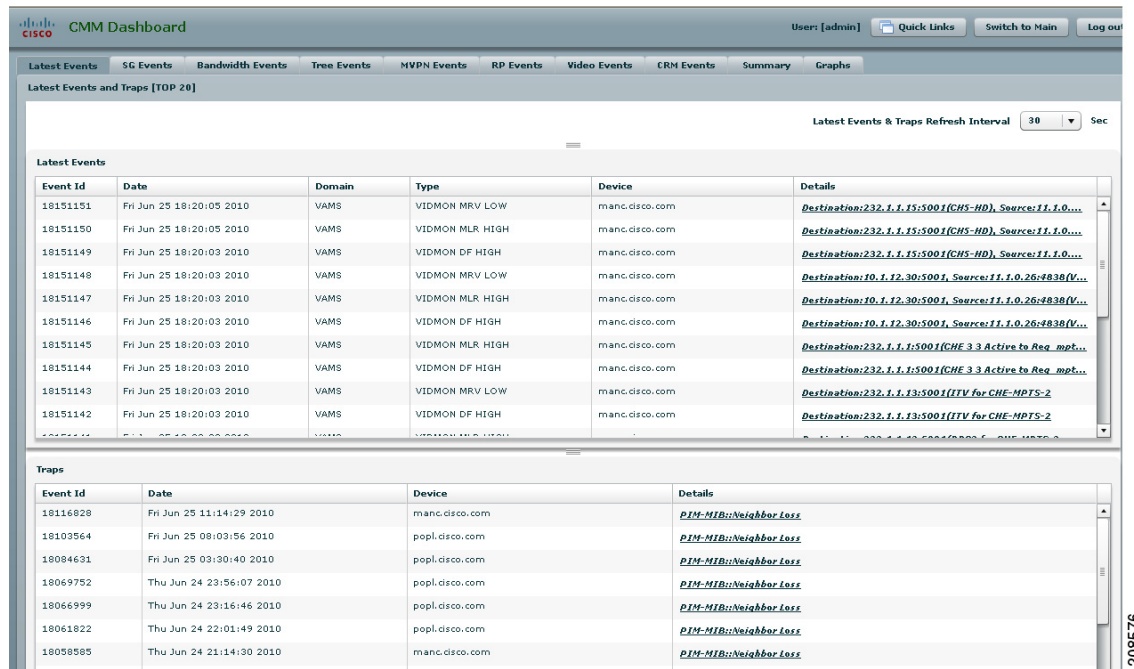


The CMM login screen appears.

Step 7 Log in to CMM.

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

Figure 3-35 CMM Dashboard Showing Video Flows



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 Encoder1,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: Counter Update Interval: (Sec)

