Newer Cisco SBA Guides Available

This guide is part of an older series of Cisco Smart Business Architecture designs. To access the latest Cisco SBA Guides, go to http://www.cisco.com/go/sba

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a new series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

SBA

MIDSIZE

COLLABORATION

Video Conference Quality Monitoring Using Medianet Deployment Guide

SMART BUSINESS ARCHITECTURE

February 2012 Series

Preface

Who Should Read This Guide

This Cisco® Smart Business Architecture (SBA) guide is for people who fill a variety of roles:

- Systems engineers who need standard procedures for implementing solutions
- Project managers who create statements of work for Cisco SBA implementations
- Sales partners who sell new technology or who create implementation documentation
- Trainers who need material for classroom instruction or on-the-job training

In general, you can also use Cisco SBA guides to improve consistency among engineers and deployments, as well as to improve scoping and costing of deployment jobs.

Release Series

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a new series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

All Cisco SBA guides include the series name on the cover and at the bottom left of each page. We name the series for the month and year that we release them, as follows:

month year Series

For example, the series of guides that we released in August 2011 are the "August 2011 Series".

You can find the most recent series of SBA guides at the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel

How to Read Commands

Many Cisco SBA guides provide specific details about how to configure Cisco network devices that run Cisco IOS, Cisco NX-OS, or other operating systems that you configure at a command-line interface (CLI). This section describes the conventions used to specify commands that you must enter.

Commands to enter at a CLI appear as follows:

```
configure terminal
```

Commands that specify a value for a variable appear as follows:

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

```
class-map [highest class name]
```

Commands shown in an interactive example, such as a script or when the command prompt is included, appear as follows:

```
Router# enable
```

Long commands that line wrap are underlined. Enter them as one command:

```
wrr-queue random-detect max-threshold 1 100 100 100 100 100 
100 100 100
```

Noteworthy parts of system output or device configuration files appear highlighted, as follows:

```
interface Vlan64
  ip address 10.5.204.5 255.255.255.0
```

Comments and Questions

If you would like to comment on a guide or ask questions, please use the forum at the bottom of one of the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel

An RSS feed is available if you would like to be notified when new comments are posted.

Table of Contents

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

What's In This SBA Guide

About SBA

Cisco SBA helps you design and quickly deploy a full-service business network. A Cisco SBA deployment is prescriptive, out-of-the-box, scalable, and flexible.

Cisco SBA incorporates LAN, WAN, wireless, security, data center, application optimization, and unified communication technologies—tested together as a complete system. This component-level approach simplifies system integration of multiple technologies, allowing you to select solutions that solve your organization's problems—without worrying about the technical complexity.

For more information, see the *How to Get Started with Cisco SBA* document:

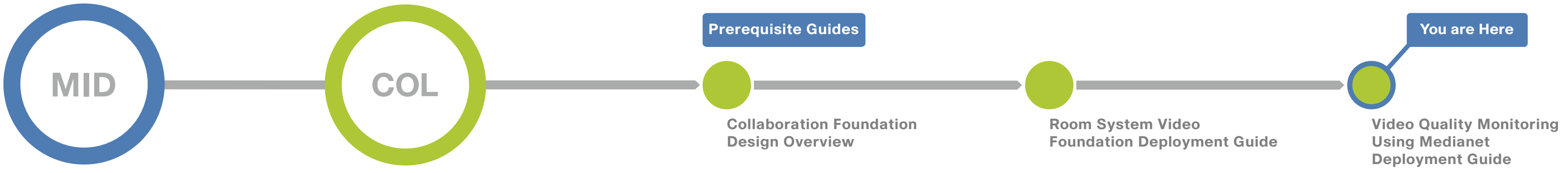
http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Smart_Business_Architecture/SBA_Getting_Started.pdf

About This Guide

This *additional deployment guide* includes the following sections:

- Business Overview—The challenge that your organization faces. Business decision makers can use this section to understand the relevance of the solution to their organizations' operations.
- Technology Overview—How Cisco solves the challenge. Technical decision makers can use this section to understand how the solution works.
- Deployment Details—Step-by-step instructions for implementing the solution. Systems engineers can use this section to get the solution up and running quickly and reliably.

This guide presumes that you have read the prerequisites guides, as shown on the Route to Success below.


MID
COL
Prerequisite Guides
You are Here
Collaboration Foundation Design Overview
Room System Video Foundation Deployment Guide
Video Quality Monitoring Using Medianet Deployment Guide

Route to Success

To ensure your success when implementing the designs in this guide, you should read any guides that this guide depends upon—shown to the left of this guide on the route above. Any guides that depend upon this guide are shown to the right of this guide.

For customer access to all SBA guides: http://www.cisco.com/go/sba
For partner access: http://www.cisco.com/go/sbachannel

Introduction

Business Overview

Businesses around the world are struggling with escalating travel costs. The high price of travel is reflected in growing corporate expense accounts, but it also takes a toll on the health and well-being of employees and their families. The time away from home and the frustration levels experienced from lost luggage, navigating through airport terminals, and driving in unfamiliar cities are burdens many employees must endure on a weekly basis.

Organizations are under increasing pressure to reduce the amount of time it takes to make informed decisions concerning their business operations. Oftentimes, the only way solve a difficult problem is to fly an expert to the location to see the issue directly and discuss it with the people at the site. When an expert cannot see what is being described, the resolution of a complex problem can take much longer.

Audio conferences can help in certain situations, but the face-to-face interaction during video collaboration meetings helps to boost information retention, promotes increased attention span, and reduces participant confusion. The nonverbal cues experienced in a visual meeting are sometimes more important than what is actually spoken.

Media applications, particularly video-oriented ones, are experiencing rapid growth on corporate networks, exponentially increasing bandwidth utilization and radically shifting traffic patterns. There are multiple business drivers behind this growth, including a globalized workforce, the pressure to go "green," the transition to high-definition media (both in consumer and corporate markets), and social networking phenomena that are crossing over into the workplace.

IP-based video conferencing has emerged as the dominant technology in the video conferencing market. This market includes a broad range of options, ranging from high-definition telepresence systems and room based solutions at the high end to dedicated desktop systems at the mid-range and PC/desktops/laptops with web cameras at the low end. The low end solutions typically rely on best-effort quality of service (QoS), and no specific capabilities are required from the network. With these lower end solutions, the video and audio quality may vary significantly depending on what other applications are currently active on the network.

As organizations begin to deploy higher-end solutions, it follows that their underlying networks must be appropriately designed to support the requirements of the video solution. Traditional IP networks are not well-suited to deal with interactive and real-time requirements, making the delivery and quality of video conferencing traffic unpredictable and increasing the complexity for network operators and managers. Organizations would like to reduce the complexity and the associated costs of deploying video conferencing.

Technology Overview

A medianet is an end-to-end architecture for a network comprising advanced, intelligent technologies and devices in a platform optimized for the delivery of rich-media experiences. A medianet has the following characteristics:

- Media-aware: Can detect and optimize different media and application types (telepresence, video surveillance, desktop collaboration, and streaming media) to deliver the best experience
- Endpoint-aware: Automatically detects and configures media endpoints
- Network-aware: Can detect and respond to changes in device, connection, and service availability

Cisco Medianet capabilities fall into two categories: autoconfiguration and media monitoring. Autoconfiguration is not covered within this guide.

Video conference quality monitoring is accomplished using Cisco Medianet media monitoring capabilities that help network operations staff proactively manage network resources and help ensure that the overall user experience of video conferencing remains positive. Other benefits of a Cisco Medianet to an organization include:

- Reduced operating costs
- Simplified installation and management of video endpoints
- Faster troubleshooting for voice, data, and video applications
- The ability to assess the impact of video, voice, and data in your network (for example, determining the right size for your network and avoiding unnecessary bandwidth upgrades)
- Service-level agreement (SLA) assurance and negotiation
- Ability to gather key metrics for the service provided
- Faster end-user adoption of rich-media applications through a high-quality, positive user experience

The focus of this guide is on providing real time visibility of active video conferences and on raising awareness of performance problems within the network that affect their quality.

Cisco Medianet media monitoring consists of three complementary technologies:

- Performance Monitor (PerfMon) allows you to analyze the performance of rich-media traffic across the network to provide a holistic view of the network service being delivered. PerfMon can also generate alerts based on defined performance thresholds.
- Mediatrace discovers Layer 2 and Layer 3 nodes along a flow path. Mediatrace implicitly uses PerfMon to provide a dynamic hop-by-hop analysis of media flows in real time to facilitate efficient and targeted diagnostics.
- IP Service Level Agreement Video Operation (IPSLA VO) generates synthetic traffic streams that are very similar to real media traffic. It can be used in conjunction with Mediatrace to perform capacity planning analysis and troubleshooting even before applications are deployed.

You can use PerfMon and Mediatrace to quickly and cost-effectively respond to any video-conferencing quality issues. This capability allows the organization to maintain a reliable and high-quality service for their video conference attendees. IPSLA VO capabilities allow an organization to plan for future growth in network capacity and provided services.

PerfMon

PerfMon maintains historical data about specific classes of flows traversing routers and switches. The metrics collected by PerfMon can be exported to a network management tool through Flexible NetFlow (FNF) Version 9 or Simple Network Management Protocol (SNMP). A collector/analysis application can further analyze, summarize, and correlate this information to provide traffic profiling, baselining, and troubleshooting services for the application and network operations staff.

PerfMon is implemented similarly to FNF, with some important differences. Both technologies use flow records to determine which parameters to use as key fields or non–key fields. Key fields define a unique flow. If a flow has one different key field than another flow, it is considered a new flow. One important difference between PerfMon and FNF is that PerfMon introduces a new type of flow record, **flow record type performance-monitor**, which includes new fields that are specifically relevant to IP voice and video.

PerfMon uses multiple flow records depending on the protocol being analyzed, either TCP or Real-Time Transport Protocol (RTP), which is commonly used for delivering video and audio that uses User Datagram Protocol (UDP) over IP networks. RTP-specific information such as the Synchronization Source Identifier (SSRC) is essential to track and evaluate overall video conferencing performance. The SSRC is a session identifier for every unique audio or video stream, which is required because the source and destination IP addresses (and sometimes the UDP ports) will be the same for each of the multiple individual audio or video streams that a high-definition video call consists of.

The available PerfMon RTP key fields are listed in Figure 1. The PerfMon fields for TCP are also useful for general-purpose traffic, but will not be covered extensively in this guide.

Figure 1 - PerfMon key fields (RTP)

IPv4
Destination (address or Prefix)
Source (Address or Prefix)
Protocol

Transport
Destination Port
Source Port
RTP SSRC

Tech Tip

PerfMon key fields uniquely determine a flow.

PerfMon non–key fields contain additional information for each flow that is stored along with key field information.

The RTP non–key fields that can be collected for each unique flow are shown in Figure 2. Video conference quality is easily degraded by loss and *jitter* (variable delay) conditions in the network. PerfMon provides a method of collecting this data at multiple points to help isolate the cause of performance problems.

Figure 2 - PerfMon non–key fields (RTP)

IPv4
Destination Mask
Source Mask
DSCP
TTL

Transport
Event Packet-Loss
Packets Expected (Counter)
Packets Lost (Counter or Rate)
Round-Trip-Time
RTP Jitter (Maximum, Mean or Minimum)

Application
Media Bytes (Counter or Rate)
Media Event
Media Packets (Counter or Rate)

Counter
Bytes
Bytes Rate
Bytes Long
Packets
Packets Dropped
Packets Long

Interface
Input
Output

Flow
Direction

Monitor
Event

Routing
Forwarding Status

Timestamp
Interval

Another key difference between FNF and PerfMon is how the flow monitor is applied on the network device. FNF uses an inbound or outbound flow monitor applied to an interface, which applies to all network traffic received or transmitted on that interface. PerfMon uses the Cisco Common Classification Policy Language (C3PL) that is used to implement QoS policies. A new type of policy map, **policy-map type performance-monitor**, is used in conjunction with the C3PL and PerfMon flow monitors, with the policy-map applied to the relevant device interfaces.

Before you configure PerfMon, please verify that you have completed all QoS procedures for all headquarters WAN routers and remote-site routers from the *Cisco SBA for Midsize Organizations—Borderless Networks Foundation Deployment Guide. Several of the procedures in this guide assume that you have already configured QoS class maps for selecting traffic. These class maps are listed for your reference.*

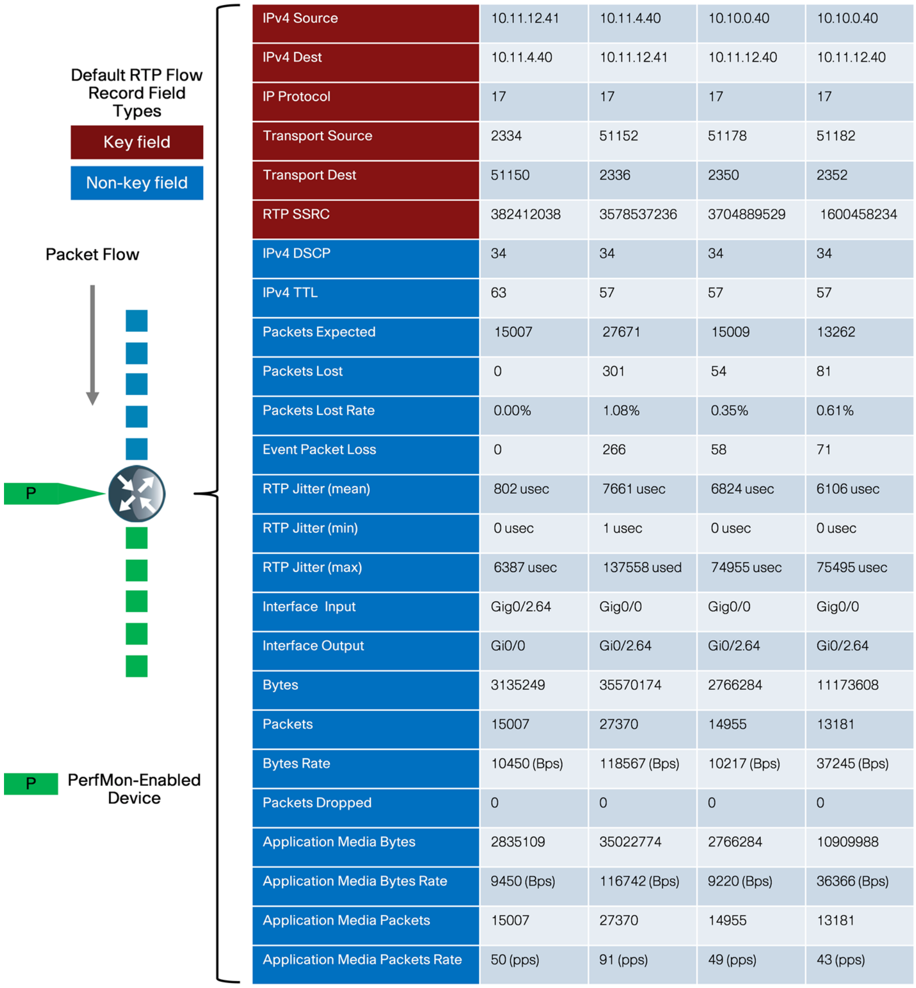
Shared Class Maps

```
class-map match-any DATA
 match dscp af21
class-map match-any INTERACTIVE-VIDEO
 match  dscp cs4  af41
class-map match-any CRITICAL-DATA
 match  dscp cs3  af31
class-map match-any VOICE
 match  dscp ef
```

Other class maps must be configured to match additional video traffic, which is described in the “Deployment Details” section of this guide. An RTP type flow record is used for audio and video traffic classes, and a TCP type flow record is used for other traffic types.

