Release Notes for Cisco Video Assurance Management Solution 2.0

Revised: April 16, 2010, OL-16499-02

Contents

Note Visit http://www.cisco.com/en/US/products/ps9518/prod_release_notes_list.html to view the latest copy of these release notes.

Introduction

Cisco VAMS 2.0 delivers to service providers real-time, centralized monitoring of headend, backbone, regional, and aggregation networks for broadcast video transport. Cisco VAMS 2.0 provides the framework for a flexible end-to-end assurance platform for video. See the "Solution Requirements" section on page 4 for descriptions of the solution components and required software versions.

Cisco VAMS 2.0 uses Cisco Multicast Manager (CMM 2.5) with patch 2.5.4 for multicast monitoring and troubleshooting functions and the Cisco ROSA Copernicus Network Management System (NMS) for monitoring of video headend events. Additionally, the Cisco VAMS 2.0 system architecture includes

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

an interface between the Cisco Info Center product suite[1] and CMM. Cisco has bundled this interface with the Object Server (central DB) and Webtop (web GUI for event list viewing) from the Cisco Info Center product suite.

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

- IBM Tivoli Business & Services Manager (TBSM), a service dashboard and visualization tool.
- IBM Tivoli Impact, which supports the definition of service and network correlations.

This combination of Cisco Info Center and Netcool functionality accomplishes two key objectives for Cisco VAMS 2.0. It provides:

- Connectivity between Cisco ANA, CMM, the Cisco ROSA NMS, and Cisco Info Center.
- A "Single Pane of Glass" toolset[2] for Cisco VAMS 2.0.

Cisco Info Center contains rules files that specify the rules that define multicast alerts from various sources, such as probes, routers, Digital Content Managers (DCMs), and other network management systems. The rules file contains code that extracts the multicast group and source information from these alerts and provides the operator with a Launch CMM Multicast Trace option.

By integrating CMM and the Cisco ROSA NMS with Cisco Info Center you can view all the alarm conditions and data for service level correlation and analysis. Additionally, for CMM events, you can launch troubleshooting and diagnostic analysis directly from Cisco Info Center.

Cisco VAMS 2.0 supports several third-party probes, including the Bridge Technologies, IneoQuest, Mixed Signals, PixelMetrix, and Tektronix video probes. You can add these video quality monitoring probes to key points in the transport network. Functionally, these probes detect impairments and validate the integrity of the Moving Pictures Expert Group (MPEG) transport stream, which carries video.

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

- The video probes communicate traps directly to Cisco Info Center. For example, the PixelMatrix probe communicates directly with Cisco Info Center (and can only communicate directly with Cisco Info Center). When you are viewing a video probe event forwarded by these probes, you can launch CMM diagnostics directly from the Cisco Info Center interface.
- Certain video probes, such as the IneoQuest probes compatible with iVMS 3.x, support direct polling by CMM 2.5. CMM 2.5 is also able to receive traps from iVMS.3.x.

