# Cisco Video Assurance Management Solution 1.0

## Solution Value Proposition

**Q.** What is Cisco® Video Assurance Management Solution (VAMS) 1.0?

**A.** Cisco VAMS 1.0 delivers to service providers real-time centralized monitoring of their backbone, regional, and aggregation networks for video transport. Cisco VAMS 1.0 focuses on broadcast video over multicast. Support for unicast services across the transport network is targeted for future release. Cisco Video Assurance Management Solution 1.0 also provides the framework for a flexible end-to-end assurance platform for video.

**Q.** What video transport issues does the system address?

**A.** VAMS is targeted at:

- Identifying video continuity errors

- Identifying whether these are caused by the transport network or whether the transport network can be eliminated as a source for video continuity errors

- Reducing the problem domain to identify whether video problems are due to the transport network and where in the transport path the video service has been affected

- Correlate transport network changes with video anomaly detection, facilitating problem isolation and diagnosis

**Q.** How does Cisco VAMS integrate with my existing OSS environment?

**A.** Cisco VAMS uses the Cisco Active Network Abstraction (ANA) platform as the mediation layer between network elements, video probes, and the presentation layer provided to network operators and network engineers. An example of the integration of Cisco VAMS into the operational environment is provided through Cisco Assurance Management Solution 1.0. This integrates Cisco ANA with the IBM Netcool suite of products and demonstrates how this system is deployed. Figure 1 illustrates how the Cisco VAMS 1.0 and Cisco AMS 1.0 solutions relate.

**Figure 1.** Cisco VAMS 1.0 and Cisco AMS 1.0
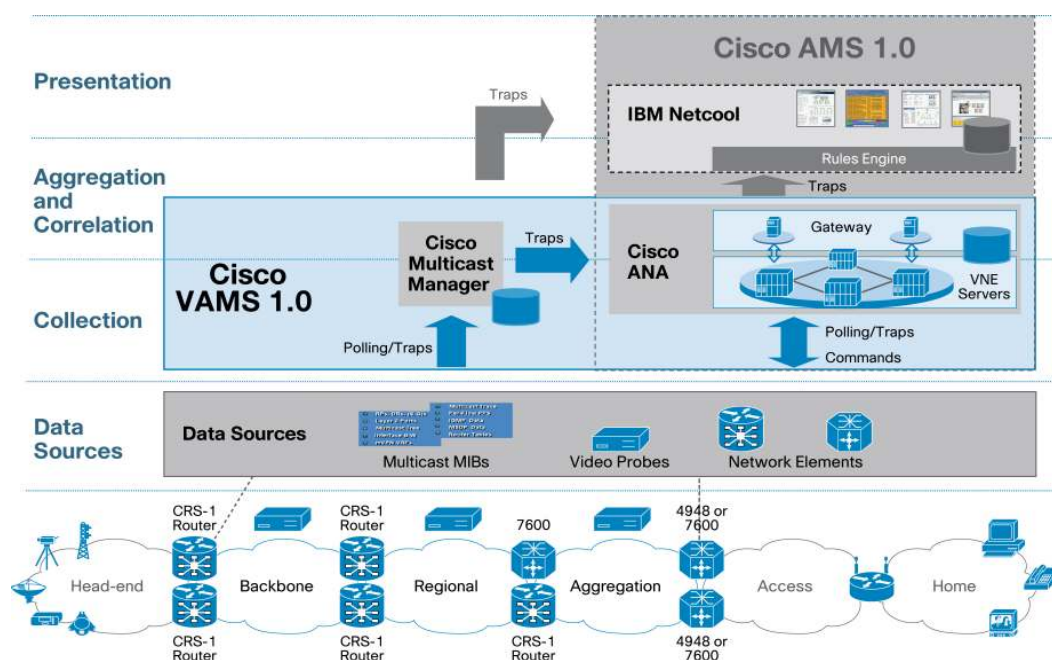


**Q. How is Cisco VAMS different from video monitoring from third-party video probe vendors?**

**A.** Cisco has partnered with a number of video probe vendors to demonstrate how their systems will interact with Cisco VAMS. Video probe monitoring devices are typically placed at demarcation points through the video path. Examples are at the acquisition point, at the handoff from the super head end to the network, at the handoff from the network to regional or local ad zones, and from these zones back to the network and from the transport network to the last mile/home environment.

