C H A P T E R 1

Overview

The *User Guide for Cisco Video Assurance Management Solution 1.5* provides a complete overview of the hardware and software products that the Cisco Video Assurance Management Solution (Cisco VAMS) comprises. This guide describes key benefits and advantages, features, and technical specifications for the products that make up the Cisco VAMS 1.5. The guide also describes installation, configuration, and troubleshooting tasks.

You can use the Cisco VAMS 1.5 to diagnose and facilitate the tasks of monitoring the transport section of a multicast video network to:

- 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.

This chapter contains:

License Information

See Appendix B, "End User License Agreement Supplement."

Introduction to Cisco VAMS 1.5

Cisco VAMS 1.5 delivers to service providers real-time, centralized monitoring of backbone, regional, and aggregation networks for broadcast video transport. Cisco VAMS 1.5 provides the framework for a flexible end-to-end assurance platform for video. See the "Solution Component Versions" section on page 1-7 for descriptions of the solution components and required software versions.

Cisco VAMS 1.5 provides a modular architecture for monitoring video networks: VAMS 1.5 uses:

- Cisco Multicast Manager (CMM 2.5) with Patch 2.5.4 for multicast monitoring and troubleshooting functions

- The Cisco Info Center (CIC) product suite[1] to monitor events from CMM.

  Cisco has bundled the CIC/Netcool the ObjectServer (central database) and Webtop (web GUI for event list viewing) from the CIC product suite with the VAM solution.

  The CIC product suite includes two additional product components from the IBM Tivoli product suite:

  – IBM Tivoli Business and Services Manager (TBSM), a service dashboard and visualization tool.

  – IBM Tivoli Impact, which supports the definition of service and network correlations.

  This combination of CIC and Netcool functionality accomplishes two key objectives for Cisco VAMS 1.5. It provides:

  – Connectivity between CMM and CIC.

  – A "Single Pane of Glass" toolset[2] for Cisco VAMS 1.5.

  CIC includes rules files that define multicast alerts from various sources like probes and routers. The rules file includes code that extracts the multicast group and source information from these alerts and provides the operator with a CMM Multicast Trace option.

  By integrating CMM with CIC you can now view all the alarm conditions and data for service level correlation and analysis. Additionally, you can launch troubleshooting and diagnostic analysis from one system instead of looking at several systems.

- Cisco ANA 3.6 Service Pack 3 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 1.5 extends the base functions of the Cisco ANA 3.6.2 VNEs for Cisco 7600 Series routers, Cisco Carrier Routing System (CRS-1) devices, and Cisco Catalyst 4948 and 6500 Series switches. These VNE extensions address the specific requirements of video delivery across the IP network.

Finally, Cisco VAMS 1.5 includes generic VNEs that support specific video probes; this release includes VNEs for IneoQuest, Mixed Signals, and Tektronix video probes.

Cisco VAMS 1.5 Network Topology

Figure 1-1 shows an example topology of the Cisco VAMS 1.5 components.

---

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.

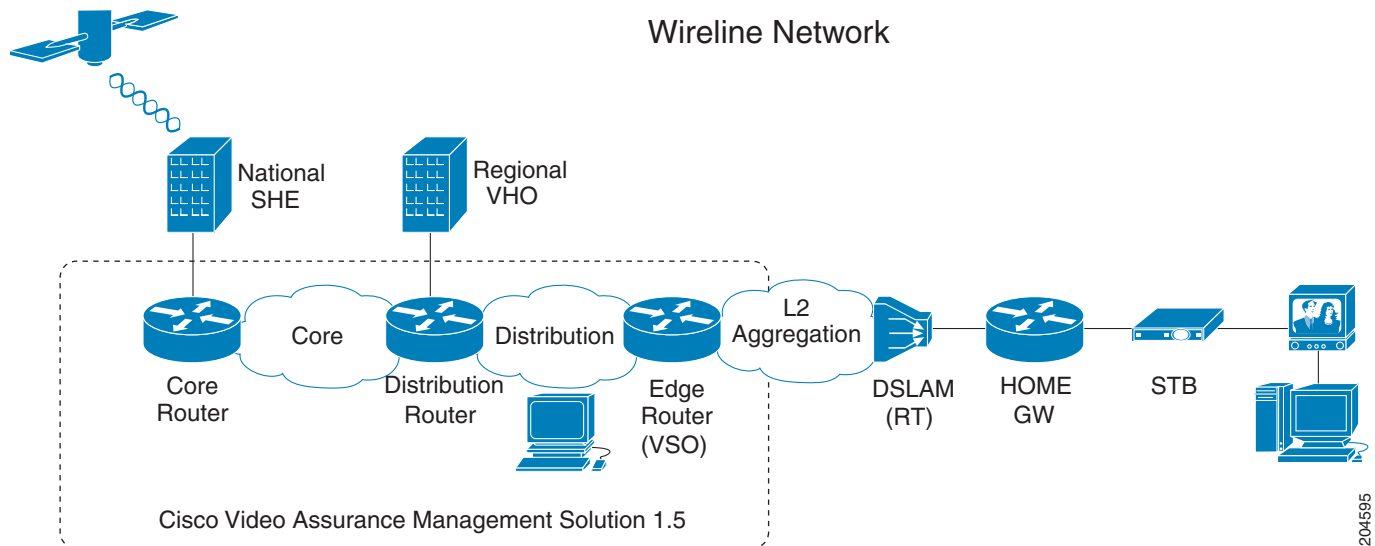**Figure 1-1   Cisco Video Assurance Management Solution 1.5 Components**
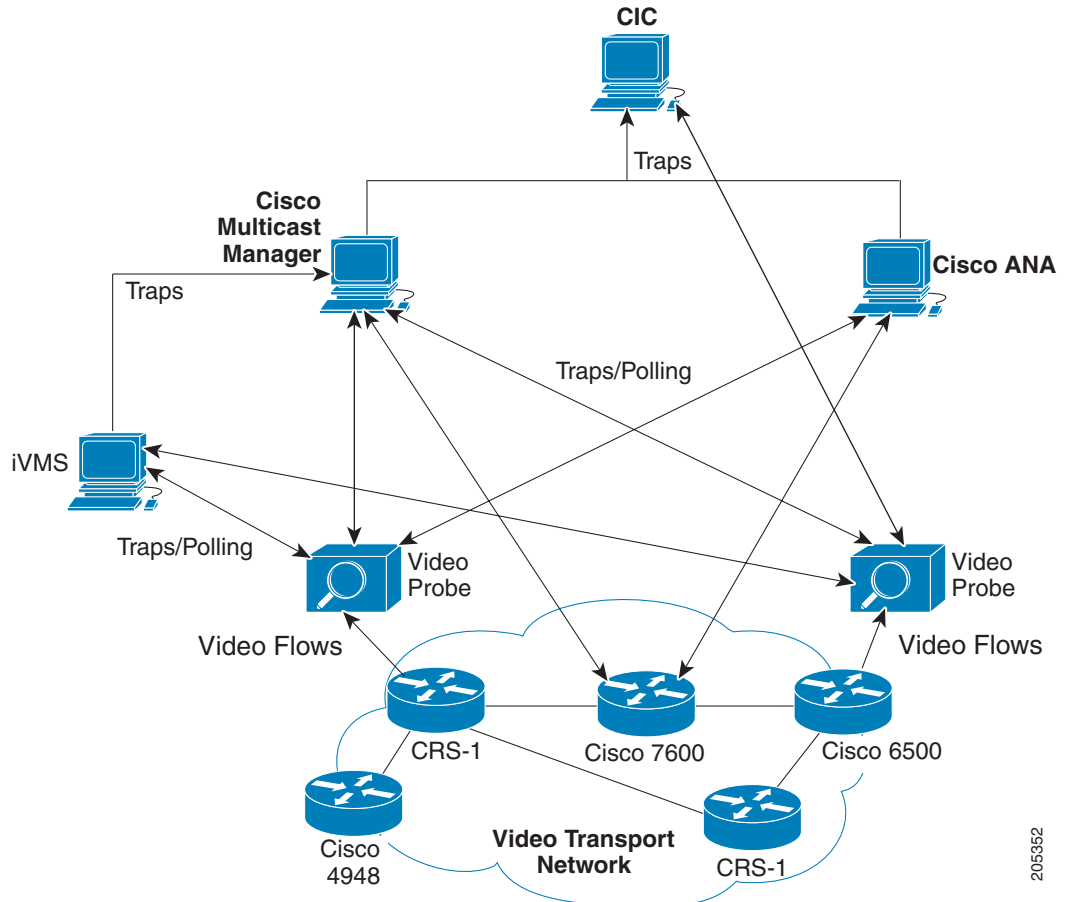
See the "Cisco VAMS Solution Components" section on page 1-6, for descriptions of the Cisco VAMS components shown in Figure 1-1.

