Newer Design Guide Available

Cisco Smart Business Architecture has become part of the Cisco Validated Designs program.

For up-to-date guidance on the designs described in this guide, see http://cvddocs.com/fw/Aug13-325

For information about the Cisco Validated Design program, go to http://www.cisco.com/go/cvd

SBA

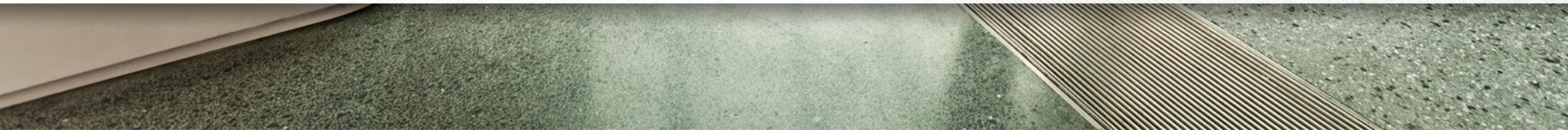
BORDERLESS NETWORKS

DEPLOYMENT GUIDE

Video Quality Monitoring Using Medianet Deployment Guide

SMART BUSINESS ARCHITECTURE

February 2013 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 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.

The Release Notes for a series provides a summary of additions and changes made in the 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 February 2013 is the "February 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 SBA feedback form.

If you would like to be notified when new comments are posted, an RSS feed is available from the SBA customer and partner pages.

Table of Contents

What's In This SBA Guide

Cisco SBA Borderless Networks

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.

Cisco SBA Borderless Networks is a comprehensive network design targeted at organizations with up to 10,000 connected users. The SBA Borderless Network architecture incorporates wired and wireless local area network (LAN) access, wide-area network (WAN) connectivity, WAN application optimization, and Internet edge security infrastructure.

Route to Success

To ensure your success when implementing the designs in this guide, you should first read any guides that this guide depends upon—shown to the left of this guide on the route below. As you read this guide, specific prerequisites are cited where they are applicable.

About This Guide

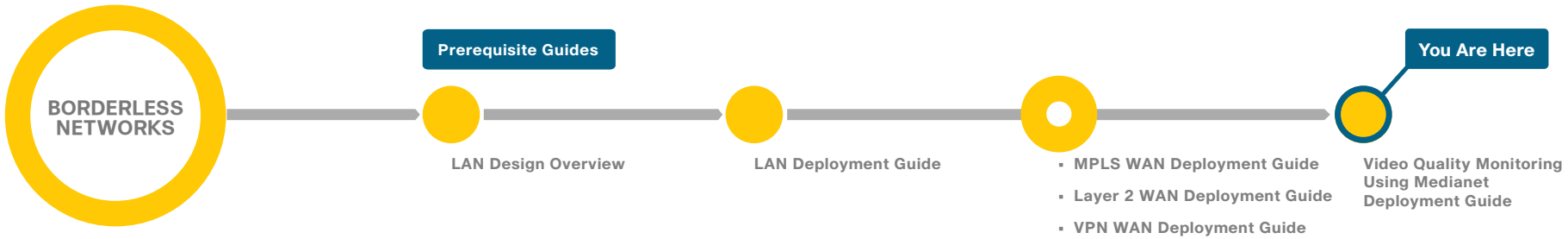
This *deployment guide* contains one or more deployment chapters, which each include the following sections:

- **Business Overview**—Describes the business use case for the design. Business decision makers may find this section especially useful.
- **Technology Overview**—Describes the technical design for the business use case, including an introduction to the Cisco products that make up the design. Technical decision makers can use this section to understand how the design works.
- **Deployment Details**—Provides step-by-step instructions for deploying and configuring the design. Systems engineers can use this section to get the design up and running quickly and reliably.

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

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

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 to 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 the 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 midrange and PC, desktops, and 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.

You can monitor the video conference quality by 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 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 in order 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 in order 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) are 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 the following table. The PerfMon fields for TCP are also useful for general-purpose traffic, but they are not covered extensively in this guide.

Figure 1 - PerfMon key fields (RTP)

Key field type	Key field value
IPv4	protocol source address destination address
transport	source-port destination-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 the following table. 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.

Table 1 - PerfMon non–key fields (RTP)

Non-key field type	Non-key field value
application	media bytes media event media packets
counter	bytes packets
flow	direction
interface	input output
IPv4	destination mask dscp source mask ttl
monitor	event
routing	forwarding-status
timestamp	interval
transport	event packet-loss packets expected packets lost round-trip-time rtp jitter maximum rtp jitter mean rtp jigger minimum

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. You use a new type of policy map, **policy-map type performance-monitor**, 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 of the QoS procedures for all WAN-aggregation routers and remote-site routers from the following Cisco SBA—Borderless Networks guides: *MPLS WAN Deployment Guide*, *Layer 2 WAN Deployment Guide*, and *VPN WAN 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
```

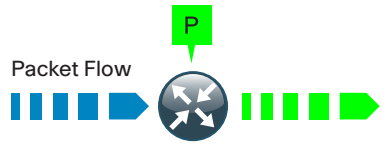
Other class maps must be configured to match additional video traffic, which is described in the "Deployment Details" section of this guide. Some class maps use Cisco Network-Based Application Recognition (NBAR) to classify applications. NBAR is an intelligent classification engine in Cisco IOS software that can recognize a wide variety of applications, including video protocols used by Cisco TelePresence.

Tech Tip

The Cisco ASR 1000 Series does not currently support NBAR on port-channel interfaces.

You assign flow records to the PerfMon policy map. 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. It is recommended to use the predefined flow records **default-tcp** and **default-rtp**. An example of the PerfMon cache using a predefined record is shown in the following figure.

Figure 2 - PerfMon cache—predefined RTP flow record



IPv4 Source	10.5.83.40	10.5.4.40	10.4.4.40	10.4.0.40
IPv4 Dest	10.5.3.40	10.5.83.40	10.5.12.40	10.5.12.40
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 Lost	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 usec	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)

Key Field
Non-Key Field
Default RTP Flow Record Field Types

P PerfMon-Enabled Device

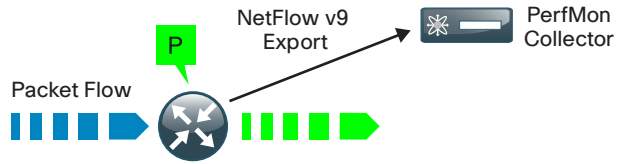
3030

PerfMon Monitoring

You can view data directly from the PerfMon-enabled device by using 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 the following figure; 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 3 - PerfMon export to collector



IPv4 Source	10.5.83.40	10.5.4.40	10.4.4.40	10.4.0.40
IPv4 Dest	10.5.3.40	10.5.83.40	10.5.12.40	10.5.12.40
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 Lost	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 usec	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)

Key Field
Non-Key Field
Default RTP Flow Record Field Types

P PerfMon-Enabled Device

303 1

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 and analysis application you use. The example deployment guidance in the "Deployment Details" section applies to the following applications:

- ActionPacked! LiveAction
- 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 you have configured PerfMon 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 the following table. 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 2 - Acceptable values for delay, jitter, and loss by application

Application	Delay (one way)	Jitter	Loss
Desktop Sharing (Cisco 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 by 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. The following is an example of a packet loss TCA:

```
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 10.5.3.40, dst ip 10.5.83.40
           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 [1.00%, 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.

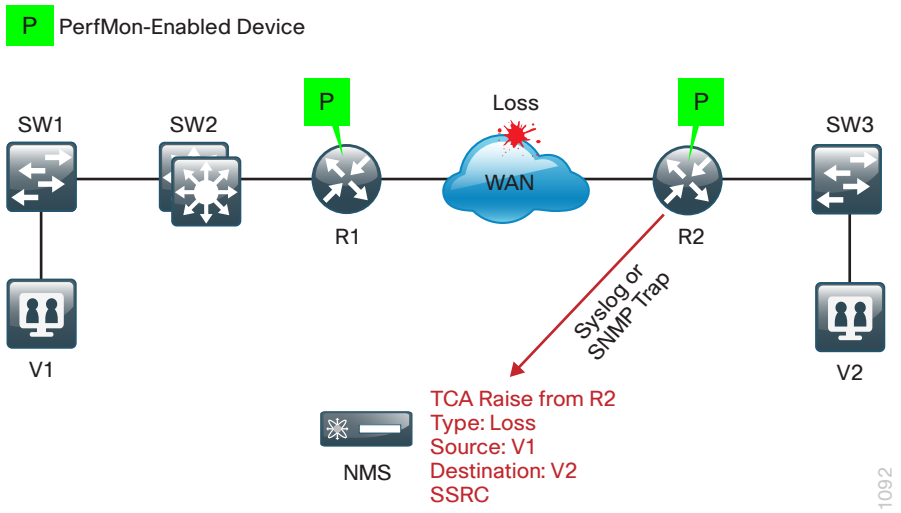
You may want to create a set of TCAs corresponding to the different severity levels listed in the following table that are triggered at various thresholds as conditions deteriorate. By using this method to layer the TCAs, you can raise awareness of potential issues before they affect service.