208613

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

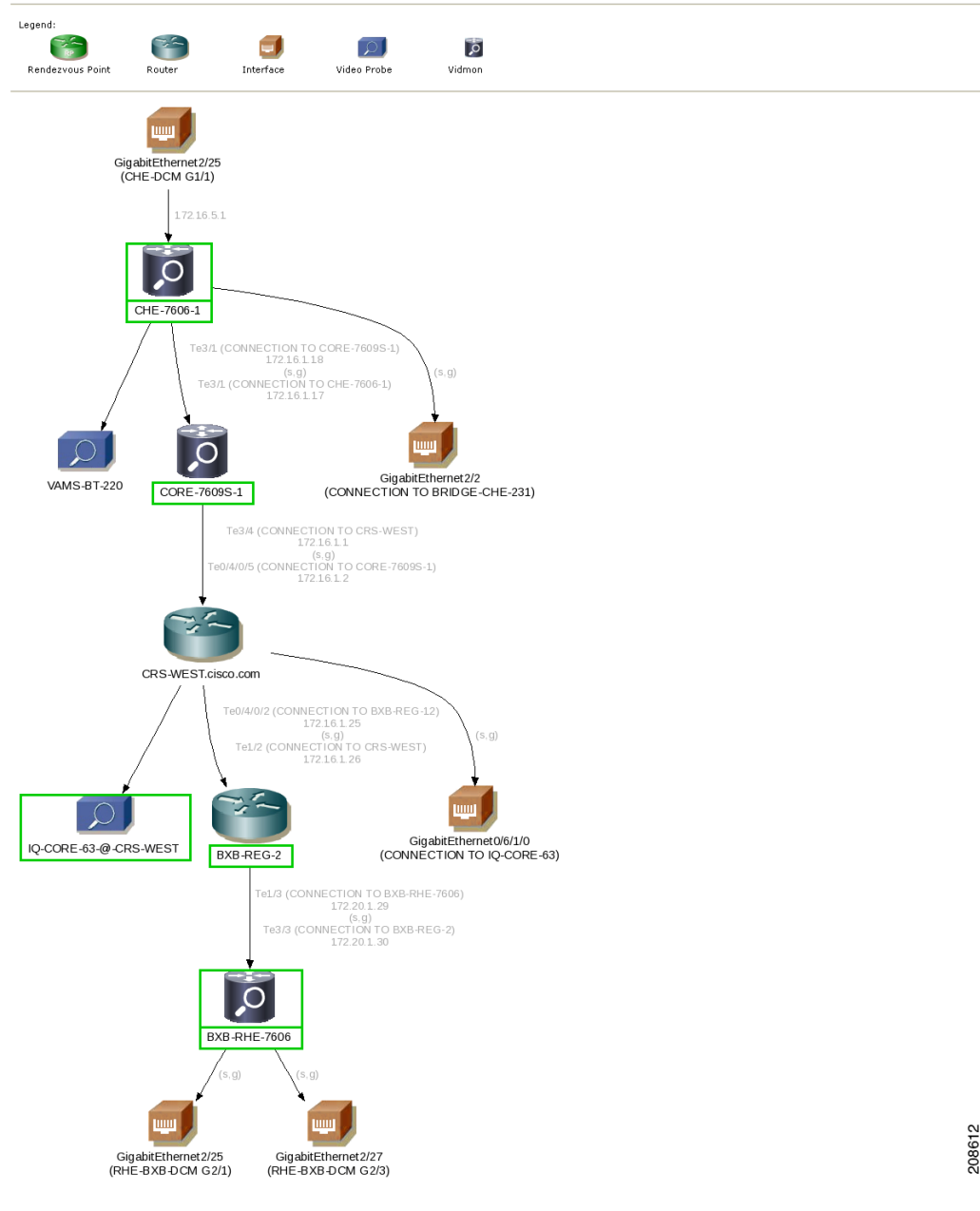
- **Flow Description**—The flow description at the top of the page indicates the unicast Group, Channel Name, Transport Description, Source IP and Source description, as configured in the CMM for the flow.
- **Trace Data Table**—Lists the routers, interfaces, and PIM neighbors that transport the multicast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



208612

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**.

