

Aamer Akhter
Enterprise medianet, cisco Systems
EDCS-874767

Performance-Monitor and Mediatrace Early Field Trial (EFT) Quickstart

Last Updated: 7/28/2010

Performance-monitor is a Cisco IOS feature that measures user traffic performance, generates alerts based on thresholds, and reports via multiple management interfaces. Mediatrace is a Cisco IOS feature that discovers the routers and switches along an IP flow's path. Mediatrace can dynamically configure and retrieve general node information as well as flow specific metrics from the performance-monitor feature.

This document is a guide for quickly getting started with the Medianet[1] 2.0 video monitoring IOS features performance-monitor and mediatrace.

Requirements

Table 1: Basic Equipment Requirements

Item	Quantity	Notes
IOS router/switch with performance-monitor and mediatrace software	2	Currently, only the ISR series of platforms are available for EFT.
Traffic impairment device	1	General x86 PC can be used with free Cisco WAN-bridge live CD[2] . For more complex and custom impairments refer to Linux netem[3].
RTP/TCP traffic generator and sink	1 generator 1 sink	The generator and sink are used to generate and receive traffic for both mediatrace and performance-monitor to monitor. Examples of RTP generators: Cisco IP phones, Cisco Telepresence, Tandberg Video Conferencing equipment, Video LAN client[4], Cisco Video SLA Assessment Agent (VSAA), packETH [5], IOS IPSLA Video Operation (IPSLA-VO) Examples of RTP sinks: Cisco IP phones, Cisco Telepresence, Tandberg Video Conferencing equipment, Video LAN client, Cisco Video SLA Assessment Agent (VSAA), IPSLA VO
(optional) SNMP Trap receiver	1	Performance-monitor can send alerts via SNMP traps Examples include: Net-SNMP[6]
(optional) syslog server	1	Performance-monitor can send alerts via syslog Examples include: Syslog-ng[7] Windows specific: Tftpd32[8], Kiwi Free Syslog Server[9]
(optional) NetFlow collector	1	Performance-monitor is able to export flow statistics via NetFlowv9 Examples include: TBD
(optional) SNMP browser	1	Performance-monitor is able to present flow statistics via a SNMP MIB.

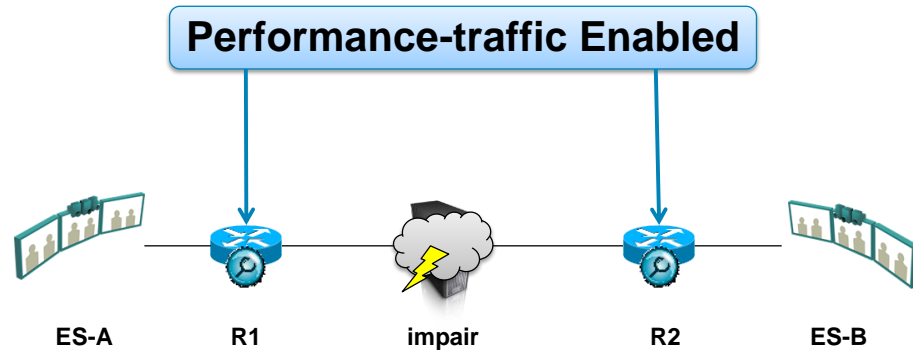


Figure 1: Basic Topology

Table 1 lists the minimal requirements for equipment and, topology and management systems. The implementor is free to add network nodes as well as end systems to align with their environment and needs. Figure 1 shows the most basic topology that will be needed to for the quick start. In the topology, it is important to note that the two monitoring points (R1 and R2) are on either side of the impairment device. This allows the monitoring points to provide before and after impairment perspectives. The management devices (syslog, SNMP etc) and infrastructure items such as the Cisco Unified Communications Manager (CUCM) and AAA server are not shown in the topology as their exact location is not important and only IP connectivity is required.

For the purposes of providing a variety of tangible examples, the basic topology has been augmented with multiple end systems as shown in Figure 2 below. The IP addressing and dial numbers shown in the diagram match the examples used in the paper. The basic configurations for the routers can be found in Appendix A.