Table 3 - TCA severity levels from lowest to highest

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

In the following figure, the TCA alert received by the NMS 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.

Figure 4 - TCA raised due to WAN loss condition



Mediatrace

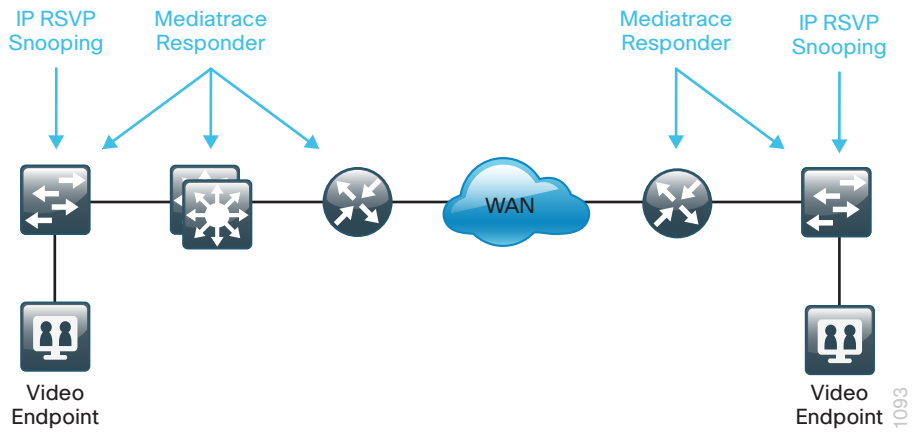
Cisco Mediatrace is a network diagnostic tool that monitors the state of an audio, video, or data flow across a network path. Mediatrace discovers Layer 2 and Layer 3 devices along the flow path and can be used to collect information from these devices. The types of information include device-specific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

Reader Tip

To present a comprehensive discussion of Cisco Medianet technology, we include information about Mediatrace; however, this guide does not describe the deployment of Mediatrace.

The IP traceroute tool is a close analog to the Cisco 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 the following figure for more details.

Figure 5 - Cisco Mediatrace responder and IP RSVP snooping by device



The Cisco 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 Cisco Mediatrace is for real-time troubleshooting after the network operator has been notified of a potentially degraded video conference as shown previously in Figure 4. 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.

Cisco Mediatrace identifies where the source of the loss was introduced by using the following steps. To identify the Mediatrace-enabled device that is nearest to both video endpoints V1 and V2, you run Mediatrace 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 6; 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.

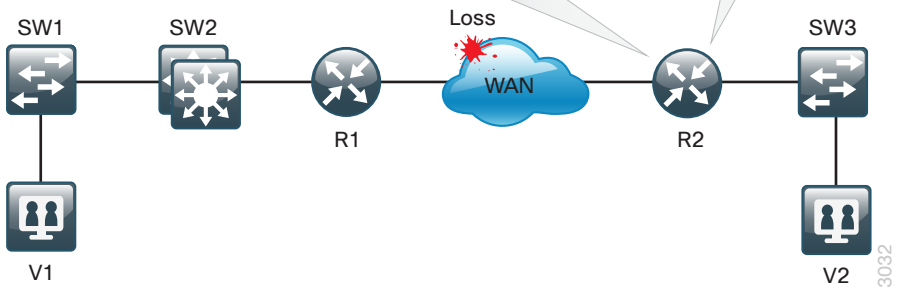
Figure 6 - Cisco Mediatrace hops in both directions from R2

Mediatrace: Source V2, Dest V1

Hop #	Device	Ingress Int	Egress Int
0	R2	None	Gig 0/0
1	R1	Gig 0/0	Gi0/1.50
2	SW2	Gig 1/1/1	Gig 1/0/1
3	SW1	Gig 0/24	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



Cisco 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 7. From the information collected, the network operator can observe that there was no RTP loss on R1 but that there was RTP loss on R2. The network operator can conclude that the loss was introduced between R1 and R2, which is somewhere within the WAN.

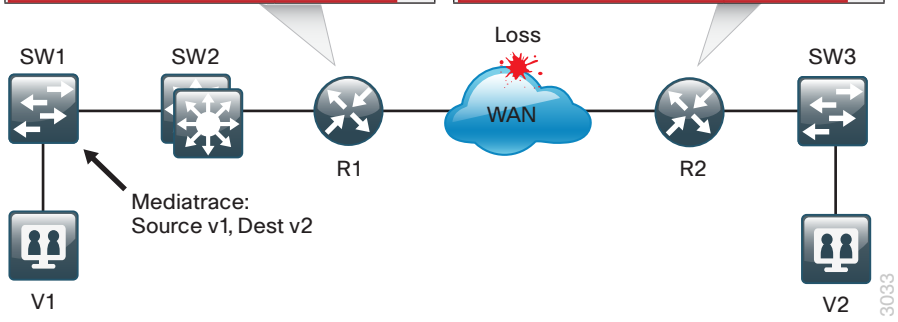
Figure 7 - Cisco Mediatrace PerfMon from SW1

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%**



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 in order to validate that the network will be able to support the expected rich-media traffic.

Reader Tip

To present a comprehensive discussion of Cisco Medianet technology, we include information about IPSLA VO; however, this guide does not describe the deployment of IPSLA VO.

PerfMon Interaction with Encryption

When configuring PerfMon, it is useful to understand how Cisco IOS processes traffic when transmitting and receiving network traffic on an interface. This is best shown as an ordered list, as illustrated in the following figure.

Figure 8 - Cisco IOS order of operations

Ingress Features	Egress Features
1. Virtual Reassembly	1. Output IOS IPS Inspection
2. IP Traffic Export	2. Output WCCP Redirect
3. QoS Policy Propagation through BGP (QPPB)	3. NM-CIDS
4. Ingress Flexible NetFlow (FNF), PerfMon	4. NAT Inside-to-Outside or NAT Enable
5. Network Based Application Recognition (NBAR)	5. Network Based Application Recognition (NBAR)
6. Input QoS Classification	6. BGP Policy Accounting
7. Ingress NetFlow (TNF)	7. Lawful Intercept
8. Lawful Intercept	8. Check crypto map ACL and mark for encryption
9. IOS IPS Inspection (inbound)	9. Output QoS Classification
10. Input Stateful Packet Inspection (IOS FW)	10. Output ACL check (if not marked for encryption)
11. Check reverse crypto map ACL	11. Crypto output ACL check (if marked for encryption)
12. Input ACL (unless existing NetFlow record was found)	12. Output Flexible Packet Matching (FPM)
13. Input Flexible Packet Matching (FPM)	13. DoS Tracker
14. IPsec Decryption (if encrypted)	14. Output Stateful Packet Inspection (IOS FW)
15. Crypto inbound ACL check (if packet had been encrypted)	15. TCP Intercept
16. Unicast RPF check	16. Output QoS Marking
17. Input QoS Marking	17. Output Policing (CAR)
18. Input Policing (CAR)	18. Output MAC/Precedence Accounting
19. Input MAC/Precedence Accounting	19. IPsec Encryption
20. Nat Outside-to-Inside	20. Output ACL check (if encrypted)
21. Policy Routing	21. Egress NetFlow (TNF)
22. Input WCCP Redirect	22. Egress Flexible NetFlow (FNF), PerfMon
	23. Egress RITE
	24. Output Queueing (CBWGQ, LLQ, WRED)

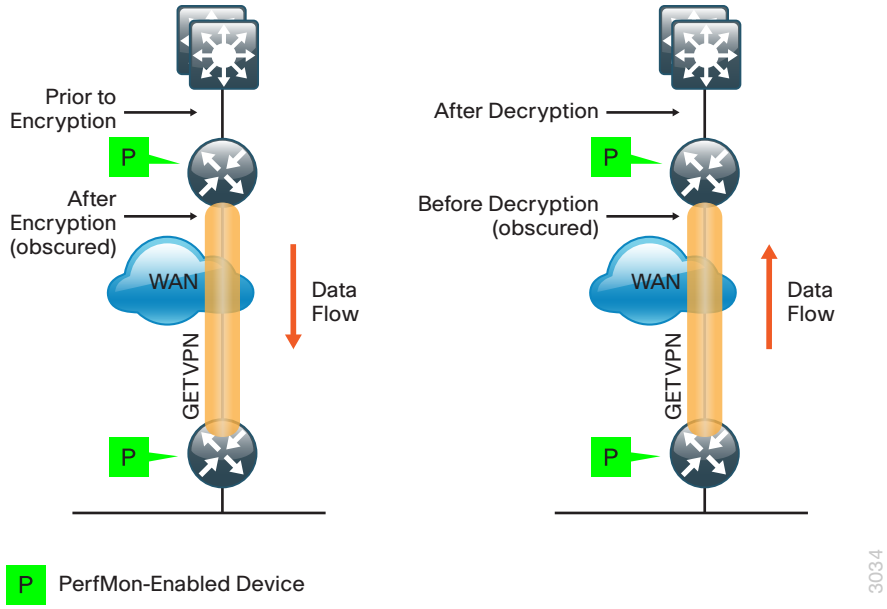
1090

Based on the order of operations, in order to classify traffic properly, PerfMon must monitor prior to encryption when transmitting and after decryption when receiving. Otherwise, the actual protocols in use remain obscured, and all traffic appears as IPSec with no other details available. Encrypted traffic from the WAN is properly classified by PerfMon with an outbound monitor on a corresponding LAN interface. Similarly, traffic bound for the WAN is properly classified by PerfMon with an inbound monitor on a corresponding LAN interface. This is illustrated in Figure 9.