The Cisco SBA recommendation is to use the predefined flow records **default-tcp** and **default-rtp**. An example of the PerfMon cache using a predefined record is shown in Figure 3.

Figure 3 - PerfMon cache - predefined RTP flow record



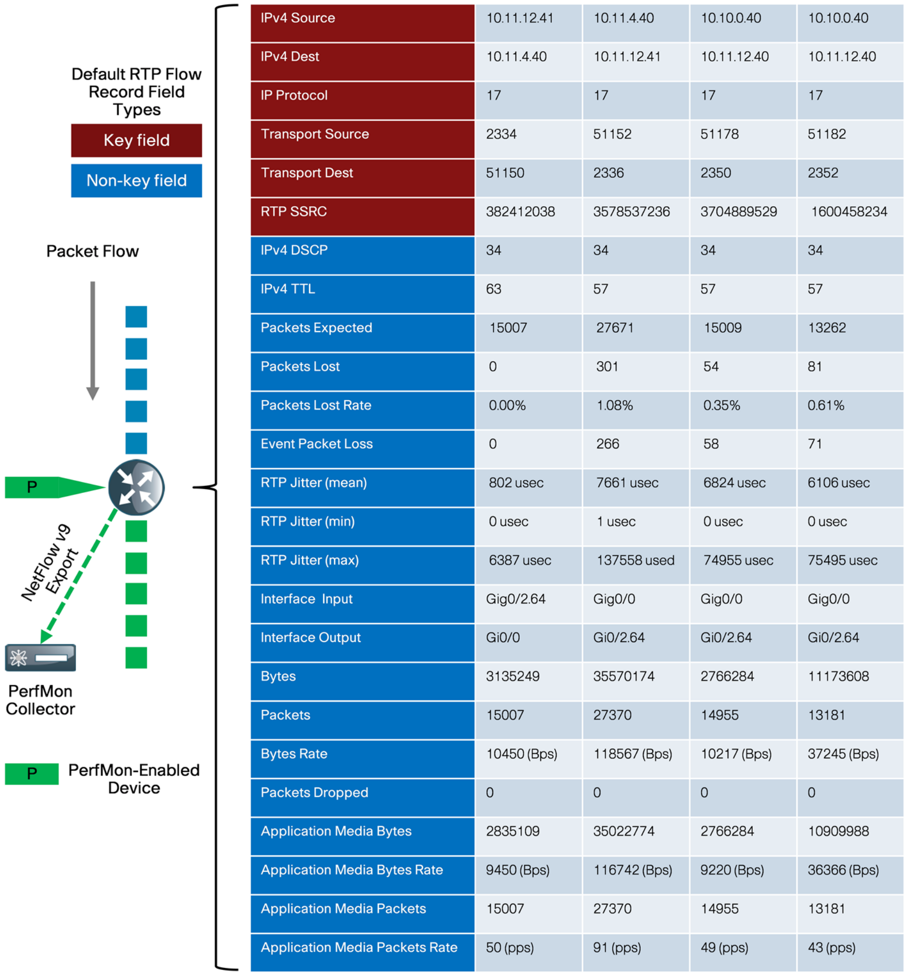
IPv4 Source	10.11.12.41	10.11.4.40	10.10.0.40	10.10.0.40
IPv4 Dest	10.11.4.40	10.11.12.41	10.11.12.40	10.11.12.40
IP Protocol	17	17	17	17
Transport Source	2334	51152	51178	51182
Transport Dest	51150	2336	2350	2352
RTP SSRC	382412038	3578537236	3704889529	1600458234
IPv4 DSCP	34	34	34	34
IPv4 TTL	63	57	57	57
Packets Expected	15007	27671	15009	13262
Packets Lost	0	301	54	81
Packets Lost Rate	0.00%	1.08%	0.35%	0.61%
Event Packet Loss	0	266	58	71
RTP Jitter (mean)	802 usec	7661 usec	6824 usec	6106 usec
RTP Jitter (min)	0 usec	1 usec	0 usec	0 usec
RTP Jitter (max)	6387 usec	137558 used	74955 usec	75495 usec
Interface Input	Gig0/2.64	Gig0/0	Gig0/0	Gig0/0
Interface Output	Gi0/0	Gi0/2.64	Gi0/2.64	Gi0/2.64
Bytes	3135249	35570174	2766284	11173608
Packets	15007	27370	14955	13181
Bytes Rate	10450 (Bps)	118567 (Bps)	10217 (Bps)	37245 (Bps)
Packets Dropped	0	0	0	0
Application Media Bytes	2835109	35022774	2766284	10909988
Application Media Bytes Rate	9450 (Bps)	116742 (Bps)	9220 (Bps)	36366 (Bps)
Application Media Packets	15007	27370	14955	13181
Application Media Packets Rate	50 (pps)	91 (pps)	49 (pps)	43 (pps)

PerfMon Monitoring

Data can be viewed directly from the PerfMon-enabled device through the use of CLI **show** commands, but this method is somewhat cumbersome and it is difficult to correlate the data across multiple devices.

PerfMon details are exported to an external device running a flow collector service as shown in Figure 4; this is essentially the same operation as a NetFlow export. The collector is capable of storing an extensive history of flow information that was switched within the PerfMon device.

Figure 4 - PerfMon export to collector



IPv4 Source	10.11.12.41	10.11.4.40	10.10.0.40	10.10.0.40
IPv4 Dest	10.11.4.40	10.11.12.41	10.11.12.40	10.11.12.40
IP Protocol	17	17	17	17
Transport Source	2334	51152	51178	51182
Transport Dest	51150	2336	2350	2352
RTP SSRC	382412038	3578537236	3704889529	1600458234
IPv4 DSCP	34	34	34	34
IPv4 TTL	63	57	57	57
Packets Expected	15007	27671	15009	13262
Packets Lost	0	301	54	81
Packets Lost Rate	0.00%	1.08%	0.35%	0.61%
Event Packet Loss	0	266	58	71
RTP Jitter (mean)	802 usec	7661 usec	6824 usec	6106 usec
RTP Jitter (min)	0 usec	1 usec	0 usec	0 usec
RTP Jitter (max)	6387 usec	137558 used	74955 usec	75495 usec
Interface Input	Gig0/2.64	Gig0/0	Gig0/0	Gig0/0
Interface Output	Gi0/0	Gi0/2.64	Gi0/2.64	Gi0/2.64
Bytes	3135249	35570174	2766284	11173608
Packets	15007	27370	14955	13181
Bytes Rate	10450 (Bps)	118567 (Bps)	10217 (Bps)	37245 (Bps)
Packets Dropped	0	0	0	0
Application Media Bytes	2835109	35022774	2766284	10909988
Application Media Bytes Rate	9450 (Bps)	116742 (Bps)	9220 (Bps)	36366 (Bps)
Application Media Packets	15007	27370	14955	13181
Application Media Packets Rate	50 (pps)	91 (pps)	49 (pps)	43 (pps)

The most effective to way to view PerfMon data is through a dedicated analysis application, which is typically paired with the flow collector service. PerfMon analysis applications are often paired with NetFlow applications, in which case you do not need to install a separate application. Some vendors have added PerfMon analysis to existing video monitoring applications, without adding full NetFlow analyzer capabilities.

The requirements for implementing PerfMon are highly dependent on which collector/analysis application you use. The example deployment guidance in the "Deployment Details" section applies to the following applications:

- Plixer Scrutinizer
- SevOne Performance Appliance Solution

These applications were selected because they have both been previously verified as a Medianet Systems Management Partner for Performance Monitor and were validated within the Cisco SBA lab environment as capable of monitoring active video conferences in real time.

Tech Tip

PerfMon also supports monitoring from a network management system (NMS) using SNMP. It is not recommended that you use SNMP as the primary method for collecting PerfMon data.

PerfMon Thresholds and Alerts

After PerfMon has been configured to monitor and collect audio and video session data, you can set up monitoring thresholds for a variety of metrics in order to generate automated threshold crossing alerts (TCAs). These metrics include RTP jitter and RTP loss. Video-related problems are often caused by jitter and/or loss conditions in the WAN; acceptable values for these metrics are listed in Table 1.These types of problems can be complex to isolate, because they may reside within a service provider network and not within the organization's network.

Table 1 - Acceptable values for delay, jitter, and loss by application

Application	Delay (one way)	Jitter	Loss
Desktop Sharing (WebEx)	< 1000 ms	< 100 ms	< 0.05%
Video Conferencing	< 150 ms	< 30 ms	< 0.1%
Telepresence	< 150 ms	< 10 ms	< 0.05%
IP Telephony	< 150 ms	< 30 ms	< 1%
IP Telephony Soft Client	< 150 ms	< 30 ms	< 0.1%

A best practice for PerfMon is to enable automated alerting for both jitter and loss. The PerfMon device can send TCAs using an SNMP trap or syslog, depending on what type of NMS is in use at the organization. Alerts will be sent as the threshold is crossed in both the increasing and decreasing directions. This provides a good indicator of when performance issues start as well as when the issues have been resolved. An example of a packet loss TCA follows:

```
Jan 26 14:50:24.960: %PERF_TRAFFIC_REACT-2-CRITSET: TCA RAISE.
Detailed info: Threshold value crossed - current value 1.16%
Flow info: src ip 10.11.4.40, dst ip 10.11.12.40
           src port 2478, dst port 2366
           ssrc 3403354540
Policy info: Policy-map PerfMon-Baseline, Class INTERACTIVE-
VIDEO, Interface GigabitEthernet0/0, Direction input
React info: id 1, criteria transport-packets-lost-rate, severity
critical, alarm type discrete, threshold range [0.10%, 100.00%]
```

Tech Tip

Actual network traffic within the monitored class must be observed in order to generate a TCA. No alerts are generated when there is no network traffic within the monitored class.

You may want to create a set of TCAs corresponding to the different severity levels listed in Table 2 that are triggered at various thresholds as conditions deteriorate. By using this method to layer the TCAs, you can raise awareness of potential issues before they affect service .

Table 2 - TCA severity levels from lowest to highest

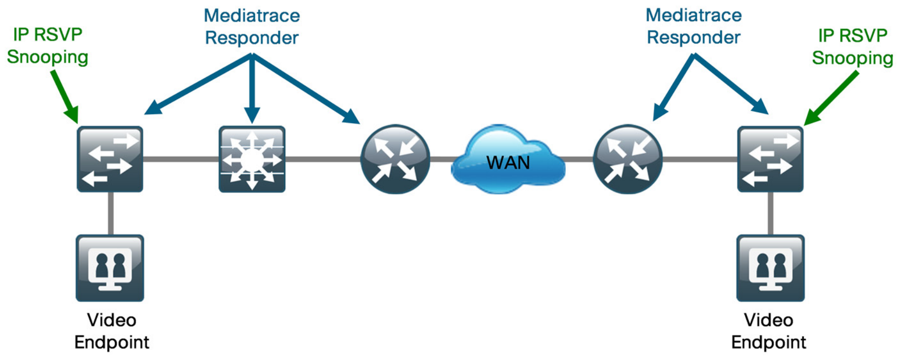
Alarm severity	Definition
Error	Error condition
Critical	Critical condition
Alert	Immediate action needed
Emergency	System unusable

Mediatrace

Mediatrace is a network diagnostic tool that monitors the state of an audio, video, or data flow across a network path. Mediatrace discovers Layer 2 and Layer 3 devices along the flow path and can be used to collect information from these devices. The types of information include device-specific and interface-specific data, as well as PerfMon data for individual flows.

The IP traceroute tool is a close analog to the Mediatrace tool; both are capable of determining the intermediate hops of a one-way path between two IP endpoints. Mediatrace extends this capability in several ways. Both Layer 2 and Layer 3 devices can be detected with Mediatrace, but this requires that the devices be configured as Mediatrace responders. An additional requirement for Layer 2 devices is that IP Resource Reservation Protocol (RSVP) snooping be enabled, so that Mediatrace traffic can be properly directed to the Medianet responder on the device. See Figure 5 for more details.

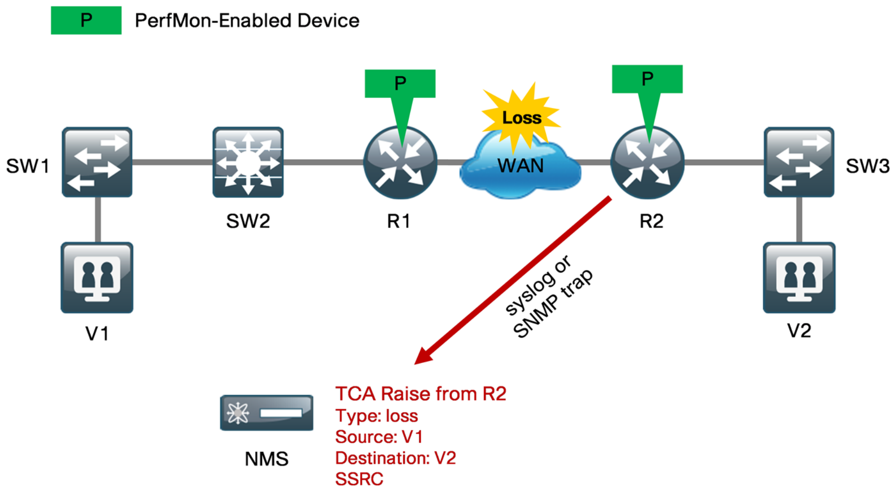
Figure 5 - Mediatrace responder and IP RSVP snooping by device



The Mediatrace initiator device can use either an on-demand or scheduled data collection session to perform a hop-by-hop discovery as well as collect the metrics of interest. Currently, the Mediatrace initiator must be a Cisco router or Cisco switch, and this guide focuses on how to use Mediatrace on these platforms.

A typical example of when to use Mediatrace is for real-time troubleshooting after the network operator has been notified of a potentially degraded video conference. The notification may be reactive, as in the case of a complaint from the video conference users, or the notification may be proactive, when PerfMon thresholds for loss and jitter are configured on the WAN routers. The TCAs include all of the relevant information that is required for initiating a Mediatrace.