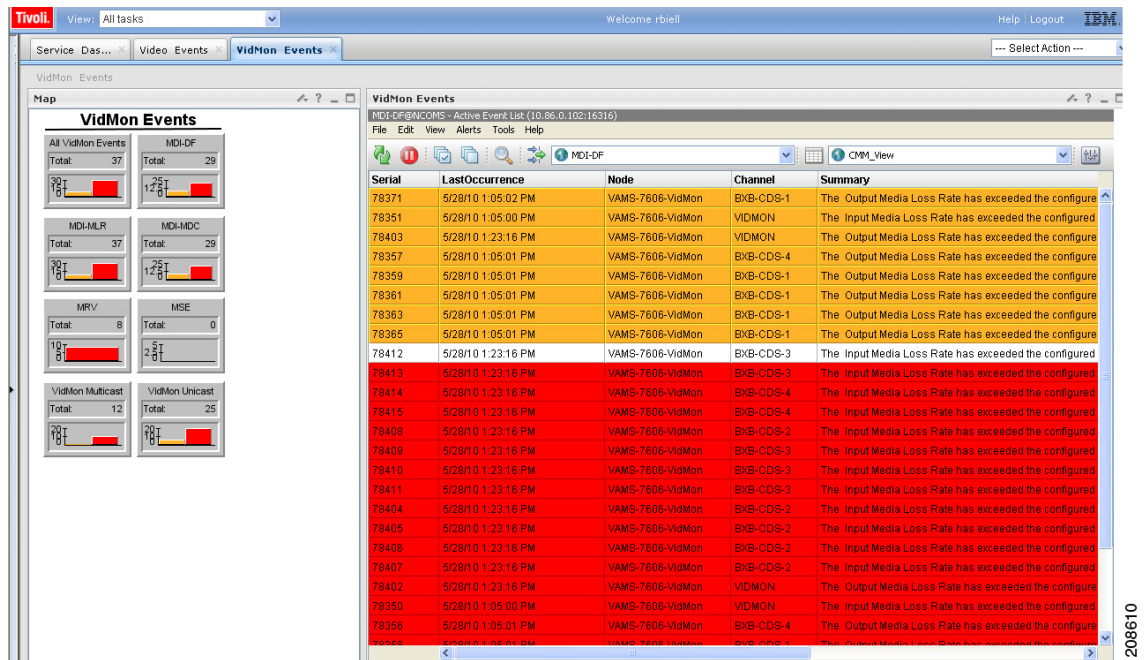
The Video Assurance Management menu appears.

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



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 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

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.

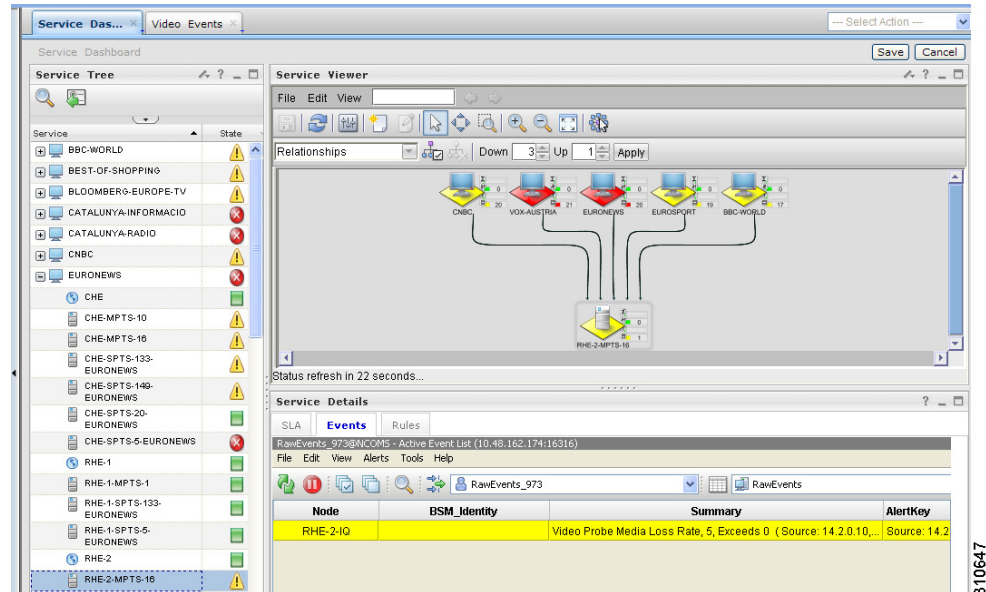
The devices in the service topology are listed in the Service Tree directory.

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



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.