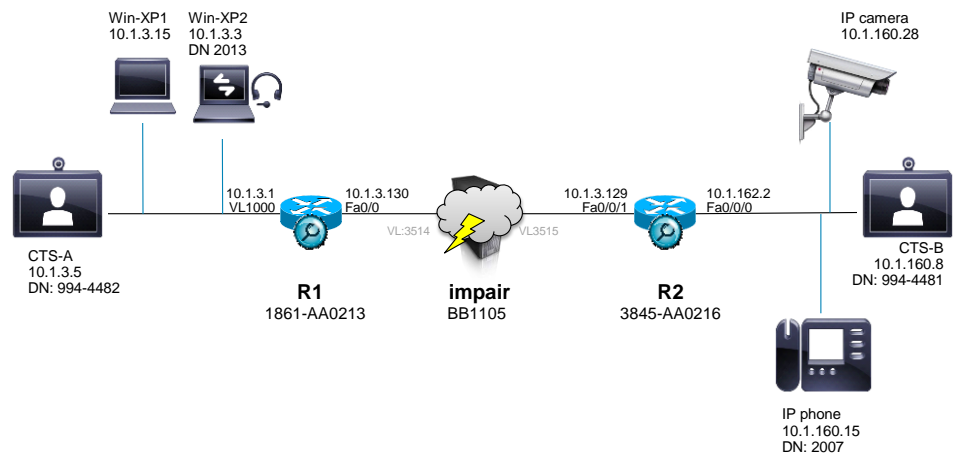


Figure 2: Test Topology

Performance-Monitor

Performance-monitor performs measurements on a specified set of traffic that is traversing a single router. The measurement point can be in a particular direction (ingress vs. egress) and on specific interfaces. By comparing the results of multiple measurement points, it is possible to create a storyline of the flow's progress within the network. Taking the topology in Figure 1 as an example: with R1 reporting 0% loss for the Cisco Telepresence System (CTS) flow and R2 reporting 10%

loss for the same flow, the operator can surmise that there is a problem in between R1 and R2. Alternatively, had both R1 and R2 reported no loss, the network operator would have validated that there is no packet loss in the span between R1 and R2.

A performance-monitor deployment should consider the following elements:

- **What traffic:** Which applications/traffic to monitor, and show within the network
- **What information:** What information to gather about the traffic flows
- **Where to monitor:** Which routers/switches will have measurement points. On a router, which interface and in which direction will the measurement occur.
- **Service targets:** Are there any service level agreements to measure the traffic against
- **Where to send information:** How will the flow metrics be made available to network management software

The Quick Inline Configuration Method

Performance-monitor allows two major methods of configuration that follow the same model but provide different balances between flexibility and simplified configuration. The below configuration is using the inline (quick) method employing a default metric collection profile.

```
Interface FastEthernet0/0
 service-policy type performance-traffic inline input
 match dscp cs5 ef af41
 flow monitor inline
 record default-rtp
 react 1 rtp-lost-fraction
 threshold value gt 10.00
 alarm severity error
 action syslog
end
```

Figure 3: Inline configuration example

Even this simple configuration can be broken down into the 5 deployment elements mentioned earlier:

Table 2: Breakdown of inline configuration example

Deployment Element	Configuration	Note
What Traffic	match dscp cs5 ef af41	All traffic that is marked with DSCP CS5, EF or AF41 will be subject to measurements.
What Information	flow monitor inline record default-rtp	The 'default-rtp' record defines best practice metrics to collect for RTP traffic. In our example, EF (VoIP), CS5 (Video Surveillance), and AF41 (Video Conferencing) traffic is based on RTP. The flow record is the only mandatory configuration in the inline configuration model. All other items have defaults.
Where to measure	Interface FastEthernet0/0 service-policy type performance-traffic inline input	As the policy is applied in the input direction on FastE0/0, it is from this perspective that the matching and measurements will be made.
Service targets	react 1 rtp-lost-fraction threshold value gt 10.00 alarm severity error action syslog	One of the metrics collected by 'default-rtp' is rtp lost fraction. The react stanza creates a threshold that will declare a severity level 'error' alarm and, generate a syslog if the rtp loss is greater than 10%.

Where to send information	action syslog	<p>A NetFlow exporter might have been configured under the monitor stanza. However, there is no periodic export method configured in this example.</p> <p>If a syslog server is configured then the alert would be sent when the alarm is triggered as well as when it is cleared (for example, here, the alarm is triggered when rtp-lost-fraction goes above 10% and the alarm is cleared when it falls to below 10% again)</p> <p>Additionally, a MIB is available for polling flow statistics and alerts.</p>
---------------------------	----------------------	---