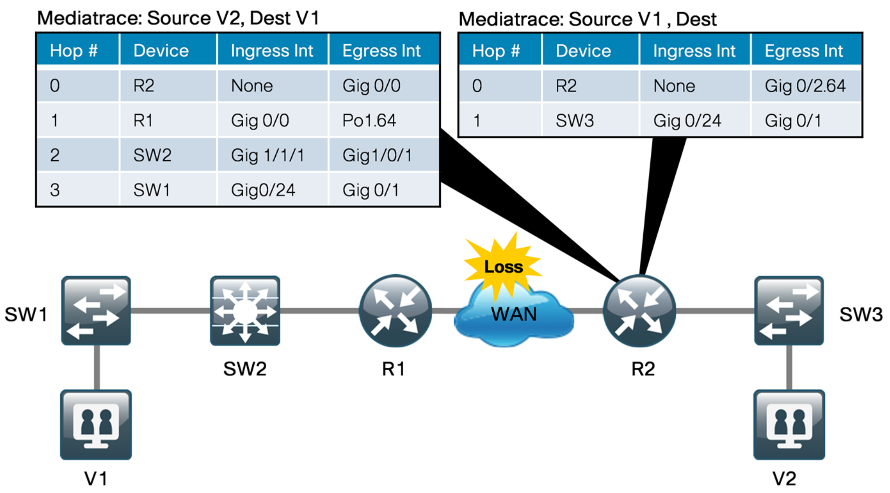
Figure 6 - TCA raised due to WAN loss condition



The TCA alert received by the NMS in Figure 6 indicates that the PerfMon-enabled router R2 observed loss that exceeded a predefined threshold. Prior to troubleshooting, the network operator may not be aware of the WAN loss condition. Mediatrace is used to identify where the source of the loss was introduced using the following steps.

To identify the Mediatrace-enabled device that is nearest to both video endpoints V1 and V2, Mediatraces are run on the TCA-reporting router R2 to collect hop data. This requires two separate unidirectional traces, one from V1 to V2 and another from V2 to V1. The results from the traces are shown in Figure 7; these results indicate that the Mediatrace device nearest to V1 is switch SW1. The next Mediatrace should be sourced from SW1 to collect PerfMon metrics.

Figure 7 - Mediatrace hops in both directions from R2



Mediatrace: Source V2, Dest V1

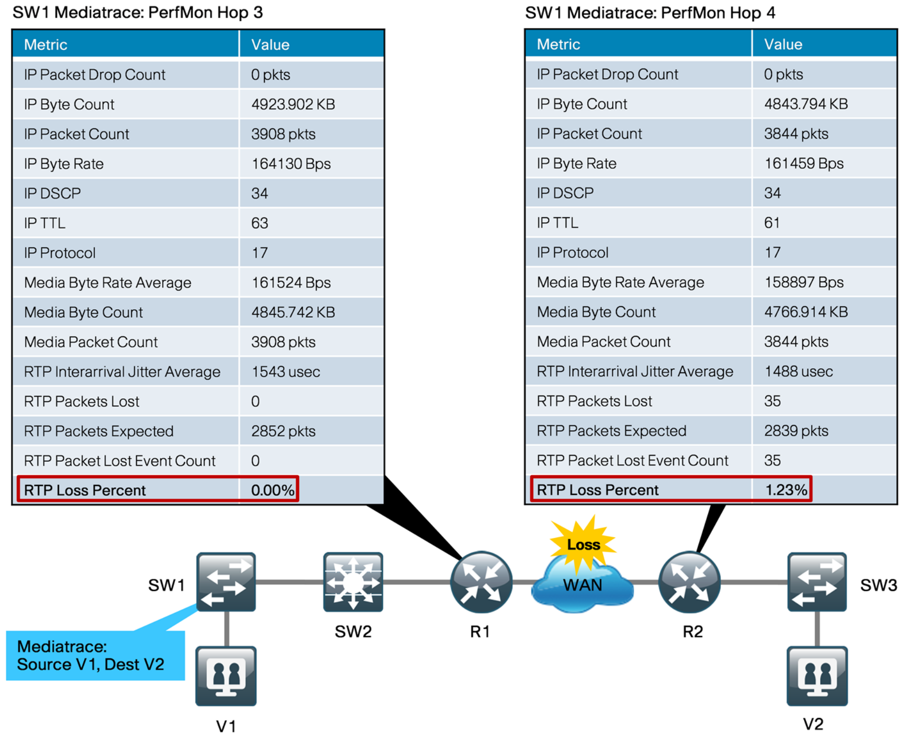
Hop #	Device	Ingress Int	Egress Int
0	R2	None	Gig 0/0
1	R1	Gig 0/0	Po1.64
2	SW2	Gig 1/1/1	Gig1/0/1
3	SW1	Gig0/24	Gig 0/1

Mediatrace: Source V1 , Dest

Hop #	Device	Ingress Int	Egress Int
0	R2	None	Gig 0/2.64
1	SW3	Gig 0/24	Gig 0/1

The Mediatrace from SW1 collects PerfMon data from each responder along the path, but only the data from hop 3 and hop 4 are shown in Figure 8. It is clear from the information collected that no RTP loss has been observed on R1, and RTP loss has been observed on R2. The network operator can conclude that the loss has been introduced between R1 and R2, which is somewhere within the WAN.

Figure 8 - Mediatrace PerfMon from SW1



SW1 Mediatrace: PerfMon Hop 3

Metric	Value
IP Packet Drop Count	0 pkts
IP Byte Count	4923.902 KB
IP Packet Count	3908 pkts
IP Byte Rate	164130 Bps
IP DSCP	34
IP TTL	63
IP Protocol	17
Media Byte Rate Average	161524 Bps
Media Byte Count	4845.742 KB
Media Packet Count	3908 pkts
RTP Interarrival Jitter Average	1543 usec
RTP Packets Lost	0
RTP Packets Expected	2852 pkts
RTP Packet Lost Event Count	0
RTP Loss Percent	0.00%

SW1 Mediatrace: PerfMon Hop 4

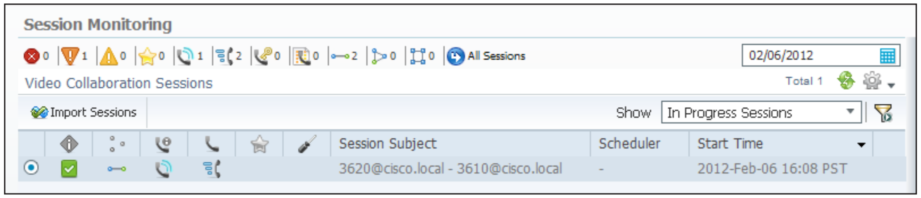
Metric	Value
IP Packet Drop Count	0 pkts
IP Byte Count	4843.794 KB
IP Packet Count	3844 pkts
IP Byte Rate	161459 Bps
IP DSCP	34
IP TTL	61
IP Protocol	17
Media Byte Rate Average	158897 Bps
Media Byte Count	4766.914 KB
Media Packet Count	3844 pkts
RTP Interarrival Jitter Average	1488 usec
RTP Packets Lost	35
RTP Packets Expected	2839 pkts
RTP Packet Lost Event Count	35
RTP Loss Percent	1.23%

Graphical Monitoring with Mediatrace

The hop-by-hop information for Mediatrace in the previous section is gathered through the use of a series of CLI commands. The network operator has to have a complete and accurate view of the network topology in order to execute the proper commands on the correct network devices. For this reason, Mediatrace is most effective when launched within a graphical application. Cisco Prime Collaboration Manager (CPCM) is the most effective tool for monitoring an end-to-end system of video collaboration devices and their supporting infrastructure. This guide references the capabilities of CPCM version 1.1.

CPCM has a broad set of capabilities for monitoring video endpoints, but the most significant capability allows for session monitoring in real time. All active sessions are detected by CPCM, which provides a view of the current usage of monitored video conferencing resources at a glance, as shown in Figure 9. The system displays minor, major, and critical alarms based on monitored thresholds and events. CPCM session–specific alarms for loss, jitter, and delay are displayed based on information collected directly from the endpoints as shown in Figure 10. This is different from the TCA notifications discussed in previous sections, which come from network devices configured for PerfMon.

Figure 9 - CPCM in progress session with no active alarms



Session Monitoring

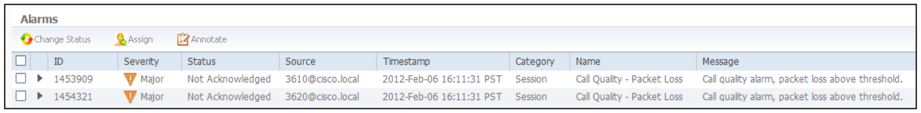
Video Collaboration Sessions

Import Sessions

Show: In Progress Sessions

							Session Subject	Scheduler	Start Time
●	✓						3620@cisco.local - 3610@cisco.local	-	2012-Feb-06 16:08 PST

Figure 10 - CPCM major alarms reported by multiple video endpoints

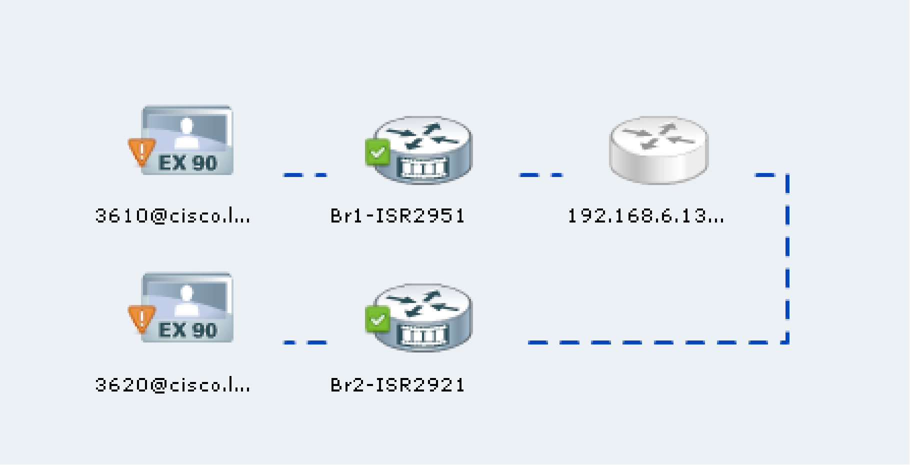


Alarms

□		ID	Severity	Status	Source	Timestamp	Category	Name	Message
□	▸	1453909	Major	Not Acknowledged	3610@cisco.local	2012-Feb-06 16:11:31 PST	Session	Call Quality - Packet Loss	Call quality alarm, packet loss above threshold.
□	▸	1454321	Major	Not Acknowledged	3620@cisco.local	2012-Feb-06 16:11:31 PST	Session	Call Quality - Packet Loss	Call quality alarm, packet loss above threshold.

One of the key capabilities of CPCM is troubleshooting session-based alarms. CPCM is able to initiate a Mediatrace on the network devices and graphically render the path between the video endpoints. This provides topology information to the network operator which can be used to further isolate the conditions that are causing the alarms. Additional PerfMon information is available from the network devices along the path.

Figure 11 - CPCM troubleshooting path view

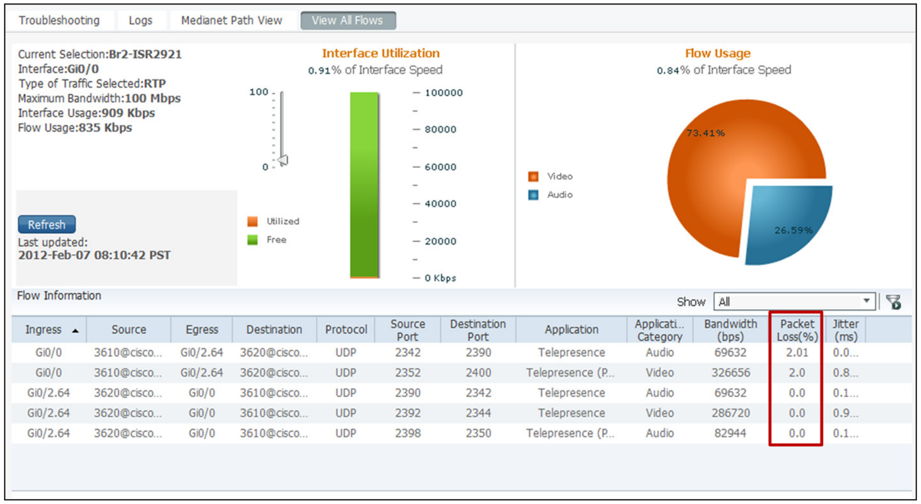


The network operator uses CPCM to request additional information without needing to manually log in to each specific device and run CLI commands. The flow-specific information is similar to the PerfMon data exported using NetFlow, but in this case is requested directly from the network device using SNMP. The available statistics are shown in Figure 12.

Tech Tip

Before CPCM can gather flow statistics, you must configure both Mediatrace and SNMP on the network device. You do not need to configure a PerfMon flow export on the network device if CPCM is the only application you use for video conference monitoring.

Figure 12 - CPCM RTP flow statistics gathered from PerfMon



Current Selection:**Br2-ISR2921**
Interface:**Gi0/0**
Type of Traffic Selected:**RTP**
Maximum Bandwidth:**100 Mbps**
Interface Usage:**909 Kbps**
Flow Usage:**835 Kbps**

Last updated:
2012-Feb-07 08:10:42 PST

Flow Information

Show All

Ingress	Source	Egress	Destination	Protocol	Source Port	Destination Port	Application	Applicati... Category	Bandwidth (bps)	Packet Loss(%)	Jitter (ms)
Gi0/0	3610@cisco...	Gi0/2.64	3620@cisco...	UDP	2342	2390	Telepresence	Audio	69632	2.01	0.0...
Gi0/0	3610@cisco...	Gi0/2.64	3620@cisco...	UDP	2352	2400	Telepresence (P...	Video	326656	2.0	0.8...
Gi0/2.64	3620@cisco...	Gi0/0	3610@cisco...	UDP	2390	2342	Telepresence	Audio	69632	0.0	0.1...
Gi0/2.64	3620@cisco...	Gi0/0	3610@cisco...	UDP	2392	2344	Telepresence	Video	286720	0.0	0.9...
Gi0/2.64	3620@cisco...	Gi0/0	3610@cisco...	UDP	2398	2350	Telepresence (P...	Audio	82944	0.0	0.1...

IPSLA VO

IPSLA Video Operation (IPSLA VO) functions as a valuable tool to assess the readiness of a network to carry rich-media traffic. It has the ability to synthetically generate video profiles that mimic real application traffic, such as Cisco TelePresence activity, IP video surveillance, or IPTV traffic. IPSLA VO can also make use of user-captured packet traces from the customer's existing network, which can then be included in the synthetically generated traffic stream. You can also use this feature to run network readiness tests prior to important collaboration meetings to validate that the network will be able to support the expected rich-media traffic.

The IPSLA VO feature was only available on a limited set of access switch platforms during the development of this deployment guide. Future revisions of this guide will include best-practice guidance on proper operation of IPSLA VO. All of the same monitoring and troubleshooting capabilities of both PerfMon and Mediatrace will also be available when used with IPSLA- VO.