Cisco VAMS 1.5 in a Wireline Network

Figure 1-2 shows the Cisco VAMS 1.5 in a wireline network.

Figure 1-2   *Cisco Video Assurance Management Solution 1.5 in a Wireline Network*

The Super Head End (SHE) is the network location for live feeds for the broadcast video service. This site contains the real-time encoders used for the broadcast video service, along with the asset distribution systems for on-demand services. This site may also contain back-office systems such as the subscriber database.

The Video Hub Office (VHO) is the network location of the video server complex, which includes the video sources for on-demand services and real-time encoders for local television stations.

Cisco VAMS 1.5 covers the video transport network and focuses on the core and distribution networks shown in Figure 1-2. See also Figure 1-1 on page 1-3 for an example of the Cisco devices Cisco VAMS 1.5 manages.

For detailed information about this supported architecture, see the *Cisco Wireline Video/IPTV Solution Design and Implementation Guide, Release 1.1,* viewable online at:

http://www.cisco.com/en/US/products/ps6902/products_implementation_design_guide_book09186a00806b5b4c.html
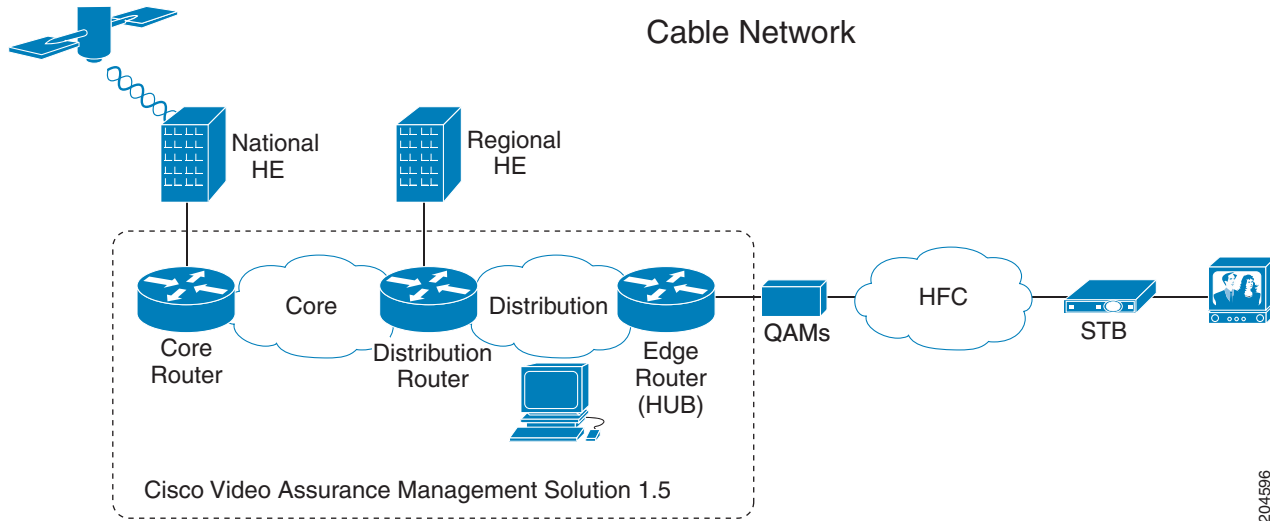
More information about Cisco Internet Protocol Television (IPTV) solutions for wireline carriers is viewable online at:

http://www.cisco.com/en/US/netsol/ns610/networking_solutions_solution_category.html

Cisco VAMS 1.5 in a Cable Network

Figure 1-3 shows the Cisco VAMS 1.5 in a cable network.