Tech Tip

The Cisco ASR 1000 router is unable to classify data using NBAR when using a port-channel interface that connects to the LAN distribution layer and GETVPN encryption on its WAN interface.

Figure 9 - Encryption and PerfMon



3034

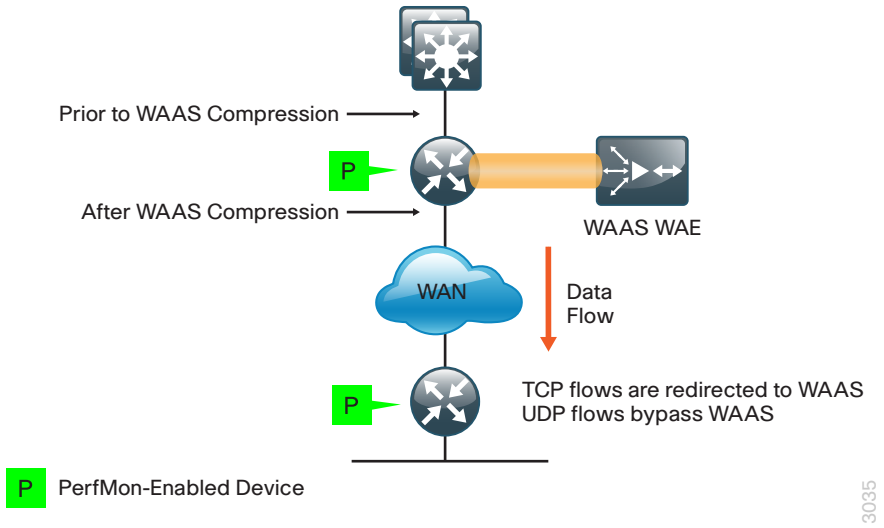
PerfMon Interaction with Application Optimization

The Cisco SBA reference designs include 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—Borderless Networks Application Optimization Deployment Guide*.

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 directions in which they are monitored affects the data cached by the network device. The topology in Figure 10 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 Cisco 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 10.

Figure 10 - Application optimization and PerfMon



PerfMon, although primarily used for RTP traffic monitoring, also provides loss and round-trip time statistics for TCP applications. For PerfMon with application optimization, it is recommended that you 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.

Deployment Details

Cisco Medianet technologies are most effective when enabled broadly on all the routers across the network. There are several prerequisites for a Cisco Medianet deployment. Configuring PerfMon is straightforward if QoS has already been configured.

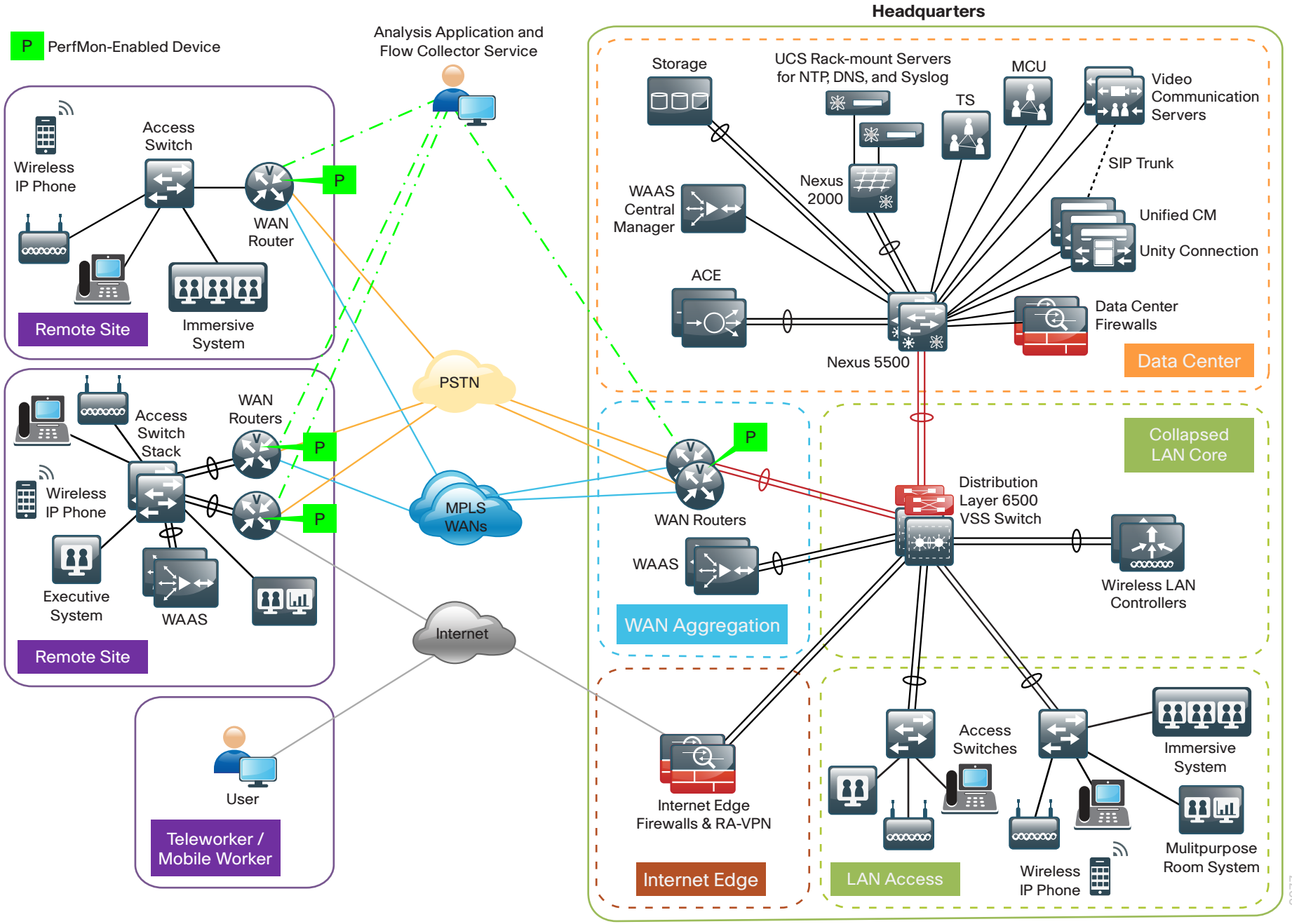
PerfMon builds upon the embedded Cisco NetFlow capabilities of the headquarters WAN router and the remote-site routers as shown in Figure 11.

Tech Tip

Either the Cisco Unified Communications (UC) or DATA technology packages are required in order to enable PerfMon on a Cisco ISR G2 series router. The Advanced Enterprise feature license is required in order to enable PerfMon on a Cisco ASR 1000 series router.

Notes

Figure 11 - PerfMon in Cisco SBA Foundation with UC and video



PerfMon is enabled on the WAN routers used in the Cisco SBA reference design. The WAN-aggregation routers should monitor both the LAN-facing and WAN-facing interfaces, with the exception of the port-channel interfaces of the Cisco ASR 1000 Series, as shown in Figure 12. Remote-site routers should monitor WAN-facing interfaces and either access-layer or distribution-layer-facing interfaces as shown in Figure 13.