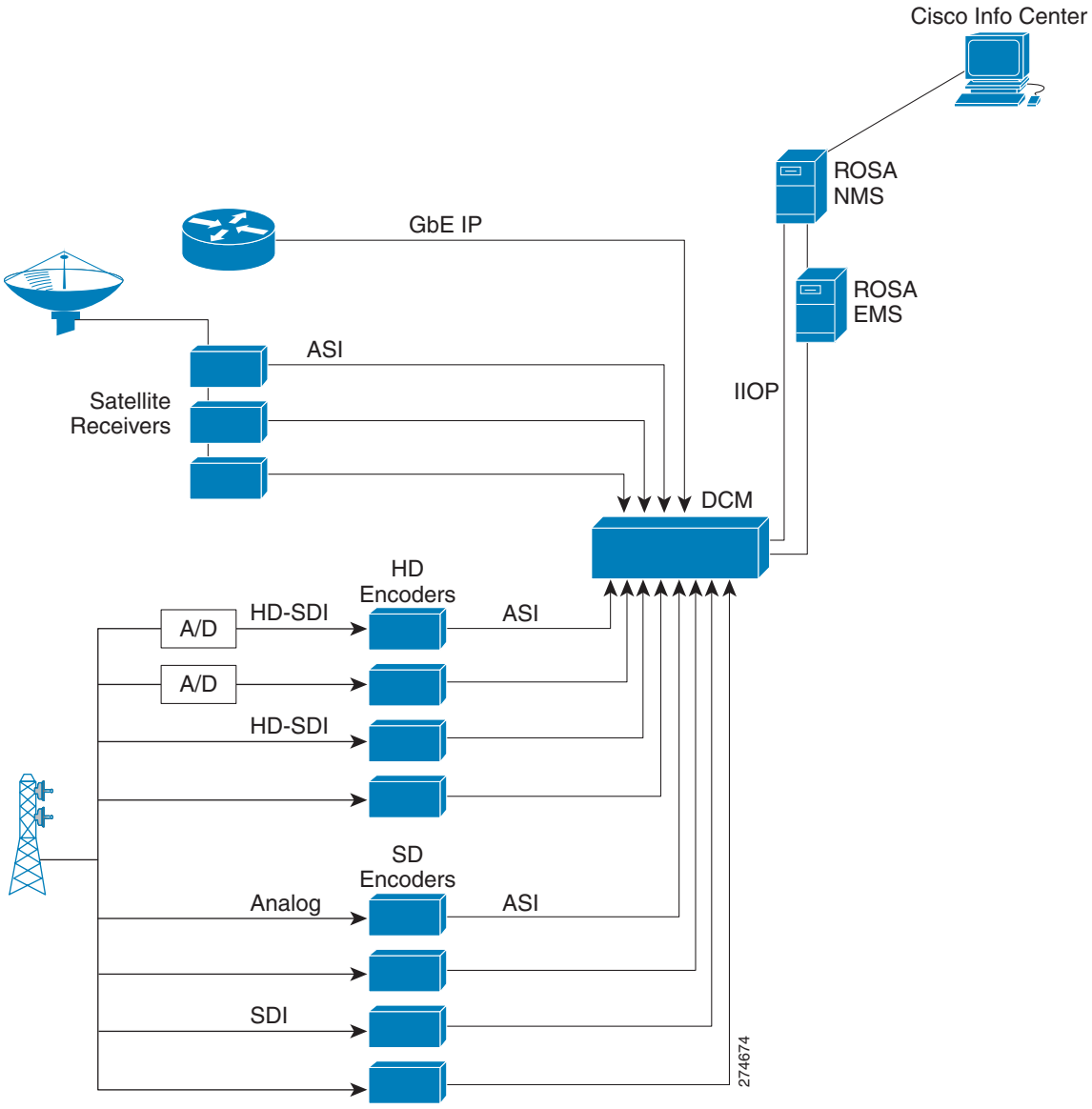
Cisco VAMS 2.0 uses Cisco ANA 3.6 Service Pack 3 to build an abstracted network model through a set of virtual network elements (VNEs). Each VNE represents an element in the managed network. Cisco VAMS 2.0 extends the base functions of the Cisco ANA 3.6.3 VNEs for Cisco 7600 Series routers, Cisco Carrier Routing System (CRS-1) devices, Cisco 12000 series routers, and Cisco Catalyst 4948 Series switches. These VNE extensions address the specific requirements of video delivery across the IP network.

Finally, Cisco VAMS 2.0 includes generic VNEs supporting specific video probes; this release includes VNEs for IneoQuest, Mixed Signals, and Tektronix video probes.

See Figure 1 and Figure 2 for an overview of the Cisco VAMS components (the topology shown in the figures are examples). Figure 1 shows Cisco VAMS in the video headend network, and Figure 2 shows Cisco VAMS in a video transport network.