Figure 1-3   Cisco Video Assurance Management Solution 1.5 in a Cable Network

Most components of the cable network are the same as those shown in the wireline network (Figure 1-2), except for the home access portion. Hybrid Fiber-Coaxial (HFC) technology provides two-way, high-speed data access to the home by using a combination of fiber optics and traditional coaxial cable.

A national headend (HE) pulls content from different sources and grooms traffic into transport streams for distribution to the regional headends. The national HE aggregates live national content, processes it, encodes it, and distributes it to regional HEs.

Regional headends receive content from the national headend and from other sources, such as satellite and off-air antennas. Multiple converged regional area networks (RANs) are connected to the Internet through peering points provided by an Internet service provider

Cisco VAMS 1.5 covers the video transport network and focuses on the core and distribution networks shown in Figure 1-3. See also Figure 1-1 on page 1-3 for an example of the Cisco devices the Cisco VAMS 1.5 manages.

For detailed information about this supported architecture, see the *Cisco Gigabit-Ethernet Optimized Video Networking Solution for Cable Design and Implementation Guide, Release 3.0,* viewable online at:

http://www.cisco.com/en/US/products/ps6902/products_implementation_design_guide_book09186a00806470d8.html

More information about Cisco cable video solutions is viewable online at:

http://www.cisco.com/en/US/netsol/ns457/networking_solutions_solution_category.html
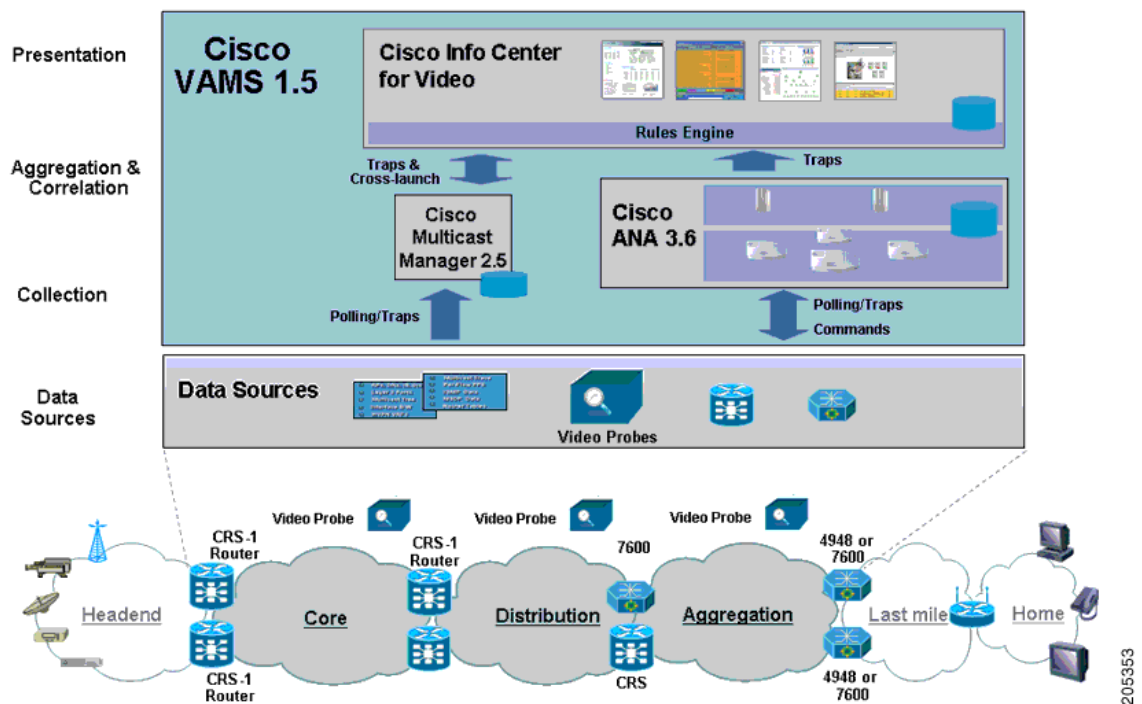
Cisco VAMS Solution Components

The Cisco VAMS 1.5 solution comprises:

- Cisco Multicast Manager 2.5.4, page 1-8
- Cisco Info Center, page 1-12
- Cisco ANA 3.6.3, page 1-17
- Third-Party Video Probes, page 1-26

Figure 1-4 shows the components in the VAMS 1.5 architecture.

Figure 1-4   *VAMS 1.5 System Architecture*

Network Elements in the Video Transport Network

Cisco VAMS 1.5 monitors these network elements (NEs), which form the core of the video transport network (see Figure 1-1 on page 1-3):

- 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 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, multilayer aggregation of high-performance servers and workstations.

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 1-7, for a list of the required IOS software.

Solution Component Versions

Besides the Cisco VAMS 1.5 software package, the Cisco VAMS 1.5 solution supports these components and software version levels:

Table 1-1   Solution Components and Version Information

Solution Component	Version Information
Active Network Abstraction (ANA)[1]	3.6 Service Pack 3 (3.6.3)
Cisco Multicast Manager	2.5.4
Cisco 7600 Series router and Cisco Catalyst 6500 Series switch (7600-SUP720-3BXL with redundant SUP720-3BXL) Line cards: 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)SRB2, 12.2(33)SRB3, 12.2(33)SRC1
Cisco CRS-1 Line cards: CRS-MSC, CRS1-SIP-800 (with SPA-8X1GE), 8-10GE	IOS-XR 3.6.1.12
Cisco Catalyst 4948 Series switch (CAT4948-10GE)	12.2(25)EWA6 or 12.2(31)SGA1
CIC (includes IBM Tivoli Netcool products)[2]	7.2 • ObjectServer - 7.2 • Webtop - 2.1 • TBSM - 4.1 • Impact - 4.0
Bridge Technologies video probe	VB Series: Version: 3.1.0-26
IneoQuest video probe	• Singulus G1-T Media Analyzer Firmware Version: TB-2.5s-060608 • Singulus G10 Firmware Version: Denali-1.3a-021808 • iVMS 3.00.00 with Patch 24 • IQ Cricket Firmware Version: Cricket-1.0a-092607

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

Solution Component	Version Information
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
PixelMetrix video probe	DVStation: Version: 4.17.0
Tektronix video probe	MTM400 Application Firmware Version: 3.1.061.000 FPGA Logic Firmware Version: 4 BIOS Version: 2.0.7 SNMP Interface Version: 2.6.0 Hardware Version: 5 QA Build: Alpha 01 Build Timestamp: Dec 19 2007 22:22:42

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 1.5 does not support carousel-related traps for the Mixed Signals Sentry 136.