Figure 12 - Where to use PerfMon—WAN aggregation

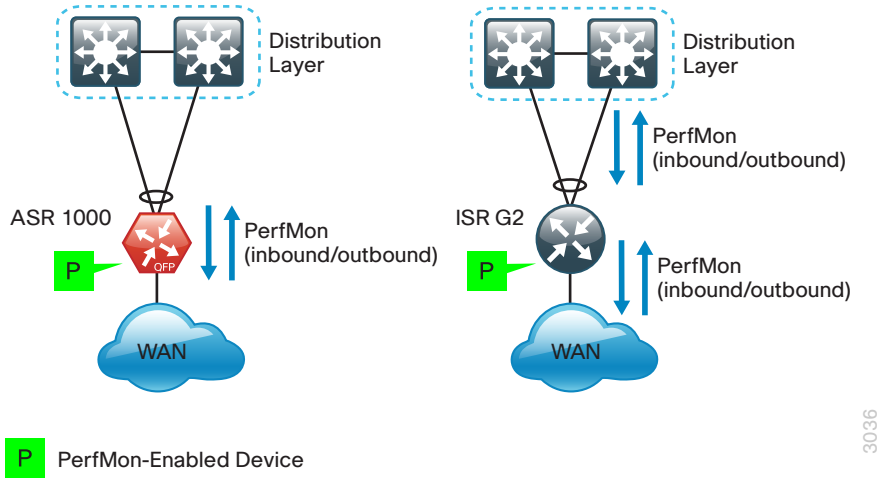
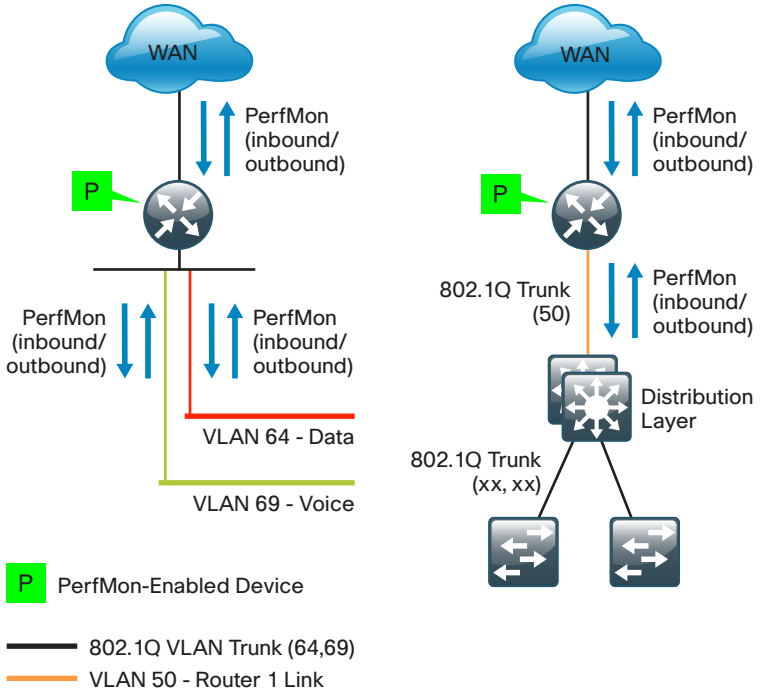


Figure 13 - Where to use PerfMon—WAN remote sites



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 WAN-aggregation routers 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 you create the flow monitor in a subsequent procedure.

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

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

Procedure 2 Create a flow exporter

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

Different Cisco 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 the following table.

Table 4 - Tested Cisco Medianet PerfMon collector parameters

Vendor	ActionPacked!	Plixer	SevOne
Application	LiveAction	Scrutinizer	Performance Appliance Solution
Version	2.6	10.0.0.23643	5.1.0.0
Capability	Flexible NetFlow	Flexible NetFlow	Flexible NetFlow
Export protocol	Netflow-v9	Netflow-v9	Netflow-v9
Destination port	UDP 2055	UDP 2055	UDP 9996

Step 1: Configure a basic flow exporter.

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

Step 2: If you are using the Cisco ISR G2 series routers, enable **output-features**. Otherwise, PerfMon traffic that originates from a WAN remote-site router will not be encrypted or tagged using QoS.

```
flow exporter [exporter name]
 output-features
```

Example (Plixer)

```
flow exporter Export-FNF-Plixer
 description FNF v9
 destination 10.4.48.171
 source Loopback0
 output-features  ! this command is not required on ASR1000
routers
 transport udp 2055
 export-protocol netflow-v9
 option interface-table
```

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 use 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 5 - 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 then 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).

If required, add additional parameters as shown in Table 5.

```
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 the following table.

Table 6 - 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 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 1.00
   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

Monitoring Video Sessions with PerfMon

1. View raw session data by IP address
2. View raw session data by SSRC
3. Configure LiveAction to generate alerts
4. Viewing alerts with LiveAction

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.

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 10.5.83.40 255.255.255.255 10.4.4.40 255.255.255.255
Match: ipv4 src addr = 10.5.83.40, ipv4 dst addr = 10.4.4.40,
ipv4 prot = udp, trns src port = 2348, trns dst port = 2462,
SSRC = 678320594
 Policy: PerfMon-Baseline, Class: INTERACTIVE-VIDEO,
Interface: GigabitEthernet0/0, Direction: output


 *counter flow                                    : 7
  counter bytes                                   : 2149488
  counter bytes rate                    (Bps)     : 10235
 *counter bytes rate per flow           (Bps)     : 10235
 *counter bytes rate per flow min       (Bps)     : 10196
 *counter bytes rate per flow max       (Bps)     : 10248
  counter packets                                 : 10500
 *counter packets rate per flow                   : 50
  counter packets dropped                         : 0
  routing forwarding-status reason                : Unknown
  interface input                                 : Po1.50
  interface output                                : Gi0/0
```

```
 monitor event                                  : false
 ipv4 dscp                                      : 34
 ipv4 ttl                                       : 62
 application media bytes counter                : 1939488
 application media packets counter              : 10500
 application media bytes rate                (Bps) : 9235
*application media bytes rate per flow       (Bps) : 9235
*application media bytes rate per flow min   (Bps) : 9200
*application media bytes rate per flow max   (Bps) : 9247
 application media packets rate              (pps) : 50
 application media event                        : Normal
*transport rtp flow count                       : 7
 transport rtp jitter mean                  (usec) : 41
 transport rtp jitter minimum               (usec) : 0
 transport rtp jitter maximum               (usec) : 739
*transport rtp payload type                     : 103
 transport event packet-loss counter            : 0
*transport event packet-loss counter min        : 0
*transport event packet-loss counter max        : 0
 transport packets expected counter             : 10500
 transport packets lost counter                 : 0
*transport packets lost counter minimum         : 0
*transport packets lost counter maximum         : 0
 transport packets lost rate                ( % ) : 0.00
*transport packets lost rate min            ( % ) : 0.00
*transport packets lost rate max            ( % ) : 0.00
```

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]
```

Example

```
Router#show performance monitor status ssrc any
  Match: ipv4 src addr = 10.4.4.40, ipv4 dst addr =
10.5.83.40, ipv4 prot = udp, trns src port = 2462, trns dst
port = 2348, SSRC = 356156570
 Policy: PerfMon-Baseline, Class: INTERACTIVE-VIDEO,
Interface: GigabitEthernet0/0, Direction: input


