# User Guide for Cisco Video Assurance Management Solution 1.0

April 2008

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

Text Part Number: OL-15678-02

*User Guide for Cisco Video Assurance Management Solution 1.0*

# CONTENTS

# Preface

This preface describes who should read the *User Guide for Cisco Video Assurance Management Solution 1.0*, and the objectives, audience, organization, and conventions for the guide.

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

This preface contains the following:



## Document Revision History

The following Document Revision History table records technical changes to this document. The table shows the document revision number for the change, the date of the change, and a brief summary of the change.

| Revision | Date | Change Summary |
|---|---|---|
| OL-15678-02 | April 21, 2008 | Revised the following tables in Chapter 1, "Overview":<br>• Table 1-3 on page 14<br>• Table 1-4 on page 14<br>• Table 1-5 on page 15<br>• Table 1-6 on page 15<br>Added the following table in Chapter 1, "Overview":<br>• Table 1-7 on page 16<br>Moved Prerequisites from Chapter 1, "Overview" to Chapter 2, "Installing the Cisco Video Assurance Management Solution."<br>Moved Performance Metrics from Chapter 1, "Overview" to Appendix A "Trap Definitions." |
| OL-15678-01 | February 25, 2008 | Initial release. |

# Objectives

This guide describes the architecture, the components, and the processes necessary for the design and implementation of the Cisco Video Assurance Management Solution (Cisco VAMS), Release 1.0.

**Note** This document is primarily for Cisco products. To establish and maintain the third-party products and applications that might be a part of the Cisco VAMS, refer to the documentation that the vendors of those products provide.

# Audience

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

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

**Note** This document addresses Cisco components only. It does not discuss how to implement third-party components typically required for video management capabilities.

# Document Organization

The major sections of this document are:

| Chapter | Title | Description |
|---|---|---|
| Chapter 1 | Overview | Introduces implementation and scope of the Cisco VAMS, its components, and miscellaneous support topics. |
| Chapter 2 | Installing the Cisco Video Assurance Management Solution | Describes installing and uninstalling the Cisco VAMS. |
| Chapter 3 | Configuring the Components of the Cisco Video Assurance Management Solution | Describes configuring the components of the Cisco VAMS. |
| Chapter 4 | Troubleshooting with the Cisco Video Assurance Management Solution | Provides information about troubleshooting with the Cisco VAMS. |
| Appendix A | Trap Definitions | Provides definitions of traps supported by the Cisco VAMS. |

# Related Documentation

For information beyond the scope of this document, or for additional information about the Cisco VAMS product and its third party documentation, refer to the following documentation:

- Cisco Product Documentation, page vii
- Third-party Documentation, page x

## Cisco Product Documentation

Cisco provides the following Cisco documentation:

- Cisco Active Network Abstraction, page viii
- Cisco Multicast Manager, page ix
- Cisco Switches and Routers, page ix
- Cisco Internet Protocol Television (IPTV) Solutions, page ix

## Cisco Active Network Abstraction

Cisco Active Network Abstraction (ANA) 3.6 Service Pack 2 is the element management platform for the Cisco VAMS.

### Cisco ANA Release Notes

The Cisco ANA Release Notes are viewable online at:

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

### Cisco ANA User and Reference Guides

- *Cisco Active Network Abstraction EventVision User Guide Version 3.6*
- *Cisco Active Network Abstraction Fault Management User Guide Version 3.6*
- *Cisco Active Network Abstraction Managing MPLS User Guide Version 3.6*
- *Cisco Active Network Abstraction NetworkVision User Guide Version 3.6*
- *Cisco Active Network Abstraction Technology Support and Information Model Reference Manual, Version 3.6*
- *Cisco Active Network Abstraction 3.6 Virtual Network Element Reference Guide*

The Cisco ANA user and reference guides are viewable online at:

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

### Cisco ANA Configuration Guides

- *Cisco Active Network Abstraction BQL User Guide 3.6*
- *Cisco Active Network Abstraction Command Builder User Guide 3.6*
- *Cisco Active Network Abstraction Customization User Guide 3.6*
- *Cisco Active Network Abstraction Workflow User Guide 3.6*

The Cisco ANA configuration guides are viewable online at:

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

### Cisco ANA Administration Guides

- *Cisco Active Network Abstraction Administrator Guide 3.6*
- *Cisco Active Network Abstraction Error Messages 3.6*
- *Cisco Active Network Abstraction High Availability User Guide 3.6*
- *Cisco Active Network Abstraction Shell User Guide 3.6*

The Cisco ANA Administrative guides are viewable online at:

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

## Cisco Multicast Manager

Cisco Multicast Manager forwards traps from the video transport network to Cisco ANA. The Cisco Multicast Manager documents include and are viewable online at:

- *Release Notes for Cisco Multicast Manager 2.4*

  http://www.cisco.com/en/US/products/ps6337/prod_release_notes_list.html
- *Installation Guide for Cisco Multicast Manager, 2.4*

  http://www.cisco.com/en/US/products/ps6337/prod_installation_guides_list.html
- *User Guide for Cisco Multicast Manager 2.4*

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

## Cisco Switches and Routers

Documentation resources for the Cisco routers and Catalyst switches include and are available online at:

### Cisco 7600 Series Routers

http://www.cisco.com/en/US/products/hw/routers/ps368/tsd_products_support_series_home.html

Release notes for the 12.2(33)SRB2 IOS software to enable Cisco 7600 Series routers for this solution:

http://www.cisco.com/en/US/products/ps6922/prod_release_note09186a00806c096f.html

### Cisco Carrier Routing System (CRS-1)

http://www.cisco.com/en/US/products/ps5763/tsd_products_support_series_home.html

Release notes for the IOS-XR 3.4.2 software to enable Cisco CRS-1 for this solution:

http://www.cisco.com/en/US/docs/ios_xr_sw/iosxr_r3.4/general/release/notes/reln_342.html

### Cisco Catalyst 4900 Series Switches

http://www.cisco.com/en/US/products/ps6021/tsd_products_support_series_home.html

Release notes for the 12.2(31)SG IOS software to enable Cisco Catalyst 4948 switches for this solution:

http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/release/note/OL_9592.html

## Cisco Internet Protocol Television (IPTV) Solutions

Video solutions that the Cisco VAMS supports include and are viewable online at:

### Cisco IPTV Wireline Solutions

*Cisco Wireline Video/IPTV Solution Design and Implementation Guide, Release 1.1*

http://www.cisco.com/en/US/products/ps6902/products_implementation_design_guide_book09186a00806b5b4c.html

### Cisco IPTV Cable Solutions

*Cisco Gigabit-Ethernet Optimized Video Networking Solution for Cable Design and Implementation Guide, Release 3.0*

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

# Third-party Documentation

Additional third-party documentation to consult include the:

**IneoQuest IQMediaMonitor Series M1 Singulus G1-T**

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

**Mixed Signals Sentry**

- *Mixed Signals Sentry Digital Content Monitor User Guide*

**Tektronix MTM400**

- *MTM400 MPEG Transport Stream Monitor User Manual*
- *MTM400 MPEG Transport Stream Monitor Technical Reference*
- *MTM400 MPEG Transport Stream Monitor Programmer Manual*

# Document Conventions

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

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

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

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

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

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

# Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

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

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

CHAPTER 1

# Overview

The *User Guide for Cisco Video Assurance Management Solution 1.0* is a reference tool that provides a complete overview of the hardware and software products that comprise the Cisco Video Assurance Management Solution (Cisco VAMS). This guide describes key benefits and advantages, key features, and technical specifications for the products that make up the Cisco VAMS. The guide also describes installation, configuration, and troubleshooting tasks.

Network administrators can use the Cisco VAMS to configure, diagnose, and facilitate the tasks of managing the transport section of a multicast video network. You can use these tools to:

- Simplify and automate configuration tasks
- Gain visibility into the health and performance of the network
- Analyze and troubleshoot faults and exceptions
- Ensure security, accountability and compliance to organizational policies and regulatory requirements

This chapter contains the following:



## License Information

See Appendix B, “End User License Agreement Supplement.”

# Introduction to Cisco VAMS

The successful deployment of video over IP creates new challenges for the service provider. Because video is sensitive to packet loss and jitter, the service provider must carefully monitor bandwidths to ensure that network resources are not overwhelmed. When potential problems are detected, the service provider must quickly determine the source of the problem and take corrective action. Therefore, video service assurance is a primary concern of cable and wireline video service providers.

The Cisco VAMS 1.0 delivers to service providers real-time, centralized monitoring of backbone, regional, and aggregation networks for broadcast video transport. The Cisco VAMS 1.0 provides the framework for a flexible end-to-end assurance platform for video.

The Cisco VAMS 1.0 uses Cisco ANA 3.6 Service Pack 2 (ANA 3.6.2) to build an abstracted network model through a set of virtual network elements (VNEs). Each VNE represents an element in the managed network. The Cisco VAMS 1.0 extends the base functions of Cisco ANA 3.6.2 VNEs for Cisco 7600s Series routers, Cisco Catalyst 4948 switches, and Cisco Carrier Routing System (CRS-1) devices. These VNE extensions address the specific requirements of video delivery across the IP network.