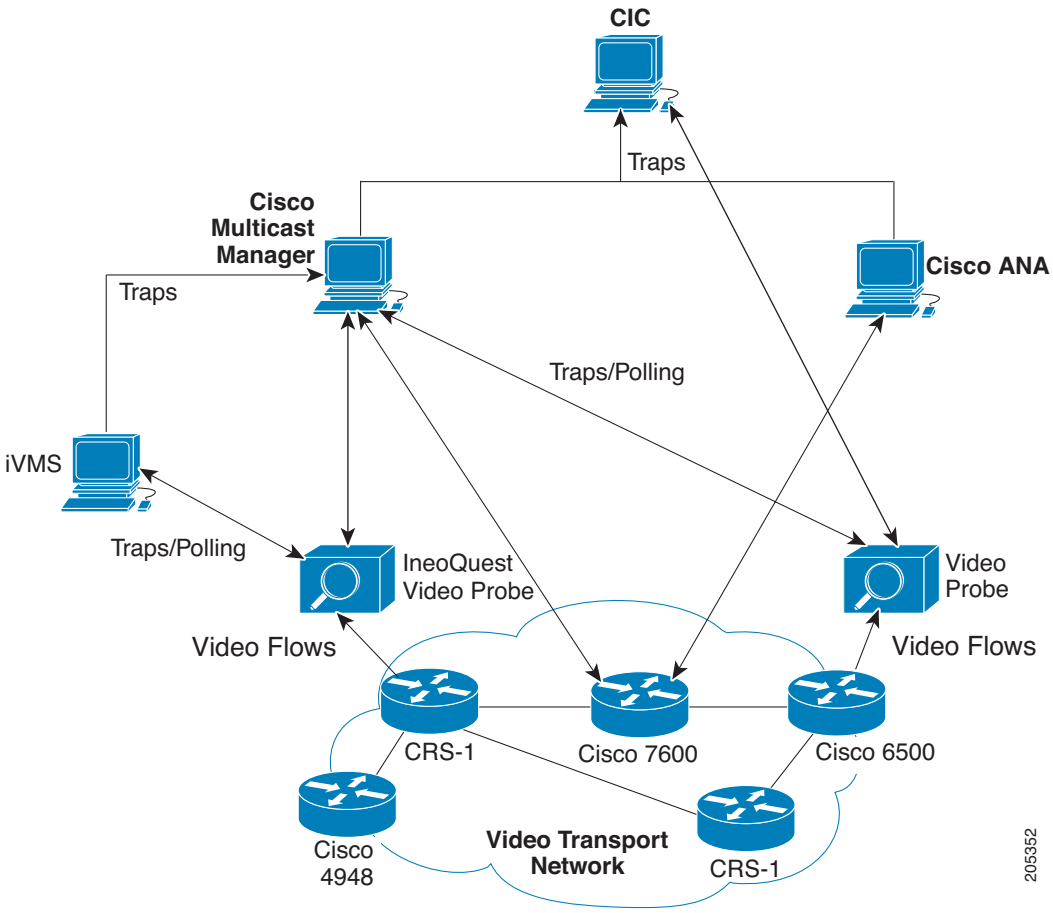
1. This is the OEM product of the IBM Tivoli Netcool Suite.
2. Single Pane of Glass—The ability to utilize multiple interconnected tools to monitor, diagnose, and troubleshoot network and video impairments from a single console.

Figure 1 *Cisco Video Assurance Management Solution 2.0 Components for Video Headend Monitoring*



The ROSA Copernicus NMS receives events either directly from the DCM, or, if the ROSA EMS is deployed in the headend network, from the ROSA EMS by way of the ROSA NMS server.

Figure 2 Cisco Video Assurance Management Solution 2.0 Components



Solution Requirements

Table 1 lists the requirements for Cisco VAMS.

Table 1 Solution Requirements

Solution Component	Version Information	Notes
Cisco VAMS	2.0	Installation script (delivered on DVD)
Active Network Abstraction (ANA)	3.6.3	ANA Gateway—Sun Fire V490, Solaris 10[1] ANA Unit—Sun Fire V480, Solaris 10[1] ANA Client—IBM or PC compatible work station, Windows 2000 or Windows XP[1]
Cisco Multicast Manager	2.5.4	Sun Fire V440—Solaris 8, 9, or 10 Linux—Red Hat Enterprise Linux 3 or 4

Table 1 Solution Requirements (continued)