 *counter flow                                  : 10
  counter bytes                                 : 3078176
  counter bytes rate                      (Bps) : 10260
 *counter bytes rate per flow             (Bps) : 10260
 *counter bytes rate per flow min         (Bps) : 10243
 *counter bytes rate per flow max         (Bps) : 10282
  counter packets                               : 15010
 *counter packets rate per flow                 : 50
  counter packets dropped                       : 0
  routing forwarding-status reason              : Unknown
  interface input                               : Gi0/0
  interface output                              : Po1.50
  monitor event                                 : false
  ipv4 dscp                                     : 34
  ipv4 ttl                                      : 56
  application media bytes counter               : 2777976
  application media packets counter             : 15010
  application media bytes rate            (Bps) : 9259
 *application media bytes rate per flow   (Bps) : 9259
 *application media bytes rate per flow min (Bps) : 9245
 *application media bytes rate per flow max (Bps) : 9280
  application media packets rate          (pps) : 50
  application media event                       : Normal
 *transport rtp flow count                      : 10
  transport rtp jitter mean                (usec) : 81
  transport rtp jitter minimum             (usec) : 0
  transport rtp jitter maximum             (usec) : 916
 *transport rtp payload type                    : 103
```

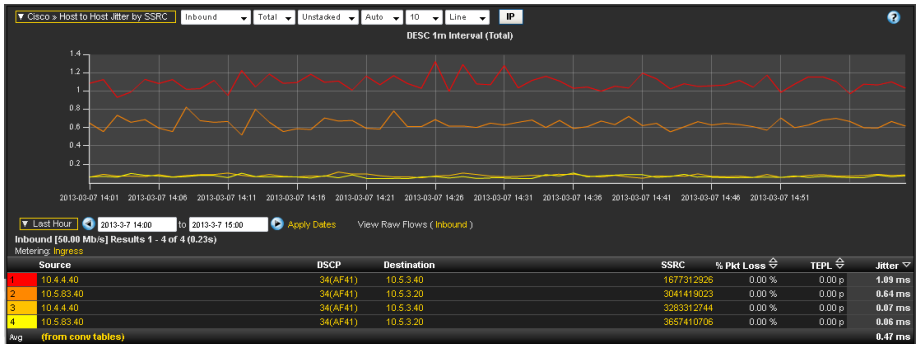
```
 transport event packet-loss counter                  : 0
*transport event packet-loss counter min              : 0
*transport event packet-loss counter max              : 0
 transport packets expected counter                   : 15010
 transport packets lost counter                       : 0
*transport packets lost counter minimum               : 0
*transport packets lost counter maximum               : 0
 transport packets lost rate                  ( % )   : 0.00
*transport packets lost rate min              ( % )   : 0.00
*transport packets lost rate max              ( % )   : 0.00
```

Creating 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.

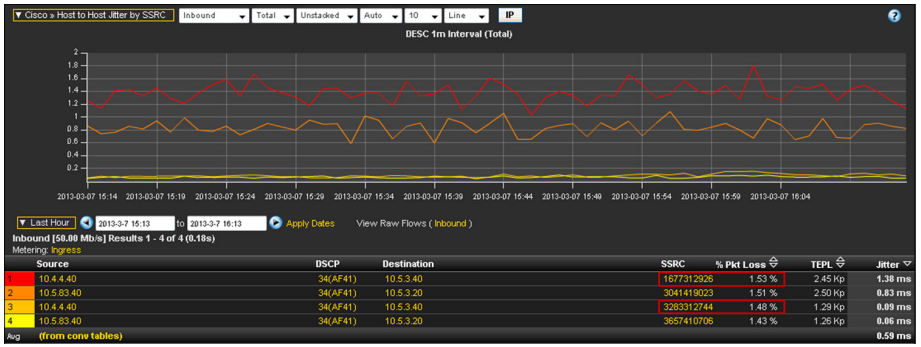
This section highlights the types of reports that are available from Plixer Scrutinizer and ActionPacked! LiveAction. One of the most effective reports lists all of the RTP data streams by specific SSRC in a table, which breaks out the audio and video streams of a video conference into its separate components. The jitter values graphed in the following figure indicate that the listed sessions as reported by a remote-site WAN router are consistently jitter-free (less than 2 ms).

Figure 14 - Plixer Scrutinizer (remote site)—host-to-host jitter by SSRC (loss free)



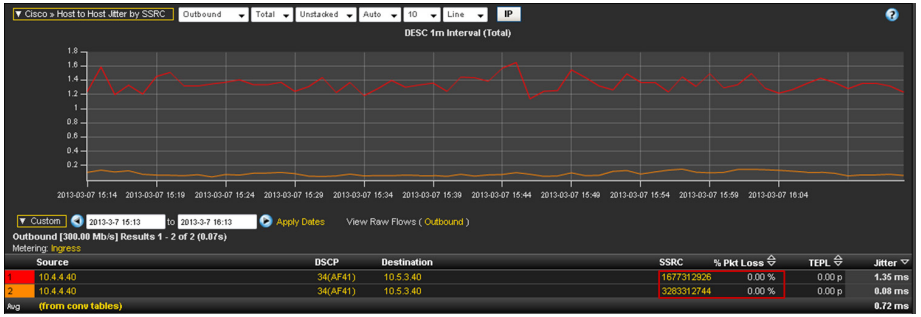
PerfMon is well-suited for identifying, isolating, and correcting video-related network problems. Using PerfMon data from WAN routers, you can generate reports that include loss values for active video sessions. The highlighted information in Figure 15 shows a set of two RTP streams with the same source and destination and different SSRCs, corresponding to the audio and video components of a video session. Each stream has significant packet loss. Another pair of streams visible on this PerfMon device is also experiencing significant loss.

Figure 15 - Plixer Scrutinizer (remote site)—host-to-host jitter by SSRC (loss conditions present)



It is important to note that although the monitoring was done inbound at this observation point (a remote site), the loss was induced upstream. To further isolate the source of the loss, another observation must be used. The highlighted information in Figure 16 shows the same video session with monitoring applied outbound on an upstream router (the primary site).

Figure 16 - Plixer Scrutinizer (primary site) —host-to-host jitter by SSRC (no loss observed)



From the information shown in the previous figures, the network operator can infer that the loss was introduced in the WAN between the primary site and the remote site.

Procedure 3 Configure LiveAction to generate alerts

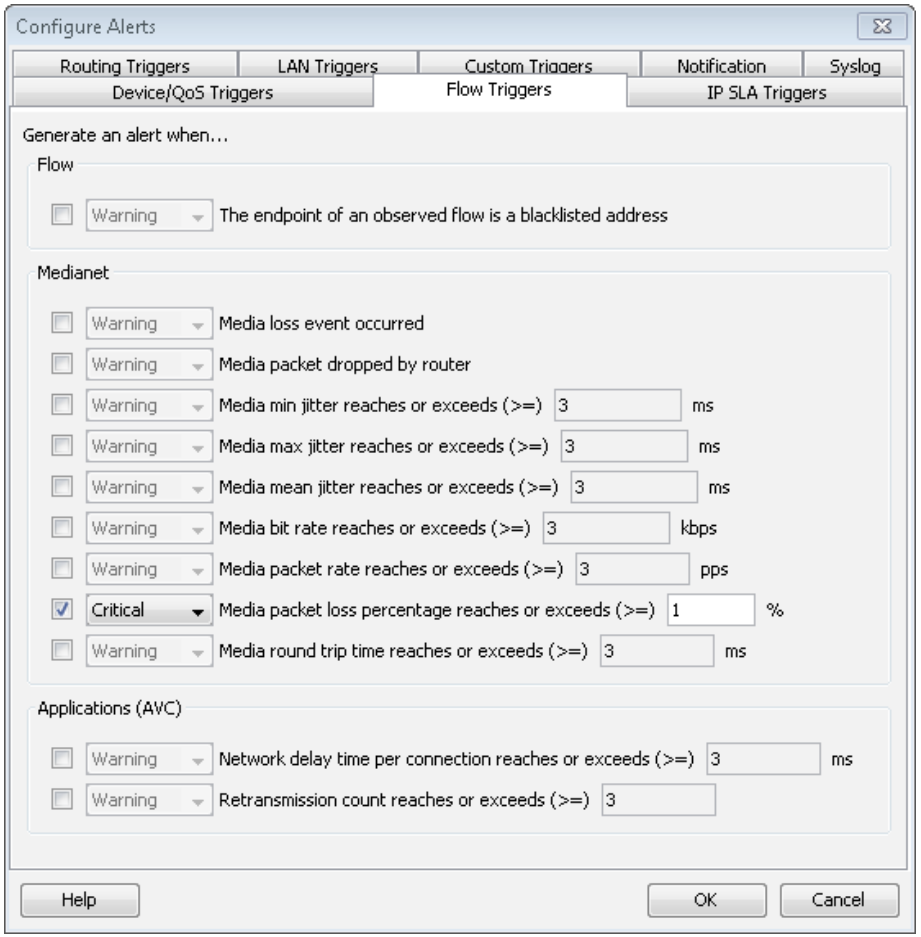
Another benefit of using a centralized collector is the ability to generate alerts when certain performance thresholds are exceeded. Using the collector for this purpose complements the capability of the PerfMon devices to send TCAs and helps to isolate which sites are affected.

Step 1: Launch the ActionPacked! Live Action application and log in.

Step 2: Navigate to **Tools** > **Configure Alerts**.

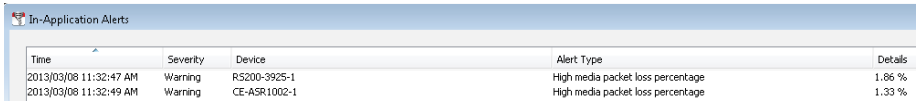
Step 3: Click the **Flow Triggers** tab.

Step 4: In the Medianet pane, select **Media packet loss percentage reaches or exceeds (>=)**, choose a severity (example: Critical), set the percentage to the desired value (example: 1%), and then click **OK**.



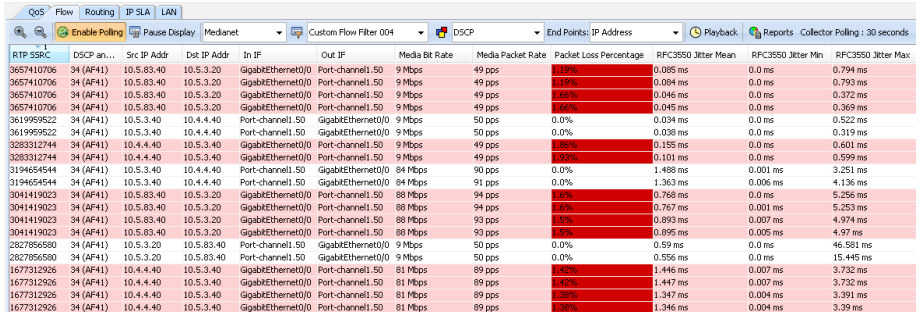
Procedure 4 Viewing alerts with LiveAction

Step 1: Navigate to **Tools** > **View Alerts**. This launches the In-Application Alerts reporting screen.



Flows affected by the specified alert are highlighted in the Medianet flow table for the reporting device.

Figure 17 - ActionPacked! LiveAction (remote site)–Medianet flow table



Notes

Appendix A: Product List

WAN Aggregation

Functional Area	Product Description	Part Numbers	Software
WAN-aggregation Router	Aggregation Services 1002 Router	ASR1002-5G-VPN/K9	IOS-XE 15.2(2)S2 Advanced Enterprise license
	Aggregation Services 1001 Router	ASR1001-2.5G-VPNK9	
WAN-aggregation Router	Cisco 3945 Security Bundle w/SEC license PAK	CISCO3945-SEC/K9	15.1(4)M5 securityk9 license datak9 license
	Cisco 3925 Security Bundle w/SEC license PAK	CISCO3925-SEC/K9	
	Data Paper PAK for Cisco 3900 series	SL-39-DATA-K9	

WAN Remote Site

Functional Area	Product Description	Part Numbers	Software
Modular WAN Remote-site Router	Cisco 3945 Voice Sec. Bundle, PVDM3-64, UC and SEC License PAK	C3945-VSEC/K9	15.1(4)M5 securityk9 license datak9 license
	Cisco 3925 Voice Sec. Bundle, PVDM3-64, UC and SEC License PAK	C3925-VSEC/K9	
	Data Paper PAK for Cisco 3900 series	SL-39-DATA-K9	
	Cisco 2951 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2951-VSEC/K9	
	Cisco 2921 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2921-VSEC/K9	
	Cisco 2911 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2911-VSEC/K9	
	Data Paper PAK for Cisco 2900 series	SL-29-DATA-K9	
	1941 WAAS Express only Bundle	C1941-WAASX-SEC/K9	
	Data Paper PAK for Cisco 1900 series	SL-19-DATA-K9	
Fixed WAN Remote-site Router	Cisco 881 SRST Ethernet Security Router with FXS FXO 802.11n FCC Compliant	C881SRST-K9	15.1(4)M5 Advanced IP license

Appendix B: Medianet-Enabled Device Configuration

PerfMon-Enabled Cisco ASR 1000 Series Router