Cisco Multicast Manager 2.5.4

This section describes the hardware and software components of CMM 2.5.4.

Cisco Multicast Manager 2.5.4 Hardware Components

CMM 2.5.4 hardware comprises:

- x86 Server, page 1-8
- Sun Microsystems Server, page 1-9

x86 Server

The CMM 2.5.4 x86 server uses one of these processors in a x86-type computer:

- Dual AMD Opteron 250.
- 2.4 GHz 64-bit (recommended for a large enterprise network of more than 500 devices).
- 2.8 GHz Intel Pentium IV.
- 2.8 GHz Intel Xeon processor.
- Dual 2.8 GHz Intel Pentium IV.
- Dual 2.8 GHz Intel Xeon processor (recommended for a large enterprise network of more than 500 devices).

Sun Microsystems Server

The CMM 2.5.4 Sun Microsystems server uses one of these Sun Fire series workstations:

- Sun Fire V440 (up to four 1.593 GHz UltraSPARC IIIi processors for a large enterprise network of more than 500 devices),
- Sun Fire V240 (one 1.34 GHz or two 1.5 GHz UltraSPARC processors).

CMM 2.5.4 Application

Using an x86-type computer running Linux or a Sun Microsystems Sun Fire series workstation running Solaris, the CMM 2.5.4 application (a web-based multicast troubleshooting tool) has two components: Administration and Multicast Manager. CMM 2.5.4 uses SNMP MIB polling to monitor devices and traffic in the network. CMM 2.5.4 also provides metrics and alerts, which it then forwards to the ANA as SNMP traps. Based on the unique requirements of the network environment, the SNMP traps are user-configurable.

The CMM 2.5.4 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

The CMM 2.5.4 also provides detailed diagnostics and a health-check capability.

You use CMM 2.5.4 to set thresholds, generate notifications, and forward them to CIC.

See the *User Guide for Cisco Multicast Manager 2.5,* viewable online at:

http://www.cisco.com/en/US/docs/net_mgmt/cisco_multicast_manager/2.5/user/guide/CMM_25_User_Guide.html

Cisco Multicast Manager 2.5.4 System Requirements

Table 1-2 lists the hardware and software requirements for the CMM 2.5.4.

Table 1-2   Cisco Multicast Manager 2.5.4 System Requirements

Item	Specifications
Hardware Requirements	
Platform type	Linux: • Dual AMD Opteron Processor 250 2.4-GHz 64-Bit (more than 500 devices) • Dual 2.8-GHz Intel Pentium IV or dual 2.8-GHz Intel Xeon processor (more than 500 devices) • 2.8-GHz Intel Pentium IV or 2.8-GHz Intel Xeon processor Solaris: • Sun Fire v440 up to four 1.593-GHz UltraSPARC IIIi processors (more than 500 devices) • Sun Fire v240 One 1.34-GHz or two 1.5-GHz UltraSPARC processors
Memory	Size: • 2 GB • 4 GB (more than 500 devices) • 2 GB or more of free space
Software Requirements	
Operating system	Linux: • Red Hat Enterprise Linux 3 • Red Hat Enterprise Linux 4 Solaris: • Solaris 8 • Solaris 9 • Solaris 10 **Note** Cisco does not support Solaris x86.
Browser	• Firefox 1.5 or higher • Internet Explorer 6 • Netscape 7.0 • Mozilla 1.7 • Safari 2.0

Cisco Multicast Manager 2.5.4 Software Components

As described previously, the CMM 2.5.4 application has an Administration and a Multicast Manager tool. You can select either tool from the menu at the upper left of CMM Web interface. You can perform the following tasks with each tool:

Administration

- Manage domains
- Use administrative utilities
- Configure security
- Manage users
- Perform discovery
- Configure devices
- Configure global polling
- Configure multicast polling
- Manage addresses

Multicast Manager

- View events through the **Home** page.
- View topology through the **Topology** page, such as:
    - Each router and its local interfaces.
    - The interfaces on each of the router's PIM neighbors.
    - The names of the routers and their PIM neighbors.
- Manage report through the **Reporting** page, such as:
    - A record of the latest SNMP traps sent.
    - Historical graphs or trends.
    - Routers in the database IOS versions.
    - Video probe reports.
    - Reports on VPN routing/forwarding instances (VRFs).
- Manage a global view and a router-specific view of your network through the **Diagnostics** page, such as:
    - Showing active sources and groups in the network.
    - Finding sources and receivers in the network.
    - Viewing the status of all devices in the current multicast domain.
    - Viewing all the routers in the database.
    - Viewing all the RPs that CMM is aware of, based on discovery.
    - Seeing the interfaces that have joined onto a particular group.
    - Viewing all the routers running Multicast Source Discovery Protocol (MSDP) and their peering connectivity. You can also view details for a specific router, such as peering information and the SA cache.
    - Viewing Layer 2 Multicast Information and Layer 2 Host IPs.
    - Running preconfigured network tests using the Health Check facility.
    - Enable the CMM to gather accurate packet forwarding statistics and other information in a timely manner.
    - Viewing the top 20 talkers, sorted by long term.

- Viewing diagnostic information about video probes and the flows that they are monitoring.

- Viewing a detailed trace about a video flow and a topology tree that shows: RPs, routers, interfaces, and probes.

- Viewing detailed information about the status of Multicast VPNs, including: VRF table configurations, Provider Edge (PE) device configurations, and the current status of a specified VRF.

- Viewing specific multicast diagnostics on a router.

- Viewing a PDF version of the *User Guide for the Cisco Multicast Manager 2.5* through the **Help** page.