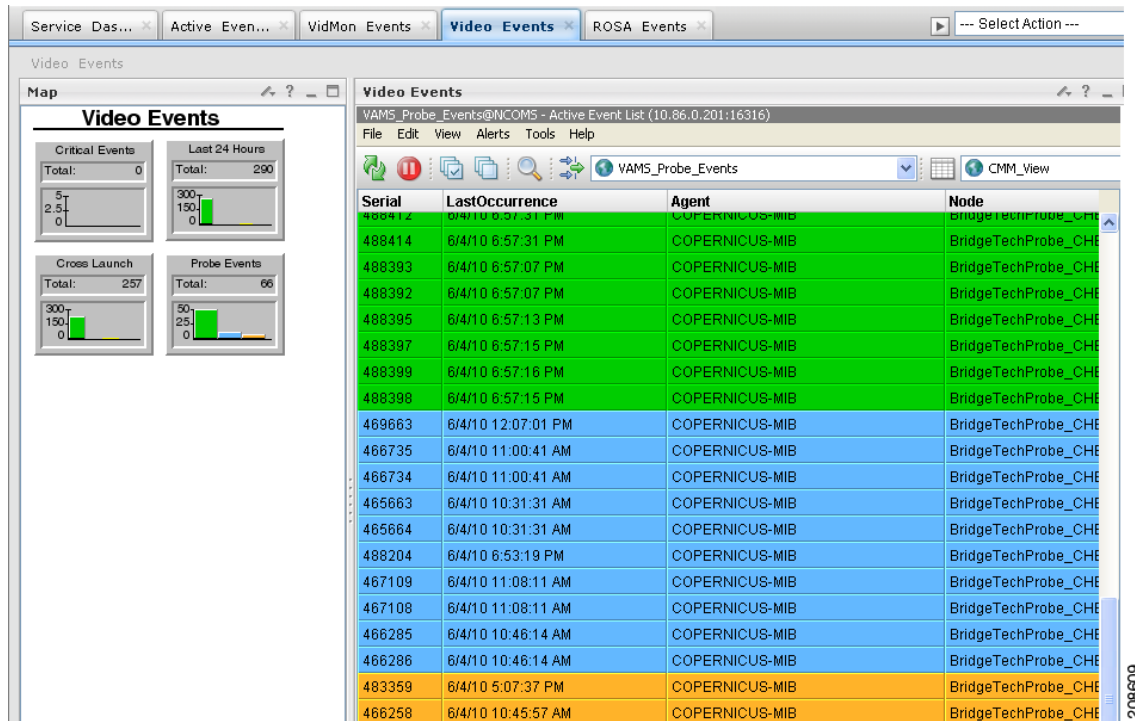
- Step 6** To view details about an event, highlight the event and right click on it.
- Step 7** To launch CMM to troubleshoot the event, right click on the event and choose **VAMS Tools > Launch CMM** or **VAMS Tools > Launch Flowtrace**.
- The CMM login screen appears.
- Step 8** Log in to CMM and 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



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.

