CHAPTER 1

Overview

This chapter provides an overview of the architecture, components, and features of Cisco Video Assurance Management Solution (Cisco VAMS) 3.0. This chapter contains:

License Information

For licensing information, see Appendix B, "End User License Agreement Supplement."

Introduction to Cisco VAMS 3.0

Cisco VAMS 3.0 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 and manage 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 1-9 for descriptions of the solution components and required software versions.

Cisco VAMS 3.0 provides a modular architecture for monitoring video networks. VAMS 3.0 uses:

- Cisco Multicast Manager (CMM 3.1) with patch 3.1.1 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 4.0 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

- The Cisco Info Center product suite.[1]

  Cisco Info Center is the Manager of Managers, and monitors events from CMM, Cisco ANA, the ROSA NMS, video probes, and Cisco devices. For the VAMS 3.0 solution, Cisco has bundled the IBM Netcool Tivoli Integrated Portal with the Cisco Info Center/Netcool ObjectServer (central database), IBM Tivoli Business and Services Manager (TBSM), a service dashboard and visualization tool, and the Tivoli Netcool/OMNIbus Web GUI.

  The Cisco Info Center product suite includes two additional product components from the IBM Tivoli product suite:

  - **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 accomplishes two key objectives for Cisco VAMS 3.0. It provides:

  - Connectivity between CMM and the ROSA NMS and Cisco Info Center.
  - A "Single Pane of Glass" toolset[2].

  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:

  - 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.

    For more information on ROSA ASSR alerts, see Service Alerts with ASSR support, page 1-17.

- Cisco ANA 3.7 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 3.0 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, and Cisco 12000 series routers.

1. This is the OEM product of the IBM Tivoli Netcool Suite.
2. 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 VAMS 3.0 Network Topology

Cisco VAMS 3.0 monitors events from the entire video network to provides end-to-end video assurance management. Figure 1-1 shows the end-to-end topology of a typical video network.

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

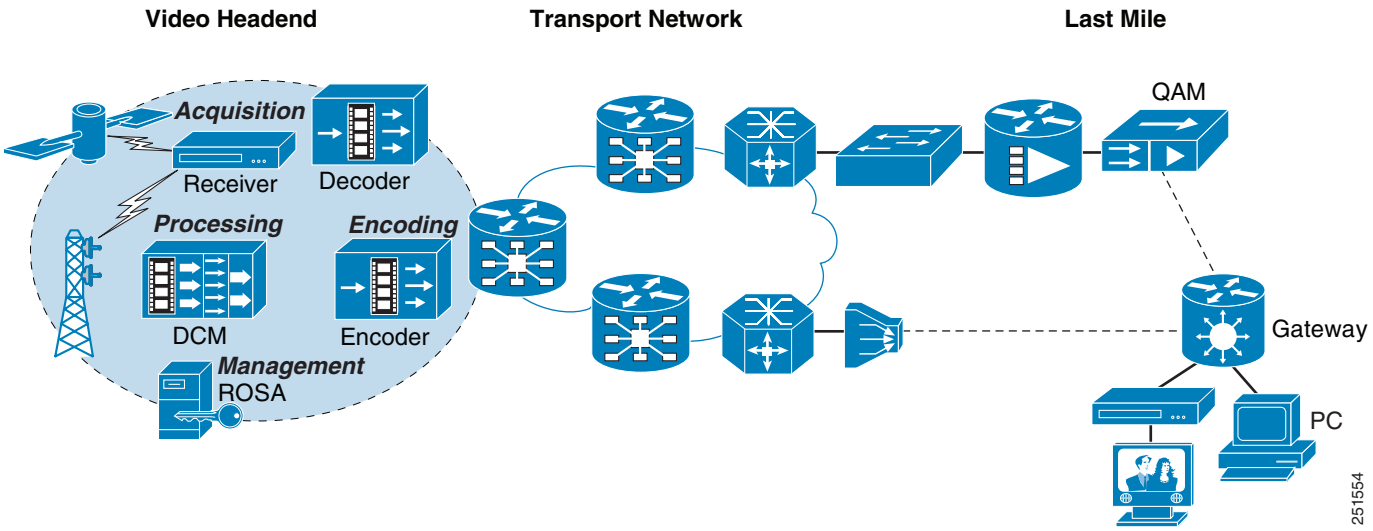


Figure 1-2 shows a Cisco VAMS topology in a video headend environment, and Figure 1-3 shows an example topology in the video transport network.