By correlating these data sources with data sources on the network, it is possible to identify, isolate, and troubleshoot video errors. The benefits are twofold, reducing the time to resolve issues in the transport network and eliminating the network where it is not the cause of video errors. Both of these are cost-intensive exercises today.

**Q. How do I integrate this solution into my existing OSS environment?**

**A.** Cisco provides deployment and integration services for Cisco Video Assurance Management Solution and will work with the chosen integration partners to provide the required services.

**Q. How does this solution relate to Cisco Video Operations Solution (VOS)?**

**A.** Cisco VOS represents the first phase of the Cisco video assurance program. Cisco VOS is a Cisco Multicast Manager–based video monitoring and troubleshooting solution and was provided as a point solution. Through enhancements to the northbound interface of Cisco Multicast Manager and integration of these into the Cisco ANA product, Cisco VAMS builds on Cisco VOS to provide a solution and framework that facilitates the integration of Cisco VOS into the OSS infrastructure.

## Solution Description

**Q.** **What are the components of Cisco Video Assurance Management Solution 1.0?**

**A.** Cisco Video Assurance Management Solution 1.0 comprises the following Cisco products and solutions:

- Cisco Active Network Abstraction (ANA) 3.6: This system operates between the network and the operations support system (OSS) layers acting as a mediation and abstraction between OSS applications and the network devices. Its abstracted network model removes the complexity of upgrading each and every OSS application when there is an upgrade of any element within the network. It also provides a gateway to the network for OSS applications supporting correlation and aggregation of events in the network and provides this correlated information northbound.

- Cisco IPTV SLA solution built around Cisco Multicast Manager (CMM) 2.4: This tool provides a rich set of multicast monitoring and troubleshooting functions that enable Cisco VAMS 1.0 to be notified of any changes in multicast or threshold events on elements in the multicast trees that may affect video performance. Cisco VAMS 1.0 collects outputs from Cisco Multicast Manager into Cisco Active Network Abstraction (ANA) providing views of both device and multicast faults.

**Q.** **When should Cisco VAMS 1.0 be applied in the network?**

**A.** Cisco VAMS is targeted to support the assurance of video traffic across the transport network. Cisco VAMS 1.0 has focused on the backbone, regional, and aggregation networks. Figure 1 highlights where in the transport network Cisco VAMS 1.0 is focused. Future releases will expand this to the access network.

Cisco VAMS 1.0 focuses on assurance of broadcast services across the transport network. This service requires the modeling of the multicast service across the network and correlation of the multicast service with monitoring of network elements and video streams.

**Q.** **What are the target markets for Cisco VAMS?**

**A.** Cisco VAMS 1.0 is targeted at tier 1 service providers, large multiservice operators (MSOs) offering broadcast TV services, and systems integrators offering a service to tier 2/3 operators for delivering broadcast TV to their customers.

**Q.** **What benefits does Cisco VAMS deliver?**

**A.** Cisco VAMS provides a framework for delivering an integrated system for video assurance across the transport network. The key benefits of Cisco VAMS are:

- Proactive identification of video continuity errors before customers begin to complain

- Rapid domain isolation: Is the transport network the cause or can it be eliminated as a source for video continuity errors?

- Problem domain reduction: For problems that occur in the transport network—where in the path has the video service been affected?

- Facilitating rapid problem isolation and diagnosis through correlation of transport network changes with video anomaly detection

**Q.** **Cisco VAMS can help assure video across my network, but does it offer a tangible return on investment (ROI)?**

**A.** Video is highly sensitive to packet drops. Typical targets for video performance require no more than one video impairment event in any one hour. This roughly translates to a maximum drop rate of one in one million.

Cost-effective rollout of video requires that the IP network be used to deliver this highly sensitive service. In an IP network there are typically many applications sharing the same resources. Great care must be taken in such an environment to isolate sensitive traffic and to be able to monitor and troubleshoot the network quickly and efficiently.

In particular, when customers start to call in problems in their service, it is often the case that an operator will unnecessarily dispatch field technicians to try to isolate and resolve problems. This is a highly costly and time-intensive effort. Cisco VAMS helps avoid such unnecessary truck-rolls and helps target engineers on the right parts of the video system to reduce Mean Time to Repair (MTTR).