```
version 15.2
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
no platform punt-keepalive disable-kernel-core
!
hostname CE-ASR1002-1
!
boot-start-marker
boot-end-marker
!
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
enable secret 4 /DtCCr53Q4B18jSIm1UEqu7cNVZTOhxTZyUnZdsSrsw
!
aaa new-model
!
!
aaa group server tacacs+ TACACS-SERVERS
 server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
!
!
!
!
!
aaa session-id common
clock timezone PST -8 0
clock summer-time PDT recurring
!
!
flow exporter Export-FNF-Plixer
 description FNF v9
 destination 10.4.48.171
 source Loopback0
 transport udp 2055
 option interface-table
 option application-table
!
!
flow exporter Export-FNF-LiveAction
 description FNF v9
 destination 10.4.48.178
 source Loopback0
 transport udp 2055
 option interface-table
 option application-table
!
!
flow exporter Export-FNF-SevOne
 description FNF v9
```

```
 destination 10.4.48.172
 source Loopback0
 transport udp 9996
 option interface-table
 option application-table
!
!
flow monitor type performance-monitor PerfMon-All-RTP
 description PerfMon RTP
 record default-rtp
 exporter Export-FNF-Plixer
 exporter Export-FNF-LiveAction
 exporter Export-FNF-SevOne
!
!
flow monitor type performance-monitor PerfMon-All-TCP
 description PerfMon TCP
 record default-tcp
 exporter Export-FNF-Plixer
 exporter Export-FNF-LiveAction
 exporter Export-FNF-SevOne
!
!
ip domain name cisco.local
ip multicast-routing distributed
!
!
ip wccp 61 redirect-list WAAS-REDIRECT-LIST group-list WAVE
password 7 130646010803557878
ip wccp 62 redirect-list WAAS-REDIRECT-LIST group-list WAVE
password 7 03070A180500701E1D
!
!
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
username admin password 7 03070A180500701E1D
!
redundancy
 mode none
!
!
!
!
!
!
ip ssh source-interface Loopback0
ip ssh version 2
!
class-map match-any DATA
 match dscp af21
class-map match-any BGP-ROUTING
 match protocol bgp
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 dscp cs1  af11
class-map match-any TP-MEDIA
 match protocol telepresence-media
class-map match-any NETWORK-CRITICAL
 match dscp cs2  cs6
!
```

```
policy-map MARK-BGP
 class BGP-ROUTING
  set dscp 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
   service-policy MARK-BGP
 class class-default
  bandwidth percent 25
  random-detect
policy-map WAN-INTERFACE-G0/0/3
 class class-default
  shape average 300000000
   service-policy WAN
policy-map type performance-monitor PerfMon-Baseline
 description PerfMon Baseline
 class INTERACTIVE-VIDEO
   react 10 transport-packets-lost-rate
    description Check for > 1% loss
    threshold value gt 1.00
    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
   flow monitor PerfMon-All-RTP
 class TP-MEDIA
   monitor metric rtp
    clock-rate 96 48000
    clock-rate 101 8000
   flow monitor PerfMon-All-RTP
 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 10.4.32.241 255.255.255.255
 ip pim sparse-mode
!
interface Port-channel1
 ip address 10.4.32.2 255.255.255.252
 ip wccp 61 redirect in
 ip pim sparse-mode
 no negotiation auto
!
interface GigabitEthernet0/0/0
 description WAN-D3750X Gig1/0/1
 no ip address
 negotiation auto
 channel-group 1
```

```
!
interface GigabitEthernet0/0/1
 description WAN-D3750X Gig2/0/1
 no ip address
 negotiation auto
 channel-group 1
!
interface GigabitEthernet0/0/2
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/0/3
 description MPLS WAN Uplink
 bandwidth 300000
 ip address 192.168.3.1 255.255.255.252
 ip wccp 62 redirect in
 negotiation auto
 service-policy output WAN-INTERFACE-G0/0/3
 service-policy type performance-monitor input PerfMon-Baseline
 service-policy type performance-monitor output PerfMon-Baseline
!
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
!
!
router eigrp 100
 distribute-list route-map BLOCK-TAGGED-ROUTES in
 default-metric 300000 100 255 1 1500
 network 10.4.0.0 0.1.255.255
 redistribute bgp 65511
 passive-interface default
 no passive-interface Port-channel1
 eigrp router-id 10.4.32.241
!
router bgp 65511
 bgp router-id 10.4.32.241
 bgp log-neighbor-changes
 network 0.0.0.0
 network 192.168.3.0 mask 255.255.255.252
 redistribute eigrp 100
 neighbor 10.4.32.242 remote-as 65511
 neighbor 10.4.32.242 update-source Loopback0
 neighbor 10.4.32.242 next-hop-self
 neighbor 192.168.3.2 remote-as 65401
!
ip forward-protocol nd
!
no ip http server
ip http authentication aaa
ip http secure-server
ip pim autorp listener
ip pim register-source Loopback0
ip tacacs source-interface Loopback0
!
ip access-list standard WAVE
 permit 10.4.32.162
 permit 10.4.32.161
!
ip access-list extended WAAS-REDIRECT-LIST
 remark WAAS WCCP Redirect List
 deny   tcp any any eq 22
 deny   tcp any eq 22 any
 deny   tcp any eq telnet any
 deny   tcp any any eq telnet
 deny   tcp any eq tacacs any
 deny   tcp any any eq tacacs
 deny   tcp any eq bgp any
 deny   tcp any any eq bgp
 deny   tcp any any eq 123
 deny   tcp any eq 123 any
```

```
 permit tcp any any
!
logging 10.4.48.35
logging 10.4.48.38
logging 10.4.48.39
logging 10.4.48.48
!
route-map BLOCK-TAGGED-ROUTES deny 10
 match tag 65401 65402 65512
!
route-map BLOCK-TAGGED-ROUTES permit 20
!
snmp-server community cisco RO
snmp-server community cisco123 RW
snmp-server trap-source Loopback0
snmp-server host 10.4.48.38 cisco
snmp-server host 10.4.48.35 cisco123
snmp-server host 10.4.48.39 cisco123
snmp-server host 10.4.48.48 cisco123
!
tacacs server TACACS-SERVER-1
 address ipv4 10.4.48.15
 key 7 00371605165E1F2D0A38
!
!
control-plane
!
!
!
!
!
line con 0
 logging synchronous
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 transport preferred none
 transport input ssh
line vty 5 15
 transport preferred none
 transport input ssh
!
ntp source Loopback0
ntp server 10.4.48.17
!
end
```

PerfMon-Enabled Cisco ISR G2 Series Routers

Remote Site with Access Layer (RS201)