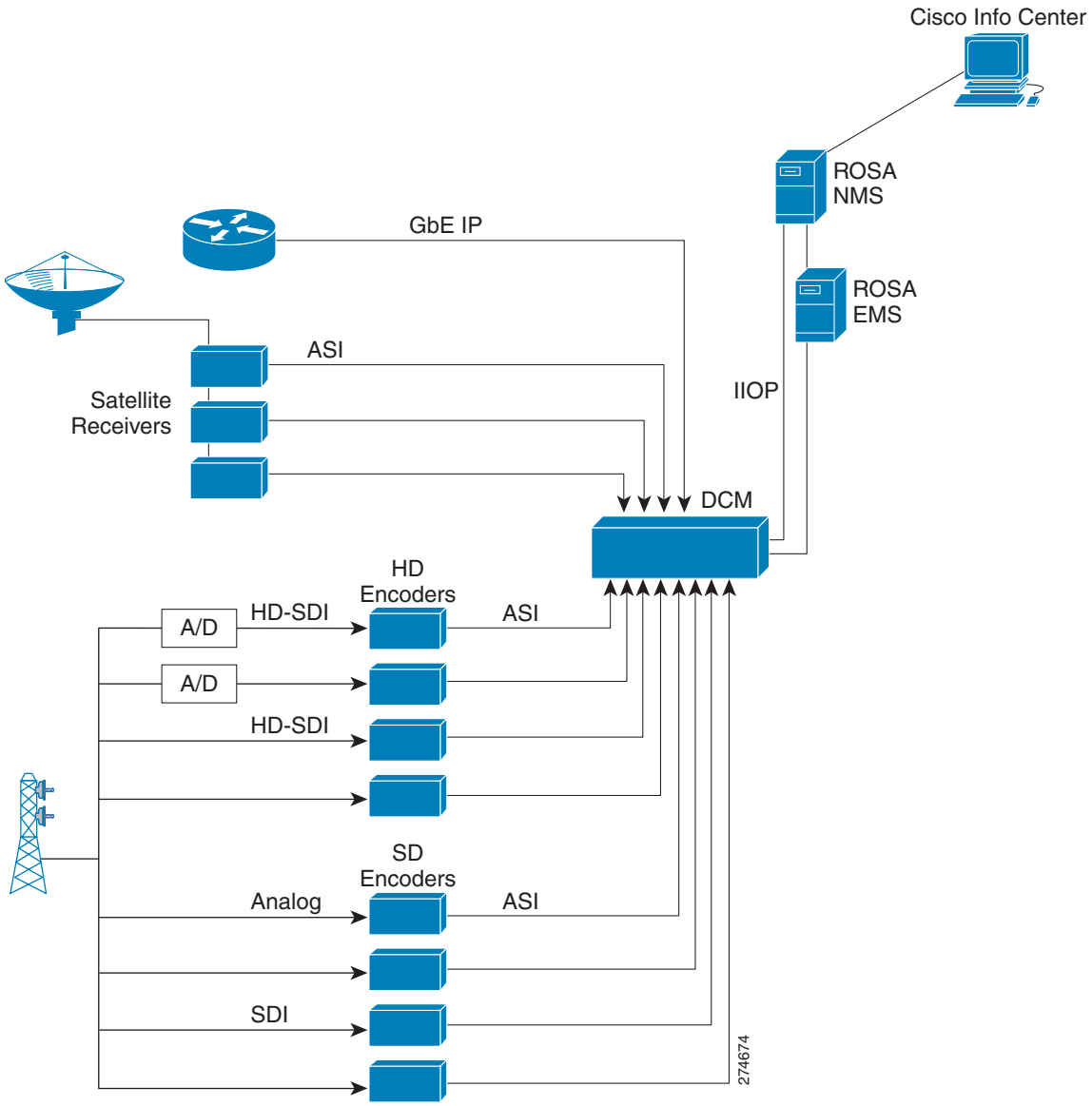
Cisco VAMS monitors devices in the video headend and in the transport network, but does not monitor events in the last mile segment.

Cisco VAMS 3.0 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 1-2 shows a Cisco VAMS topology in a video headend environment.