Solution Component	Version Information	Notes
ROSA Copernicus Element Management System	3.03.10	The ROSA EMS is supported on the following operating systems: • Microsoft Windows 2000 • Microsoft Windows Server 2003 • Windows XP, Service Pack 2 • Microsoft Windows Vista
ROSA Copernicus NMS	3.0.63	—
Digital Content Manager	DCM software V06.05.02	Model D9900 and D9901 with GbE interface card
Cisco 7600 Series router	12.2(33)SRB2, 12.2(33)SRB3, or 12.2(33)SRD1	Supervisor card: 7600-SUP720-3BXL with redundant SUP720-3BXL Line cards include WS-X6704-10GE, WS-X6708-10GE, WS-X6748-SFP, WS-X6748-GE-TX, WS-X6724-SFP, RSP720-3CXL, 7600-ES20-10G3CXL, 7600-SIP-400, 7600-SIP-600, SPA-1XTENGE-XFP, SPA-2X1GE, and optional WS-F6700-DFC3BXL
Cisco 12000 series routers	IOS XR 3.7.1	—
Cisco Catalyst 6500 switch	12.2(33)SXI	—
Cisco Carrier Routing System-1 (CRS-1)	IOS-XR 3.7.1	Line cards include CRS-MSC, CRS1-SIP-800 (with SPA-8X1GE), 8-10GE
Cisco Catalyst 4948 switch (CAT4948-10GE)	12.2(25)EWA6 or 12.2(31)SGA1	—
Cisco Info Center	—	Cisco Info Center includes the following OEM IBM Tivoli Netcool products • ObjectServer - 7.2 • Webtop - 2.1 • TBSM - 4.1 • Impact - 4.0
Bridge Technologies	VB Series	Version: 3.1.0-26
IneoQuest	Singulus G1-T Cricket	Singulus G1-T Media Analyzer Firmware Version: TB-2.5s-060608 Singulus G10 Firmware Version: Denali-1.3a-021808 iVMS 3.00.00 with Patch 24 IQ Cricket Firmware Version: Cricket-1.0a-092607

Table 1 Solution Requirements (continued)

Solution Component	Version Information	Notes
Mixed Signals	Sentry Digital Content Monitor	Sentry 136 Digital Content Monitor[2] Sentry Engine Version: PDM (build 1460.84) Sentry Database Version: 3.0.31 Sentry Configuration: TRANSPORT
PixelMetrix	DVStation	Version: 4.17.0
Tektronix	MTM400	Application Firmware Version: 3.1.061.000 FPGA Logic Firmware Version: 4 BIOS Version: 2.0.7 SNMP Interface Version: 2.6.0 Hardware Version: 5 QA Build: Alpha 01 Build Timestamp: Dec 19 2007 22:22:42

1. See the *User Guide for Cisco Video Assurance Management Solution 2.0* at http://www.cisco.com/en/US/docs/net_mgmt/cisco_video_assurance_mgt_solution/2.0/user/guide/vams_20_user.html for detailed specifications.
2. Cisco VAMS 2.0 does not support carousel-related traps for Mixed Signals Sentry 136.

Table 2 indicates the requirements for the computer used to run the ROSA NMS client.

Table 2 ROSA NMS Client Requirements

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

Installation Notes

Installation of the Cisco VAMS involves installation of its key components:

Hardware Installation

- The core network elements of the video transport network:
  - Cisco 7600 Series router
  - Cisco Catalyst 6500 Series switch
  - Cisco 12000 series router
  - Cisco CRS-1
  - Cisco Catalyst 4948 Series switch
- Management servers for Cisco Multicast Manager (CMM) 2.5.4
- Management servers for Cisco Active Network Abstraction (ANA) 3.6.3 (includes gateway, unit, and client installation)
- ROSA Copernicus NMS 3.0.63
- Digital Content Manager and related video headend equipment
- Third-party video probes:
  - Bridge Technologies VB Series
  - IneoQuest Singulus G1-T
  - Mixed Signals Sentry Digital Content Monitor
  - Pixelmetrix DVStation
  - Tektronix MTM400
- Management servers for Cisco Info Center/Netcool suite