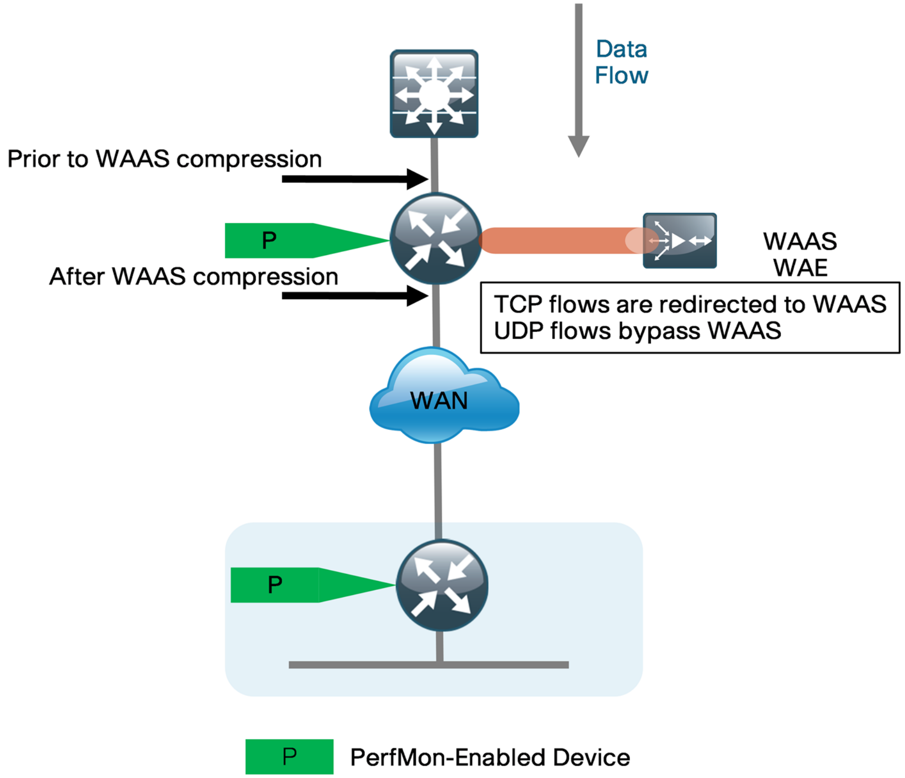
Medianet Interaction with Application Optimization

The Cisco SBA Midsize architecture includes Application Optimization using Cisco Wide Area Application Services (WAAS) to accelerate and optimize data over a WAN network. Full deployment details are available in the *Cisco SBA for Midsize Organizations—Borderless Networks Foundation Deployment Guide* in the Application Optimization Module.

PerfMon information is gathered at multiple points along the path between a source and destination. When you use Application Optimization, the device interfaces you choose to monitor and the direction(s) in which they are monitored affects the data cached by the network device. The topology in Figure 13 illustrates the potential complexity.

You can monitor traffic bound for a remote site across the WAN in two places. The flows cached inbound on the LAN-facing interface reflect uncompressed data before it has been optimized by the WAAS. The same flows when cached outbound on the WAN-facing interface reflect compressed data that has been optimized by the WAAS. The recommended WAAS configuration on the router is to redirect TCP traffic for optimization and forward UDP traffic as usual. Video conferencing traffic is typically UDP, and therefore it is unaffected by application optimization with the configuration in Figure 13.

Figure 13 - Application optimization and PerfMon



PerfMon, although primarily used for RTP traffic monitoring, also provides loss and round-trip time statistics for TCP applications. The Cisco SBA recommendation for PerfMon with Application Optimization is to configure inbound and outbound flow monitoring on both the LAN-facing and WAN-facing interfaces. This ensures that all of the flow information is captured for both TCP-based and UDP-based applications., The flow data that is collected on the LAN-facing interfaces provides an accurate view of the applications in use and their true network usage. The flow data that is collected on the WAN-facing interfaces accurately reflects the amount of network traffic that is transmitted and received to and from the WAN.

Tech Tip

You must filter data during analysis depending on whether you require a LAN-facing or WAN-facing analysis.

Notes

Deployment Details

Medianet is most effective when enabled broadly on all the routers and switches across the network. There are several prerequisites for a Medianet deployment. Configuring PerfMon is straightforward if QoS has already been configured. To enable graphical monitoring for Mediatrace, you must configure device access using Secure Shell (SSH) Protocol, HTTPS, and SNMP. These steps are clearly outlined in the *Cisco SBA for Midsize Organizations—Borderless Networks Foundation Deployment Guide*.

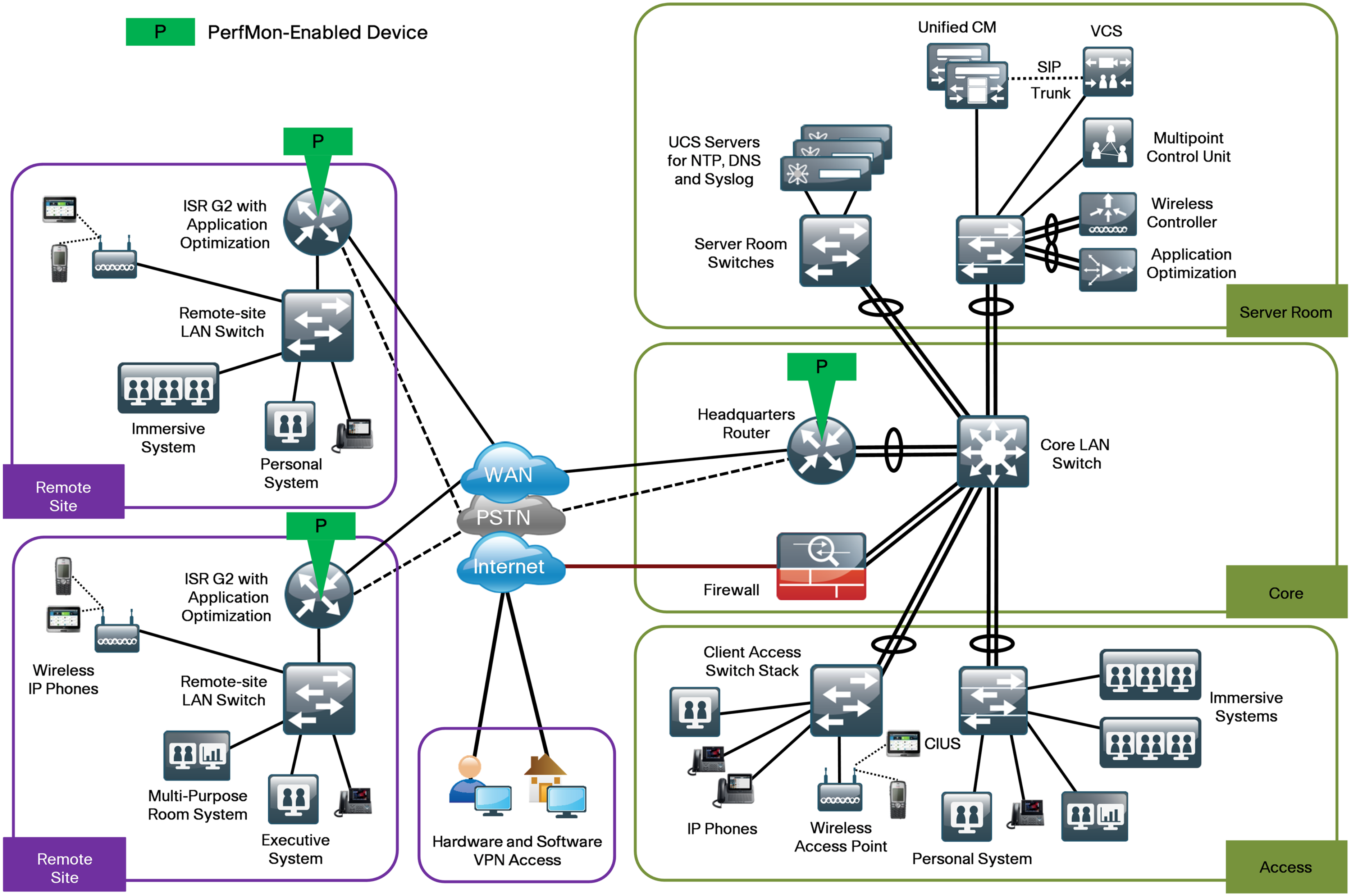
PerfMon builds upon the embedded NetFlow capabilities of the headquarters WAN router and the remote-site routers as shown in Figure 14.

Tech Tip

Either the Unified Communications (UC) or DATA technology packages are required to enable PerfMon on a router.

Notes

Figure 14 - Cisco SBA midsize architecture with PerfMon enabled



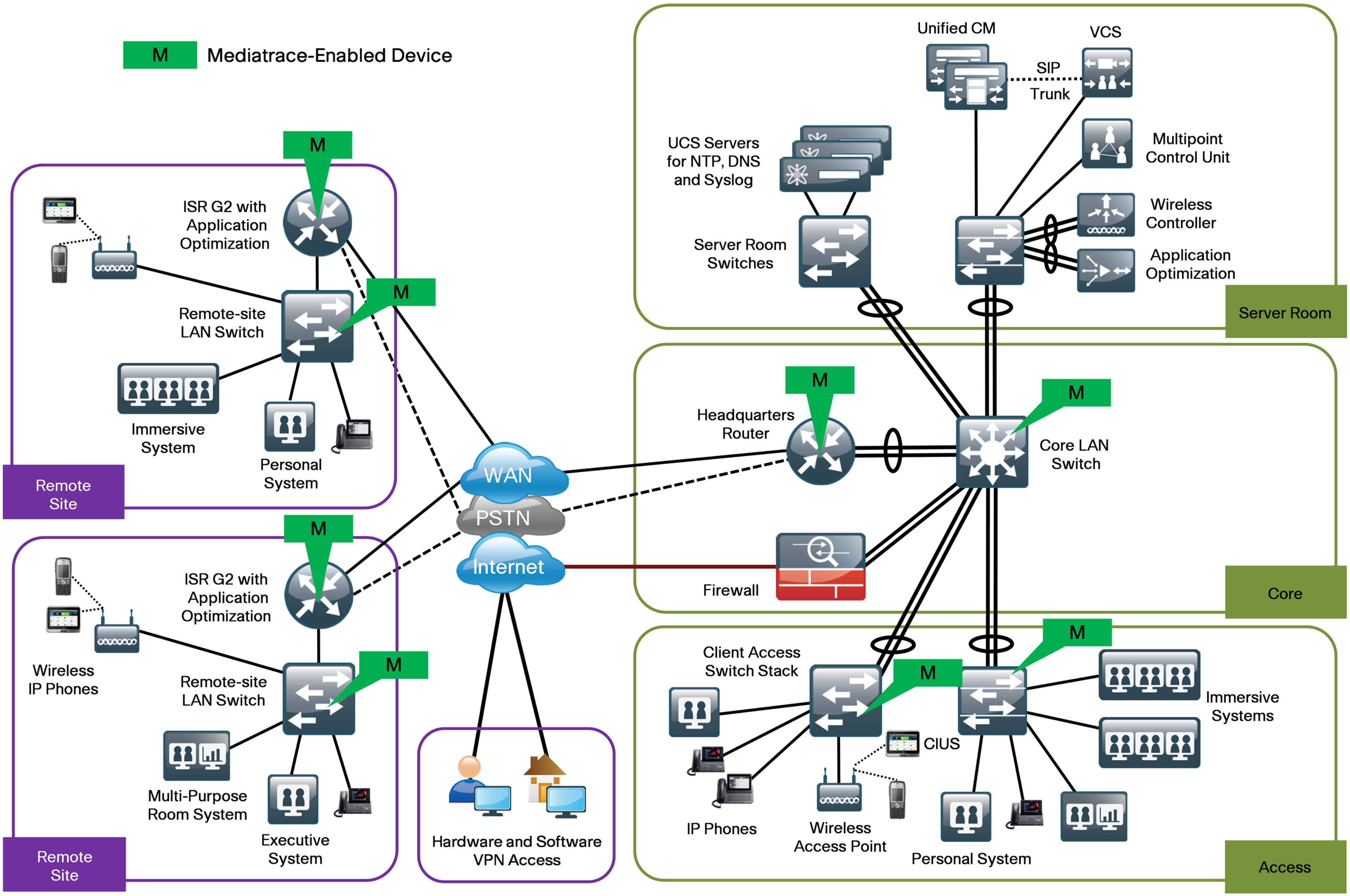
Mediatrace is initiated from a configured network device, which can be either a router or a switch. For proper operation, you must broadly enable Mediatrace responder capabilities across the network. It is recommended that Mediatrace be enabled on all supported devices, as shown in Figure 15.

Tech Tip

Either of the UC or DATA technology packages are required to enable Mediatrace on a router. The IP Base license is required to enable Mediatrace on the 3560X and 3750X switches.

Notes

Figure 15 - Cisco SBA midsize architecture with Mediatrace enabled



Process

Configuring PerfMon

1. Configure class maps for video apps
2. Create a flow exporter
3. Create a PerfMon flow monitor
4. Configure the PerfMon policy map
5. Configure PerfMon reactions
6. Apply the policy map to interfaces

This set of procedures is completed on the headquarters router and all of the remote-site routers.

Procedure 1 Configure class maps for video apps

This procedure assumes that the following set of QoS class maps has been configured:

```
class-map match-any DATA
 match dscp af21
class-map match-any INTERACTIVE-VIDEO
 match  dscp cs4  af41
class-map match-any CRITICAL-DATA
 match  dscp cs3  af31
cclass-map match-any VOICE
 match  dscp ef
```

These class maps and the class map configured in the following step must be configured before the flow monitor is created in a subsequent procedure.

Step 1: Create additional class map matching TelePresence using Network-Based Application Recognition (NBAR).

```
class-map match-any TP-MEDIA
 match protocol telepresence-media
```

Procedure 2 Create a flow exporter

Step 1: You can more effectively analyze the PerfMon data that is stored in the cache of the network device if you export it to an external collector.

Tech Tip

You only need to create a flow exporter if you are exporting data to an external collector. You can skip this procedure if you are analyzing data only on the network device.

Step 2: Different Medianet collector applications expect to receive the exported data on a particular UDP or TCP port. The collector applications used for testing used the parameters designated in Table 3.

Table 3 - Tested Medianet PerfMon collector parameters

Vendor	Application	Version	Capability	Export protocol	Destination port
Plixer	Scrutinizer	8.6.2	Flexible NetFlow	netflow-v9	UDP 2055
SevOne	Performance Appliance Solution	4.1.3.74	Flexible NetFlow	netflow-v9	UDP 9996

Step 3: Configure a basic flow exporter.

```
flow exporter [exporter name]
 description [exporter description]
 destination [NetFlow collector IP address]
 source Loopback0
 transport [UDP or TCP] [port number]
 export-protocol [export protocol]
```

Example (Plixer)

```
flow exporter Export-FNF-Plixer
 description FNF v9
 destination 10.10.48.171
 source Loopback0
 transport udp 2055
 export-protocol netflow-v9
```

Procedure 3 Create a PerfMon flow monitor

You must configure the router to monitor the flows through the device on a per-interface basis. The flow monitor must include a flow record and, optionally, one or more flow exporters if you want to collect and analyze data. After you create the flow monitor, you apply it to a PerfMon policy map. You will need to perform this procedure twice, once for the RTP flow record and once for the TCP flow record.

Step 1: Create an RTP or TCP flow monitor and associated flow record.

Use the predefined flow records **default-rtp** and **default-tcp**. Custom flow records are also supported, but are not required for this configuration.

```
flow monitor type performance-monitor [monitor name]
 description [monitor description]
 record [record name]
```

Step 2: If you are using an external NetFlow collector, associate exporter(s) to the flow monitor.

Add additional lines when using multiple exporters.

```
flow monitor type performance-monitor [monitor name]
 exporter [exporter name]
```

Example (Plixer)

```
flow monitor type performance-monitor PerfMon-All-RTP
 description PerfMon RTP
 record default-rtp
 exporter Export-FNF-Plixer
flow monitor type performance-monitor PerfMon-All-TCP
 description PerfMon TCP
 record default-tcp
 exporter Export-FNF-Plixer
```

Procedure 4 Configure the PerfMon policy map

Each of the classes configured previously must be listed in the policy map with either an RTP or TCP flow record. To correctly calculate jitter, some classes require additional monitor parameters depending on the encoding clock rate of the source.