Figure 1-2 Cisco Video Assurance Management Solution 3.0 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

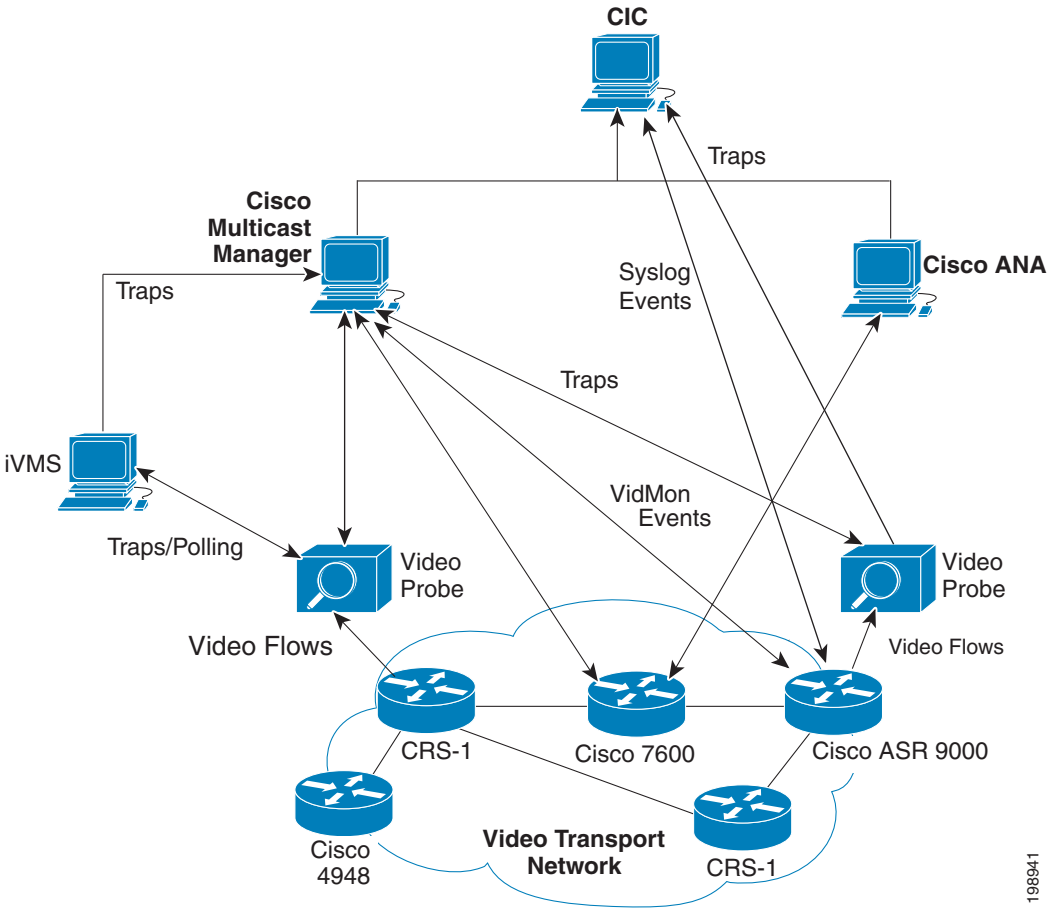
The DCM can export alerts related to these features into the ROSA Management system for video service correlation and association with other events solicited from the IP transport.

In the Cisco VAMS 3.0 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 1-3 shows Cisco VAMS 3.0 in a video transport network.

Figure 1-3 Cisco Video Assurance Management Solution 3.0 Components for Video Transport Monitoring



Cisco VAMS 3.0 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 3.0 environment, see Cisco Info Center, page 1-20.