Software Installation

- The IPTV-enabled IOS software versions:
  - 12.2(33)SRB2, 12.2(33)SRB3, or 12.2(33)SRD1 on the Cisco 7600 Series
  - 12.2(33)SXI on the Cisco Catalyst 6500 switch
  - IOS XR 3.7.1 on the Cisco CRS-1
  - IOS XR 3.7.1 on the Cisco 12000 series router
  - 12.2(25)EWA6 or 12.2(31)SGA1 on the Cisco Catalyst 4948 Series switch
- Cisco ANA 3.6.3 (includes gateway, unit, and client installation)
- Cisco Multicast Manager (CMM) 2.5.4 software on dedicated server
- Management software for the Cisco Info Center/Netcool suite:
  - Object Server 7.2
  - Webtop 2.1
  - Impact 4.0
  - TBSM 4.1

For complete details of the installation workflow, including procedures and references to installation documents, see the *User Guide for the Cisco Video Assurance Management Solution 2.0* at http://www.cisco.com/en/US/docs/net_mgmt/cisco_video_assurance_mgt_solution/2.0/user/guide/vams_20_user.html .

Uninstall

You uninstall the Cisco VAMS 2.0 by running the uninstall script. This action removes the IPTV extensions that enable Cisco devices to monitor video conditions in the transport network. The uninstallation procedure is contained in the *User Guide for the Cisco Video Assurance Management Solution 2.0*.

Important Notes

This section includes the following topics:

Nonclearing Events in Cisco Info Center When Repetitive Alarm Suppression Rule Is Enabled in the ROSA NMS

When a ROSA NMS has the Repetitive Alarm Suppression Rule enabled, events might not clear automatically in Cisco Info Center because this ROSA rule causes the ROSA NMS to generate Summary messages in place of individual alarm messages. These Summary messages use incremented `trpMsgID` values, so Cisco Info Center cannot associate them with the initial alarm event.

The ROSA Repetitive Alarm Suppression Rule is disabled by default.

The workaround for this issue is to:

- Disable the ROSA NMS Repetitive Alarm Suppression rule if it is enabled.
- Configure End Debouncing timers on the DCM Interface Alarms settings page.

For information on these tasks, see “Ensuring that the Alarm Suppression Rule is Disabled” and “Configuring End Debouncing Timers on the DCM” in chapter 5 of the *User Guide for Cisco Video Assurance Management System, 2.0,* “Configuring the Components of Cisco Video Management Solution 2.0.” The *User Guide for Cisco Video Assurance Management System, 2.0* is available online at this location:

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

Incorrect Generation of S, G Threshold High Events in CMM with CLI Polling of Cisco 7600

CMM might incorrectly generate S,G Threshold High events from CLI polling of Cisco 7600 devices following a reconvergence event. This is due to the condition described in **CSCsy82569**—"Show ip mroute count reports negative pps or > 10 x pps for CBR flows." There is no workaround for this issue; however, the false event will clear when the 7600 internal counters are corrected at the next counter interval.

Limitations and Restrictions

This section contains these topics:

Java Version for Cisco Info Center Browsers

The IBM TBSM browser must run on JRE 1.4.2 or JRE 1.5. Java versions higher than 1.5 in client web browsers might result in a failure of the Service Viewer and Service Details in the TBSM window.

Cisco Multicast Manager Limitation with Naming Services

Disable any naming service such as Network Information Service (NIS) or NIS+ before running CMM 2.5.4.

Cisco Multicast Manager Trap Limitations

The following Cisco Multicast Manager *Normalized* traps do not clear their corresponding *Threshold Exceeded* traps:

```
'High L2 Port Threshold Exceeded',
'Low L2 Port Threshold Exceeded',
'L2 Threshold Normailzed',
---
'SG Delta Threshold Exceeded',
'SG Threshold Normalized',
---
'Multicast Bandwidth Percent High Threshold Exceeded',
'Multicast Bandwidth Percent Low Threshold Exceeded',
'Multicast Bandwidth Percent Threshold Normalized',
---
'High BPS Threshold Exceeded',
'Low BPS Threshold Exceeded',
'BPS Threshold Normalized',
```

Cisco ANA processes all Cisco Multicast Manager traps, but currently lacks the capability to correlate threshold normalized traps to their corresponding threshold exceeded traps.