There are two pre-packaged flow records shipped with performance-monitor: 'default-rtp' and 'default-tcp. The 'default-rtp' record is shown below:

```
1861-AA0213#show flow record type performance-traffic default-rtp
Load for five secs: 6%/4%; one minute: 5%; five minutes: 5%
Time source is NTP, 03:37:04.288 EST Sun Jun 6 2010
flow record type performance-traffic default-rtp:
  Description:          VM default RTP record
  No. of users:         1
  Total field space:    76 bytes
  Fields:
    match ipv4 protocol
    match ipv4 source address
    match ipv4 destination address
    match transport source-port
    match transport destination-port
    match transport rtp ssrc
    collect routing forwarding-status
    collect transport packets expected counter
    collect transport packets lost counter
    collect transport packets lost rate
    collect transport event packet-loss counter
    collect transport rtp jitter mean
    collect transport rtp jitter minimum
    collect transport rtp jitter maximum
    collect interface input
    collect interface output
    collect counter bytes rate
    collect timestamp interval
    collect application media bytes counter
    collect application media bytes rate
    collect application media packets counter
    collect application media event
    collect monitor event
```

Figure 4: Detail of pre-packaged 'default-rtp' flow record

Basic Observation of Traffic

In our test network, RTP video is being streamed from the IP camera (10.1.160.28) to Win-XP1 (10.1.3.15). The video surveillance traffic is set to DSCP CS5. Additionally, there is a video enabled VoIP call between the IP phone at 10.1.160.15 and a soft phone running on Win-XP2 (10.1.3.3). As this telephone case is video enabled, the DSCP value is set to AF41.

Performance traffic is now able to discover and measure the performance of the voice and video flows coming into R2 on FastE0/0.

Flow statistics filtered to show video IP phone:

3845-AA0216#show performance traffic status ip 10.1.160.31/32 any

```

3845-AA0216#show performance traffic status ip 10.1.160.31/32 any
Flow Spec: SrcAddress = 10.1.160.31, DstAddress = 10.1.3.3, Protocol =
udp, SrcPort = 20000, DstPort = 24584, SSRC = 1114735
Policy: inline, Class: inline, Interface: FastEthernet0/0/0, Direction:
input

Flow Status:

IP Stats:
Byte Count           : 3002000
Packet Count        : 15010
Drop Count          : 0
Byte Rate Average   : 10 kBps
Byte Rate Minimum   : 10 kBps
Byte Rate Maximum   : 10 kBps
Packet Rate         : 50 pps
TTL Average         : 59
TTL Minimum         : 0
TTL Maximum        : 59

Common Stats:
Event Lost Count Sum      : 0
Event Lost Count Minimum : 0
Event Lost Count Maximum : 0

Media Stats:
Byte Rate Average   : 9006 Bps
Byte Rate Minimum   : 9006 Bps
Byte Rate Maximum   : 9006 Bps
Media Event         : Media-Normal

RTP Stats:
Payload Type        : 0
Expected Packet Count : 15010
Packet Lost Count Sum : 0
Packet Lost Count Minimum : 0
Packet Lost Count Maximum : 0
Inter Arrival Jitter Average : 631 usec
Inter Arrival Jitter Minimum : 0 usec
Inter Arrival Jitter Maximum : 7052 usec
Fraction Lost Count Average : 0.00
Fraction Lost Count Minimum : 0.00
Fraction Lost Count Maximum : 0.00

Flow Spec: SrcAddress = 10.1.160.31, DstAddress = 10.1.3.3, Protocol =
udp, SrcPort = 20002, DstPort = 5445, SSRC = 3080896
Policy: inline, Class: inline, Interface: FastEthernet0/0/0, Direction:
input

Flow Status:

IP Stats:
Byte Count           : 1810887
Packet Count        : 9250
Drop Count          : 0
Byte Rate Average   : 6036 Bps
Byte Rate Minimum   : 5586 Bps
Byte Rate Maximum   : 7318 Bps
Packet Rate         : 30 pps
TTL Average         : 59

```

```

TTL Minimum           : 0
TTL Maximum           : 59

Common Stats:
Event Lost Count Sum   : 0
Event Lost Count Minimum : 0
Event Lost Count Maximum : 0

Media Stats:
Byte Rate Average      : 5419 Bps
Byte Rate Minimum      : 4974 Bps
Byte Rate Maximum      : 6680 Bps
Media Event            : Media-Normal

RTP Stats:
Payload Type           : 97
Expected Packet Count  : 9250
Packet Lost Count Sum  : 0
Packet Lost Count Minimum : 0
Packet Lost Count Maximum : 0
Inter Arrival Jitter Average : 4705 usec
Inter Arrival Jitter Minimum : 1 usec
Inter Arrival Jitter Maximum : 34569 usec
Fraction Lost Count Average : 0.00
Fraction Lost Count Minimum : 0.00
Fraction Lost Count Maximum : 0.00

```

Figure 5: 3845-AA0216 measurements for traffic coming from video phone

In the 'show performance traffic status' output the statistics are broken down into sections depending on the measurement layer. As the IP phone is sending voice and video we are seeing two RTP flows (SSRC=1114735 and SSRC=3080896). As the phone is sending audio over a well-known payload type (PT=0 is PCMU) [10], we are able to identify which flow is audio and which flow is video. As we are collecting RTP statistics and our traffic happens to be RTP, we are able to determine metrics such as packet loss and jitter.