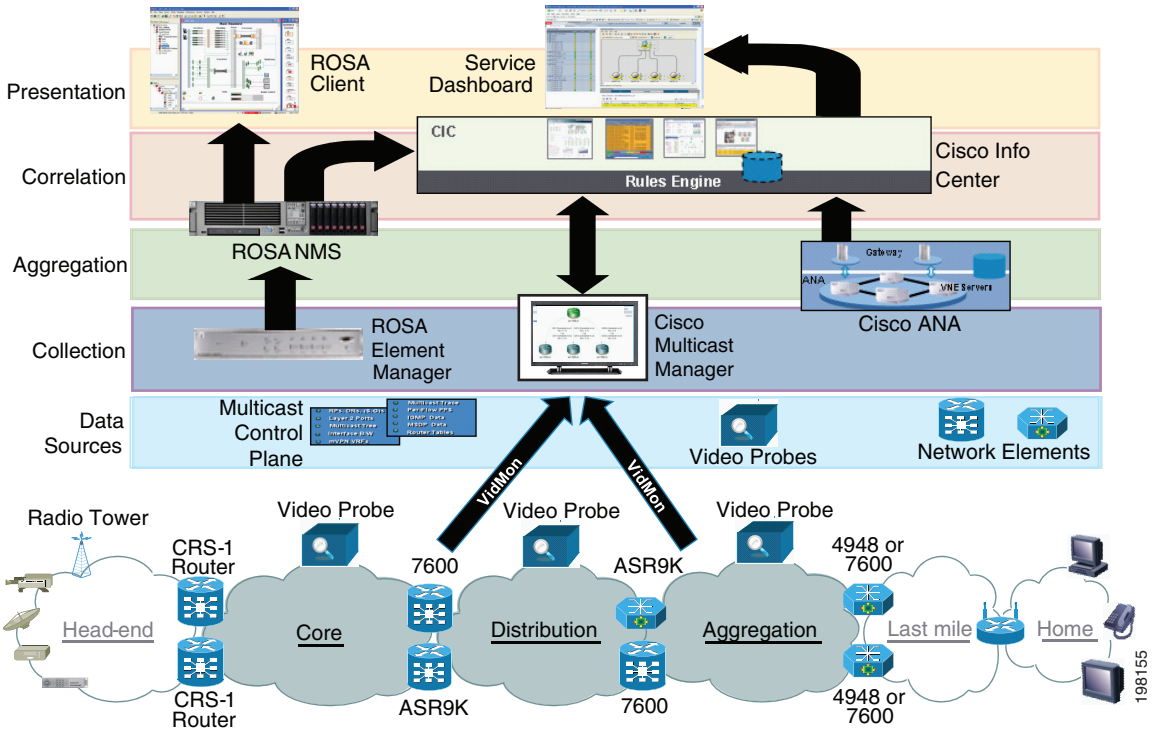
Cisco VAMS Solution Components

The Cisco VAMS 3.0 solution includes the following components:

- Cisco Multicast Manager 3.1, page 1-12
- ROSA NMS, page 1-15
- Cisco Info Center, page 1-20
- Cisco ANA 3.7, page 1-23
- Third-Party Video Probes, page 1-30

Figure 1-4 shows the components in the VAMS 3.0 architecture.

Figure 1-4 VAMS 3.0 System Architecture



Network Elements in the Video Transport Network

Cisco VAMS 3.0 monitors these network elements (NEs), which form the core of the video transport network (see Figure 1-3 on page 1-7):

- **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 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 IOS software that enables the NEs to monitor multicast video flows in the network. See the "Solution Component Versions" section on page 1-9, for a list of the required IOS software.

Solution Component Versions

Cisco VAMS 3.0 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
Cisco Multicast Manager	3.1.1

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

Solution Component	Version Information
ROSA Element Management System	4.0 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	4.0.4.8
Digital Content Manager (DCM)	Model D9900 and D9901 with GbE interface card. DCM software V06.05.02.
Cisco 7600 Series router (7600-SUP720-3BXL with redundant SUP720-3BXL) Line cards include Ethernet Services Plus (ES+) line card, WS-X6704-10GE, WS-X6708-10GE, WS-X6748-SFP, WS-X6748-GE-TX, WS-X6724-SFP, RSP720-3CXL, 7600-ES20-10G3CXL, 7600-SIP-400, 7600-SIP-600, SPA-1XTENGE-XFP, SPA-2X1GE, and optional WS-F6700-DFC3BXL	12.2(33)SREV
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 3.9
Cisco Catalyst 4948 Series switch (CAT4948-10GE)	12.2(46)SG
Cisco ASR 9000 router	IOS XR 3.9
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
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	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 3.0 does not support carousel-related traps for the Mixed Signals Sentry 136.

Cisco Multicast Manager 3.1

This section describes the components of CMM 3.1.

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 has three components: an Event Dashboard, a Devices tab, and a Main Menu.

CMM 3.1 uses SNMP MIB polling to monitor devices and traffic in the network. CMM 3.1 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 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 monitors video transmission by monitoring:

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

CMM 3.1 also provides detailed diagnostics and a health-check capability.