```
version 15.1
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname RS201-2911
!
boot-start-marker
boot system flash:c2900-universalk9-mz.SPA.151-4.M5.bin
boot-end-marker
!
!
enable secret 4 /DtCCr53Q4B18jSIm1UEqu7cNVZTOhxTZyUnZdsSrsw
!
aaa new-model
!
!
aaa group server tacacs+ TACACS-SERVERS
 server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authentication login MODULE none
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
!
!
!
!
!
aaa session-id common
!
clock timezone PST -8 0
clock summer-time PDT recurring
!
no ipv6 cef
!
!
flow exporter Export-FNF-LiveAction
 description FNF v9
 destination 10.4.48.178
 source Loopback0
 output-features
 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-LiveAction
!
!
flow monitor type performance-monitor PerfMon-All-TCP
 description PerfMon TCP
 record default-tcp
 exporter Export-FNF-LiveAction
!
!
ip source-route
ip cef
!
!
!
ip vrf INET-PUBLIC1
 rd 65512:1
!
ip multicast-routing
!
!
```

```
ip domain name cisco.local
ip wccp 61 redirect-list WAAS-REDIRECT-LIST group-list WAVE
password 7 141443180F0B7B7977
ip wccp 62 redirect-list WAAS-REDIRECT-LIST group-list WAVE
password 7 04585A150C2E1D1C5A
!
multilink bundle-name authenticated
!
!
!
!
voice-card 0
 dspfarm
 dsp services dspfarm
!
!
!
!
!
!
!
license udi pid CISCO2911/K9 sn FTX1451AHP7
license boot module c2900 technology-package securityk9
hw-module pvdm 0/0
!
hw-module sm 1
!
!
!
username admin password 7 06055E324F41584B56
!
redundancy
!
!
!
!
ip ssh source-interface Loopback0
ip ssh version 2
!
class-map match-any DATA
 match  dscp af21
class-map match-any BGP-ROUTING
 match protocol bgp
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  dscp cs1  af11
class-map match-any TP-MEDIA
 match protocol telepresence-media
class-map match-any NETWORK-CRITICAL
 match  dscp cs2  cs6
 match access-group name ISAKMP
!
!
policy-map MARK-BGP
 class BGP-ROUTING
  set dscp 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
  service-policy MARK-BGP
 class class-default
  bandwidth percent 25
  random-detect
policy-map WAN-INTERFACE-G0/1
 class class-default
  shape average 10000000
  service-policy WAN
policy-map WAN-INTERFACE-G0/0
 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 1.00
    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
!
!
crypto keyring DMVPN-KEYRING1 vrf INET-PUBLIC1
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 2
!
crypto isakmp keepalive 30 5
crypto isakmp profile FVRF-ISAKMP-INET-PUBLIC1
   keyring DMVPN-KEYRING1
   match identity address 0.0.0.0 INET-PUBLIC1
!
!
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-
sha-hmac
 mode transport
!
crypto ipsec profile DMVPN-PROFILE1
 set transform-set AES256/SHA/TRANSPORT
 set isakmp-profile FVRF-ISAKMP-INET-PUBLIC1
!
!
!
!
!
interface Loopback0
 ip address 10.255.251.201 255.255.255.255
 ip pim sparse-mode
!
interface Tunnel10
```

```
 bandwidth 10000
 ip address 10.4.34.201 255.255.254.0
 no ip redirects
 ip mtu 1400
 ip wccp 62 redirect in
 ip pim dr-priority 0
 ip pim nbma-mode
 ip pim sparse-mode
 ip hello-interval eigrp 200 20
 ip hold-time eigrp 200 60
 ip nhrp authentication cisco123
 ip nhrp map 10.4.34.1 172.16.130.1
 ip nhrp map multicast 172.16.130.1
 ip nhrp network-id 101
 ip nhrp holdtime 600
 ip nhrp nhs 10.4.34.1
 ip nhrp registration no-unique
 ip nhrp shortcut
 ip nhrp redirect
 ip tcp adjust-mss 1360
 ip summary-address eigrp 200 10.5.40.0 255.255.248.0
 tunnel source GigabitEthernet0/1
 tunnel mode gre multipoint
 tunnel vrf INET-PUBLIC1
 tunnel protection ipsec profile DMVPN-PROFILE1
 service-policy type performance-monitor input PerfMon-Baseline
 service-policy type performance-monitor output PerfMon-Baseline
!
interface Port-channel1
 description EtherChannel Link to RS201-2960S
 no ip address
!
interface Port-channel1.64
 description Wired_Data
 encapsulation dot1Q 64
 ip address 10.5.44.1 255.255.255.0
 ip helper-address 10.4.48.10
 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
!
interface Port-channel1.69
 description Wired_Voice
 encapsulation dot1Q 69
 ip address 10.5.45.1 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim sparse-mode
 service-policy type performance-monitor input PerfMon-Baseline
 service-policy type performance-monitor output PerfMon-Baseline
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 bandwidth 10000
 ip address 192.168.3.21 255.255.255.252
 ip wccp 62 redirect in
 duplex auto
 speed auto
 no cdp enable
 service-policy output WAN-INTERFACE-G0/0
 service-policy type performance-monitor input PerfMon-Baseline
 service-policy type performance-monitor output PerfMon-Baseline
!
interface GigabitEthernet0/1
 ip vrf forwarding INET-PUBLIC1
 ip address dhcp
 ip access-group ACL-INET-PUBLIC in
 duplex auto
 speed auto
 no cdp enable
 service-policy output WAN-INTERFACE-G0/1
```

```
!
interface GigabitEthernet0/2
 description RS201-A2960S Gig1/0/24
 no ip address
 duplex auto
 speed auto
 channel-group 1
!
interface GigabitEthernet0/0/0
 description RS201-A2960S Gig2/0/24
 no ip address
 duplex auto
 speed auto
 channel-group 1
!
interface SM1/0
 ip address 192.0.2.2 255.255.255.252
 service-module external ip address 10.5.44.8 255.255.255.0
 !Application: Restarted at Wed Jan  2 04:14:46 2013
 service-module ip default-gateway 10.5.44.1
!
interface SM1/1
 description Internal switch interface connected to Service
Module
 no ip address
!
interface Vlan1
 no ip address
!
!
!
router eigrp 200
 network 10.4.34.0 0.0.1.255
 network 10.5.0.0 0.0.255.255
 network 10.255.0.0 0.0.255.255
 passive-interface default
 no passive-interface Tunnel10
 eigrp router-id 10.255.251.201
 eigrp stub connected summary
!
router bgp 65511
 bgp router-id 10.255.251.201
 bgp log-neighbor-changes
 network 10.5.44.0 mask 255.255.255.0
 network 10.5.45.0 mask 255.255.255.0
 network 10.255.251.201 mask 255.255.255.255
 network 192.168.3.20 mask 255.255.255.252
 aggregate-address 10.5.40.0 255.255.248.0 summary-only
 neighbor 192.168.3.22 remote-as 65401
!
ip forward-protocol nd
!
ip pim autorp listener
ip pim register-source Loopback0
no ip http server
ip http authentication aaa
ip http secure-server
!
ip tacacs source-interface Loopback0
!
ip access-list standard WAVE
 permit 10.5.44.8
!
ip access-list extended ISAKMP
 permit udp any eq isakmp any eq isakmp
ip access-list extended WAAS-REDIRECT-LIST
 remark WAAS WCCP Redirect List
 deny   tcp any any eq 22
 deny   tcp any eq 22 any
 deny   tcp any eq telnet any
 deny   tcp any any eq telnet
 deny   tcp any eq tacacs any
 deny   tcp any any eq tacacs
 deny   tcp any eq bgp any
```

```
 deny   tcp any any eq bgp
 deny   tcp any any eq 123
 deny   tcp any eq 123 any
 permit tcp any any
!
logging trap debugging
logging 10.4.48.38
logging 10.4.48.35
logging 10.4.48.39
logging 10.4.48.48
access-list 55 permit 10.4.48.0 0.0.0.255
access-list 67 permit 192.0.2.2
!
!
!
!
!
snmp-server community cisco RO 55
snmp-server community cisco123 RW 55
snmp-server trap-source Loopback0
snmp-server host 10.4.48.35 cisco
snmp-server host 10.4.48.38 cisco
snmp-server host 10.4.48.35 cisco123
snmp-server host 10.4.48.39 cisco123
snmp-server host 10.4.48.48 cisco123
tacacs server TACACS-SERVER-1
 address ipv4 10.4.48.15
 key 7 0812494D1B1C113C1712
!
!
!
control-plane
!
!
ccm-manager sccp local Loopback0
!
!
mgcp profile default
!
!
gatekeeper
 shutdown
!
!
!
line con 0
 logging synchronous
line aux 0
line 2
 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 67
 access-class 67 in
 login authentication MODULE
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output none
 stopbits 1
line vty 0 4
 access-class 55 in
 transport preferred none
 transport input ssh
line vty 5 15
 access-class 55 in
 transport preferred none
 transport input ssh
!
```