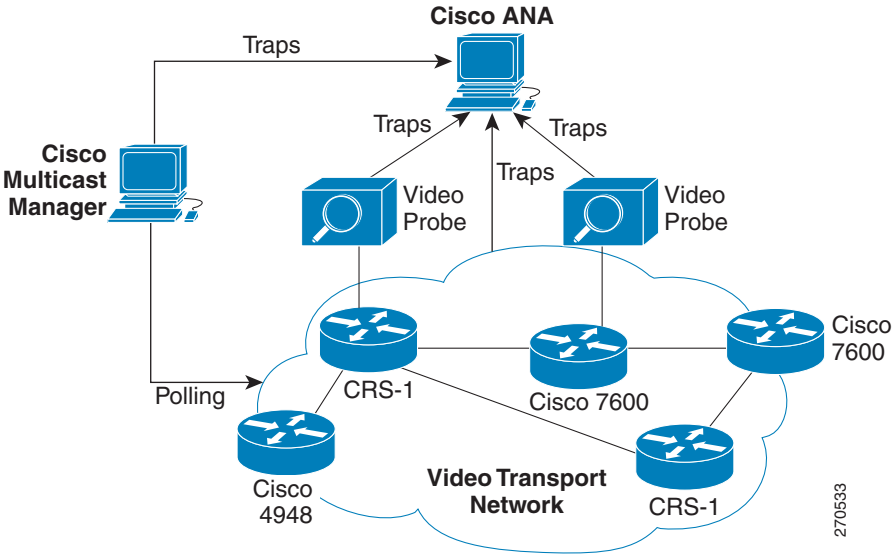
The Cisco VAMS 1.0 uses the Cisco Multicast Manager 2.4 for multicast monitoring and troubleshooting functions. The Cisco Multicast Manager notifies Cisco ANA of any changes in multicast or threshold events on elements in the multicast trees that may affect video performance. The ANA displays device and multicast fault information in the ANA NetworkVision, ANA EventVision, and ANA Manage software tools.

In addition, the Cisco VAMS 1.0 includes dedicated VNEs supporting specific video probes; this release includes VNEs for Ineoquest, Mixed Signals, and Tektronics video probes.

## Components of Cisco VAMS

Figure 1-1 shows the components of the Cisco VAMS (the topology is an example).

***Figure 1-1 Cisco Video Assurance Management Solution Components***

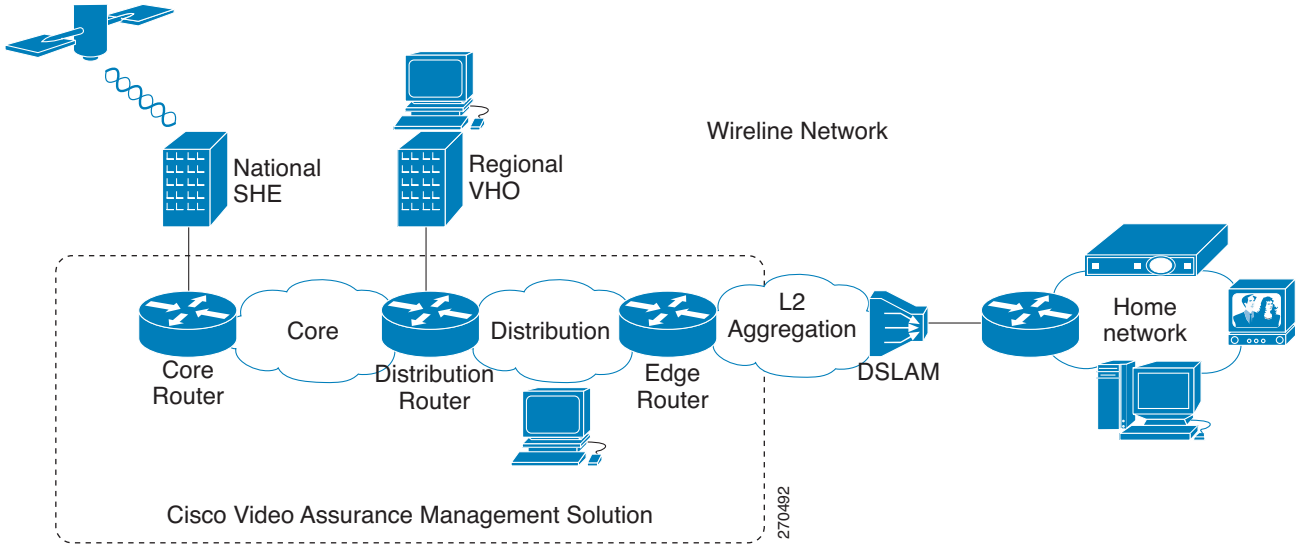



See Solution Components, page 1-5, for descriptions of the Cisco VAMS components shown in Figure 1-1.

# Cisco VAMS in a Wireline Network

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

***Figure 1-2 Cisco Video Assurance Management Solution in 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.

The Cisco VAMS covers the video transport network and focuses on the core and distribution networks shown in Figure 1-2. The Cisco VAMS manages the Cisco devices shown in Figure 1-1 on page 1-2.

A Digital Subscriber Line Access Multiplexer (DSLAM) connects digital subscriber lines to the network by multiplexing the traffic onto one or more network trunk lines.

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

http://www.cisco.com/en/US/products/ps6902/products_implementation_design_guide_book09186a00806b5b4c.html

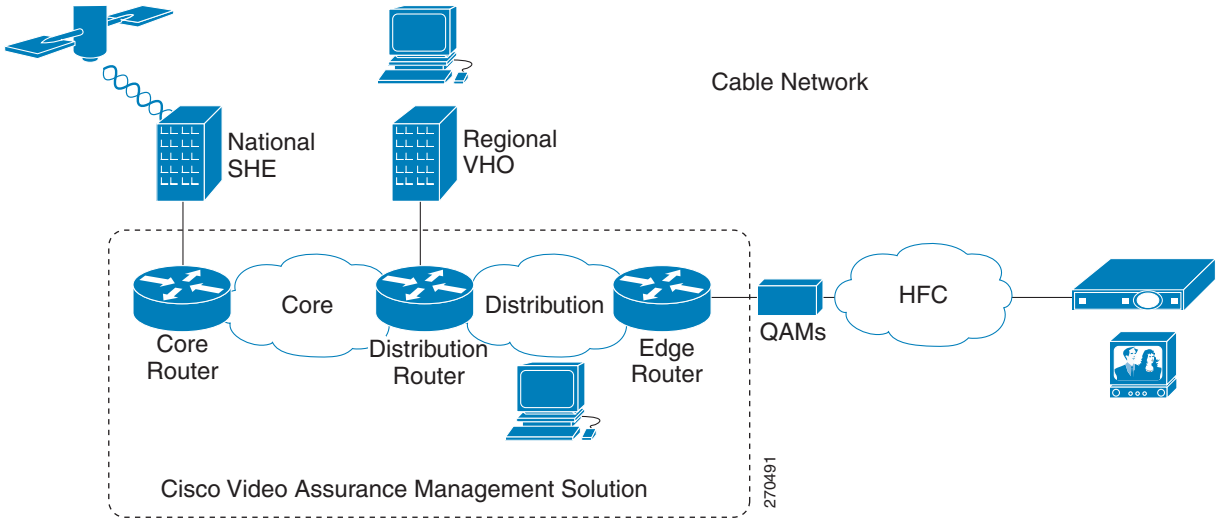
More information about Cisco IPTV solutions for wireline carriers is available here:

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

# Cisco VAMS in a Cable Network

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

***Figure 1-3 Cisco Video Assurance Management Solution in 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-Coax technology provides two-way, high-speed data access to the home using a combination of fiber optics and traditional coaxial cable.

The Cisco VAMS covers the video transport network and focuses on the core and distribution networks shown in Figure 1-2. The Cisco VAMS manages the Cisco devices shown in Figure 1-1 on page 1-2.

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*:

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

More information about Cisco cable video solutions is available here:

http://www.cisco.com/en/US/netsol/ns457/networking_solutions_solution_category.html

# Solution Components

This solution includes several software and hardware components:



## Network Elements in the Video Transport Network

The Cisco VAMS manages these NEs, which form the core of the video transport network (Figure 1-1 on page 1-2):

- Cisco 7600 Series—A carrier-class edge router that offers integrated, high-density Ethernet switching, carrier-class IP/MPLS routing, and 10-Gb/s interfaces.
- Cisco Carrier Routing System (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—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 Solution Components and Versions, page 1-13, for a list of the required IOS software.

## Cisco ANA

The Cisco ANA provides mediation and abstraction between NEs and OSS applications, and supports fault collection and root cause analysis for the transport network. The Cisco ANA manages the NEs listed in Network Elements in the Video Transport Network, page 1-5. The Cisco ANA features for the Cisco VAMS include:

- Soft properties and activation scripts (also called, 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, Catalyst 4948, Cisco CRS-1).
- Generic VNEs to support Cisco Multicast Manager and video probes.
- Event-handling and threshold-crossing alerts (TCA) for video-affecting conditions.
- New trap and syslog support through event configuration and customization.

The ANA automatically detects and manages the network elements in its domain, including their physical and logical inventories. In addition, VNEs provide support for the Cisco Multicast Manager (see Cisco Multicast Manager, page 1-12) and several third-party probes (Third-Party Video Probes, page 1-12) that monitor the video quality of the transport network.