For complete hardware and software requirements, see the following books:

Installation Guide for the Cisco Multicast Manager 2.5, viewable online at:
http://www.cisco.com/en/US/docs/net_mgmt/cisco_multicast_manager/2.5/installation/guide/
CMM_25_install_guide.html

User Guide for the Cisco Multicast Manager 2.5, viewable online at:

http://www.cisco.com/en/US/docs/net_mgmt/cisco_multicast_manager/2.5/user/guide/CMM_25_User
_Guide.html

Cisco Info Center

CIC/Netcool delivers real-time centralized monitoring and root-cause analysis by integrating the IBM Tivoli Netcool 7.1 components and the CIC with Cisco ANA 3.6.3, CMM 2.5.4, and video probe devices.

CIC 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 CIC/Netcool components comprise:

- IBM Tivoli Netcool/OMNIbus and ObjectServer, page 1-12

- IBM Tivoli Netcool/Webtop, page 1-14

- IBM Tivoli Netcool/Impact, page 1-15

- IBM Tivoli Business Service Manager, page 1-15

- IBM Tivoli Netcool GUI Foundation, page 1-16

- IBM Tivoli Netcool Probes, page 1-16

- Rules Files, page 1-16

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.

3. For a detailed definition, see the Glossary.

- Logs 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, you can use their network management skills.

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 visible in the event list.

See the following books:

- *Netcool/OMNIbus v7 User Guide is* viewable online at:

  http://www.cisco.com/en/US/products/sw/netmgtsw/ps996/products_user_guide_book09186a0080 47d044.html

- *Netcool/OMNIbus v7 ObjectServer Gateway Guide* is viewable online at:

  http://www.cisco.com/en/US/products/sw/netmgtsw/ps996/products_technical_reference_book091 86a008047d049.html

IIBM Tivoli Netcool/OMNIbus and ObjectServer Requirements

On Sun Microsystems SPARC-based platforms, Cisco supports:

- Solaris 8

- Solaris 9

- Solaris 10

On Hewlett-Packard PA-RISC-based platforms, Cisco supports:

HP-UX 11i (11.11)

On IBM PowerPC-based platforms:

- AIX 5L (5.2 RS/6000 32-bit)

- AIX 5L (5.3 RS/6000 32-bit)

On Intel x86 processor and chipset-based platforms, Cisco supports:

- Microsoft Windows 2000 Server

- Microsoft Windows 2000 Advanced Server

- Microsoft Windows 2003 Server

- Microsoft Windows 2000 Professional—desktop component only

- Microsoft Windows XP—desktop component only

- Red Hat Enterprise Linux AS, ES, and WS 3

- Red Hat Enterprise Linux AS, ES, and WS 4

- SUSE Linux Enterprise Server 9.2

JRE Requirements

The Netcool/OMNIbus Administrator GUI and the **nco_confpack** utility require the JRE to be installed on your system.

Netcool/OMNIbus supports the following JREs:

- Javasoft JRE 1.5 on Linux, Solaris, and Windows platforms
- IBM JRE 1.4.2 on AIX platforms
- HP JRE 1.5 on HP-UX platforms

User Interface Requirements

Netcool/OMNIbus supports the following user interface environments:

- UNIX/Motif 1.2 or CDE
- Microsoft Windows 2000, 2003, and XP

IBM Tivoli Netcool/Webtop

IBM Tivoli Netcool/Webtop publishes alerts for viewing in a web browser. Users can manipulate them by using an active event list launched from a web browser. The Webtop includes server administration pages to set up users, table views, and other configurable elements.

Webtop includes the Webtop Editor; a tool for creating and editing maps (filters and views). Webtop publishes Netcool alerts and active event list applets over HTTP or HTTPS[4] (HTTP with SSL) protocol to supported web browsers. Launched from a web browser, the active event list offers the functionality of Netcool/Java EventList (JEL) to acknowledge, prioritize, and delete alerts by using the Webtop technology.

Using a client-server architecture, the Webtop server runs inside the IBM Tivoli Netcool GUI Foundation application (see the "IBM Tivoli Netcool GUI Foundation" section on page 1-16 for more information). Clients connect to the IBM Tivoli Netcool GUI Foundation to access Netcool/Webtop.

See the administration guide for this product, available on the IBM website.

You can also launch Netcool/Webtop from the Tivoli Business Service Manager (TBSM) application. For information on launching TBSM and Netcool/Webtop to view VAMS 1.5 alerts, see Monitoring ANA, CMM, and Video Probe Events with TBSM, page 6-1.

IBM Tivoli Netcool/Webtop Requirements

On Sun Microsystems SPARC-based platforms, Cisco supports:

- Solaris 9
- Solaris 10

On Hewlett-Packard PA-RISC-based platforms, Cisco supports:

HP-UX 11i (11.11)

On IBM PowerPC-based platforms:

AIX 5L (5.3 RS/6000 32-bit)

On Intel x86 processor and chipset-based platforms, Cisco supports:

- Microsoft Windows 2003 Server (32 and 64 bit)

4. HTTPS—HTTP with SSL (secure sockets layer) encryption for security.

- Microsoft Windows XP SP2

- Red Hat Enterprise Linux AS, ES, and WS 3

- Red Hat Enterprise Linux AS, ES, and WS 4

- SUSE Linux Enterprise Server 9

- SUSE Linux Enterprise Server 10

Note Ensure that the IBM Tivoli Netcool Security Manager is installed, running, and accessible; and that you know the host, port, and administrative user name and password for the IBM Tivoli Netcool Security Manager before you install IBM Tivoli Netcool/Webtop. For information about how to install and configure the IBM Tivoli Netcool Security Manager, see the security manager installation guide for this product, available on the IBM website.

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.

See the administration, user interface, and solutions guides for this product, available on the IBM website.

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:

- 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 4.1.1 requires the Java Runtime Environment (JRE) to be installed on your system.

Netcool/TBSM supports the following JREs:

- Javasoft JRE 1.5 on Linux, Solaris, and Windows platforms
- IBM JRE 1.4.2 on AIX platforms
- HP JRE 1.5 on HP-UX platforms

⬥

Note   JRE versions higher than 1.5 in client web browsers result in a failure of the Service Viewer and the Service Details within the TBSM window.

IBM Tivoli Netcool GUI Foundation

The IBM Tivoli Netcool GUI Foundation (NGF) is a server application that delivers web-based Netcool products in a single, unified framework. The IBM Tivoli Netcool GUI Foundation provides single sign-on, consolidated user management, and a single point of access for different IBM Tivoli Netcool applications. The IBM Tivoli Netcool GUI Foundation also provides the ability to create customized pages and administer access to content by user, role, or group.