```
scheduler allocate 20000 1000
ntp source Loopback0
ntp update-calendar
ntp server 10.4.48.17
end
```

Remote Site with Distribution Layer (RS208)

```
version 15.1
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname RS208-2951-1
!
boot-start-marker
boot system flash flash:c2951-universalk9-mz.SPA.151-4.M5.bin
boot-end-marker
!
!
card type t1 0 0
! card type command needed for slot/vwic-slot 0/1
enable secret 4 /DtCCr53Q4B18jSIm1UEqu7cNVZTOhxTZyUnZdsSrsw
!
aaa new-model
!
!
aaa group server tacacs+ TACACS-SERVERS
 server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authentication login MODULE none
aaa authorization console
aaa authorization exec default group TACACS-SERVERS local
!
!
!
!
!
aaa session-id common
!
clock timezone PST -8 0
clock summer-time PDT recurring
network-clock-participate wic 0
!
no ipv6 cef
ipv6 spd queue min-threshold 62
ipv6 spd queue max-threshold 63
!
!
flow exporter Export-FNF-LiveAction
 description FNF v9
 destination 10.4.48.178
 source Loopback0
 output-features
 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-LiveAction
!
!
flow monitor type performance-monitor PerfMon-All-TCP
 description PerfMon TCP
 record default-tcp
 exporter Export-FNF-LiveAction
!
!
ip source-route
ip cef
!
```

```
!
!
ip multicast-routing
!
!
ip domain name cisco.local
ip wccp 61 redirect-list WAAS-REDIRECT-LIST group-list WAVE
password 7 104D580A061843595F
ip wccp 62 redirect-list WAAS-REDIRECT-LIST group-list WAVE
password 7 0205554808095E731F
!
multilink bundle-name authenticated
!
!
!
!
isdn switch-type primary-ni
!
voice-card 0
 dspfarm
 dsp services dspfarm
!
!
!
!
!
!
license udi pid CISCO2951/K9 sn FTX1440AKR8
license boot module c2951 technology-package securityk9
hw-module pvdm 0/0
!
hw-module sm 2
!
!
!
username admin password 7 011057175804575D72
!
redundancy
!
!
!
!
controller T1 0/0/0
 cablelength short 110
 pri-group timeslots 1-24
 description PSTN PRI
!
ip ssh source-interface Loopback0
ip ssh version 2
!
class-map match-any DATA
 match  dscp af21
class-map match-any BGP-ROUTING
 match protocol bgp
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  dscp cs1  af11
class-map match-any TP-MEDIA
 match protocol telepresence-media
class-map match-any NETWORK-CRITICAL
 match  dscp cs2  cs6
!
!
policy-map MARK-BGP
 class BGP-ROUTING
  set dscp 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
  service-policy MARK-BGP
 class class-default
  bandwidth percent 25
  random-detect
policy-map WAN-INTERFACE-G0/0
 class class-default
  shape average 50000000
  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 1.00
    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 10.255.251.208 255.255.255.255
 ip pim sparse-mode
!
interface Port-channel1
 description EtherChannel link to RS208-D3750X
 no ip address
 hold-queue 150 in
!
interface Port-channel1.50
 description R1 routed link to distribution layer RS208-D3750X
 encapsulation dot1Q 50
 ip address 10.5.80.1 255.255.255.252
 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
!
interface Port-channel1.99
 description Transit Net
 encapsulation dot1Q 99
 ip address 10.5.80.9 255.255.255.252
 ip pim sparse-mode
```

```
 service-policy type performance-monitor input PerfMon-Baseline
 service-policy type performance-monitor output PerfMon-Baseline
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 bandwidth 50000
 ip address 192.168.3.45 255.255.255.252
 ip wccp 62 redirect in
 duplex auto
 speed auto
 service-policy output WAN-INTERFACE-G0/0
 service-policy type performance-monitor input PerfMon-Baseline
 service-policy type performance-monitor output PerfMon-Baseline
!
interface GigabitEthernet0/1
 description RS208-D3750X Gig1/0/12
 no ip address
 duplex auto
 speed auto
 channel-group 1
!
interface GigabitEthernet0/2
 description RS208-D3750X Gig2/0/12
 no ip address
 duplex auto
 speed auto
 channel-group 1
!
interface Serial0/0/0:23
 no ip address
 encapsulation hdlc
 isdn switch-type primary-ni
 isdn incoming-voice voice
 no cdp enable
!
interface SM2/0
 ip address 192.0.2.2 255.255.255.252
 service-module external ip address 10.5.87.8 255.255.255.0
 !Application: Restarted at Wed Jan  2 04:15:41 2013
 service-module ip default-gateway 10.5.87.1
!
interface SM2/1
 description Internal switch interface connected to Service
Module
 no ip address
 shutdown
!
interface Vlan1
 no ip address
!
!
router eigrp 100
 default-metric 50000 100 255 1 1500
 network 10.4.0.0 0.1.255.255
 network 10.5.0.0 0.0.255.255
 network 10.255.0.0 0.0.255.255
 redistribute bgp 65511
 passive-interface default
 no passive-interface Port-channel1.50
 no passive-interface Port-channel1.99
!
router bgp 65511
 bgp router-id 10.255.251.208
 bgp log-neighbor-changes
 network 10.5.81.0 mask 255.255.255.0
 network 10.5.82.0 mask 255.255.255.0
 network 10.255.251.208 mask 255.255.255.255
 network 10.255.252.208 mask 255.255.255.255
 network 192.168.3.44 mask 255.255.255.252
 aggregate-address 10.5.80.0 255.255.248.0 summary-only
 neighbor 10.5.80.10 remote-as 65511
 neighbor 10.5.80.10 next-hop-self
 neighbor 192.168.3.46 remote-as 65401
```

```
 neighbor 192.168.3.46 route-map PREFER-MPLS-A in
 neighbor 192.168.3.46 route-map NO-TRANSIT-AS out
!
ip forward-protocol nd
!
ip as-path access-list 1 permit _65401$
ip as-path access-list 10 permit ^$
ip pim autorp listener
ip pim register-source Loopback0
no ip http server
ip http authentication aaa
ip http secure-server
!
ip tacacs source-interface Loopback0
!
ip access-list standard WAVE
 permit 10.5.87.8
 permit 10.5.87.9
!
ip access-list extended WAAS-REDIRECT-LIST
 remark WAAS WCCP Redirect List
 deny   tcp any any eq 22
 deny   tcp any eq 22 any
 deny   tcp any eq telnet any
 deny   tcp any any eq telnet
 deny   tcp any eq tacacs any
 deny   tcp any any eq tacacs
 deny   tcp any eq bgp any
 deny   tcp any any eq bgp
 deny   tcp any any eq 123
 deny   tcp any eq 123 any
 permit tcp any any
!
logging 10.4.48.38
logging 10.4.48.35
logging 10.4.48.39
logging 10.4.48.48
access-list 67 permit 192.0.2.2
!
!
!
!
nls resp-timeout 1
cpd cr-id 1
route-map NO-TRANSIT-AS permit 10
 match as-path 10
!
route-map PREFER-MPLS-A permit 10
 match as-path 1
 set local-preference 200
!
route-map PREFER-MPLS-A permit 20
!
!
snmp-server community cisco RO
snmp-server community cisco123 RW
snmp-server trap-source Loopback0
snmp-server host 10.4.48.38 cisco
snmp-server host 10.4.48.35 cisco123
snmp-server host 10.4.48.39 cisco123
snmp-server host 10.4.48.48 cisco123
tacacs server TACACS-SERVER-1
 address ipv4 10.4.48.15
 key 7 03375E08140A35674B10
!
!
!
control-plane
!
!
voice-port 0/0/0:23
!
!
!
mgcp profile default
!
```

```
!
!
gatekeeper
 shutdown
!
!
!
line con 0
 logging synchronous
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line 131
 access-class 67 in
 login authentication MODULE
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output none
 stopbits 1
line vty 0 4
 transport preferred none
 transport input ssh
line vty 5 15
 transport preferred none
 transport input ssh
!
scheduler allocate 20000 1000
ntp source Loopback0
ntp update-calendar
ntp server 10.4.48.17
end
```

Notes

Appendix C: Changes

This appendix summarizes the changes to this guide since the Cisco SBA February 2012 Series.

- We updated the guide to support up to 10,000 connected users.
- We added the Cisco ASR1000 Series router family.
- We updated the code version for the Cisco ISR platform.
- We added ActionPacked! LiveAction as a PerfMon collector and updated the software versions of other PerfMon collectors.
- We made changes to improve the readability and technical accuracy of this guide.

Notes

Feedback

Please use the feedback form to send comments and suggestions about this guide.

SMART BUSINESS ARCHITECTURE

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-0000325-1 3/13