This section of the guide contains these topics:



## VNEs

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

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

***Table 1-1 VNEs for the Cisco VAMS***

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

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

## Activation Scripts

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

The Cisco VAMS provides an IPTV activation script for the Cisco 7600, CRS-1, and Catalyst 4948 VNEs. The script runs at installation time and whenever managed devices reload. In addition, the operator can run the IPTV activation script on demand. See Run the Setup for IPTV Script, page 3-7.

## 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 be polled 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** Soft properties and TCAs are already configured in the IPTV activation script (see Activation Scripts, page 1-6) delivered as part of this solution.

## Configuration Management and Inventory

The Cisco ANA automatically detects managed network elements (NEs) in the video transport network along with their physical and logical inventories. The Cisco ANA 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.

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

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

- Cisco 7600 Series routers
- Cisco Carrier Routing System-1 (CRS-1)
- Cisco Catalyst 4948 switch

This support includes:

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

See Network Elements in the Video Transport Network, page 1-5, for details about the Cisco NEs.

## Fault Management

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

- Event and Alarm Management, page 1-8
- Polling and CPU Utilization, page 1-8
- GUIs for Fault Management, page 1-8

See the *Cisco ANA Fault Management User Guide* for a description of the Cisco ANA fault management system:

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 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.

### Polling and CPU Utilization

The Cisco ANA monitors CPU utilization of the supported NEs in the Cisco VAMS. 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*:

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

The Cisco ANA also supports Internet Control Message Protocol (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.

For more information about ICMP polling, see the *Cisco ANA Administrator User Guide*:

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

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

See the *Cisco ANA Command Builder User Guide*:

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

The Cisco ANA provides GUIs that show NE:

- Status information on the components that this solution supports (See Network Elements in the Video Transport Network, page 1-5, for descriptions of the supported NEs.)
- Events, including severity levels and timestamps

**Note** Cisco ANA EventVision, page 1-11, and Cisco ANA NetworkVision, page 1-11 are the software tools that provide these GUIs.

## Security Management

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

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

## Multicast and Video Management

The Cisco VAMS provides these multicast and video metrics:


- PIM Alarms, page 1-9
- Multicast Routes, page 1-9
- Non-RPF Drops, page 1-10


### PIM Alarms

The Cisco VAMS 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. The Cisco VAMS creates alarms for the following multicast-related SNMP traps:

- pimNeighborLoss—Signifies the loss of an adjacency with a neighbor. This trap is generated 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

The Cisco VAMS uses a VNE soft property to display the number of multicast routes in the device (Cisco 7600, Catalyst 4948, and Cisco CRS-1). ANA NetworkVision displays the number of multicast routes on the selected device.

The Cisco VAMS 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. The ANA receives the trap and creates an event in the ANA EventVision.

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

- Whether an NE is enabled for multicast.
- PIM configurations on an interface (whether PIM is enabled, 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 IGMP leave is enabled, the IGMP protocol version, and the number of IGMP interface groups).

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

### Non-RPF Drops

The Cisco VAMS monitors non-Reverse Path Forwarding (non-RPF) drops on each multicast stream. Non-RPF packets, also called RPF failure packets, are RPF packets that have been transmitted backwards, against the flow from the source. Multicast streams include video and nonvideo streams. If the number of non-RPF drops on a multicast stream exceeds 5 during a polling period, the device sends an SNMP notification. The ANA receives the notification and generates an alarm. The ANA correlates subsequent alarms and generates subalarms.

### Troubleshooting

You perform most fault management tasks through the ANA software tools. You perform advanced troubleshooting of the multicast video network by using the Cisco Multicast Manager 2.4. See Chapter 4, "Troubleshooting with the Cisco Video Assurance Management Solution."

## Cisco ANA Software Tools

Cisco ANA includes several application suites that are built on top of the virtual network as the mediation layer. The Cisco ANA applications are:

- Cisco ANA Manage, page 1-10
- Cisco ANA NetworkVision, page 1-11
- Cisco ANA EventVision, page 1-11

### Cisco ANA Manage

You use the ANA Manage to add, delete, or modify the Cisco NEs in the Layer 2 transport sections of multicast video networks.

Cisco ANA Manage is the GUI tool that you use 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*:

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

Cisco ANA NetworkVision is the main GUI for Cisco ANA. Cisco ANA NetworkVision is a user interface for viewing the network inventory and topology. The ANA NetworkVision also displays events. The mediation layer collects information from the network elements and displays the objects in a topology map. ANA NetworkVision displays status and event information (including severities and timestamps) for supported NEs.

You use 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.

The NetworkVision maps provide a graphical display of active faults and alarms and serves as an easy access point for activation of services. See the *Cisco ANA NetworkVision User Guide*:

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

## Cisco ANA EventVision

The Cisco ANA EventVision is a GUI for browsing the events in the system. You can use EventVision to view and manage alarms, traps, syslog, provisioning, and system and security events. Monitoring EventVision helps predict and identify the sources of network problems, which may prevent future problems.

You can configure EventVision to display:

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

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

See the *Cisco ANA EventVision User Guide*:

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

# Cisco Multicast Manager

The Cisco Multicast Manager (CMM) is a web-based multicast troubleshooting tool that uses SNMP MIB polling to monitor devices and traffic in the network. The Cisco Multicast Manager also provides metrics and alerts, which it then forwards to ANA as SNMP traps. These traps are based on the unique requirements of the network environment and are user-configured.

The Cisco Multicast Manager 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).
- L3 multicast trees.

The Cisco Multicast Manager also provides detailed diagnostics and health-check capability.

You use the Cisco Multicast Manager to set thresholds, generate notifications, and forward them to the Cisco ANA. See Chapter 3, “Configuring the Components of the Cisco Video Assurance Management Solution.”

# Third-Party Video Probes

The Cisco VAMS supports the IneoQuest, Mixed Signals, and Tektronix video probes. These video quality monitoring probes are added to key points within the transport network. Their function is to detect impairments and validate the integrity of the Moving Pictures Expert Group (MPEG) transport stream, which carries video.

The ANA discovers physical and logical inventories for the video probes through standard inventory MIBs (depending on the level of support that the probes provide for these MIBS).

Generic VNEs in Cisco ANA 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 Cisco VAMS receives events from the probes based on thresholds that you configure in the video probes. See Configure Video Probes, page 3-6. The Cisco VAMS associates probe events with a severity level in the ANA.

The video probe VNEs enable the ANA to receive SNMP traps from the video probes. See Appendix A, “Trap Definitions.”

# Prerequisites

You must have these prerequisites in place before installing the Cisco VAMS:


- Solution Components and Versions, page 1-13
- ANA Hardware and Software Requirements, page 1-14
- Software Product Description, page 1-16


## Solution Components and Versions

The Cisco VAMS requires these components and version levels:

*Table 1-2 Solution Components and Version Information*

| Solution Component | Version Information |
|---|---|
| Active Network Abstract (ANA)[1] | 3.6 Service Pack 2 (3.6.2) |
| Cisco VAMS | 1.0 |
| Cisco Multicast Manager | 2.4 |
| Cisco 7600 (7600-SUP720-3BXL with redundant SUP720-3BXL)<br>Line cards: WS-X6704-10GE, WS-X6748-SFP, WS-X6748-GE-TX, WS-X6724-SFP, and optional WS-F6700-DFC3BXL | 12.2(33)SRB2 |
| Cisco CRS-1<br>Line cards: CRS-MSC, CRS1-SIP-800 (with SPA-8X1GE), 8-10GE | IOS-XR 3.4.2 |
| Cisco Catalyst 4948 (CAT4948-10GE) | 12.2(31)SG |
| Tektronix video probe | MTM400<br>Application Firmware Version: 3.1.061.000<br>FPGA Logic Firmware Version: 4<br>BIOS Version: 2.0.7<br>SNMP Interface Version: 2.6.0<br>Hardware Version: 5<br>QA Build: Alpha 01<br>Build Timestamp: Dec 19 2007 22:22:42 |
| IneoQuest video probe | Singulus GT-1 Media Analyzer<br>Firmware Version: TB-2.3a-011707 |
| Mixed Signals video probe | Sentry 136 Digital Content Monitor[2]<br>Sentry Engine Version: PDM (build 1455.38)<br>Sentry Database Version: 2.7.0.25<br>Sentry Configuration: TRANSPORT |

1. You must purchase base VNEs before installing the VNE extensions. For example, you must acquire the 7600 group VNE license to use the 7600 VNE extensions.
2. The Cisco VAMS 1.0 does not support carousel-related traps for Mixed Signals Sentry 136.

# ANA Hardware and Software Requirements

See these sections for more information:

- ANA Gateway Requirements, page 1-14
- ANA Unit Requirements, page 1-14
- ANA Client Requirements, page 1-15

**Note** Cisco ANA requires an Oracle database. Steps for installing the Oracle database are in the *Cisco Active Network Abstraction Installation Guide, Version 3.6 Service Pack 2*.