You use CMM 3.1 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 System Requirements

Table 1-2 lists the hardware and software requirements for the CMM 3.1.

Table 1-2 Cisco Multicast Manager3.1 System Requirements

Item	Specifications
Hardware Requirements	
Processor	**Cores** • 4 cores for less than 500 devices • 8 cores for 500 devices or more **AMD Linux** • Dual, Quad, or 6-Core AMD Opteron processor **Linux-Intel** • Xeon Dual or Quad Core (equivalent or better) **Solaris-SPARC** • Sun UltraSPARC IIIi or better
Memory	• 4 GB for less than 500 devices • 8 GB for Large Enterprise
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

Cisco Multicast Manager 3.1 Software Components

The CMM 3.1 user interface provides three components:

- Event Dashboard, page 1-14
- Devices Tab, page 1-14
- Main Menu, page 1-14

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

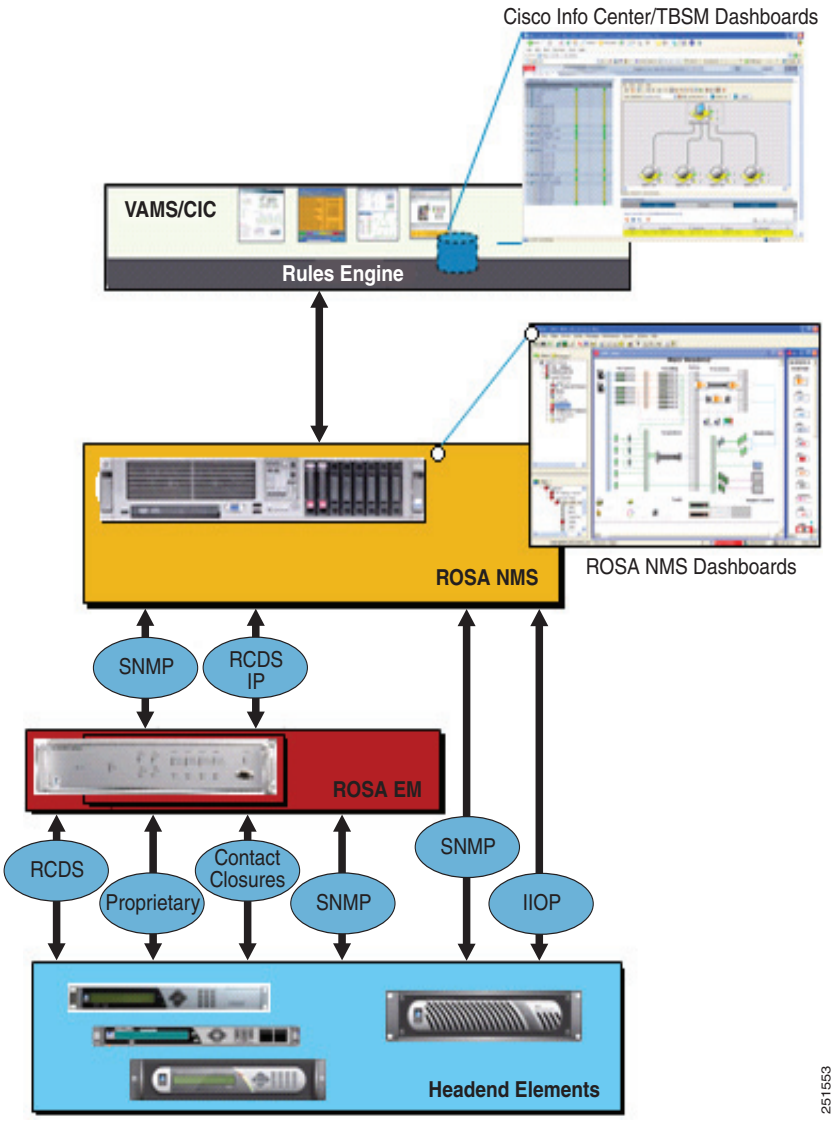
The computer used to run the ROSA NMS client must meet these requirements:

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 1-5 shows the ROSA NMS architecture.

Figure 1-5 ROSA NMS Process Flow



In the VAMS 3.0 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 3.0 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 3.0 Cisco Info Center dashboard.
- 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 1-17.
- **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 3.0 architecture are:

- Service Backup Protection, page 1-19

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 3.0 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 1-17.