The IBM Tivoli Netcool GUI Foundation is installed automatically with the first IBM Tivoli Netcool GUI Foundation-enabled product. Subsequent products may install updated versions of the IBM Tivoli Netcool GUI Foundation. The Netcool GUI Foundation is not available separately.

The IBM Tivoli Netcool GUI Foundation uses IBM Tivoli Netcool/Security Manager for authentication and authorization.

See the administration guide for this product, available on the IBM website.

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.

Rules Files

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

Cisco ANA 3.6.3

This section describes the hardware and software components of Cisco ANA 3.6.3.

Cisco ANA 3.6.3 Hardware Components

Cisco ANA 3.6.3 hardware comprises:

- Cisco ANA Servers, page 1-17
- Cisco ANA Clients, page 1-20

> ✎
> **Note**   The hardware recommendations assume that the Cisco ANA 3.6.3 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 1-17
- Cisco ANA Unit, page 1-18

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 1-18). 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 3.6.3 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*

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, Version 3.6.2*, viewable online at:
	http://www.cisco.com/en/US/docs/net_mgmt/active_network_abstraction/3.6_sp2/release_notes/rn36_sp2.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 3.6.3 servers (gateway and unit) with any application other than Cisco ANA 3.6.3.

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 3.6.3 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 may 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 the exact patch list, see the *Cisco ANA Release Notes, Version 3.6 Service Pack 2,* viewable online at: http://www.cisco.com/en/US/docs/net_mgmt/active_network_abstraction/3.6_sp2/release_notes/rn36_sp2.html
Third-party tools	• Java v1.3.1_08 • Active Perl v5.6

Note   Do not use the Cisco ANA 3.6.3 servers (gateway and unit) with any application other than Cisco ANA 3.6.3.

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 1-24.)

Cisco ANA Client Requirements

Table 1-5 lists the hardware and software requirements for the Cisco ANA 3.6.3 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 3.6.3 Software Components

Cisco ANA 3.6.3 provides mediation and abstraction between NEs and OSS applications, and supports fault collection and root-cause analysis for the transport network. Cisco ANA 3.6.3 manages the NEs listed in the "Network Elements in the Video Transport Network" section on page 1-6. The Cisco ANA 3.6.3 features for the Cisco VAMS 1.5 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 3.6.3 automatically detects and manages the NEs in its domain, including their physical and logical inventories.

VNEs

The Cisco ANA 3.6.3 provides a VNE mediation layer between the managed NEs and the network management applications in the Cisco ANA 3.6.3. Generally, a one-to-one correspondence exists between an NE in the managed network and the VNE that depicts it in the Cisco ANA 3.6.3. The VNEs collect information from their corresponding NEs for management purposes.

Cisco VAMS 1.5 uses VNEs to represent the solution components in Table 1-6.

Table 1-6   VNEs for the Cisco VAMS 1.5

Solution Component	VNE Description
Cisco 7600 Series routers	7600 VNE[1]
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
Tektronix Video Probe	Generic SNMP VNE

1. Cisco ANA 3.6.3 activation scripts and soft properties created for the Cisco VAMS 1.5 enable the VNE to monitor multicast video flows.

Command Builder Scripts

Cisco VAMS 1.5 introduces command builder scripts (created in the ANA Command Builder tool) that configure managed devices to collect, calculate, and analyze multicast and video data; and notify the Cisco ANA 3.6.3 when preconfigured conditions occur. These command builder scripts use the Event MIB and a rules engine to provide support for multicast alarms in the Cisco ANA 3.6.3.

Cisco VAMS 1.5 provides an Internet Protocol Television (IPTV) command builder script for the Cisco 7600 Series router, CRS-1, and Catalyst 4948 Series switch VNEs. The script runs at installation time and whenever managed devices reload. In addition, you can run the IPTV command builder script on demand. See the "Run the Setup for IPTV Script" section on page 5-15.

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.

Note   Delivered as part of this solution, the Cisco VAMS 1.5 already configures the soft properties and TCAs in the IPTV command builder script. (See the "Command Builder Scripts" section on page 1-21.)

Configuration Management and Inventory

Cisco ANA 3.6.3 automatically detects managed NEs in the video transport network along with their physical and logical inventories. Cisco ANA 3.6.3 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 3.6.3 also supports discovery of the network topology (automatically and manually).

Cisco ANA 3.6.3 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

- 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 1-6, for details about the Cisco NEs.

Fault Management

The Cisco ANA 3.6.3 provides fault management for the video transport network:

- Event and Alarm Management, page 1-22
- Polling and CPU Utilization, page 1-22
- GUIs for Fault Management, page 1-23

See the *Cisco ANA Fault Management User Guide 3.6 Service Pack 2* for a description of the Cisco ANA fault management system, viewable online at:

http://www.cisco.com/en/US/docs/net_mgmt/active_network_abstraction/3.6_sp2/fault/user/guide/chp1.html

Event and Alarm Management

The Cisco ANA 3.6.3 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.
- Changing severity of alarms in the Cisco VAMS 1.5.

Polling and CPU Utilization

Cisco ANA 3.6.3 monitors CPU utilization of the supported NEs in the Cisco VAMS 1.5. You can define polling groups and designate polling intervals for the ANA-managed NEs. The ANA uses an adaptive polling mechanism to ensure that the NEs are not overpolled.

For more information about ANA polling and its interaction with the CPU utilization of managed NEs, see the *Cisco ANA Administrator User Guide 3.6 Service Pack 2,* viewable online at:

http://www.cisco.com/en/US/docs/net_mgmt/active_network_abstraction/3.6_sp2/administrator/administration/guide/global.html#wp1041531

Cisco ANA 3.6.3 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 1.5.

For more information about ICMP polling, see the *Cisco ANA Administrator User Guide 3.6 Service Pack 2,* viewable online at:

http://www.cisco.com/en/US/docs/net_mgmt/active_network_abstraction/3.6_sp2/administrator/administration/guide/manavm.html#wp1041967

Cisco ANA 3.6.3 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 3.6 Service Pack 2,* viewable online at:

http://www.cisco.com/en/US/docs/net_mgmt/active_network_abstraction/3.6_sp2/command_builder/developer/guide/cmdbuild-Book-Wrapper.html

GUIs for Fault Management

Cisco ANA 3.6.3 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 1-6, for descriptions of the supported NEs.)