In addition, the following Cisco Multicast Manager traps do not have corresponding *clears*.

```
'RP Group Threshold Exceeded',

---
'RPF Failure Threshold Exceeded',

---
'High Threshold Exceeded PPS',
'Low Threshold Exceeded PPS',
```

Open Caveats

Table 3 indicates the open caveats for Cisco VAMS 2.0.

Table 3 Open Defects in Cisco VAMS 2.0

Defect ID	Description
CSCsu67694	**Symptom** Video Service alarm for IneoQuest doesn't increment. **Conditions** The Video Fault page has a Video Services Events sidebar; under this there are icons for different probe vendors. The IneoQuest probe vendor item does not increment. Any Ineoquest events go straight into the All Video Events counter. **Workaround** None.
CSCsu99456	**Symptom** CMM tree change/revert not working properly. **Conditions** CMM is able to display multicast tree traces; however, it will not generate alerts or reports for the latest events. For example, when performing a health check, the tree status is shown as “N/A.” **Workaround** None.
CSCsr96319	**Symptom** ANAServerIP value is recorded incorrectly. **Conditions** For any ticket reported by Cisco ANA, the LocalNodeAlias field is mapped to the ANAServerIP field. This occurs with version NCW_V2.1.59 running on Solaris 2.9. **Workaround** None
CSCsr98713	**Symptom** Cisco Multicast Manager discovery does not complete if NIS+ is enabled. **Conditions** When running CMM 2.5.4 on Solaris 10, with Network Information Service Plus (NIS+) enabled, CMM discovery does not complete. The .snmp library initialization call gets stuck and the discovery process does not proceed. Running truss shows that the process is not able to open the */etc/nisplus.conf* file. **Workaround** Disable any naming service such as NIS or NIS+ before running CMM 2.5.4.

Table 3 Open Defects in Cisco VAMS 2.0 (continued)

Defect ID	Description
CSCsr98477	**Symptom** The ANA Topological link properties entry is incorrect. **Conditions** Media type is incorrect in the link attributes GUI; for example, the link property is shown as RJ45 when it should be an "Optic Fi." This condition occurs in the attributes for ports with pluggable modules, such as SFP. **Workaround** None
CSCsu21758	**Symptom** 7600 Redundancy status is only shown on one module. **Conditions** This condition occurs when ANA 3.6.0.3.9 running and a Cisco 7606 is running SRC1. When Cisco 7600s are viewed, Network Vision only shows the correct SSO redundancy status on the card that is in module 5. Module 6 shows the status "none." **Workaround** None.
CSCsu59544	**Symptom** The ciscoIpMRouteNumberOfEntries count is inconsistent for SSM groups. **Conditions** When the ciscoIpMRouteNumberOfEntries OID is polled, the value returned for number of groups reflects not only the SSM (s,g) but also the SSM (*,g), which are internal, hidden entries. Thus, the number indicated is higher than the number that is shown when the `show ip mroute count` command is entered. **Workaround** None.

Related Documentation

Refer to the following sections for information on related documentation:

- Cisco VAMS 2.0 Documentation, page 11
- Documentation for VAMS Components, page 12

Cisco VAMS 2.0 Documentation

In addition to the *User Guide for Cisco Video Management Solution, 2.0*, the Cisco VAMS documentation set comprises:

- *User Guide for Cisco Video Management Solution, 2.0*

  Provides an overview of the solution features and architecture, installation and configuration instructions, and information on using the TBSM and Webtop interfaces to view events and troubleshoot events in the video network. This document is viewable online at:

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

- *Documentation Guide for Cisco Video Management Solution, 2.0*

Provides links to the documentation for the Cisco VAMS 2.0 component products and for related products. This document is available online at:

http://www.cisco.com/en/US/docs/net_mgmt/cisco_video_assurance_mgt_solution/2.0/roadmap/vams20dg.html

Documentation for VAMS Components

For links to the documentation for the VAMS product components, see the *Documentation Guide for Cisco Video Management Solution, 2.0,* viewable online at:

http://www.cisco.com/en/US/docs/net_mgmt/cisco_video_assurance_mgt_solution/2.0/roadmap/vams20dg.html

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.

This document is to be used in conjunction with the documents listed in the Related Documentation section.