Jitter values are calculated by analyzing the time-stamp field in the RTP header. The time stamp does not actually refer to regular time, but the “ticks” of the encoder’s clock. Video codecs typically uses a 90 KHz clock rate, which is the default for PerfMon. Modern wideband audio codecs use a variety of different values for the encoding clock rate. PerfMon clock rates are configured statically when using values other than 90 KHz and when the sources have dynamic RTP payload types within the range of 96 through 127.

Table 4 - PerfMon monitored classes

Class	Protocol	Monitor parameters	Comments
Interactive Video	RTP (UDP)		
TP Media	RTP (UDP)	monitor metric rtp clock-rate 96 48000 clock-rate 101 8000	RTP payload type 96 at 48 KHz is Advanced Audio Codec (AAC) RTP payload type 101 at 8 KHz is dual-tone multifrequency (DTMF)
Data	TCP		
Critical Data	TCP		
Voice	RTP (UDP)		

Step 1: Create the PerfMon policy map, and add a description.

```
policy-map type performance-monitor [policy map name]
 description [policy map description]
```

Step 2: Add classes and flow monitors (repeat as necessary). Add additional parameters if required in Table 4.

```
policy-map type performance-monitor [policy map name]
 class [class name]
  flow monitor [monitor name]
  monitor [monitor parameters]
    [parameter list 1]
    [parameter list 2]
```

Example

```
policy-map type performance-monitor PerfMon-Baseline
 description PerfMon Baseline
 class INTERACTIVE-VIDEO
   flow monitor PerfMon-All-RTP
 class TP-MEDIA
   flow monitor PerfMon-All-RTP
   monitor metric rtp
    clock-rate 96 48000
    clock-rate 101 8000
 class DATA
   flow monitor PerfMon-All-TCP
 class CRITICAL-DATA
   flow monitor PerfMon-All-TCP
 class VOICE
   flow monitor PerfMon-All-RTP
```

Procedure 5 Configure PerfMon reactions

(Optional)

PerfMon is able to monitor and react to the reaction types listed in Table 5.

Table 5 - PerfMon reaction types

Reaction type	Description	Threshold value operators
media-stop	Occurs when traffic is no longer found for the flow	
rtp-jitter-average	Average statistical variance of the RTP data interarrival time	ge, gt, le, lt, range (usec)
transport-packets-lost-rate	Number of packets lost/number of packets expected in an interval period	ge, gt, le, lt, range (%)

Step 1: Configure multiple react statements and prioritize them by the react number.

```
policy-map type performance-monitor [policy map name]
 class [class name]
 react [react number] [reaction type]
  description [description]
  threshold value [operator] [value]
  alarm severity [severity]
  action [action type]
```

Example

The following example generates both a critical syslog message and an SNMP trap if the monitored class INTERACTIVE-VIDEO experiences loss greater than 0.1 percent or average jitter exceeds 25 ms.

```
policy-map type performance-monitor PerfMon-Baseline
 class INTERACTIVE-VIDEO
   flow monitor PerfMon-All-RTP
   react 10 transport-packets-lost-rate
    description Check for > .1% loss
    threshold value gt 0.10
    alarm severity critical
    action syslog
    action snmp
   react 20 rtp-jitter-average
    description Check for > 25 ms average jitter
    threshold value gt 25000
    alarm severity critical
    action syslog
    action snmp
```

Procedure 6 Apply the policy map to interfaces

Tech Tip

Be sure to apply the policy map inbound and outbound on all device interfaces.

Step 1: Apply the policy map.

```
interface [name]
 service-policy type performance-monitor input [policy map name]
 service-policy type performance-monitor output [policy map name]
```

Example

```
interface GigabitEthernet0/0
 description MPLS WAN Uplink
 service-policy type performance-monitor input PerfMon-Baseline
 service-policy type performance-monitor output PerfMon-Baseline
interface GigabitEthernet0/2.64
 description Wired Data
 service-policy type performance-monitor input PerfMon-Baseline
 service-policy type performance-monitor output PerfMon-Baseline
interface GigabitEthernet0/2.65
 description Wired Voice
 service-policy type performance-monitor input PerfMon-Baseline
 service-policy type performance-monitor output PerfMon-Baseline
```

Process

Configuring Mediatrace

1. Configure router or switch for Mediatrace
2. Configure Web Services

Procedure 1 Configure router or switch for Mediatrace

Option 1. Router

The responder must be configured on all intermediate devices so that Mediatrace initiators can gather statistics at every hop along the path. Each device can also potentially be an initiator, so you also configure a source interface.

Step 1: Enable the Mediatrace responder.

```
mediatrace responder
```

Step 2: Configure the source interfaces for the Mediatrace initiator.

```
mediatrace initiator source-interface [interface name]
```

Example

```
mediatrace responder
mediatrace initiator source-interface Loopback0
```

Option 2. Switch

The switch configuration is identical to that of the router, but may use a VLAN interface instead of a loopback. Switches also require an additional step: if the switch is a Layer 2–only device (that is, it performs no Layer 3 routing), you must enable RSVP snooping.

Step 1: Enable the Mediatrace responder.

```
mediatrace responder
```

Step 2: Configure the source interfaces for the Mediatrace initiator.

```
mediatrace initiator source-interface [interface name]
```

Step 3: Enable RSVP snooping.

```
ip rsvp snooping
```

Example

```
ip rsvp snooping
mediatrace responder
mediatrace initiator source-interface Vlan64
```

Procedure 2 Configure Web Services

(Optional)

To start a Mediatrace by using the CLI on any Mediatrace initiator, you use a series of commands as shown in a following process. If you choose to run Mediatraces using the graphical interface of CPCM, you must enable the Web Services Management Agent (WSMA) on all of the routers and switches that run Mediatrace.

This procedure assumes that the HTTP secure server and HTTP local authentication have already been configured as recommended in the *Cisco SBA for Midsize Organizations—Borderless Networks Foundation Deployment Guide*.

Step 1: Create a WSMA profile for HTTPS.

```
wsma profile listener [profile name]
 transport [transport type]
```

Step 2: Create WSMA agents for the exec and config profiles.

```
wsma agent [agent type] profile [profile name]
```

Step 3: Set the HTTP timeout policy.

```
ip http timeout-policy idle 60 life 86400 requests 10000
```

Example

```
wsma profile listener WSMA-LISTENER-HTTPS
 transport https
wsma agent exec profile WSMA-LISTENER-HTTPS
wsma agent config profile WSMA-LISTENER-HTTPS
ip http timeout-policy idle 60 life 86400 requests 10000
```

Process

Monitoring Video Sessions with PerfMon and Mediatrace

1. View raw session data by IP address
2. View raw session data by SSRC
3. Create reports from PerfMon collectors
4. Run a Mediatrace using CPCM

You can use the CLI to view the data stored in the PerfMon cache of the network device to get information about specific video conferences. However, this approach is somewhat limited by the characteristics of a text-based display and the fact that the data provides only a snapshot in time.

The PerfMon data cached locally on the network device is relatively short-lived and is typically replaced by new flows within minutes. An external collector is essential to maintain a long-term view of the traffic patterns on a network. PerfMon data exported to a PerfMon collector such as Plixer Scrutinizer can be analyzed and presented graphically, with additional capabilities to filter on parameters of interest.

Mediatrace information is most useful when troubleshooting active video sessions. It is possible to run a series of manual Mediatraces using the CLI on the appropriate devices along the path. However, this method is cumbersome and requires detailed knowledge of the topology under investigation. It is recommended that you use CPCM to run Mediatrace; this can greatly simplify your troubleshooting.

Procedure 1 View raw session data by IP address

The simplest method to view data about any session stored in the PerfMon cache is via the following CLI command, which lists a series of individual cache entries. This same command can also be repeated with either a specific IP source or destination, or a specific IP source and destination pair. This provides data on video-related sessions as well as general TCP or UDP sessions.

Step 1: View raw session data by IP address.

```
show performance monitor status
show performance monitor status ip [source IP addr][mask] any
show performance monitor status ip any [dst IP addr][mask]
show performance monitor status ip [source IP addr][mask] [dst
IP addr][mask]
```

Example

```
Router#show performance monitor status ip 10.10.48.20
255.255.255.255 10.11.5.12 255.255.255.255
Match: ipv4 src addr = 10.10.48.20, ipv4 dst addr =
10.11.5.12, ipv4 prot = udp, trns src port = 35986, trns dst
port = 51066,
Policy: PerfMon-Baseline, Class: CRITICAL-DATA, Interface:
GigabitEthernet0/0, Direction: input


 *counter flow                                           : 2
  counter bytes                                          : 47
  counter bytes rate                               (Bps) : 0
 *counter bytes rate per flow                      (Bps) : 0
 *counter bytes rate per flow min                  (Bps) : 0
```

```
*counter bytes rate per flow max              (Bps) : 1
 counter packets                                    : 1
*counter packets rate per flow                      : 0
 counter packets dropped                            : 0
 routing forwarding-status reason                   : Unknown
 interface input                                    : Gi0/0
 interface output                                   : Po1.69
 monitor event                                      : false
 ipv4 dscp                                          : 24
 ipv4 ttl                                           : 57
 application media bytes counter                    : 27
 application media packets rate               (pps) : 0
 application media event                            : Stop
 transport event packet-loss counter                : NA
*transport event packet-loss counter min            : NA
*transport event packet-loss counter max            : NA
*transport tcp flow count                           : 0
*transport round-trip-time sum               (msec) : NA
*transport round-trip-time samples                  : NA
 transport round-trip-time                   (msec) : NA
*transport round-trip-time min               (msec) : NA
*transport round-trip-time max               (msec) : NA
```

Procedure 2 View raw session data by SSRC

The most straightforward way to monitor RTP sessions and their individual video and audio stream data stored in the PerfMon cache is via the following CLI command, which lists a series of individual cache entries. This same command can also be repeated with specific SSRC values.

Step 1: View raw session data by SSRC.

```
show performance monitor status ssrc any
show performance monitor status ssrc [SSRC value]
```

Step 2: Example

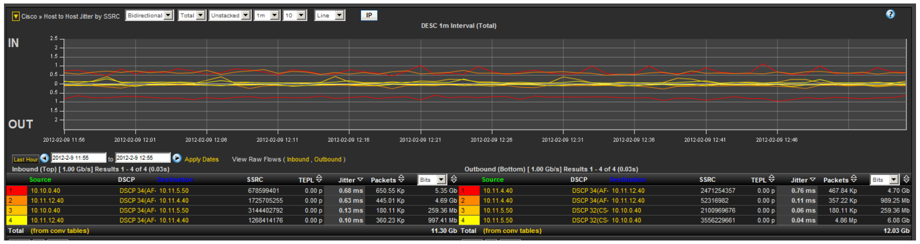
```
Router#show performance monitor status ssrc any
  Match: ipv4 src addr = 10.10.48.27, ipv4 dst addr =
10.11.12.40, ipv4 prot = udp, trns src port = 51182, trns dst
port = 2352, SSRC = 1600458234
 Policy: PerfMon-Baseline, Class: INTERACTIVE-VIDEO,
Interface: GigabitEthernet0/0, Direction: input

 *counter flow                                       : 10
  counter bytes                                      : 11173608
  counter bytes rate                           (Bps) : 37245
 *counter bytes rate per flow                  (Bps) : 37245
 *counter bytes rate per flow min              (Bps) : 36919
 *counter bytes rate per flow max              (Bps) : 37661
  counter packets                                    : 13181
 *counter packets rate per flow                      : 43
  counter packets dropped                            : 0
  routing forwarding-status reason                   : Unknown
  interface input                                    : Gi0/0
  interface output                                   : Gi0/2.64
  monitor event                                      : true
  ipv4 dscp                                          : 34
  ipv4 ttl                                           : 57
  application media bytes counter                    : 10909988
  application media packets counter                  : 13181
  application media bytes rate                 (Bps) : 36366
 *application media bytes rate per flow        (Bps) : 36366
 *application media bytes rate per flow min    (Bps) : 36230
 *application media bytes rate per flow max    (Bps) : 36531
  application media packets rate               (pps) : 43
  application media event                            : Normal
 *transport rtp flow count                           : 10
  transport rtp jitter mean                   (usec) : 6106
  transport rtp jitter minimum                (usec) : 0
  transport rtp jitter maximum                (usec) : 75495
 *transport rtp payload type                         : 104
  transport event packet-loss counter                : 71
 *transport event packet-loss counter min            : 0
 *transport event packet-loss counter max            : 15
  transport packets expected counter                 : 13262
 transport packets lost counter                    : 81
*transport packets lost counter minimum            : 0
*transport packets lost counter maximum            : 27
 transport packets lost rate                 ( % ) : 0.61
*transport packets lost rate min             ( % ) : 0.00
*transport packets lost rate max             ( % ) : 1.56
```

Procedure 3 Create reports from PerfMon collectors

One key advantage of using an external collector is the ability to aggregate the information collected across multiple network devices. A good collector provides the ability to view data collected from a particular device and interface as well as to correlate data collected from multiple devices and interfaces across the network.

This procedure highlights the types of reports that are available from Plixer Scrutinizer. One of the most effective reports lists all of the RTP data streams by specific SSRC in a table, which breaks out the audio and video components of a video conference into its separate components. The jitter values graphed in Figure 16 indicate that the listed sessions are consistently jitter-free (less than 1 ms).

Figure 16 - Plixer Scrutinizer - Host to Host Jitter by SSRC (jitter free)



2012-2-9 11:55 to 2012-2-9 12:55

View Raw Flows (Inbound , Outbound)

Inbound (Top) [1.00 Gb/s] Results 1 - 4 of 4 (0.03s)

	Source	DSCP	Destination	SSRC	TEPL	Jitter	Packets	Bits
1	10.10.0.40	DSCP 34(AF4	10.11.5.50	678599401	0.00 p	0.68 ms	650.55 Kp	5.35 Gb
2	10.11.12.40	DSCP 34(AF4	10.11.4.40	1725705255	0.00 p	0.63 ms	445.01 Kp	4.69 Gb
3	10.10.0.40	DSCP 34(AF4	10.11.5.50	3144402792	0.00 p	0.13 ms	180.11 Kp	259.36 Mb
4	10.11.12.40	DSCP 34(AF4	10.11.4.40	1268414176	0.00 p	0.10 ms	360.23 Kp	997.41 Mb
Total	(from conv tables)							11.30 Gb

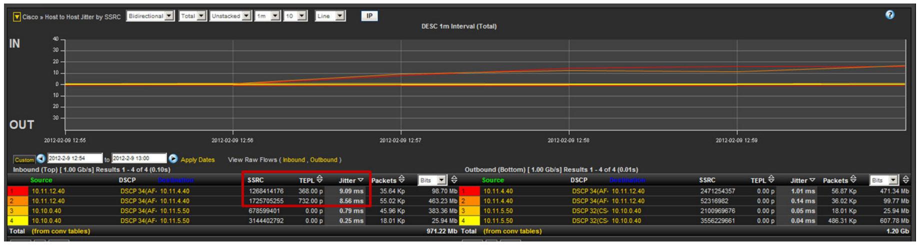
Outbound (Bottom) [1.00 Gb/s] Results 1 - 4 of 4 (0.03s)

	Source	DSCP	Destination	SSRC	TEPL	Jitter	Packets	Bits
1	10.11.4.40	DSCP 34(AF4	10.11.12.40	2471254357	0.00 p	0.76 ms	467.84 Kp	4.70 Gb
2	10.11.4.40	DSCP 34(AF4	10.11.12.40	52316982	0.00 p	0.11 ms	357.22 Kp	989.25 Mb
3	10.11.5.50	DSCP 32(CS4	10.10.0.40	2100969676	0.00 p	0.06 ms	180.11 Kp	259.36 Mb
4	10.11.5.50	DSCP 32(CS4	10.10.0.40	3556229661	0.00 p	0.04 ms	4.86 Mp	6.08 Gb
Total	(from conv tables)							12.03 Gb

PerfMon is well-suited for identifying, isolating, and correcting video-related network problems. It is possible to generate a report that includes jitter and trans-event packet loss (TEPL) values for multiple video sessions. The highlighted information in Figure 17 shows a set of two RTP streams with the same source and destination and different SSRCs, corresponding to the audio and video components of the session. Each stream has jitter of approximately 9 ms and significant packet loss. The graphic provides details about when the jitter conditions initially became active. Another session visible on this PerfMon device is monitored as jitter-free and loss-free.