- Events, including severity levels and timestamps.

Note   Cisco ANA NetworkVision, page 1-25 and Cisco ANA EventVision, page 1-26 are the software tools that provide these GUIs.

Security Management

Cisco ANA 3.6.3 provides user identification and authentication for accessing the Cisco ANA 3.6.3 to perform configuration and fault management tasks on the supported NEs. For more information about security information in Cisco ANA 3.6.3, view the information online at:

http://www.cisco.com/en/US/docs/net_mgmt/active_network_abstraction/3.6/administrator/mansec.html

Multicast and Video Management

Cisco ANA 3.6.3 provides these multicast and video metrics:

- PIM Alarms, page 1-23
- Multicast Routes, page 1-24
- Non-RPF Drops, page 1-24

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.

You can view PIM alarms in the ANA EventVision tool. Cisco ANA creates alarms for the following multicast-related SNMP traps:

- pimNeighborLoss—Signifies the loss of an adjacency with a neighbor. The router generates the trap when the neighbor timer expires, and the router has no other neighbors on the same interface with a lower IP address than itself.

- ciscoPimInterfaceUp—Signifies the restoration of a PIM interface.

- ciscoPimInterfaceDown—Signifies the loss of a PIM interface.

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.

Cisco VAMS 1.5 creates soft properties on VNEs to support viewing:

- Multicast (whether you are enabling an NE for multicast).
- PIM configurations on an interface (whether you are enabling the PIM, the PIM mode, and the designated router (DR) address for the PIM interface).
- IGMP configurations on an interface for a Cisco 7600 router or Catalyst 4948 switch (whether you are enabling the IGMP leave, the IGMP protocol version, or the number of IGMP interface groups).

> **Note** The current Cisco VAMS 1.5 release does not support viewing IGMP status on Cisco CRS-1 NEs.

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 3.6.3 receives the notification and generates an alarm. The Cisco ANA 3.6.3 correlates subsequent alarms and generates subalarms.

Troubleshooting

You perform most fault management tasks through the Cisco ANA 3.6.3 software tools. You perform advanced troubleshooting of the multicast video network by using the CMM 2.5.4. See Chapter 6, "Troubleshooting with the Cisco Video Assurance Management Solution 1.5."

Cisco ANA Client Software Tools

Cisco ANA 3.6.3 includes several applications built on top of the virtual network as the mediation layer.

Cisco ANA 3.6.3 applications include:

- Cisco ANA Manage, page 1-24
- Cisco ANA NetworkVision, page 1-25
- Cisco ANA EventVision, page 1-26

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.

Specifically, you use the Cisco ANA Manage tool to perform system administration activities including:

- Adding and removing Cisco ANA units, Autonomous Virtual Machines (AVMs), and VNEs.
- Starting and stopping VNEs.

- Setting polling information per VNE.

- Customizing polling groups and protection groups.

- Managing static and persistent topology links.

- Installing and managing Cisco ANA client licenses.

- Defining and managing user accounts.

See the *Cisco ANA Administrators Guide 3.6 Service Pack 2,* viewable online at:

http://www.cisco.com/en/US/docs/net_mgmt/active_network_abstraction/3.6_sp2/administrator/
administration/guide/Admin-Book-Wrapper.html

Cisco ANA NetworkVision

You use the Cisco ANA NetworkVision tool (the main GUI for Cisco ANA 3.6.3) 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.

You use the Cisco ANA NetworkVision to:

- View network inventory and multilayer connectivity.

- Troubleshoot, monitor, and manage NEs.

- Model and view network maps maintaining up-to-date topological information on device connections, traffic, and routes.

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 NetworkVision User Guide 3.6 Service Pack 2,* viewable online at:

http://www.cisco.com/en/US/docs/net_mgmt/active_network_abstraction/3.6_sp2/networkvision/user/guide/nvug.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 may prevent future problems.

You can configure Cisco ANA EventVision to display:

- Number of events per page
- Number of events to export to a file
- Filter options
- Information that appears in EventVision tabs

Administrators periodically review and manage the events list by using the Cisco ANA EventVision tool. In addition, when an event occurs in the Cisco ANA 3.6.3 system, Cisco ANA EventVision displays specific details.

See the *Cisco ANA EventVision User Guide 3.6 Service Pack 2,* viewable online at:

http://www.cisco.com/en/US/docs/net_mgmt/active_network_abstraction/3.6_sp2/eventvision/user/guide/Event-Book-Wrapper.html

Third-Party Video Probes

Cisco VAMS 1.5 supports several third-party probes including the Bridge Technologies, IneoQuest, Mixed Signals, PixelMetrix, and Tektronix 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:

- The video probes communicate traps directly to CIC. When you are viewing a video probe event forwarded by these probes, you can launch CMM diagnostics directly from the CIC interface.
- Certain video probes, such as the IneoQuest probe and the iVMS NMS, communicate traps directly to CMM—CMM can then be configured to forward the traps to CIC.

Cisco VAMS 1.5 receives events from the probes based on thresholds that you configure in the video probes. The Cisco VAMS 1.5 associates probe events with a severity level in Cisco CIC.

Generic VNEs in the Cisco ANA 3.6.3 support the video-monitoring probes. Generic SNMP VNEs handle the IneoQuest and Tektronix probes. A Generic ICMP VNE (no inventory support) handles the Mixed Signals probe.

The video probe VNEs enable the Cisco ANA 3.6.3 to receive SNMP traps from the video probes. (See Appendix A, "Trap Definitions.")

Note IneoQuest probes are polled directly by the CMM 2.5.4 application.

See the appropriate video probe guides for this product listed in the "Related Documentation" section on page ix.

Cisco VAMS 1.5 Solution Software Description

Table 1-7 lists the software product information and Cisco part numbers for the Cisco VAMS 1.5 release.