## ANA Gateway Requirements

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

***Table 1-3 ANA Gateway Requirements***

| Specification | Description |
|---|---|
| Sun Fire V490 | • 4 UltraSPARC IV processors<br>• 16 GB memory<br>• 2 73-GB hard disk drives<br>• 1 DVD drive |
| Operating system | Solaris 10 |
| Third-party tools | • Java v1.3.1_08<br>• Active Perl v5.6. |

## ANA Unit Requirements

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

***Table 1-4 ANA Unit Requirements***

| Specification | Description |
|---|---|
| Sun Fire V490 | • 4 1 GHz UltraSPARC IV processors<br>• 16 GB memory<br>• 2 73-GB hard disk drives<br>• 1 DVD drive |
| Operating system | Solaris 10 |
| Third-party tools | • Java v1.3.1_08<br>• Active Perl v5.6. |

## ANA Client Requirements

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

*Table 1-5 ANA Client Requirements*

| Specification | Description |
|---|---|
| IBM or PC compatible work station | • Pentium IV, 2.66 GHz processor or better<br>• 1 GB RAM<br>• 2 GB of free disk space<br>• DVD drive<br>• 512 MB of free nonvirtual memory |
| Monitor | • Minimum screen resolution of 1024 x 768 pixels<br>• True color (32-bit) setting |
| Operating system | Microsoft Windows 2000 or Windows XP |
| Internet connection (minimum) | A fast internet connection with a minimum bandwidth of 1.5 MB |

# Cisco Multicast Manager Requirements

Table 1-6 lists the hardware and software requirements for the Cisco Multicast Manager.

*Table 1-6 Cisco Multicast Manager Unit Requirements[1]*

| Specification | Description |
|---|---|
| Hardware | Linux<br>• Dual AMD Opteron Processor 250 2.4-GHz 64 Bit (more than 500 devices)<br>• Dual 2.8-GHz Intel Pentium IV or dual 2.8-GHz Intel Xeon processor (more than 500 devices)<br>• 2.8-GHz Intel Pentium IV or 2.8-GHz Intel Xeon processor<br>Solaris<br>• Sun Fire v440 up to four 1.593-GHz UltraSPARC IIIi processors (more than 500 devices)<br>• Sun Fire v240 One 1.34-GHz or two 1.5-GHz UltraSPARC processors |

*Table 1-6 Cisco Multicast Manager Unit Requirements[1] (continued)*

| Specification | Description |
|---|---|
| Memory | • 2 GB<br>• 4 GB (more than 500 devices)<br>• 2 GB or more of free space |
| Operating system | Linux<br>• Red Hat Enterprise Linux 3<br>• Red Hat Enterprise Linux 4<br>Solaris<br>• Solaris 8<br>• Solaris 9<br>• Solaris 10<br>**Note** Solaris x86 is not supported |

1. For complete hardware and software requirements, see the *Installation Guide for Cisco Multicast Manager 2.4*: http://www.cisco.com/en/US/products/ps6337/products_installation_guide_chapter09186a0080841bec.html#wp1044006.

# Software Product Description

Table 1-7 lists the software product information and Cisco part numbers for the Cisco VAMS 1.0 release.

*Table 1-7 Software Products with Cisco Part Number[1]*

| Description | Cisco Part Number |
|---|---|
| Cisco Video Assurance Management Solution 1.5 (top level part number) | VAMS-1.0-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 |
| 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 |
| Tektronics Video Probe—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 IQ probe (optional, qty 0-1) | VAMS-1.0-3.6MSRTU |
| Tektronix Video Probe RTU—Right-to-use for one IQ probe (optional, qty 0-1) | VAMS-1.0-3.6TKRTU |

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

CHAPTER 2

# Installing the Cisco Video Assurance Management Solution

## Before You Install

Before you install the Cisco VAMS, ensure that you complete the following tasks:

*Table 2-1 Prerequisite Tasks*

| Tasks | Reference |
|---|---|
| 1. Install Cisco 7600 routers, CRS-1 routers, and Catalyst 4948 switches for the supported cable or wireline architecture. | Cisco 7600 Series installation guides: http://www.cisco.com/en/US/products/hw/routers/ps368/prod_installation_guides_list.html<br>Cisco CRS-1 installation guides: http://www.cisco.com/en/US/products/ps5763/prod_installation_guides_list.html<br>Cisco Catalyst 4948 installation guides: http://www.cisco.com/en/US/docs/switches/lan/catalyst4900/4948-10ge/4948_10.html |
| 2. Configure the Cisco 7600 routers, CRS-1 routers, and Catalyst 4948 switches for the supported cable or wireline architecture. | Cisco 7600 Series configuration guides: http://www.cisco.com/en/US/products/hw/routers/ps368/products_installation_and_configuration_guides_list.html<br>Cisco CRS-1 configuration guides: http://www.cisco.com/en/US/products/ps5763/products_installation_and_configuration_guides_list.html<br>Cisco Catalyst 4948 configuration guides: http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/25ewa/configuration/guide/conf.html<br>http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/31sg/configuration/guide/conf.html<br>Also, consult configuration tasks documented in Cisco Internet Protocol Television (IPTV) Solutions, page ix. |

*Table 2-1 Prerequisite Tasks (continued)*

| Tasks | Reference |
|---|---|
| 3. Install multicast-enabled IOS images:[1]<br>• Cisco 7600 with 12.2(33)SRB2 image<br>• Cisco CRS-1 with IOS-XR 3.4.2 image<br>• Cisco Catalyst 4948 with 12.2(31)SG image | Cisco 7600 release notes:<br>http://www.cisco.com/en/US/products/ps6922/prod_release_note09186a00806c096f.html<br>Cisco CRS-1 release notes:<br>http://www.cisco.com/en/US/docs/ios_xr_sw/iosxr_r3.4/general/release/notes/reln_342.html<br>Cisco Catalyst 4948 release notes:<br>http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/release/note/OL_9592.html |
| 4. Install Cisco Multicast Manager 2.4 on a dedicated server. | Cisco Multicast Manager installation guides:<br>http://www.cisco.com/en/US/products/ps6337/prod_installation_guides_list.html |

1. Download IOS software from http://www.cisco.com/public/sw-center/index.shtml.

# Installation

Installing the Cisco Video Assurance Management Solution (Cisco VAMS) involves these high-level tasks:

| Task | Reference |
|---|---|
| 1. Ensure that you meet all prerequisites. | Prerequisites, page 1-13 |
| 2. Install Cisco ANA 3.6 on the target server. | http://www.cisco.com/en/US/docs/net_mgmt/active_network_abstraction/3.6/installation/install_1.html |
| 3. Install Cisco ANA 3.6.1 on the target server. | http://www.cisco.com/en/US/docs/net_mgmt/active_network_abstraction/3.6_sp1/installation/guide/Install-Book-Wrapper.html |
| 4. Install Cisco ANA 3.6.2 on the target server.[1] | http://www.cisco.com/en/US/docs/net_mgmt/active_network_abstraction/3.6_sp2/installation/guide/Install-Book-Wrapper.html |
| 5. Install the Cisco VAMS. | Install the Cisco VAMS, page 2-3 |

1. If you encounter an error during installation of ANA 3.6.2, follow the workaround described here: http://www.cisco.com/en/US/docs/net_mgmt/active_network_abstraction/3.6_sp2/release_notes/rn36_sp2.html#wp82640

# Install the Cisco VAMS

To install the Cisco VAMS:

**Step 1** Log in to the server as the root user.

**Step 2** Insert the Cisco VAMS installation DVD into the DVD drive on your system.

**Step 3** Check the system prerequisites such as required disk space. See Prerequisites, page 1-13.

**Step 4** If an older version of the Cisco VAMS exists, uninstall it. See Uninstall the Cisco VAMS, page 2-4.

**Step 5** Change the directory to the root directory on the DVD. For example:

**cd /cdrom/cdrom0/**

**Step 6** Start the installation script. For example:

**./install.sh**

The installation script prompts you to enter site-specific values for the installation.

**Step 7** When prompted to enter login information for the ANA, you must enter an administrative-level user ID and password. If necessary, obtain this information from your administrator.

**Step 8** If your login information does not authenticate, retry by entering **r**, or bypass the ANA authentication by entering **y**.

```
The specified login and password do not authenticate.
Do you wish to continue with the installation? [Y(es)/N(o)/R(etry)]:
```

**Caution** If you enter **y** to bypass authentication, you must run the *setCimsCredentials.sh* script later! That script is in the *iptv/scripts/* directory. The Cisco VAMS will not operate correctly if you do not run the *setCimsCredentials.sh* script after a failed authentication.

**Step 9** After successful installation, continue to Chapter 3, "Configuring the Components of the Cisco Video Assurance Management Solution."

A message similar to this one should appear on your screen:

```
Installation of <CSCOcims> was successful.
Modifying configuration files
preparing client configuration..
updating client configuration..
Restarting ANA Gateway
...
Installation completed.
```

# Uninstall the Cisco VAMS

To uninstall the Cisco VAMS:

**Step 1** Log in to the server as the root user.

**Step 2** Insert the Cisco VAMS installation DVD into the DVD drive on your system.

**Step 3** Change the directory to the uninstallation directory. For example:

**cd** *$ANAROOT*/**iptv/scripts**

where *$ANAROOT* is the ANA installation directory.