### Video Transport Principles

**Q.** **How is video encapsulated across the network?**

**A.** The typical protocol stack for video across the transport network is constructed as shown in Table 1.

**Table 1.** A Typical Protocol Stack for Video across the Transport Network

| Protocol Layer | Protocol | Description |
|---|---|---|
| **Presentation/session** | MPEG(2/4) | MPEG-2 is a standard for the coding of video and associated audio information; it is a combination of lossy video compression and lossy audio compression methods. |
| **Transport** | RTP | The Real-Time Transport Protocol (RTP) is a transport-layer protocol to manage the real-time transmission of multimedia data. It is combined with a control protocol (RTCP) that facilitates monitoring of data delivery for large multicast networks. Monitoring allows the receiver to detect whether there is any packet loss. |
| | UDP | User Datagram Protocol (UDP) is a stateless core Internet transport protocol that supports efficient data transmission without the guarantees of TCP. Avoiding the overhead of checking whether every packet actually arrived makes UDP faster and more efficient. |
| **Network (see Figure 2 for an overview of a typical IP multicast network configuration)** | IGMP | The Internet Group Management Protocol (IGMP) is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. |
| | PIM | Protocol-Independent Multicast (PIM) is a family of multicast routing protocols that can provide one-to-many and many-to-many distribution of data over the Internet. PIM-SSM, Source Specific Multicast, is typically used to support the broadcast of video content across an IP network |
| | IP | IP provides connectionless datagram delivery service for transport-layer protocols such as UDP and RTP |

**Figure 2.**    A Typical IP multicast network configuration
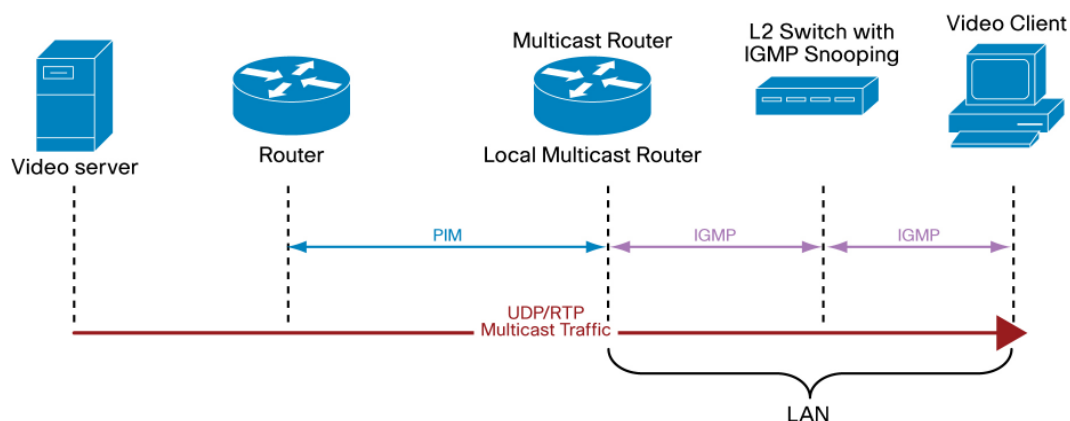


**Q.** **What is the typical topology of a video broadcast service?**

**A.** Figure 3 illustrates the typical structure of a video broadcast service. Note that video-on-demand functions are included here for completeness.