It is important to note that although the monitoring was done at this observation point, the jitter and loss were induced upstream. It is possible that some of the streams were tagged with different differentiated services code point (DSCP) values or were routed through different paths, which would explain the different behaviors.

Figure 17 - Plixer Scrutinizer - host-to-host jitter by SSRC (jitter and loss conditions present)



2012-2-9 12:54 to 2012-2-9 13:00

View Raw Flows (Inbound , Outbound)

Inbound (Top) [1.00 Gb/s] Results 1 - 4 of 4 (0.10s)

	Source	DSCP	Destination	SSRC	TEPL	Jitter	Packets	Bits
1	10.11.12.40	DSCP 34(AF4	10.11.4.40	1268414176	368.00 p	9.09 ms	35.64 Kp	98.70 Mb
2	10.11.12.40	DSCP 34(AF4	10.11.4.40	1725705255	732.00 p	8.56 ms	55.02 Kp	463.23 Mb
3	10.10.0.40	DSCP 34(AF4	10.11.5.50	678599401	0.00 p	0.79 ms	45.96 Kp	383.36 Mb
4	10.10.0.40	DSCP 34(AF4	10.11.5.50	3144402792	0.00 p	0.25 ms	18.01 Kp	25.94 Mb
Total	(from conv tables)							971.22 Mb

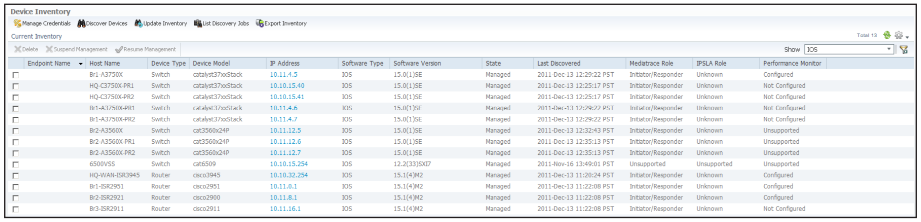
Outbound (Bottom) [1.00 Gb/s] Results 1 - 4 of 4 (0.01s)

	Source	DSCP	Destination	SSRC	TEPL	Jitter	Packets	Bits
1	10.11.4.40	DSCP 34(AF4	10.11.12.40	2471254357	0.00 p	1.01 ms	56.87 Kp	471.34 Mb
2	10.11.4.40	DSCP 34(AF4	10.11.12.40	52316982	0.00 p	0.14 ms	36.02 Kp	99.77 Mb
3	10.11.5.50	DSCP 32(CS4	10.10.0.40	2100969676	0.00 p	0.05 ms	18.01 Kp	25.94 Mb
4	10.11.5.50	DSCP 32(CS4	10.10.0.40	3556229661	0.00 p	0.04 ms	486.31 Kp	607.78 Mb
Total	(from conv tables)							1.20 Gb

Procedure 4 Run a Mediatrace using CPCM

This procedure assumes that you have already installed CPCM and have followed the guidance in *Cisco Prime Collaboration Manager 1.1 Quick Start Guide* (http://www.cisco.com/en/US/docs/net_mgmt/prime/collaboration_manager/1.1/quickstart/guide/cm_qsg.pdf) and the *Cisco Prime Collaboration Manager 1.1 Users Guide*. (http://www.cisco.com/en/US/docs/net_mgmt/prime/collaboration_manager/1.1/user/guide/cm_ug.html). All of the network infrastructure devices that were enabled for PerfMon and Mediatrace in previous procedures must be added to the CPCM inventory, including both the SNMP and CLI credentials. The status for the network infrastructure devices must be **Managed** within the CPCM inventory as in the following figure.

Figure 18 - CPCM inventory of routers and switches

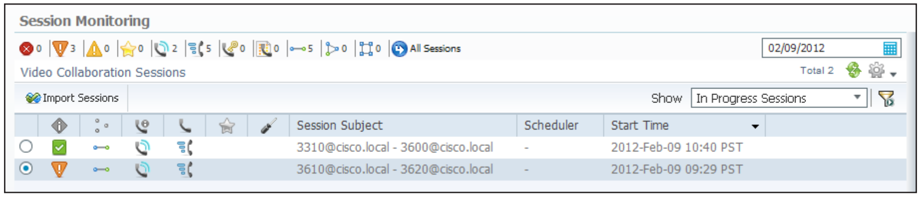


Show: IOS

	Endpoint Name	Host Name	Device Type	Device Model	IP Address	Software Type	Software Version	State	Last Discovered	Mediatrace Role	IPSLA Role	Performance Monitor
□		Br1-A3750X	Switch	catalyst37xxStack	10.11.4.5	IOS	15.0(1)SE	Managed	2011-Dec-13 12:29:22 PST	Initiator/Responder	Unknown	Configured
□		HQ-C3750X-PR1	Switch	catalyst37xxStack	10.10.15.40	IOS	15.0(1)SE	Managed	2011-Dec-13 12:25:17 PST	Initiator/Responder	Unknown	Not Configured
□		HQ-C3750X-PR2	Switch	catalyst37xxStack	10.10.15.41	IOS	15.0(1)SE	Managed	2011-Dec-13 12:25:17 PST	Initiator/Responder	Unknown	Not Configured
□		Br1-A3750X-PR1	Switch	catalyst37xxStack	10.11.4.6	IOS	15.0(1)SE	Managed	2011-Dec-13 12:29:22 PST	Initiator/Responder	Unknown	Not Configured
□		Br1-A3750X-PR2	Switch	catalyst37xxStack	10.11.4.7	IOS	15.0(1)SE	Managed	2011-Dec-13 12:29:22 PST	Initiator/Responder	Unknown	Not Configured
□		Br2-A3560X	Switch	cat3560x24P	10.11.12.5	IOS	15.0(1)SE	Managed	2011-Dec-13 12:32:43 PST	Initiator/Responder	Unknown	Unsupported
□		Br2-A3560X-PR1	Switch	cat3560x24P	10.11.12.6	IOS	15.0(1)SE	Managed	2011-Dec-13 12:35:13 PST	Initiator/Responder	Unknown	Unsupported
□		Br2-A3560X-PR2	Switch	cat3560x24P	10.11.12.7	IOS	15.0(1)SE	Managed	2011-Dec-13 12:35:13 PST	Initiator/Responder	Unknown	Unsupported
□		6500VSS	Switch	cat6509	10.10.15.254	IOS	12.2(33)SXI7	Managed	2011-Nov-16 13:49:01 PST	Unsupported	Unsupported	Unsupported
□		HQ-WAN-ISR3945	Router	cisco3945	10.10.32.254	IOS	15.1(4)M2	Managed	2011-Dec-13 11:20:24 PST	Initiator/Responder	Unknown	Configured
□		Br1-ISR2951	Router	cisco2951	10.11.0.1	IOS	15.1(4)M2	Managed	2011-Dec-13 11:22:08 PST	Initiator/Responder	Unknown	Configured
□		Br2-ISR2921	Router	cisco2900	10.11.8.1	IOS	15.1(4)M2	Managed	2011-Dec-13 11:22:08 PST	Initiator/Responder	Unknown	Configured
□		Br3-ISR2911	Router	cisco2911	10.11.16.1	IOS	15.1(4)M2	Managed	2011-Dec-13 11:22:08 PST	Initiator/Responder	Unknown	Not Configured

You also need to add a variety of other device types to the CPCM inventory, including any supported video endpoints, Cisco Unified Communications Manager (CUCM), Cisco TelePresence Video Communication Server (VCS), and Multipoint Control Unit (MCU). The session monitoring screen in Figure 19 indicates two active sessions, one with an active major alarm.

Figure 19 - CPCM session monitoring



Session Monitoring

0 | 3 | 0 | 0 | 2 | 5 | 0 | 0 | 5 | 0 | 0 | All Sessions — 02/09/2012

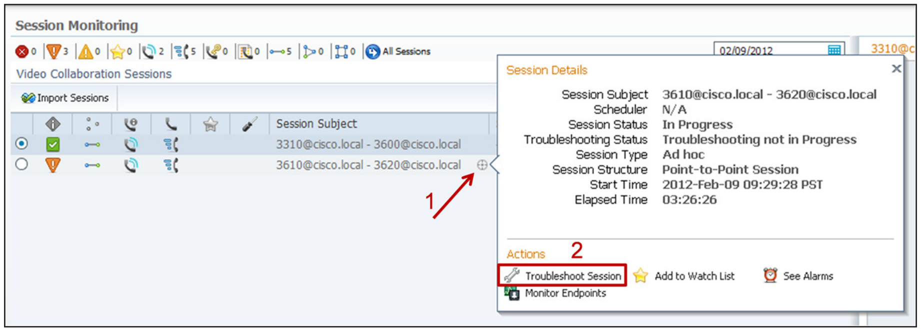
Video Collaboration Sessions — Total 2

Import Sessions — Show: In Progress Sessions

							Session Subject	Scheduler	Start Time
○	✓						3310@cisco.local - 3600@cisco.local	-	2012-Feb-09 10:40 PST
●	!						3610@cisco.local - 3620@cisco.local	-	2012-Feb-09 09:29 PST

You can use CPCM to initiate a troubleshooting session by first placing the mouse over the crosshairs to bring up the Session Details screen and then clicking Troubleshoot Session, as shown in Figure 20.

Figure 20 - CPCM Session Details screen



Session Monitoring

0 | 3 | 0 | 0 | 2 | 5 | 0 | 0 | 5 | 0 | 0 | All Sessions — 02/09/2012

Video Collaboration Sessions

Import Sessions

							Session Subject
●	✓						3310@cisco.local - 3600@cisco.local
○	!						3610@cisco.local - 3620@cisco.local

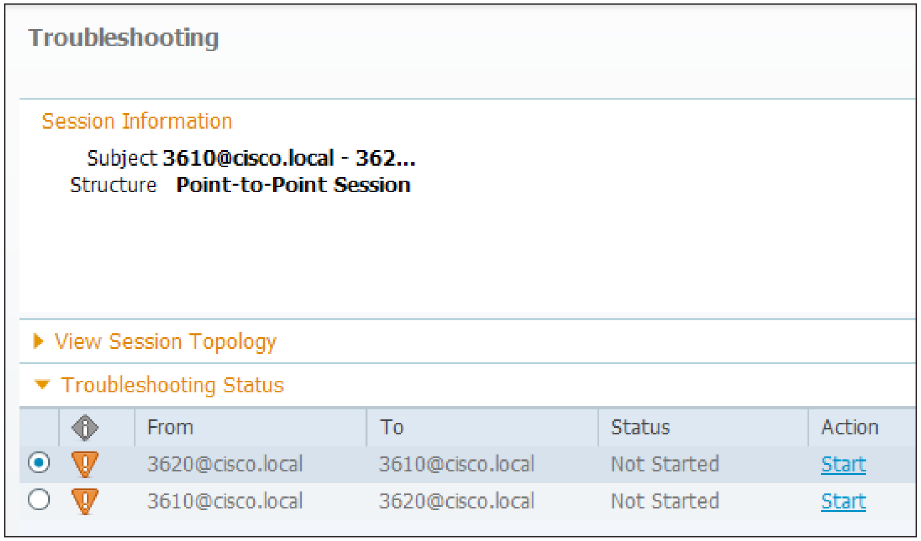
Session Details

Session Subject	3610@cisco.local - 3620@cisco.local
Scheduler	N/A
Session Status	In Progress
Troubleshooting Status	Troubleshooting not in Progress
Session Type	Ad hoc
Session Structure	Point-to-Point Session
Start Time	2012-Feb-09 09:29:28 PST
Elapsed Time	03:26:26

Actions: Troubleshoot Session | Add to Watch List | See Alarms | Monitor Endpoints

You use the Troubleshooting screen to gather additional information from the network devices between the session endpoints. You gather this information in either direction—you must select the path of interest, which, due to the potential for asymmetric routing, might not be the same in both directions. To begin troubleshooting, click **Start**.

Figure 21 - CPCM Troubleshooting screen



Troubleshooting

Session Information

Subject **3610@cisco.local - 362...**
Structure **Point-to-Point Session**

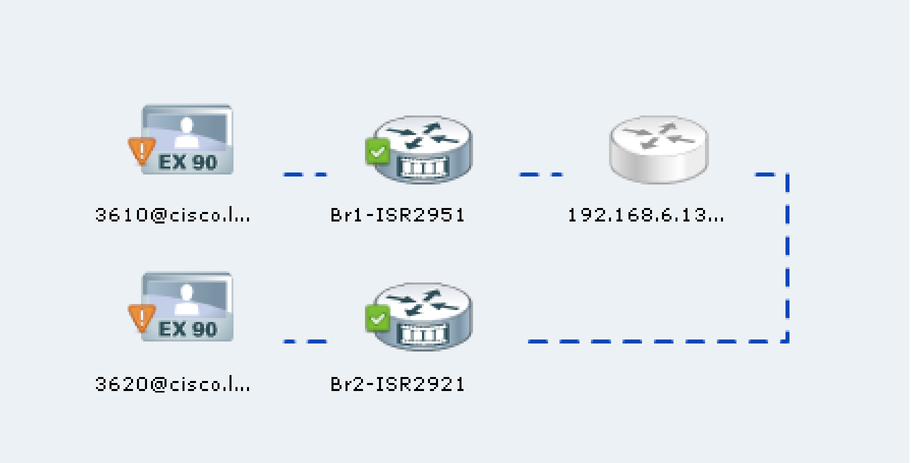
▸ View Session Topology

▾ Troubleshooting Status

		From	To	Status	Action
●	!	3620@cisco.local	3610@cisco.local	Not Started	Start
○	!	3610@cisco.local	3620@cisco.local	Not Started	Start

CPCM gathers topology information, which may take a minute or so depending on the number of devices in the path and topology, and then graphically renders the path between the video endpoints.

Figure 22 - CPCM Troubleshooting - Service Path Topology



By placing the mouse near the left side of a network device (router or switch) and then clicking on the crosshairs, you open a window where System Status, Interface Details, Mediatrace Flow Information, and View All Flows can be displayed, as shown in Figure 23 and Figure 24.