**Step 4** Start the uninstall script.

**./uninstall.sh**

```
Do you want to remove this package? [y,n,?,q] ?
```

**Step 5** Enter **y** to continue. A message similar to this one should appear on your screen:

```
## Removing installed package instance <CSCOcims>
## Verifying package <CSCOcims> dependencies in global zone
## Processing package information.
## Executing preremove script.
Restoring configuration file
...

Restarting ANA Gateway
...

Removal of <CSCOcims> was successful.
```

CHAPTER 3

# Configuring the Components of the Cisco Video Assurance Management Solution

After you have completed the installation of the Cisco Video Assurance Management Solution (Cisco VAMS), you are ready to configure the components of the solution for operation.

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

To configure the components of the Cisco VAMS:

**Step 1** Ensure that you have met all prerequisites. (See "Before You Install" section on page 2-1.)

**Note** An important prerequisite is that all Cisco devices in the video transport network be loaded with IOS software that supports the Cisco VAMS.

**Step 2** In Cisco ANA, create new virtual network elements (VNEs) for the Cisco VAMS components. See Create VNEs, page 3-2.

**Step 3** Add the Cisco VAMS devices to the ANA network map. See Add Solution Components to ANA Network Map, page 3-4.

**Step 4** Configure the Cisco Multicast Manager to set thresholds and forward notifications to Cisco ANA. See Configure the Cisco Multicast Manager, page 3-5.

**Step 5** Configure the video probes to set thresholds and send events to Cisco ANA. See Configure Video Probes, page 3-6.

**Note** All components of the Cisco VAMS are now operational. The Cisco devices in the video transport network are forwarding notifications to the Cisco Multicast Manager, which forwards them to Cisco ANA. The video probes are forwarding notifications to Cisco ANA. The remaining steps of this procedure are optional.

**Step 6** (Optional) To manually run the **Setup for IPTV** activation script, see Run the Setup for IPTV Script, page 3-7.

**Note** Step 6 is usually not required. The **Setup for IPTV** activation script runs automatically at installation time, hourly, and whenever a managed device reloads.

**Step 7** (Optional) To manually run the **Cleanup from IPTV** activation script, see Run the Cleanup from IPTV Script, page 3-7.

**Note** Step 7 is typically performed when you want to remove a device from the Cisco VAMS. The **Cleanup from IPTV** activation script removes the IPTV extensions.

# Create VNEs

Use this procedure to create a VNE for each component of the Cisco VAMS. Table 3-1 lists important values for the VNEs of the Cisco VAMS. You will need this information when you create VNEs for the Cisco VAMS.

*Table 3-1 VNE Information for Cisco VAMS[1]*

| Name | Type | Scheme |
|---|---|---|
| Cisco 7600 | Generic SNMP | default |
| Cisco CRS-1 | Generic SNMP | IpCore |
| Cisco 4948 | Generic SNMP | default |
| Cisco Multicast Manager | ICMP | default |
| Tektronics video probe | Generic SNMP | default |
| IneoQuest video probe | Generic SNMP | default |
| Mixed Signals video probe | ICMP | default |

1. Column headings in this table are the names of fields in the New VNE window, under the General tab.

To create VNEs for the Cisco VAMS:

**Step 1** Log in to ANA Manage.

**Step 2** Click the **ANA Servers** item in the navigation tree (left pane).

**Step 3** Click and expand the **ANA Gateway** item in the navigation tree.

**Step 4** Create an Autonomous Virtual Machine (AVM) to contain the VNE objects for the Cisco VAMS.

a. Right-click the ANA Gateway in the left pane.

b. Choose **New AVM** from the drop-down menu.

c. Enter an ID number and key.

d. Check the **Activate on creation** check box and click **OK**.

**Note** You may create more than one AVM. For example, you could create one AVM for the Cisco devices and a different AVM for the video probes.

**Step 5** Right-click the AVM that contains the IPTV devices.

**Step 6** In the right-click menu, choose **New VNE**.

**Step 7** Complete these fields in the New VNE window under the General tab:

- Name (as ANA identifies it)
- IP Address
- Type (see Table 3-1)
- Scheme (see Table 3-1)
- Initial State (Stop or Start)

**Step 8** Under the SNMP tab, in the SNMP V1/V2 Settings pane, complete these fields:

- Community Read
- Community Write

**Step 9** Enable Telnet or SSH under the Telnet/SSH tab. This information enables discovery of the device.

**Step 10** If the VNE type is ICMP (see Table 3-1), enter a polling rate under the ICMP tab.

**Step 11** If required, add the VNE to a polling group under the Polling tab.

**Note** The IPTV extensions of the Cisco VAMS provide two new polling groups: *30-minute config* and *60-minute config*. Depending on your polling requirements, choose one of these groups to obtain status, configuration, and system information.

**Step 12** Enter any other required information in the remaining tabs of the New VNE window and click **OK**.

**Step 13** Verify that the new VNE appears in the VNEs table in the right pane of the ANA Manage window.

**Step 14** To start the new VNE, right-click it in the table and choose **Actions > Start**.

**Step 15** To continue to add new VNEs, repeat this procedure from Step 5.

# Add Solution Components to ANA Network Map

Use this procedure to add these components to the Cisco ANA Network Map:

- Cisco 7600
- Cisco CRS-1
- Cisco 4948
- Video probes:
  - Tektronics
  - IneoQuest
  - Mixed Signals
- Cisco Multicast Manager

To add the previous components:

**Step 1** Log in to ANA NetworkVision.

**Step 2** If not already done, create a new network map:

**File > New Map**

**Step 3** To open the device list, choose **File > Add Device**.

**Step 4** Choose the device that you want to add to the network map.

**Step 5** Click **Add Device**.

**Step 6** Verify that the device appears in the network map and links appear between connected devices.

**Note** If links do not appear, and the devices are connected, you can manually create the links as described in the *Release Notes for Cisco Active Network Abstraction 3.6 Service Pack 1*: http://www.cisco.com/en/US/docs/net_mgmt/active_network_abstraction/3.6_sp2/release_notes/rn36_sp2.html#wp39153 (see defect CSCsi50166).

**Step 7** To add other solution components to the network map, repeat this procedure from Step 3.

# Configure the Cisco Multicast Manager

To enable notifications and set thresholds for multicast conditions, you must configure the Cisco Multicast Manager. Configuration tasks include:

- Adding devices for discovery.
- Device configuration of routers, Layer 2 switches, and video probes.
- Global configuration of polling intervals and run times for Layer 2 polling, Designated Router (DR) polling, and polling of Rendevouz Point (RP) status.
- Multicast threshold configuration for Layer 2 and router groups.

**Note** A summary procedure of configuration tasks follows. For complete details about these, and other configuration tasks, see the *User Guide for the Cisco Multicast Manager 2.4*:

http://www.cisco.com/en/US/products/ps6337/products_user_guide_book09186a008083390a.html

To configure the Cisco Multicast Manager for the Cisco VAMS:

**Step 1** In a browser window, open and log in to the Cisco Multicast Manager.

**Step 2** In the Tool drop-down menu, click **Administration**.

**Step 3** To add users, choose **User Management > Manage Users**.

**Step 4** To add the Cisco VAMS devices, choose **User Management > Manage Users**.

**Step 5** To configure the devices, choose **User Management > Device Configuration**.

**Step 6** To configure multicast thresholds, choose **User Management > Multicast Polling Configuration**. To activate your changes, click the **Start** button.

**Step 7** To configure polling intervals and run times, choose **User Management > Global Polling Configuration**. To activate your changes, click the **Start** button.

**Step 8** Forward notifications to Cisco ANA:

a. Choose **User Management > Global Polling Configuration**.

b. Click **Domain Trap/Email**.

c. In the right pane, enter the IP address of the ANA in the Add Trap Receiver field.

d. Click the **Add Trap Receiver** button. This action adds the ANA IP address to the Configured Trap Receivers drop-down list.

e. Choose a trap receiver from the Configured Trap Receivers drop-down list.

f. To activate your changes, click the **Start** button.

The Cisco Multicast Manager forwards notifications to Cisco ANA, the designated trap receiver.

# Configure Video Probes

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

For each video probe deployed in the network, you must configure the thresholds for the conditions that you want to monitor. You must also configure the video probes to forward traps to the Cisco ANA. (Refer to the probe documentation to add the ANA IP address and related SNMP information to the video probe settings.)

Once you configure the video probe, if a monitored condition exceeds a configured threshold, the probe sends a corresponding trap to Cisco ANA, which displays the event in the EventVision GUI.

## IneoQuest Video Probe

To configure the IneoQuest video probe for operation in the video transport network, refer to the documentation that comes with the product. These documents assist the network planner to integrate IneoQuest video probes with the Cisco VAMS:

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

## Tektronics Video Probe

To configure the Tektronix video probe for operation in the video transport network, refer to the documentation that comes with the product. These documents assist the network planner to integrate Tektronix video probes with the Cisco VAMS.

Documents that are useful for configuring the Tektronics MTM400 video probe include these:

- *MTM400 MPEG Transport Stream Monitor User Manual*
- *MTM400 MPEG Transport Stream Monitor Technical Reference*
- *MTM400 MPEG Transport Stream Monitor Programmer Manual*

## Mixed Signals Video Probe

To configure the Mixed Signals video probe for operation in the video transport network, refer to the documentation that comes with the product. These documents assist the network planner to integrate Mixed Signals video probes with the Cisco VAMS:

The *Mixed Signals Sentry Digital Content Monitor User Guide* is included with the video probe hardware and describes how to configure thresholds for events that you want to forward to the ANA.