Table 1-7   Software Products with Cisco Part Number

Description	Cisco Part Number
Cisco Video Assurance Management Solution 1.5 (top level part number)	VAMS-1-SOFTWARE
Video Extension to 4948 (G2) VNE—Software (optional, qty 0-1)	VAMS-1.0-3.6VNE4948
Video Extension to 7600 (G3) VNE—Software (optional, qty 0-1)	VAMS-1.0-3.6VNE7600
Video Extension to CRS-1 (G5) VNE—Software (optional, qty 0-1)	VAMS-1.0-3.6VNEG5
Video Extension to CRS-1 (G6) VNE—Software (optional, qty 0-1)	VAMS-1.0-3.6VNEG6
Video Extension Cisco Multicast Manager (CMM) VNE—Software (optional, qty 0-1)	VAMS-1.0-3.6VNECMM
IneoQuest Video Probe VNE—Software (optional, qty 0-1)	VAMS-1.0-3.6VNEIQ
Mixed Signals Video Probe VNE—Software (optional, qty 0-1)	VAMS-1.0-3.6VNEMS
Tektronix Video Probe VNE—Software (optional, qty 0-1)	VAMS-1.0-3.6VNETK
IneoQuest Video Probe RTU—Right-to-use for one IQ probe (optional, qty 0-1)	VAMS-1.0-3.6IQRTU
Mixed Signals Video Probe RTU—Right-to-use for one MS probe (optional, qty 0-1)	VAMS-1.0-3.6MSRTU
Tektronix Video Probe RTU—Right-to-use for one TK probe (optional, qty 0-1)	VAMS-1.0-3.6TKRTU
CMM 2.5.4	
VAMS 1.5 ANA Extensions	
VAMS 1, Extensions to ANA 3.6 (top level part number)	VAMS1-ANA3.6-SW
VAMS 1, Extension to 4948 (G2) VNE - ANA 3.6 (optional, qty 0-1)	VAMS1-ANA36VNE4948
VAMS 1, Extension to 7600 (G3) VNE - ANA 3.6 (optional, qty 0-1)	VAMS1-ANA36VNE7600
VAMS 1, Extension to CRS-1(G5) VNE - ANA 3.6 (optional, qty 0-1)	VAMS1-ANA36VNEG5
VAMS 1, Extension to CRS-1(G6) VNE - ANA 3.6 (optional, qty 0-1)	VAMS1-ANA36VNEG6
VAMS 1, Cisco Multicast Manager VNE - ANA 3.6 (optional, qty 0-1)	VAMS1-ANA36VNECMM
VAMS 1, IneoQuest Video Probe VNE - ANA 3.6 (optional, qty 0-1)	VAMS1-ANA36VNEIQ
VAMS 1, Mixed Signals Video Probe VNE - ANA 3.6 (optional, qty 0-1)	VAMS1-ANA36VNEMS
VAMS 1, Tektronix Video Probe VNE - ANA 3.6 (optional, qty 0-1)	VAMS1-ANA36VNETK
VAMS 1, IneoQuest Video Probe RTU - ANA 3.6—Right-to-use for one IQ probe (optional, no limit on qty)	VAMS1-ANA36IQRTU
VAMS 1, Mixed Signals Video Probe RTU - ANA 3.6—Right-to-use for one MS probe (optional, no limit on qty)	VAMS1-ANA36MSRTU
VAMS 1, Tektronix Video Probe RTU - ANA 3.6—Right-to-use for one TK probe (optional, no limit on qty)	VAMS1-ANA36TKRTU

Table 1-7   Software Products with Cisco Part Number (continued)

Description	Cisco Part Number
VAMS 1.5 CIC Extensions	
VAMS 1, Extensions to CIC (top level part number)	VAMS1-CIC-SW
VAMS 1, Extensions to CIC 7.2 ObjectServer/Webtop (optional, qty 0-1)	VAMS-CICMOM72-K9
VAMS 1, Extensions to CIC 7.2 ObjectServer/Webtop - Failover (optional, qty 0-1)	VAMS-CICMOM72F-K9
VAMS 1, Extensions to CIC 7.2 ObjectServer/Webtop - Non Prod (optional, qty 0-1)	VAMS-CICMOM72N-K9
VAMS 1, Extensions to CIC 7.2 TBSM 4.1 (optional, qty 0-1)	VAMS-CICTBSM41-K9
VAMS 1, Extensions to CIC 7.2 TBSM 4.1 - Failover (optional, qty 0-1)	VAMS-CICTBSM41F-K9
VAMS 1, Extensions to CIC 7.2 TBSM 4.1 - Non Prod (optional, qty 0-1)	VAMS-CICTBSM41N-K9
VAMS 1, Extensions to CIC 7.2 Impact 4.0 (optional, qty 0-1)	VAMS-CICIMPT40-K9
VAMS 1, Extensions to CIC 7.2 Impact 4.0 - Non Prod (optional, qty 0-1)	VAMS-CICIMPT40N-K9

Cisco Advanced Services Support for VAMS

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

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

This section describes:

- Cisco Lifecycle Approach, page 1-28
- Prepare Phase, page 1-29
- Plan Phase, page 1-30
- Design Phase, page 1-30
- Implement Phase, page 1-30

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 1.5, 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 1-1 lists each phase in the product lifecycle and describes the type of support that Advanced Services and other consulting groups at Cisco provide.

Table 1-8   Cisco Lifecycle 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 both ANA and CIC integration. The solution complexity scales based on the number of multicast streams (channels), ad-zones, multicast-enabled routes. Addition of probes, ANA and CIC will increase the complexity of the integration. Probes can be added to any offering whether base or a fully integration with ANA and CIC.

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 ANA managed nodes and alarm thresholds (ANA only).
- Data collection regarding VAMS CIC-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 CIC) and associated Low-Level Design (LLD) documents.
- VAMS test plan development (CMM, probes, ANA, and/or CIC.
- VAMS implementation plan.
- VAMS design validation and review.
- Probes placement methodology.
- Network management for probes.
- Probe configuration.
- Probe network management plan.
- ANA-plug in configuration for VAMS (ANA).
- Specific configuration for CIC.

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 CIC plug-in (CIC only).

- Test plan execution.

- CMM cases.

- Probes cases.

- ANA VAMS-plug in cases.

- CIC-plug in cases.

- AS build documents and support for on-site knowledge transfer.