Figure 23 - CPCM Troubleshooting - Device Details

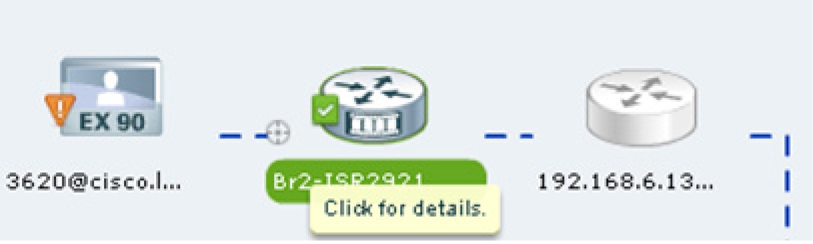
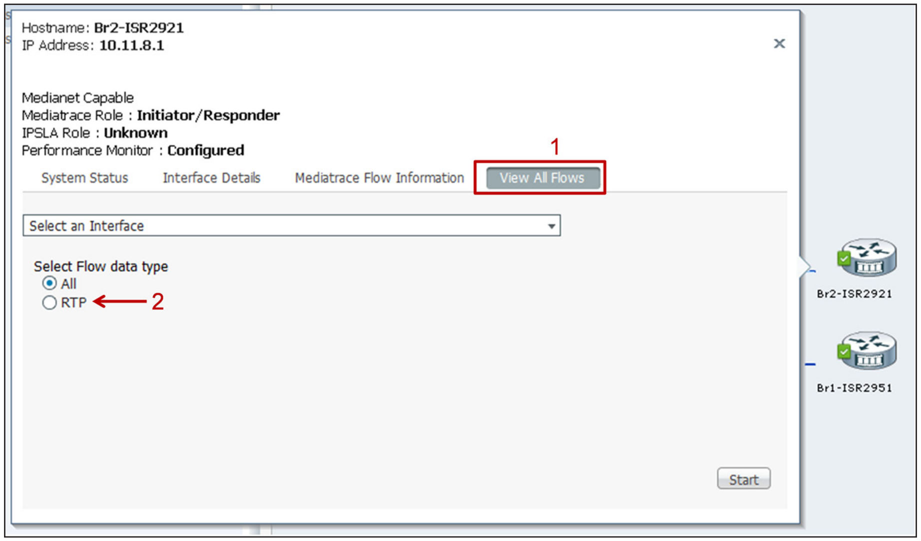


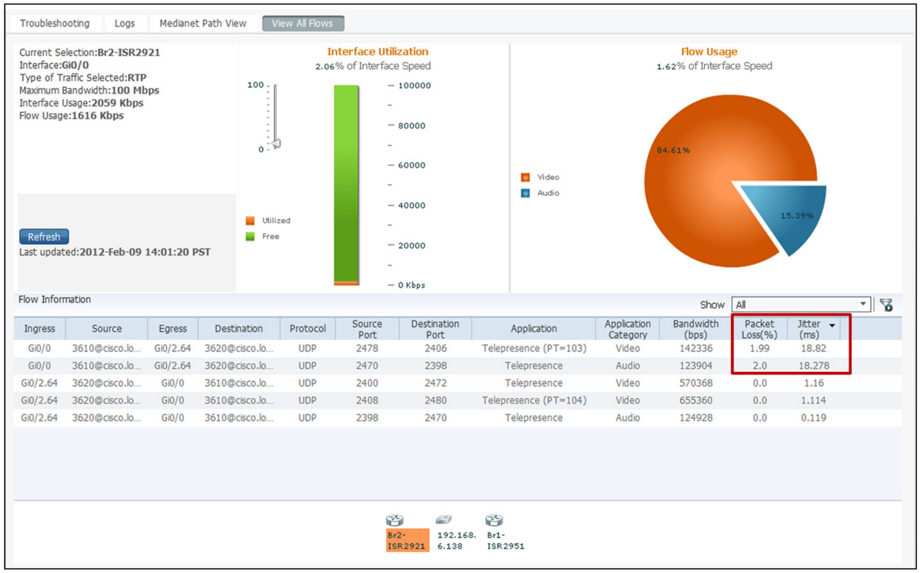
Figure 24 - CPCM Troubleshooting - Device Details Popup


Hostname: **Br2-ISR2921**
IP Address: **10.11.8.1**

Medianet Capable
Mediatrace Role : **Initiator/Responder**
IPSLA Role : **Unknown**
Performance Monitor : **Configured**

The View All Flows data provides PerfMon metrics that are similar to information gathered from PerfMon export data by using NetFlow. You need to select the appropriate interface, which in most cases will be the WAN-facing interface, and the flow data type of RTP. This final step, as shown in Figure 25, clearly identifies that traffic inbound from the WAN is experiencing roughly 2.0 percent packet loss and 18 ms jitter.

Figure 25 - CPCM Troubleshooting - View All Flows RTP



Current Selection:**Br2-ISR2921**
Interface:**Gi0/0**
Type of Traffic Selected:**RTP**
Maximum Bandwidth:**100 Mbps**
Interface Usage:**2059 Kbps**
Flow Usage:**1616 Kbps**

Last updated:**2012-Feb-09 14:01:20 PST**

Flow Information

Show All

Ingress	Source	Egress	Destination	Protocol	Source Port	Destination Port	Application	Application Category	Bandwidth (bps)	Packet Loss(%)	Jitter (ms)
Gi0/0	3610@cisco.lo...	Gi0/2.64	3620@cisco.lo...	UDP	2478	2406	Telepresence (PT=103)	Video	142336	1.99	18.82
Gi0/0	3610@cisco.lo...	Gi0/2.64	3620@cisco.lo...	UDP	2470	2398	Telepresence	Audio	123904	2.0	18.278
Gi0/2.64	3620@cisco.lo...	Gi0/0	3610@cisco.lo...	UDP	2400	2472	Telepresence	Video	570368	0.0	1.16
Gi0/2.64	3620@cisco.lo...	Gi0/0	3610@cisco.lo...	UDP	2408	2480	Telepresence (PT=104)	Video	655360	0.0	1.114
Gi0/2.64	3620@cisco.lo...	Gi0/0	3610@cisco.lo...	UDP	2398	2470	Telepresence	Audio	124928	0.0	0.119

Appendix A: Product List

The following products and software versions have been validated for Cisco SBA.

Functional Area	Product	Part Numbers	Software Version
Headquarters WAN router	Cisco 3945, 3925, or 2951 Integrated Services Router G2	C3945-VSEC/K9 C3925-VSEC/K9 C2951-VSEC/K9	15.1(4)M2
Remote Site router	Cisco 2951 Integrated Services Router Cisco 2921 Integrated Services Router Cisco 2911 Integrated Services Router	C2951-VSEC/K9 C2921-VSEC/K9 C2911-VSEC/K9	15.1(4)M2
Headquarters 100-600 Network Core	Cisco Catalyst 3750-X Stackable 12 & 24 Port SFP and IP Services Image	WS-C3750X-12S-E WS-C3750X-24S-E	15.0(1)SE1
Headquarters or remote-site access switch	Cisco Catalyst 3750-X Stackable 24 &48 Ethernet 10/100/1000 ports with PoE+ and IP Base. Cisco Catalyst 3560-X Standalone 24 & 48 Ethernet 10/100/1000 ports with PoE+ and IP Base	WS-C3750X-24P-S WS-C3750X-48PF-S WS-C3560X-24P-S WS-C3560X-48PF-S	15.0(1)SE1
Network Management	Cisco Prime Collaboration Manager	R-CM-1.1-BASE-K9=	1.1 image (cpcm-va-1.1.0-10719.x86_64.ova) 1.1 patch (cpcm-patchbundle-1.1.0-11714.tar.gz)

Appendix B: Medianet-Enabled Device Configuration

PerfMon and Mediatrace Enabled Router

```
version 15.1
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname HQ-WAN-ISR3945
!
boot-start-marker
boot system flash flash0:c3900-universalk9-mz.SPA.151-4.M2.bin
boot-end-marker
!
!
card type t1 0 0
enable secret 5 $1$VsKH$Xrtn7whTkv8p.tV.ajM1A0
!
no aaa new-model
!
clock timezone PST -8 0
clock summer-time PDT recurring
network-clock-participate wic 0
!
!
flow exporter Export-FNF-Plixer
 description FNF v9
 destination 10.10.48.171
 source Loopback0
 transport udp 2055
 option interface-table
 option application-table
!
!
flow monitor type performance-monitor PerfMon-All-RTP
 description PerfMon RTP
 record default-rtp
 exporter Export-FNF-Plixer
!
!
flow monitor type performance-monitor PerfMon-All-TCP
 description PerfMon TCP
 record default-tcp
 exporter Export-FNF-Plixer
!
ip source-route
ip cef
!
!
ip multicast-routing
!
!
ip domain name cisco.local
ip name-server 10.10.48.10
ip wccp 61 redirect-list WAAS-REDIRECT-LIST group-list BN-WAE 
password 7 0508571C22431F5B4A
ip wccp 62 redirect-list WAAS-REDIRECT-LIST group-list BN-WAE 
password 7 104D580A061843595F
!
multilink bundle-name authenticated
!
!
!
!
isdn switch-type primary-ni
!
```

```
voice-card 0
 dspfarm
 dsp services dspfarm
!
!
!
voice service voip
 fax protocol t38 version 0 ls-redundancy 0 hs-redundancy 0 fallback none
 sip
  bind control source-interface Port-channel32
  bind media source-interface Port-channel32
!
voice class codec 1
 codec preference 1 g711ulaw
 codec preference 2 g711alaw
 codec preference 3 g729r8
 codec preference 4 ilbc
!
!
!
!
!
license udi pid C3900-SPE150/K9 sn FOC14314JFF
hw-module pvdm 0/0
!
!
!
username admin privilege 15 password 7 0508571C22431F5B4A
!
redundancy
!
!
!
!
controller T1 0/0/0
 cablelength short 110
 pri-group timeslots 1-24
 description PSTN PRI
!
controller T1 0/0/1
 cablelength long 0db
!
ip ssh version 2
!
class-map match-any DATA
 match ip dscp af21
class-map match-any INTERACTIVE-VIDEO
 match  dscp cs4  af41
class-map match-any CRITICAL-DATA
 match  dscp cs3  af31
class-map match-any VOICE
 match  dscp ef
class-map match-any SCAVENGER
 match ip dscp cs1  af11
class-map match-any TP-MEDIA
 match protocol telepresence-media
class-map match-any NETWORK-CRITICAL
 match ip dscp cs2 cs6
!
!
policy-map WAN
 class VOICE
  priority percent 10
 class INTERACTIVE-VIDEO
  priority percent 23
 class CRITICAL-DATA
  bandwidth percent 15
  random-detect dscp-based
 class DATA
  bandwidth percent 19
  random-detect dscp-based
 class SCAVENGER
  bandwidth percent 5
 class NETWORK-CRITICAL
  bandwidth percent 3
 class class-default
  bandwidth percent 25
  random-detect
policy-map WAN-QOS-POLICY
 class class-default
  shape average 10000000
  service-policy WAN
!
policy-map type performance-monitor PerfMon-Baseline
 description PerfMon Baseline
 class INTERACTIVE-VIDEO
   flow monitor PerfMon-All-RTP
   react 10 transport-packets-lost-rate
    description Check for > .1% loss
    threshold value gt 0.10
    alarm severity critical
    action syslog
    action snmp
   react 20 rtp-jitter-average
    description Check for > 25 ms average jitter
    threshold value gt 25000
    alarm severity critical
    action syslog
    action snmp
 class TP-MEDIA
   flow monitor PerfMon-All-RTP
   monitor metric rtp
    clock-rate 96 48000
    clock-rate 101 8000
 class DATA
   flow monitor PerfMon-All-TCP
 class CRITICAL-DATA
   flow monitor PerfMon-All-TCP
 class VOICE
   flow monitor PerfMon-All-RTP
```

```
!
!
interface Loopback0
 ip address 10.10.32.254 255.255.255.255
 ip pim sparse-mode
!
interface Port-channel32
 ip address 10.10.32.126 255.255.255.128
 ip wccp 61 redirect in
 ip pim sparse-mode
 service-policy type performance-monitor input PerfMon-Baseline
 service-policy type performance-monitor output PerfMon-Baseline
 hold-queue 150 in
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 description MPLS WAN uplink
 ip address 192.168.6.129 255.255.255.252
 ip wccp 62 redirect in
 ip pim sparse-mode
 service-policy type performance-monitor input PerfMon-Baseline
 service-policy type performance-monitor output PerfMon-Baseline
 duplex auto
 speed auto
 service-policy output WAN-QOS-POLICY
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 channel-group 32
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 channel-group 32
!
interface Serial0/0/0:23
 no ip address
 encapsulation hdlc
 isdn switch-type primary-ni
 isdn incoming-voice voice
 no cdp enable
!
interface GigabitEthernet0/1/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
!
!
router eigrp 1
 network 10.10.0.0 0.0.255.255
 redistribute static metric 50000 100 255 1 1500
 passive-interface GigabitEthernet0/0
!
ip forward-protocol nd
!
ip pim rp-address 10.10.15.252 10
ip pim register-source Loopback0
no ip http server
ip http authentication local
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip route 10.11.0.0 255.255.0.0 192.168.6.130
ip route 192.168.6.128 255.255.255.224 192.168.6.130
!
ip access-list standard BN-WAE
 permit 10.10.32.10
 !
ip access-list extended WAAS-REDIRECT-LIST
 remark WAAS WCCP Redirect Exempt/Permit List
 deny   tcp any any eq 22
 deny   tcp any eq 22 any
 deny   tcp any any eq 2000
 deny   tcp any eq 2000 any
 deny   tcp any any eq 5060
 deny   tcp any eq 5060 any
 deny   tcp any any eq 5061
 deny   tcp any eq 5061 any
 deny   tcp any any eq 123
 deny   tcp any eq 123 any
 permit tcp any any
!
logging trap errors
logging 10.10.48.35
access-list 10 permit 239.1.0.0 0.0.255.255
access-list 55 permit 10.10.48.0 0.0.0.255
!
!
!
!
nls resp-timeout 1
cpd cr-id 1
!
snmp-server community cisco RO 55
snmp-server community cisco123 RW 55
snmp-server ifindex persist
snmp-server source-interface informs Loopback0
!
control-plane
!
!
voice-port 0/0/0:23
mediatrace responder
mediatrace initiator source-interface Loopback0
!
ccm-manager sccp local Port-channel32
!
!
mgcp profile default
!
sccp local Port-channel32
sccp ccm 10.10.48.21 identifier 2 priority 1 version 7.0
sccp ccm 10.10.48.20 identifier 1 priority 2 version 7.0
sccp
!
sccp ccm group 1
 bind interface Port-channel32
 associate ccm 2 priority 1
 associate ccm 1 priority 2
 associate profile 1 register CFBHQ1
 switchback method graceful
 switchback interval 60
!
dspfarm profile 1 conference
 description HQ Conference Bridges
 codec g729br8
 codec g729r8
 codec g729abr8
 codec g729ar8
 codec g711alaw
 codec g711ulaw
 codec g722-64
 codec ilbc
 maximum sessions 5
 associate application SCCP
!
dial-peer voice 100 voip
 description SIP TRUNK to CUCM1
 preference 2
 destination-pattern 230530....
 session protocol sipv2
 session target ipv4:10.10.48.20
 incoming called-number .
 voice-class codec 1
!
dial-peer voice 101 voip
 description SIP TRUNK to CUCM2
 preference 1
 destination-pattern 230530....
 session protocol sipv2
 session target ipv4:10.10.48.21
 incoming called-number .
 voice-class codec 1
!
dial-peer voice 911 pots
 destination-pattern 911
 port 0/0/0:23
 forward-digits 3
!
dial-peer voice 9911 pots
 destination-pattern 9911
 port 0/0/0:23
 forward-digits 3
!
dial-peer voice 7 pots
 destination-pattern 9[2-9]......
 port 0/0/0:23
 forward-digits 7
!
dial-peer voice 11 pots
 destination-pattern 91[2-9]..[2-9]......
 port 0/0/0:23
 forward-digits 11
!
dial-peer voice 9011 pots
 destination-pattern 9011T
 incoming called-number .
 direct-inward-dial
 port 0/0/0:23
 prefix 011
!
!
!
!
gatekeeper
 shutdown
!
!
!
line con 0
line aux 0
line 2
 login local
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 exec-timeout 120 0
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
scheduler allocate 20000 1000
ntp update-calendar
ntp server 10.10.48.17
!
wsma agent exec profile WSMA-LISTENER-HTTPS
wsma agent config profile WSMA-LISTENER-HTTPS
!
wsma profile listener WSMA-LISTENER-HTTPS
 transport https
end
```