# Run the Setup for IPTV Script

The Setup for IPTV activation script sets up network configuration parameters for the Cisco devices in the Cisco VAMS. The script runs:

- ANA startup
- Every two hours
- Whenever the managed device reloads
- When you activate it in ANA NetworkVision (see procedure)

The hourly run checks the IPTV configuration of the managed VNEs. If a VNE does not have the expected IPTV configuration, the script applies the IPTV configuration parameters to the device.

**Note** Configure the supported devices and load them with IPTV-enabled IOS images. The IPTV script does not recognize the devices without IPTV-enabled IOS images. See Table 2-1 on page 2-1.

You can also manually run the Setup for IPTV script. To manually run the IPTV activation script:

**Step 1** Log in to ANA NetworkVision.

**Step 2** Right-click a VNE in the network map.

**Step 3** In the right-click menu, choose **Management > Setup for IPTV**.

**Step 4** In the Setup for IPTV window, click the **Execute** button.

The result of the script appears in the same window under the Result tab.

**Note** If the selected VNE already has its IPTV configuration, the result indicates *ALREADY CREATED*, and the script does not run.

# Run the Cleanup from IPTV Script

You run the *Cleanup for IPTV* activation script when you want to remove the IPTV extensions from a VNE that is in the Cisco VAMS. When the extensions have been removed, the VNE will not be able to process IPTV requests.

To run the *Cleanup from IPTV* script:

**Step 1** Log in to ANA NetworkVision.

**Step 2** Right-click the VNE in the network map.

**Step 3** In the right-click menu, choose **Management > Cleanup from IPTV**.

The *Cleanup from IPTV* script runs and removes the IPTV extensions from the selected VNE.

CHAPTER 4

# Troubleshooting with the Cisco Video Assurance Management Solution

Troubleshooting with the Cisco Video Assurance Management Solution (Cisco VAMS) involves use of:

- Cisco ANA for basic troubleshooting
- Cisco Multicast Manager for advanced troubleshooting

This chapter contains:

# Troubleshooting with Cisco ANA

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

This section contains:



## Fault Management

Table 4-1 highlights important aspects of the fault management system in Cisco ANA.

***Table 4-1 Cisco ANA Fault Management***

| Troubleshooting Area | Description and Reference |
|---|---|
| Fault detection and isolation | Describes:<br>• How the various VNEs use reachability to check connectivity with the NEs.<br>• Basic alarm sources that indicate problems in the network.<br>• What happens when a VNE with associated open alarms shuts down.<br>• The integrity service tests that run on the gateway and the units.<br>http://www.cisco.com/en/US/docs/net_mgmt/active_network_abstraction/3.6_sp2/fault/user/guide/chp1.html |
| Causality correlation and root cause analysis | Describes:<br>• Enabling or disabling port-down, port-up, link-down and link-up alarms.<br>• The root-cause correlation concept.<br>• The root-cause alarm and weights concepts.<br>• Correlation by flow and correlation by key.<br>http://www.cisco.com/en/US/docs/net_mgmt/active_network_abstraction/3.6_sp2/fault/user/guide/chp2.html |
| Advanced correlation scenarios | Describes alarms that use advanced correlation logic on top of the root cause analysis flow.<br>http://www.cisco.com/en/US/docs/net_mgmt/active_network_abstraction/3.6_sp2/fault/user/guide/chp4.html |

# ANA NetworkVision

Network administrators use Cisco ANA NetworkVision to manage, fulfill, plan, and assure the integrity of network resources. Table 4-2 lists important aspects of using Cisco ANA NetworkVision for troubleshooting.

*Table 4-2 Cisco ANA NetworkVision*

| Troubleshooting Area | Description and Reference |
|---|---|
| Working with ANA tickets | Cisco ANA NetworkVision:<br>• Correlates alarms, and enables you to view tickets and tickets properties, including correlated alarms, active alarms, and alarm history.<br>• Describes ticket management and the different ways in which a ticket is displayed in the ticket pane, depending on the status or severity of the alarm.<br>For detailed information about working with tickets, see the *Cisco Active Network Abstraction NetworkVision User Guide 3.6 Service Pack 1*:<br>http://www.cisco.com/en/US/docs/net_mgmt/active_network_abstraction/3.6_sp2/networkvision/user/guide/8tickets.html |
| Working with ANA PathTracer | You use the Cisco ANA PathTracer to view a network path between two network objects in packet-switched networks such as Ethernet and IP.<br>For detailed information about working with the ANA PathTracer, see the *Cisco Active Network Abstraction NetworkVision User Guide 3.6 Service Pack 1*:<br>http://www.cisco.com/en/US/docs/net_mgmt/active_network_abstraction/3.6_sp2/networkvision/user/guide/9ptracer.html |

# ANA EventVision

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

*Table 4-3 Cisco ANA EventVision*

| Troubleshooting Area | Description and Reference |
|---|---|
| Viewing events | Events appear in different event categories in the ANA EventVision. For detailed information about displaying events, see the *Cisco Active Network Abstraction EventVision User Guide 3.6 Service Pack 1*:<br>http://www.cisco.com/en/US/docs/net_mgmt/active_network_abstraction/3.6_sp2/eventvision/user/guide/3viewevn.html |
| Working with EventVision | For detailed information about working with EventVision, see the *Cisco Active Network Abstraction EventVision User Guide 3.6 Service Pack 1*:<br>http://www.cisco.com/en/US/docs/net_mgmt/active_network_abstraction/3.6_sp2/eventvision/user/guide/4workev.html |

# Advanced Troubleshooting with Cisco Multicast Manager

The Cisco Multicast Manager provides a diagnostics tool that gives you a global view and a router-specific view of your network. Table 4-4 lists important areas of the Cisco Multicast Manager that you can use to troubleshoot the Cisco VAMS:

*Table 4-4 Cisco Multicast Manager*

| Troubleshooting Area | Task and Reference |
|---|---|
| Viewing network status | View the status of all devices in the current multicast domain. See:<br>http://www.cisco.com/en/US/products/ps6337/products_user_guide_chapter09186a0080834d83.html#wp1130975 |
| Viewing RP status | View all routers in the database, their RPs, and the active groups. See:<br>http://www.cisco.com/en/US/products/ps6337/products_user_guide_chapter09186a0080834d83.html#wp1130983 |
| IGMP diagnostics | View the interfaces that have joined a particular group. See:<br>http://www.cisco.com/en/US/products/ps6337/products_user_guide_chapter09186a0080834d83.html#wp1131002 |
| Layer 2 switches | View Layer 2 multicast information and host IPs. The table that is generated, shows, from a Layer 2 perspective, which multicast groups are being forwarded out which interfaces. See:<br>http://www.cisco.com/en/US/products/ps6337/products_user_guide_chapter09186a0080834d83.html#wp1131025 |
| Cisco 6500/7600 troubleshooting | Gather accurate packet-forwarding statistics and other information. See:<br>http://www.cisco.com/en/US/products/ps6337/products_user_guide_chapter09186a0080834d83.html#wp1131042 |
| Top-20 video flows | View the top-20 video flows. The top-20 video flows are dynamically updated at every polling interval. See:<br>http://www.cisco.com/en/US/products/ps6337/products_user_guide_chapter09186a0080834d83.html#wp1131050 |
| Video probe status[1] | View diagnostic information about video probes and the flows that they are monitoring. See:<br>http://www.cisco.com/en/US/products/ps6337/products_user_guide_chapter09186a0080834d83.html#wp1221364 |

1. Cisco Multicast Manager 2.4 supports only the Ineoquest video probe.

# Monitoring and Troubleshooting in the Wireline Network

The *Cisco Wireline Video/IPTV Solution Design and Implementation Guide, Release 1.1*, provides an introduction to monitoring and troubleshooting the Cisco Ethernet switches in the Cisco wireline-based IPTV solution. Troubleshooting areas include:

- Network Time Protocol (NTP)
- Syslog
- Quality of Service (QoS)
- Multicast

Monitoring and troubleshooting information is available here:

http://www.cisco.com/en/US/products/ps6902/products_implementation_design_guide_chapter09186a00806ac2e0.html

# Monitoring and Troubleshooting in the Cable Network

The *Cisco Gigabit-Ethernet Optimized Video Networking Solution for Cable Design and Implementation Guide, Release 3.0*, provides an introduction to monitoring and troubleshooting the Cisco Ethernet switches in the Cisco cable-based IPTV solution. Troubleshooting areas include:

- Troubleshooting multicast
- Show commands
- Debug commands
- Viewing hardware rate limiter (HWRL) counters

Monitoring and troubleshooting information is available here:

http://www.cisco.com/en/US/products/ps6902/products_implementation_design_guide_chapter09186a0080645ae0.html

APPENDIX A

# Trap Definitions

The Cisco Video Assurance Management Solution (Cisco VAMS) supports traps (alarms) for:



## Cisco Multicast Manager

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

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

1. See Glossary for abbreviations that are used in alarm message text.

# Textronix Video Probe

| Alarm Message Text[1] | Severity |
|---|---|
| Number of packet received out of order exceeds Warning threshold | Warning |
| Inter packet delay exceeds Warning threshold | Warning |
| IP Packets lost exceeds Warning threshold | Warning |
| IP Packets in error exceeds Warning threshold | Warning |
| Number of packet received out of order exceeds threshold | Minor |
| IP Packets lost exceeds threshold | Minor |
| IP Packets in error exceed threshold | Minor |
| 1.5a PMT | Major |
| 2.5 PTS | Minor |
| 1.5 Ind PMT Error Timer | Major |
| 2.3b PCR Discontinuity Indicator - The difference between two consecutive PCR values (PCRi + 1 - PCRi) is outside the range of 0ms to 100 ms without the discontinuity_indicator set | Minor |
| 2.3a PCR Repetition - Error Timer | Minor |
| 1.4 Continuity | Major |
| 2.3b PCR Discontinuity Indicator - This test applies only to PIDs that are indicated as PCR_PID in the current PMT | Minor |
| 2.3a PCR EVID_INDIVIDUAL_PCR_ERR_TIMER | Minor |
| 1.5 PMT Error Scrambling | Major |
| 1.5 PMT Error Timer | Major |
| 1.3 PAT Error Scrambling | Major |
| 1.3 PAT Error Table Id | Major |
| 1.3 PAT Error Timer | Major |
| 2.4 PCR Accuracy | Minor |
| CAT (DVB test 2.6) | Minor |
| PTS (DVB test 2.5) | Minor |
| PCR Accuracy (DVB test 2.4) | Minor |
| CRC (DVB test 2.2) | Minor |
| Transport (DVB test 2.1) | Minor |
| PMT (DVB test 1.5) | Major |
| PAT Table (DVB test 1.3) | Major |
| 1.6 PID | Major |
| PID (DVB test 1.6) | Major |
| Continuity Error (DVB test 1.4) | Major |

| Alarm Message Text[1] (continued) | Severity |
|---|---|
| Sync Byte (DVB test 1.2) | Major |
| Sync Loss (DVB test 1.1) | Major |

1. See Glossary for abbreviations that are used in alarm message text.

# IneoQuest Video Probe

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

1. See Glossary for abbreviations that are used in alarm message text.

# Mixed Signals Video Probe

| Alarm Message Text [1] | Severity |
|---|---|
| Table bit rate | Warning |
| Table detect | Warning |
| Table cycle time | Warning |
| PID bit rate | Warning |
| PID detect | Warning |
| PID discontinuity | Minor |
| PID audio silence | Minor |
| PID video freeze | Minor |
| PID table bit rate | Warning |
| PID table detect | Warning |
| PID table cycle time | Warning |
| Program bit rate | Warning |
| Program detect | Warning |
| Program discontinuity | Warning |
| Program audio silence | Warning |
| Program video freeze | Warning |
| Program PCR interval | Warning |
| Program PCR jitter | Warning |
| Program table PMT bit rate | Warning |
| Program table PMT detect | Warning |
| Program table PMT cycle time | Warning |
| DSM-CC DII bit rate | Warning |
| DSM-CC DII detect | Warning |
| DSM-CC DII cycle time | Warning |
| DSM-CC DC bit rate | Warning |
| DSM-CC DC detect | Warning |
| DSM-CC DC cycle time | Warning |
| Carousel bit rate | Warning |
| Carousel source file add-delete | Warning |
| Carousel source DSM-CC DII bit rate | Warning |
| Carousel source DSM-CC DII detect | Warning |
| Carousel source DSM-CC DII cycle time | Warning |
| Carousel source DSM-CC DC bit rate | Warning |
| Carousel source DSM-CC DC detect | Warning |
| Carousel source DSM-CC DC cycle time | Warning |

| Alarm Message Text [1] (continued) | Severity |
|---|---|
| Carousel file bit rate | Warning |
| Carousel file detect | Warning |
| Carousel file cycle time | Warning |
| Carousel file change | Warning |
| Port IP arrival interval | Warning |
| Port delay factor | Warning |

1. See Glossary for abbreviations that are used in alarm message text.

# Cisco 7600, CRS-1, and 4948 Devices

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

1. See Glossary for abbreviations that are used in alarm message text.

# Performance Metrics

For the Cisco VAMS, the Cisco ANA supports a:

- Sustained trap rate of 35 traps per second
- Cut-off rate of 5 traps per second per VNE

Cisco ANA drops traps that exceed the cut-off rate. For example, if a VNE receives six traps per second, the ANA drops the sixth trap. Also, the cut-off rate is cumulative. For example, for two VNEs, the cut-off rate is 10 traps per second.

APPENDIX **B**

# End User License Agreement Supplement

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

Dear Customer,

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

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

For purposes of the SEULA, the Product name and the Product description you have ordered is one or more of:

- VAMS1.0-3.6VNE4948—Video Assurance 1.0, Extension to 4948 (G2) VNE - ANA 3.6.2
- VAMS1.0-3.6VNE7600—Video Assurance 1.0, Extension to 7600 (G3) VNE - ANA 3.6.2
- VAMS1.0-3.6VNEG5—Video Assurance 1.0, Extension to CRS-1 (G5) VNE - ANA 3.6.2
- VAMS1.0-3.6VNEG6—Video Assurance 1.0, Extension to CRS-1 (G6) VNE - ANA 3.6.2
- VAMS1.0-3.6VNECMM—Video Assurance 1.0, Cisco Multicast Mgr VNE - ANA 3.6.2
- VAMS1.0-3.6VNEIQ—Ineoquest Video Probe VNE - ANA 3.6.2
- VAMS1.0-3.6VNEMS—Mixed Signals Video Probe VNE - ANA 3.6.2
- VAMS1.0-3.6VNETK—Tektronics Video Probe VNE - ANA 3.6.2
- VAMS1.0-3.6IQRTU—Ineoquest Video Probe RTU - Right to Use for one IQ probe

- VAMS1.0-3.6MSRTU—Mixed Signals Video Probe RTU - Right to Use for one MS probe
- VAMS1.0-3.6TKRTU—Tektronics Video Probe VNE RTU - Right to Use for one TK probe

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

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

# ADDITIONAL LICENCE RESTRICTIONS

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

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

- Customer may install and use following Software components:
  - Cisco Video Assurance Management Solution - Video extensions to 4948 (G2) VNE license: Customer may install and run the Software on unlimited number of processors in the Customer's network environment, subject to a limitation on the number of 4948 devices managed that equals the number of ANA Group 2 licenses purchased from Cisco and in effect.
  - Cisco Video Assurance Management Solution - Video extensions to 7600 (G3) VNE license: Customer may install and run the Software on unlimited number of processors in the Customer's network environment subject to a limitation on the number of 7600 devices managed that equals the number of ANA Group 3 licenses purchased from Cisco and in effect.
  - Cisco Video Assurance Management Solution - Video extensions to CRS-1 (G5) VNE license: Customer may install and run the Software on unlimited number of processors in the Customer's network environment, subject to a limitation on the number CRS-1(G5) devices managed that equals the number of ANA Group 5 licenses purchased from Cisco and in effect.
  - Cisco Video Assurance Management Solution - Video extensions to CRS-1 (G6) VNE license: Customer may install and run the Software on unlimited number of processors in the Customer's network environment, subject to a limitation on the number of CRS-1(G6) devices managed that equals the number of ANA Group 6 licenses purchased from Cisco and in effect.
  - Cisco Video Assurance Management Solution - Cisco Multicast Manager VNE license: Customer may install and run the Software on unlimited number of processors in the Customer's network environment to enable ANA to interface with Cisco Multicast Manager installations in the Customer's network environment.
  - Cisco Video Assurance Management Solution - Ineoquest Video Probe VNE license: Customer may install and run the Software on unlimited number of processors in the Customer's network environment, subject to a limitation on the number of Ineoquest probe devices managed that equals the number of Ineoquest licenses purchased from Cisco and in effect.
  - Cisco Video Assurance Management Solution - Mixed Signals Video Probe VNE license: Customer may install and run the Software on unlimited number of processors in the Customer's network environment, subject to a limitation on the number of Mixed Signals probe devices managed that equals the number of Mixed Signals licenses purchased from Cisco and in effect.

  - Cisco Video Assurance Management Solution - Tektronics Video Probe VNE license: Customer may install and run the Software on unlimited number of processors in the Customer's network environment, subject to a limitation on the number Tektronics probe devices managed that equals the number of Tektronics Video Probe licenses purchased from Cisco and in effect.

- Other license restrictions on software:
  - Cisco Video Assurance Management Solution - Ineoquest Video Probe license: Each license permits the Customer to manage one Ineoquest probe device.
  - Cisco Video Assurance Management Solution - Mixed Signals Video Probe RTU license: Each license permits the Customer to manage one Mixed Signals probe device.
  - Cisco Video Assurance Management Solution - Tektronics Video Probe license: Each license permits the Customer to manage one Tektronics probe device.
  - Reproduction and Distribution. Customer may not reproduce nor distribute Software.

# DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS

Please refer to the Cisco Systems, Inc. End User License Agreement

# GLOSSARY

## A

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

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

**ANA** — See Active Network Abstraction.

**ANA EventVision** — The GUI tool in Cisco ANA that serves as a browser for viewing and retrieving detailed information about the different types of system events and tickets that are generated within the Cisco ANA system.