**Figure 3.**    Typical Structure of a Video Broadcast Service
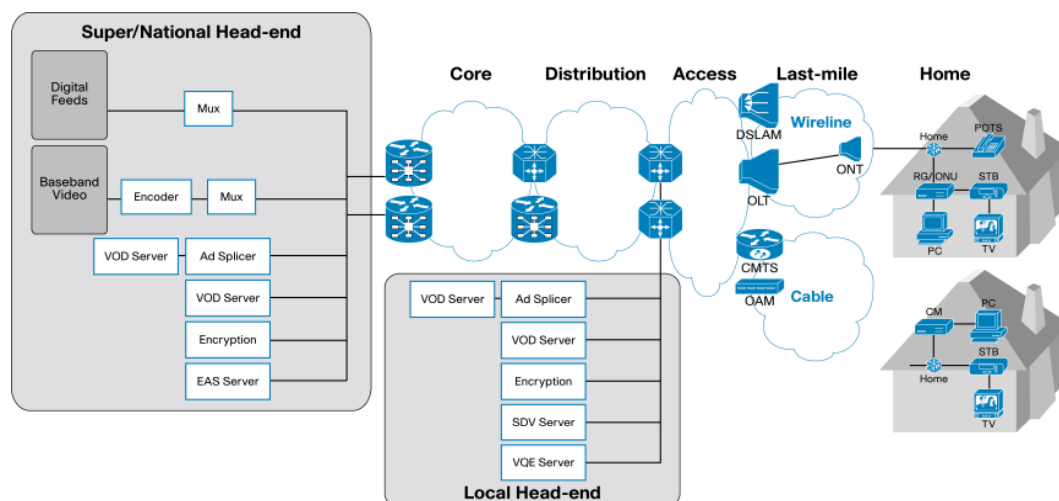


**Q.** **What are the critical problems the may occur end to end? From face to glass, where do video problems occur?**

**A.** Problems may occur at any of the following points:

- Super/national head-end
  ◦ Poor content quality from video provider
  ◦ Program identifier (PID) mappings or data table mappings from video source
  ◦ Transcoding lip sync issues
  ◦ Transcoding bandwidth misconfiguration

- Core/distribution network
  - Packet loss, high sensitivity, for example, one loss in every one million packets
  - Error correction performance: Must reconverge rapidly
  - Misprovisioning
  - Mistakes here are catastrophic
- Local head end
  - Video on demand (VoD) server capacity
  - VoD service availability
  - Ad insertion
  - Errors in local channel feed
  - Subscriber management
  - Error correction and channel fill capacity
- Aggregation and last mile
  - Misprovisioned network
  - PIM/IGMP multicast performance
  - Policy management/oversubscription
  - Error correction/channel fill capacity
  - Loop performance and stability
  - Noise and impulse on loop
- Customer premises
  - Impulse noise events that impair video streams across
  - Residential gateway performance problems
  - Security/authentication/policy management misconfigurations
  - Home link (such as Cat3/5 cabling, MoCA, HPNA) performance problems

**Q. What is the sensitivity of video to transport problems?**

**A.** MPEG streams consist of I frames, B frames, and P frames. B-frames and P-frames build upon the content of the I-frame, essentially using the I-frame as a reference and indicating how the next frame in the video is different from the I-frame. If an I-frame is lost, then all following frames are meaningless until the next I-frame is received by the set-top box. Typical MPEG encodings send an I-frame every 300–500 ms. Thus if an I-frame is lost, the user can experience significant video impairments.

Other critical video control data, such as PAT (Program Association Tables) and PMT (Program Mapping Tables), contain information to enable the set-top-box (STB) identify and correlate video streams correctly. Loss of information can lead to such problems as loss of audio information, loss of video information, or even total loss of the channel.

Thus, dropping a single packet in the transport network can lead to major degradation in the user experience. If such losses occur frequently, the customer is unlikely to continue to use the video service.

**Q.** **Isn't it easy to identify video-affecting problems in the network? Isn't it just packet drops?**

**A.** In one sense, yes, it is easy to spot packet drops in the network. Simply look at the right MIB information from the network devices. The issue is that it is unclear how these affect the user experience. All packet drops are not the same. For example, error-correction protocols may be in place across the network that address certain packet drop conditions without affecting the user, or, as shown above, the dropped packet may contain information relating to multiple channels and have dramatic impact at a service level.

For this reason it is crucial to combine knowledge of network performance with analysis of the video streams from a user perspective and correlate this information to provide clear root-cause analysis.

## For More Information

For more information about Cisco VAMS 1.0, visit http://www.cisco.com/go/vams or contact your local account representative.

---

**CISCO**

| Americas Headquarters | Asia Pacific Headquarters | Europe Headquarters |
|---|---|---|
| Cisco Systems, Inc. | Cisco Systems (USA) Pte. Ltd. | Cisco Systems International BV |
| San Jose, CA | Singapore | Amsterdam, The Netherlands |

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA                                                                                                                        C67-452658-00   03/08

---