Mediatrace Enabled Switch

```
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Br2-A3560X
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$Jex5$sQoa3S6zLe9X9ou3S/Svn.
!
username admin privilege 15 password 7 121A540411045D5679
no aaa new-model
clock timezone PST -8 0
clock summer-time PDT recurring
system mtu routing 1500
!
!
ip arp inspection vlan 64,69
!
!
ip dhcp snooping vlan 64,69
no ip dhcp snooping information option
ip dhcp snooping
ip domain-name cisco.local
ip name-server 10.10.48.10
ip device tracking
vtp mode transparent
```

```
udld enable

!
mls qos map policed-dscp  0 10 18 24 46 to 8
mls qos map cos-dscp 0 8 16 24 32 46 48 56
mls qos srr-queue input bandwidth 70 30
mls qos srr-queue input threshold 1 80 90
mls qos srr-queue input priority-queue 2 bandwidth 30
mls qos srr-queue input cos-map queue 1 threshold 2 3
mls qos srr-queue input cos-map queue 1 threshold 3 6 7
mls qos srr-queue input cos-map queue 2 threshold 1 4
mls qos srr-queue input dscp-map queue 1 threshold 2 24
mls qos srr-queue input dscp-map queue 1 threshold 3 48 49 50 51
52 53 54 55
mls qos srr-queue input dscp-map queue 1 threshold 3 56 57 58 59
60 61 62 63
mls qos srr-queue input dscp-map queue 2 threshold 3 32 33 40 41
42 43 44 45
mls qos srr-queue input dscp-map queue 2 threshold 3 46 47
mls qos srr-queue output cos-map queue 1 threshold 3 4 5
mls qos srr-queue output cos-map queue 2 threshold 1 2
mls qos srr-queue output cos-map queue 2 threshold 2 3
mls qos srr-queue output cos-map queue 2 threshold 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 0
mls qos srr-queue output cos-map queue 4 threshold 3 1
mls qos srr-queue output dscp-map queue 1 threshold 3 32 33 40 41
42 43 44 45
mls qos srr-queue output dscp-map queue 1 threshold 3 46 47
mls qos srr-queue output dscp-map queue 2 threshold 1 16 17 18 19
20 21 22 23
mls qos srr-queue output dscp-map queue 2 threshold 1 26 27 28 29
30 31 34 35
mls qos srr-queue output dscp-map queue 2 threshold 1 36 37 38 39
mls qos srr-queue output dscp-map queue 2 threshold 2 24
mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51
52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59
60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3 0 1 2 3 4 5
6 7
mls qos srr-queue output dscp-map queue 4 threshold 1 8 9 11 13
15
mls qos srr-queue output dscp-map queue 4 threshold 2 10 12 14
mls qos queue-set output 1 threshold 1 100 100 50 200
mls qos queue-set output 1 threshold 2 125 125 100 400
mls qos queue-set output 1 threshold 3 100 100 100 400
mls qos queue-set output 1 threshold 4 60 150 50 200
mls qos queue-set output 1 buffers 15 25 40 20
mls qos
!
crypto pki trustpoint TP-self-signed-4274817536
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-4274817536
 revocation-check none
 rsakeypair TP-self-signed-4274817536
!
!
crypto pki certificate chain TP-self-signed-4274817536
 certificate self-signed 01
  3082024D 308201B6 A0030201 02020101 300D0609 2A864886 F70D0101
04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D
43657274
  69666963 6174652D 34323734 38313735 3336301E 170D3933 30333031
30303031
  33395A17 0D323030 31303130 30303030 305A3031 312F302D 06035504
03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D34
32373438
  31373533 3630819F 300D0609 2A864886 F70D0101 01050003 818D0030
81890281
  8100AFBC 1F82B5ED EF25679B DC7F4675 9E4E3FFF A423D7C6 77E406AB
6CB444F0
  5B83C85D 4AB9062F BEB39335 FB42A93A F6384B1F 2BBE4AAB 1CC6DC5D
```

```
9C721A6D
  8CB067E1 3C231DFD 3CA8F0FA D0381480 68ECF838 6DAFABF6 06292461
79BAC3BE
  26319D9F 328C0F32 F69B2F12 39411068 33A89FBB CDF52A34 C6D2A7FD
CA7BF363
  B6F30203 010001A3 75307330 0F060355 1D130101 FF040530 030101FF
30200603
  551D1104 19301782 15427232 2D333536 30582E63 6973636F 2E6C6F63
616C301F
  0603551D 23041830 16801437 C7032C93 E988847C 6B93B208 DF1BDEE5
E8937D30
  1D060355 1D0E0416 041437C7 032C93E9 88847C6B 93B208DF 1BDEE5E8
937D300D
  06092A86 4886F70D 01010405 00038181 00267B24 F11A8D5E 07BE3418
1E914415
  AD84E49D FDF8292C 6623FC28 AF8544A5 A947E431 A186428C E72D5E4B
4122BFB1
  7DC101F0 70532AB3 43347857 AF081519 7F2B92C1 C1F6F078 AAF11004
2A0017C2
  AF9157DC F3BE6B76 B66DA7A7 127E3C66 C964F734 CFFAA45D 54A129AE
8C222D1B
  CE14B3FC 543D373E 6611D24B 2E9E31B1 0C
       quit
license boot level ipservices
!
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
auto qos srnd4
!
!
!
!
vlan internal allocation policy ascending
!
vlan 64
 name Wired-Data
!
vlan 65
 name Wireless-Data
!
vlan 69
 name Wired-Voice
!
vlan 70
 name Wireless-Voice
!
vlan 999
 name NATIVE
!
ip ssh version 2
!
class-map match-all AUTOQOS_VOIP_DATA_CLASS
  match ip dscp ef
class-map match-all AUTOQOS_DEFAULT_CLASS
  match access-group name AUTOQOS-ACL-DEFAULT
class-map match-all AUTOQOS_VOIP_SIGNAL_CLASS
  match ip dscp cs3
!
policy-map AUTOQOS-SRND4-CISCOPHONE-POLICY
 class AUTOQOS_VOIP_DATA_CLASS
   set dscp ef
  police 128000 8000 exceed-action policed-dscp-transmit
 class AUTOQOS_VOIP_SIGNAL_CLASS
   set dscp cs3
  police 32000 8000 exceed-action policed-dscp-transmit
 class AUTOQOS_DEFAULT_CLASS
   set dscp default
  police 10000000 8000 exceed-action policed-dscp-transmit
policy-map type performance-monitor PERF-MON-BASELINE
!
!
```

```
!
!
macro name AccessEdgeQoS
auto qos voip cisco-phone
@
macro name EgressQoS
mls qos trust dscp
queue-set 2
srr-queue bandwidth share 1 30 35 5
priority-queue out
@
!
!
interface FastEthernet0
 no ip address
 shutdown
!
interface GigabitEthernet0/1
 switchport access vlan 64
 switchport mode access
 switchport voice vlan 69
 switchport port-security maximum 11
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 ip arp inspection limit rate 100
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust device cisco-phone
 mls qos trust cos
 macro description AccessEdgeQoS
 auto qos voip cisco-phone
 spanning-tree portfast
 spanning-tree bpduguard enable
 service-policy input AUTOQOS-SRND4-CISCOPHONE-POLICY
 ip verify source
 ip dhcp snooping limit rate 100
!
interface GigabitEthernet0/2
 switchport access vlan 64
 switchport mode access
 switchport voice vlan 69
 switchport port-security maximum 11
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 ip arp inspection limit rate 100
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust device cisco-phone
 mls qos trust cos
 macro description AccessEdgeQoS
 auto qos voip cisco-phone
 spanning-tree portfast
 spanning-tree bpduguard enable
 service-policy input AUTOQOS-SRND4-CISCOPHONE-POLICY
 ip verify source
 ip dhcp snooping limit rate 100
!
interface GigabitEthernet0/3
 description ** WAAS Connection **
 switchport access vlan 64
 switchport mode access
 ip arp inspection trust
 srr-queue bandwidth share 1 30 35 5
 queue-set 2
 priority-queue out
 mls qos trust dscp
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet0/4
```

```
 switchport access vlan 64
 switchport mode access
 switchport voice vlan 69
 switchport port-security maximum 11
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 ip arp inspection limit rate 100
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust device cisco-phone
 mls qos trust cos
 macro description AccessEdgeQoS
 auto qos voip cisco-phone
 spanning-tree portfast
 spanning-tree bpduguard enable
 service-policy input AUTOQOS-SRND4-CISCOPHONE-POLICY
 ip verify source
 ip dhcp snooping limit rate 100
!
interface GigabitEthernet0/5
 switchport access vlan 64
 switchport mode access
 switchport voice vlan 69
 switchport port-security maximum 11
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 ip arp inspection limit rate 100
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust device cisco-phone
 mls qos trust cos
 macro description AccessEdgeQoS
 auto qos voip cisco-phone
 spanning-tree portfast
 spanning-tree bpduguard enable
 service-policy input AUTOQOS-SRND4-CISCOPHONE-POLICY
 ip verify source
 ip dhcp snooping limit rate 100
!
interface GigabitEthernet0/6
 switchport access vlan 64
 switchport mode access
 switchport voice vlan 69
 switchport port-security maximum 11
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 ip arp inspection limit rate 100
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust device cisco-phone
 mls qos trust cos
 macro description AccessEdgeQoS
 auto qos voip cisco-phone
 spanning-tree portfast
 spanning-tree bpduguard enable
 service-policy input AUTOQOS-SRND4-CISCOPHONE-POLICY
 ip verify source
 ip dhcp snooping limit rate 100
!
interface GigabitEthernet0/7
 switchport access vlan 64
 switchport mode access
 switchport voice vlan 69
 switchport port-security maximum 11
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 ip arp inspection limit rate 100
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust device cisco-phone
 mls qos trust cos
 macro description AccessEdgeQoS
 auto qos voip cisco-phone
 spanning-tree portfast
 spanning-tree bpduguard enable
 service-policy input AUTOQOS-SRND4-CISCOPHONE-POLICY
 ip verify source
 ip dhcp snooping limit rate 100
!
interface GigabitEthernet0/8
 switchport access vlan 64
 switchport mode access
 switchport voice vlan 69
 switchport port-security maximum 11
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 ip arp inspection limit rate 100
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust device cisco-phone
 mls qos trust cos
 macro description AccessEdgeQoS
 auto qos voip cisco-phone
 spanning-tree portfast
 spanning-tree bpduguard enable
 service-policy input AUTOQOS-SRND4-CISCOPHONE-POLICY
 ip verify source
 ip dhcp snooping limit rate 100
!
interface GigabitEthernet0/9
 switchport access vlan 64
 switchport mode access
 switchport voice vlan 69
 switchport port-security maximum 11
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 ip arp inspection limit rate 100
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust device cisco-phone
 mls qos trust cos
 macro description AccessEdgeQoS
 auto qos voip cisco-phone
 spanning-tree portfast
 spanning-tree bpduguard enable
 service-policy input AUTOQOS-SRND4-CISCOPHONE-POLICY
 ip verify source
 ip dhcp snooping limit rate 100
!
interface GigabitEthernet0/10
 switchport access vlan 64
 switchport mode access
 switchport voice vlan 69
 switchport port-security maximum 11
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 ip arp inspection limit rate 100
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust device cisco-phone
 mls qos trust cos
 macro description AccessEdgeQoS
 auto qos voip cisco-phone
 spanning-tree portfast
 spanning-tree bpduguard enable
 service-policy input AUTOQOS-SRND4-CISCOPHONE-POLICY
 ip verify source
 ip dhcp snooping limit rate 100
!

! <additional port configuration deleted>

!
interface GigabitEthernet0/24
 description Links to Br2-2921
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan 64,65,69,70
 switchport mode trunk
 ip arp inspection trust
 logging event link-status
 srr-queue bandwidth share 1 30 35 5
 queue-set 2
 priority-queue out
 mls qos trust dscp
 macro description EgressQoS
 ip dhcp snooping trust
!
interface GigabitEthernet1/1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan 64,65,69,70
 switchport mode trunk
 ip arp inspection trust
 srr-queue bandwidth share 1 30 35 5
 queue-set 2
 priority-queue out
 mls qos trust dscp
 macro description EgressQoS | EgressQoS
 ip dhcp snooping trust
!
```

```
interface GigabitEthernet1/2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan 64,65,69,70
 switchport mode trunk
 ip arp inspection trust
 srr-queue bandwidth share 1 30 35 5
 queue-set 2
 priority-queue out
 mls qos trust dscp
 ip dhcp snooping trust
!
interface GigabitEthernet1/3
!
interface GigabitEthernet1/4
!
interface TenGigabitEthernet1/1
!
interface TenGigabitEthernet1/2
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan64
 ip address 10.11.12.5 255.255.255.0
!
ip default-gateway 10.11.12.1
ip http server
ip http authentication local
no ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip rsvp snooping
!
ip access-list extended AUTOQOS-ACL-DEFAULT
 permit ip any any
```

```
!
logging esm config
logging trap errors
logging 10.10.48.35
access-list 55 permit 10.10.48.0 0.0.0.255
snmp-server community cisco RO 55
snmp-server community cisco123 RW
snmp ifmib ifindex persist
mediatrace responder
mediatrace initiator source-ip 10.11.12.5
!
!
line con 0
line vty 0 4
 login local
 length 0
 transport input ssh
line vty 5 15
 login local
 length 0
 transport input ssh
!
ntp server 10.10.48.17
wsma agent exec profile WSMA-LISTENER-HTTPS
wsma agent config profile WSMA-LISTENER-HTTPS
!
wsma profile listener WSMA-LISTENER-HTTPS
 transport https
end
```

Notes

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.**

B-0000582-1 3/12