**ANA Manage** — The GUI tool in Cisco ANA that is used for performing various system administration activities for simple system control.

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

**ANA NetworkVision** — The GUI tool in Cisco ANA that is used by network administrators for the management, fulfillment, planning and assurance of the integrity of network resources. It provides topology and event views.

**AVM** — See Autonomous Virtual Machine.

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

## C

**Carrier Routing System-1** — A Cisco large-scale core router for carrier networks.

**Cisco Multicast Manager** — A Web-based network management application that simplifies the holistic discovery, visualization, monitoring, and troubleshooting of multicast networks. Cisco Multicast Manager is applicable to multiple system operators that utilize multicast to transport video over IP.

**CPU** — Central Processing Unit.

**CRC** — See Cyclic Redundancy Check.

**CRS-1** See Carrier Routing System-1.

**Cyclic Redundancy Check** Error-checking technique in which the frame recipient calculates a remainder by dividing frame contents by a prime binary divisor and compares the calculated remainder to a value stored in the frame by the sending node.

## D

**Delay Factor** A time value indicating the amount of data that buffers must contain to eliminate jitter.

**Desginated Router** A router in a multiaccess network that is designated to originate network link advertisements and establish adjacencies with all routers in the network.

**DF** See Delay Factor.

**Digital Storage Media - Command and Control** A toolkit for developing control channels associated with MPEG-1 and MPEG-2 streams.

**Digital Subscriber Line Access Multiplexer** A device that connects many digital subscriber lines to a network by multiplexing the DSL traffic onto one or more network trunk lines.

**Digital Video Broadcast** A European standard for digital television.

**DR** See Designated Router.

**DSLAM** See Digital Subscriber Line Access Multiplexer.

**DSM-CC** See Digital Storage Media - Command and Control.

**DVB** See Digital Video Broadcast.

## E

**EMS** See Element Management System.

**Element Management System** A system that manages a network of elements.

## H

**HDD** Hard disk drive.

**HFC** See Hybrid Fiber-Coax.

**Hybrid Fiber-Coax** Technology being developed by the cable TV industry to provide two-way, high-speed data access to the home using a combination of fiber optics and traditional coaxial cable.

## I

**ICMP** See Internet Control Message Protocol.

**IGMP** See Internet Group Management Protocol.

**Internet Control Message Protocol** Network layer Internet protocol that reports errors and provides other information relevant to IP packet processing. Documented in RFC 792.

**Internet Group Management Protocol** Used by IP hosts to report their multicast group memberships to an adjacent multicast router.

**Internet Protocol Television** Video transport over IP.

**IPTV** See Internet Protocol Television.

**IPTV extensions** Configurations that extend the capabilities of the VNEs to include functions that are unique to the Cisco Video Assurance Management Solution. These extensions are applied to supported VNEs with an activation script.

## M

**Management Information Base** Database of network management information that is used and maintained by a network management protocol, such as SNMP. The value of a MIB object can be changed or retrieved using SNMP commands, usually through a GUI network management system.

**MDT** See Multicast Distribution Tree.

**Media Loss Rate** The number of lost or out-of-order media packets per second.

**MIB** See Management Information Base.

**MLR** See Media Loss Rate.

**Motion Picture Experts Group** Standard for compressing video. MPEG1 is a bit stream standard for compressed video and audio optimized to fit into a bandwidth of 1.5 Mbps. MPEG2 is intended for higher quality video-on-demand applications and runs at data rates between 4 and 9 Mbps. MPEG4 is a low-bit-rate compression algorithm intended for 64-kbps connections.

**MPEG** See Motion Picture Experts Group.

**MPLS** See Multiprotocol Label Switching.

**MVPN** Multicast VPN.

**Multicast Distribution Tree** A distribution tree that controls the path that IP multicast traffic takes through the network to deliver traffic to all receivers. The two basic types of multicast distribution trees are source trees and shared trees.

**Multiprotocol Label Switching** Switching method that forwards IP traffic using a label. This label instructs the routers and the switches in the network where to forward the packets based on preestablished IP routing information.

## N

**NE** See Network Element.

**Network Element** A user-named physical component or device existing in the network.

**Network Time Protocol** Protocol built on top of TCP that ensures accurate local time-keeping with reference to radio and atomic clocks located on the Internet. This protocol is capable of synchronizing distributed clocks within milliseconds over long time periods.

**NTP** See Network Time Protocol.

## O

**Object Identifier** Values are defined in specific MIB modules. The Event MIB allows a user or an NMS to watch over specified objects and to set event triggers based on existence, threshold, and boolean tests. An event occurs when a trigger is fired; this means that a specified test on an object returns a value of true. To create a trigger, a user or an NMS configures a trigger entry in the mteTriggerTable of the Event MIB. This trigger entry specifies the OID of the object to be watched. For each trigger entry type, corresponding tables (existence, threshold, and boolean tables) are populated with the information required for carrying out the test. The MIB can be configured so that when triggers are activated (fired) either an SNMP Set is performed, a notification is sent out to the interested host, or both.

**OID** See Object Identifier.

## P

**Packet ID** The ID of a packet in a transport stream.

**PAT** See Program Association Table.

**PCR** See Program Clock Reference.

**PE** See Provider Edge.

| | |
|---|---|
| **PID** | See Packet ID. |
| **PIM** | See Protocol Independent Protocol. |
| **PMT** | See Program Map Table. |
| **PPS** | Packets per second. |
| **Presentation Time Stamp** | The time stamp when a video or audio frame must be presented to the user. |
| **Program Association Table** | A table that lists the PIDs that are associated with the PMTs in the transport stream. |
| **Program Clock Reference** | A clock reference on a program PID that helps to present programs on time and at the right speed. |
| **Program Map Table** | A table that provides information about a program on a video transport stream. The PMT lists the PIDs of the streams associated with the program. |
| **Protocol Independent Protocol** | Multicast routing architecture that allows the addition of IP multicast routing on existing IP networks. PIM is unicast routing protocol independent and can be operated in two modes: dense and sparse. |
| **Provider Edge** | A router at the edge of a network service provider area. |
| **PTS** | See Presentation Time Stamp. |

## Q

| | |
|---|---|
| **QAM** | See Quadratrue Amplitude Modulation. |
| **Quadrature Amplitude Modulation** | Method for encoding digital data in a n analog signal in which each combination of phase and amplitude represents one of sixteen four-bit patterns. Also refers to devices that encode digital cable channels for transmission over cable. |
| **QoS** | See Quality of Service. |
| **Quality of Service** | Measure of performance for a transmission system that reflects its transmission quality and service availability. |

## R

| | |
|---|---|
| **Realtime Transport Protocol** | IP transport protocol that provides media-specific time stamp data for real-time flows. |
| **Rendezvous Point** | Router specified in PIM sparse mode implementations to track membership in multicast groups and to forward messages to known multicast group addresses. |

**Reverse Path Forwarding** Multicasting technique in which a multicast datagram is forwarded out of all but the receiving interface if the receiving interface is the one used to forward unicast datagrams to the source of the multicast datagram. Non-RPF packets, also called RPF failure packets, are RPF packets that have been transmitted backwards, against the flow from the source.

**RP** See Rendezvous Point.

**RPF** See Reverse Path Forwarding.

**RTP** See Realtime Transport Protocol.

## S

**SHE** See Super Head End.

**Simple Network Management Protocol** Network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

**SNMP** See Simple Network Management Protocol.

**Soft Properties** Cisco ANA offers the soft properties mechanism to enable user-configurable extension of device modeling, which can cover any unsupported MIB variable. This enables adding new monitored NE properties in runtime to the default set of supported properties.

Every soft property is implemented through a set of definitions that determine how to retrieve, parse and display a certain MIB variable from the NE. The definition process is done through a simple GUI utility, and does not require system restart. Soft properties are retrieved from the NE using SNMP, or Telnet/SSH.

See also Alarm Thresholding.

**Super Head End** Network location for live feeds for the broadcast video service. This site contains the real-time encoders used for the broadcast video service, along with the asset distribution systems for on-demand services. This site may also contain back-office systems such as the subscriber database. The SHE typically resides in the core of the transport network.

## T

**TCA** See Threshold Crossing Alert.

**Threshold Crossing Alert** A system message that alerts the operator that a provisionable threshold has been crossed.

## V

**VHO** See Video Hub Office.

**Video Hub Office** Network location of the video server complex, which includes the video sources for on-demand services and real-time encoders for local television stations. A VHO typically serves a metropolitan area of between 100,000 and 1,000,000 homes.

**Virtual Network Element** A virtual representation of a single network element as a modeled component. VNEs all communicate with each other to present ANA-based applications with a single, common device abstraction for network element discovery, configuration, status collection, fault analysis and other basic network functions. VNEs can be extended to support new application functionality.

**Virtual Private Network** Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses tunneling to encrypt all information at the IP level.

**VNE** See Virtual Network Element.

**VPN** See Virtual Private Network

**VPN routing/forwarding** A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table.

**VRF** See VPN routing/forwarding.

## Z

**ZAP** See Zone Announcement Protocol.

**Zone Announcement Protocol** A multicast protocol for discovering the multicast administrative scope zones that are relevant at a particular location. See RFC 2776.