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, CMM 3.1, and video probe devices.

Cisco Info Center alone provides real-time monitoring, management, and event deduplication[3] 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 1-20
- IBM Tivoli Netcool/Impact, page 1-21
- IBM Tivoli Integrated Portal, page 1-21
- IBM Tivoli Business Service Manager, page 1-21
- IBM Tivoli Netcool Probes, page 1-22
- Rules Files, page 1-22

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.

3. 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 3.0 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 3.0 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 3.0, 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

This section describes the hardware and software components of Cisco ANA 3.7.

Cisco ANA 3.7 Hardware Components

Cisco ANA 3.7 hardware comprises:

- Cisco ANA Servers, page 1-23
- Cisco ANA Clients, page 1-26

Note The hardware recommendations assume that the Cisco ANA 3.7 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 1-23
- Cisco ANA Unit, page 1-24

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 1-24). 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 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.
Software Requirements	

Table 1-3 Cisco ANA Gateway Requirements (continued)

Item	Specifications
Hardware 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* 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 servers (gateway and unit) with any application other than Cisco ANA 3.7.

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 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* 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 servers (gateway and unit) with any application other than Cisco ANA 3.7.

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 1-29.)

Cisco ANA Client Requirements

Table 1-5 lists the hardware and software requirements for the Cisco ANA 3.7 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 Software Components

Cisco ANA 3.7 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 manages the NEs listed in the "Network Elements in the Video Transport Network" section on page 1-8. The Cisco ANA 3.7 features for the Cisco VAMS 3.0 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 automatically detects and manages the NEs in its domain, including their physical and logical inventories.

VNEs

Cisco ANA 3.7 provides a VNE mediation layer between the managed NEs and the network management applications in Cisco ANA 3.7. 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. The VNEs collect information from their corresponding NEs for management purposes.

Cisco VAMS 3.0 uses VNEs to represent the solution components in Table 1-6.

Table 1-6 VNEs for the Cisco VAMS 3.0

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 activation scripts and soft properties created for the Cisco VAMS 3.0 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 automatically detects managed NEs in the video transport network along with their physical and logical inventories. Cisco ANA 3.7 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 also supports discovery of the network topology (automatically and manually).

Cisco ANA 3.7 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 1-8, for details about the Cisco NEs.

Fault Management

Cisco ANA 3.7 provides fault management for the video transport network:

See the *Cisco ANA User Guide 3.7* 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 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 monitors CPU utilization of the supported NEs in the Cisco VAMS 3.0. For more information about ANA polling and its interaction with the CPU utilization of managed NEs, see the *Cisco ANA User Guide, 3.7,* viewable online at:

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

Cisco ANA 3.7 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 3.0.

For more information about ICMP polling, see the *Cisco ANA User Guide, 3.7,* viewable online at:

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

Cisco ANA 3.7 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,* viewable online at:

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

GUIs for Fault Management

Cisco ANA 3.7 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 1-8, 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 provides user identification and authentication for accessing the Cisco ANA 3.7 to perform configuration and fault management tasks on the supported NEs. For more information about security information in Cisco ANA 3.7, see the *Cisco ANA Administrator Guide, 3.7*, viewable online at:

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

Multicast and Video Management

Cisco ANA 3.7 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 receives the notification and generates an alarm. The Cisco ANA 3.7 correlates subsequent alarms and generates subalarms.

Cisco ANA Client Software Tools

Cisco ANA 3.7 includes several applications built on top of the virtual network as the mediation layer.

Cisco ANA 3.7 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,* 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) 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,* 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,* viewable online at:

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

Third-Party Video Probes

Cisco VAMS 3.0 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 3.0 receives events from the probes based on thresholds that you configure in the video probes or in CMM. Cisco VAMS 3.0 associates probe events with a severity level in Cisco Info Center.

Note IneoQuest probes are polled directly by the CMM 3.1 application.

See the video probe guides for VAMS 3.0, which are listed in the *Documentation Guide for Cisco Video Assurance Manager, 3.0*, 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:

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 3.0, see the *Video Assurance Monitoring Delivery Cisco Advanced Services* document at the following URL (TBD):

Cisco Lifecycle Approach

Cisco takes a lifecycle approach to 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 adjustment 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.