

Medianet Media Monitoring Q&A

Q. What is Media Monitoring?

A. Media Monitoring is a Cisco IOS® family of features that enhances visibility into the network to accelerate voice, video, and data application deployment. These features facilitate application baselining, network validation, and fault isolation in many scenarios including pre-deployment, profiling, and troubleshooting.

Media Monitoring has three functional areas: **Performance Monitor**, **Mediatrace**, and **IP service-level agreement (IP SLA) video operation (VO)**. These three features work to aid in application monitoring and troubleshooting. Mediatrace can use Performance Monitor to provide hop-by-hop analysis of a media flow in real time, while a call is still active. IP SLA VO can be used in conjunction with Mediatrace to validate and troubleshoot a network by injecting simulated application traffic, thereby mitigating the need for a fully functioning application.

Q. Why do I need Media Monitoring? Can I monitor my network and get statistics today?

A. Today, when users report rich-media quality issues, understanding what the problem is and its location is nearly impossible. Traditional troubleshooting techniques such as ping, interface statistics, or IP SLA are limited in the level of information they can provide. Differentiated services code point (DSCP) marking is not enough (all video applications look the same) and network management solutions are not designed to take video traffic into account.

Media Monitoring specifically considers what traffic to monitor, what information to gather, where to monitor (which router, which switch interface is involved in the media flow), service-level agreements against which to measure the traffic, and finally where and which method of information transfer to network management applications.

Media Monitoring, via IPSLA VO, also provides network administrators the ability to generate synthetic media flows replicating exact video requirements to test the impact of a particular video communication (Cisco TelePresence® operations, Cisco® Unified Communications, Cisco WebEx® solutions, video surveillance, Digital Media System (DMS), IPTV, and so on) and assess the network.

Q. What is Performance Monitor?

A. [Performance Monitor](#) is a Medianet Cisco IOS Software feature that measures the performance of Real Time Protocol (RTP), TCP, and IP constant bit rate (CBR) traffic on network devices. Performance Monitor analyzes RTP based audio and video flows and reports on service affecting metrics like packet loss and network jitter. For TCP flows, Performance Monitor reports on round trip time and packet loss occurrences. Hop-by-hop knowledge of these metrics along the network path leads to granular fault isolation and thus easier troubleshooting of user traffic flows.

Performance Monitor maintains historical data about analyzed flows traversing routers and switches. The metrics collected by Performance Monitor can be exported to a network management tool through NetFlow Version 9 or Simple Network Management Protocol (SNMP). Network management software can further analyze, summarize, and correlate this information to provide traffic profiling, baselining, and troubleshooting services for the application and network operator.

Performance Monitor has the ability to send alarms from the routers and switches through syslog and SNMP traps. Different media applications, for example, Cisco TelePresence compared to video on demand (VoD), have different sensitivities to packet loss and jitter. These varying sensitivities can be encoded into

Performance Monitor threshold evaluations and actions. An example would be the generation of an SNMP trap when Cisco TelePresence traffic loss is greater than 1 percent. When a threshold is crossed, an alarm is generated that can notify the operator of the issue. This event may eventually engage further diagnostics such as Mediatrace to troubleshoot and further isolate the cause of the degradation.

Q. Where must I configure Performance Monitor?

A. While it is not necessary to configure all nodes on the network with Performance Monitor, the more nodes recording the experience of the flow as it travels through the network the better the granularity of the reporting. A single Performance Monitor can be used to perform validation. Multiple Performance Monitor-enabled devices can be used for fault isolation.

It is recommended to activate Performance Monitor on nodes adjacent to problematic areas of the network (for example the WAN edge) or administrative boundaries (for problem ownership resolution).

Mediatrace will be used to automate this collection of information on the fly.

Q. What if I haven't turned Performance Monitor on and a problem occurred?

A. [Mediatrace](#) provides a "one-screen" report of the flow path by tracing the flow across the network and collecting information about the flow from Mediatrace-enabled routers and switches. Mediatrace collects system information from network devices along the path (for example, 1 minute CPU utilization) and can implicitly enable Performance Monitor to gather flow-specific information such as loss and jitter.

Mediatrace supports the initiation of the request from an off-path router. Mediatrace can be initiated through the command-line interface (CLI), a network management tool, or a Media Services Interface (MSI)-enabled media endpoint.

With all the relevant statistics available for the flow, from the network nodes along the path, Mediatrace easily and very accurately pinpoints the source or sources of degradation along the network path.

Q. How can Media Monitoring help me to assess my network for future video deployment?

A. One of the key features of Media Monitoring is [IP SLA video operation](#). It has the ability to synthetically generate video traffic mimicking real application traffic, like Cisco TelePresence, IP video surveillance, and IPTV. IP SLA VO can also work using a captured packet trace of user traffic at a customer's premises to synthetically generate similar traffic.

IP SLA VO can also be used to run readiness tests prior to sensitive collaboration meetings to test the network and, in collaboration with Performance Monitor and Mediatrace, to accelerate troubleshooting if issues are found.

IP SLA VO adds to the existing IP SLA probes that are available in Cisco IOS Software such as User Datagram Protocol (UDP) jitter and Domain Name System (DNS). Users of IP SLA will find that IP SLA VO simply extends the familiar IP SLA control and scheduling CLI and MIB framework, allowing for easy integration with existing network management tools.

Q. Can we use Performance Monitor to monitor SAP traffic?

A. Yes, Performance Monitor can be used to monitor not only SAP traffic but also many other different types of traffic. Please refer to the white paper [Application Performance Assurance using Cisco Performance Manager](#), which talks about how Performance Monitor can be used to monitor different types of applications.

Q. What network management solution supports Media Monitoring features today?

A. Media Monitoring makes use of standardized protocols such as SNMP, NetFlow, and Web Services to transfer information to network management systems.

There are several tools that support the Medianet capabilities depending on customers' needs and environment. For example, when deploying Medianet in conjunction with Cisco TelePresence, [Cisco Prime™ Collaboration Manager](#) provides visibility into video traffic by leveraging Mediatrace. Cisco Prime Assurance Manager leverages Medianet Performance Monitoring statistics and provides consistent performance visibility across the network.

There are also [tools from other vendors](#) that partner with us through our Enterprise Medianet Systems Management Cisco Developer Network Program. Please check the [Medianet datasheet](#) to learn about options.

- Q.** In a Medianet deployment when do I use Cisco Prime Collaboration Manager vs Cisco Prime Assurance Manager
- A.** Cisco Prime Collaboration Manager is an application management tool that leverages Mediatrace and Performance Monitoring capabilities of Medianet. It can be used when trying to troubleshoot and isolate telepresence and tandberg sessions issues in real-time. Prime Assurance Manager is a network management tool. It leverages Medianet Performance Monitoring capabilities among many of the Cisco's rich embedded infrastructures. It gives a holistic view of the deployment by providing contextual drilldowns and helps troubleshoot issues across sites, applications, devices, interfaces and users. For more details refer to the [Network Management and Application Management Made Simpler](#) white paper.
- Q.** Which Cisco platforms and software releases are supported?
- A.** Please refer to the [Medianet 2.2 datasheet](#) for an up-to-date detailed description of platforms and versions supported



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV 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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)