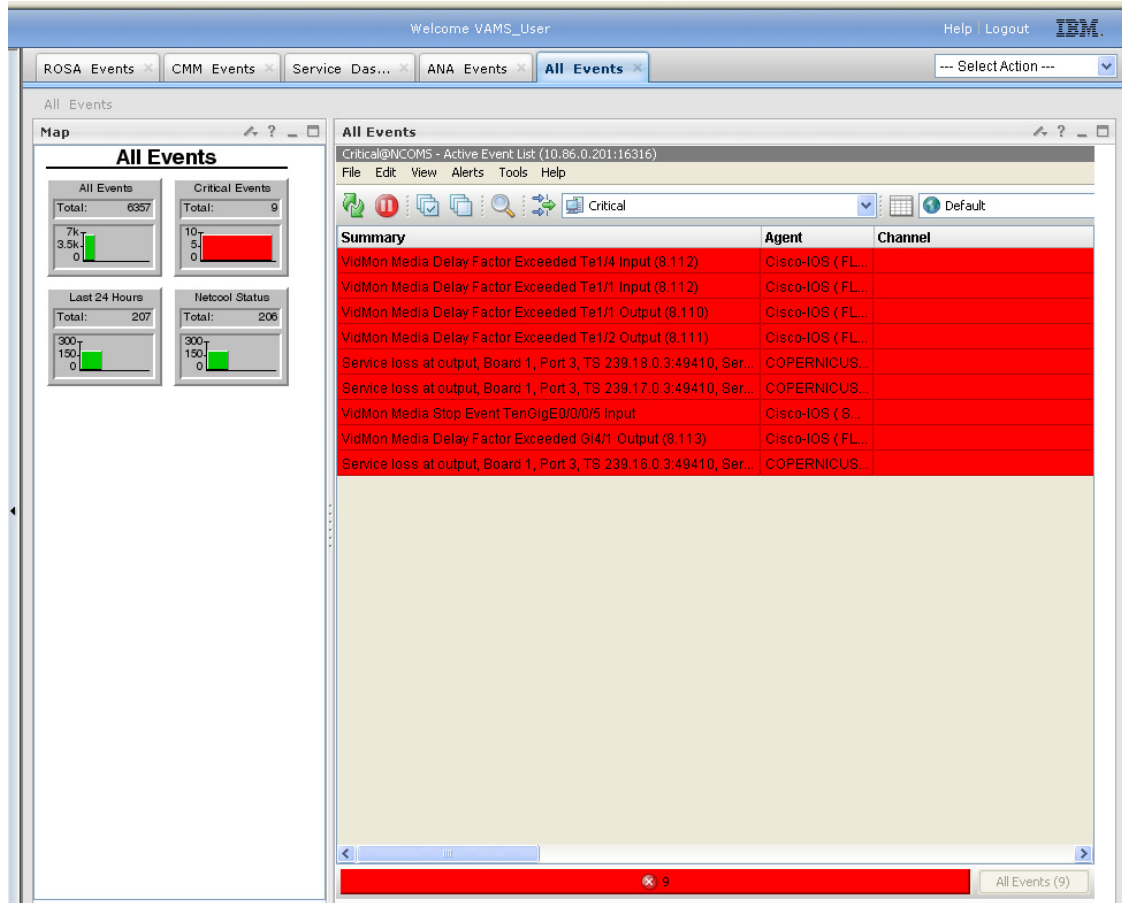
Viewing Events in the ANA Event Views

-
- 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



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	<p>Describes:</p> <ul style="list-style-type: none"> • 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. <p>For detailed information about working with fault detection and isolation, see the <i>Cisco Active Network Abstraction User Guide, 3.7</i>, viewable online at: http://www.cisco.com/en/US/docs/net_mgmt/active_network_abstraction/3.7/user/guide/User_Guide_3_7.html</p>
Casualty correlation and root-cause analysis	<p>Describes:</p> <ul style="list-style-type: none"> • 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. <p>For detailed information about working with casualty correlation and root-cause analysis, see the <i>Cisco Active Network Abstraction User Guide, 3.7</i>, viewable online at: http://www.cisco.com/en/US/docs/net_mgmt/active_network_abstraction/3.7/user/guide/User_Guide_3_7.html</p>
Advanced correlation scenarios	<p>Describes alarms that use advanced correlation logic on top of the root cause analysis flow.</p> <p>For detailed information about working with advanced correlation scenarios, see the <i>Cisco Active Network Abstraction User Guide, 3.7</i>, viewable online at: http://www.cisco.com/en/US/docs/net_mgmt/active_network_abstraction/3.7/user/guide/User_Guide_3_7.html</p>

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	<p>Cisco ANA NetworkVision:</p> <ul style="list-style-type: none"> 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. <p>For detailed information about working with tickets, see the <i>Cisco Active Network Abstraction User Guide, 3.7</i>, viewable online at: http://www.cisco.com/en/US/docs/net_mgmt/active_network_abstraction/3.7/user/guide/User_Guide_3_7.html</p>
Working with ANA PathTracer	<p>You use the Cisco ANA PathTracer to view a network path between two network objects in packet-switched networks such as Ethernet and IP.</p> <p>For detailed information about working with the Cisco ANA PathTracer, see the <i>Cisco Active Network Abstraction User Guide, 3.7</i>, viewable online at: http://www.cisco.com/en/US/docs/net_mgmt/active_network_abstraction/3.7/user/guide/User_Guide_3_7.html</p>

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