The traffic matching statistics and applied policies can be seen via the 'show policy-map type performance-traffic' command structure. Note the match statements and match rate for the inline policy.

```

3845-AA0216#show policy-map type performance-traffic interface fast0/0/0
FastEthernet0/0/0

Service-policy performance-traffic input: inline

Class-map: inline (match-any)
 3207222 packets, 3812332437 bytes
 30 second offered rate 3662000 bps, drop rate 0 bps
Match: dscp af41 (34) cs5 (40) ef (46)
 3207223 packets, 3812332437 bytes
 30 second rate 3662000 bps
media-monitoring:
 flow monitor inline
 record default-rtp
 monitor parameters
 interval duration 30
 timeout 10
 history 10
 flows 8000
 monitor metric rtp
 min-sequential 5
 max-dropout 5
 max-reorder 5

```

```

clock-rate default 90000
ssrc maximum 5
react 1 rtp-lost-fraction
threshold value gt 10.00
alarm type discrete
alarm severity error
action syslog

Class-map: class-default (match-any)
  77447 packets, 26909035 bytes
  30 second offered rate 8000 bps, drop rate 0 bps
Match: any

```

Figure 6: show policy-map performance-monitor example

Measurement Intervals

Performance-monitor posts measurements in regularly spaced monitor intervals. The default monitor interval is 30 seconds, but can be changed on a per class basis. As shown in Figure 7, at the end of each monitor interval, the measurements may be aggregated and then tested against configured thresholds. If NetFlow export is configured, the information is then sent towards the NetFlow collector(s). Finally, the information is added to the historical interval database. Up to 60 monitor intervals can be stored on the router. The number of monitor intervals is configurable with the default being 10 intervals. Performance-monitor monitors on a router with the same monitor-interval are synchronized to start and stop at the same time. If multiple routers are time synchronized (for example via NTP), then their monitors with matching intervals configured will have synchronized reports. The information in the monitor intervals is available via CLI, IOS Web Services Management Agent (WSMA) [11], and a MIB.

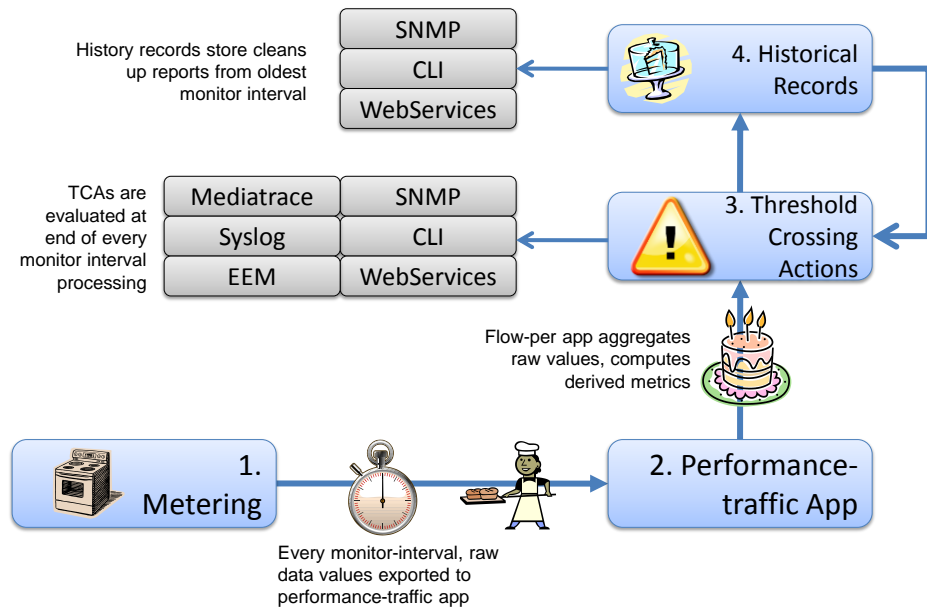


Figure 7: Performance-monitor information flow

The historical data can be accessed via the 'show performance traffic history' command structure as shown below. By default, this command gives information from the latest historical interval. With the 'interval option' option all stored intervals can be displayed.

```
3845-AA0216#show performance traffic history interval all ssrc 3080896

Flow Spec: SrcAddress = 10.1.160.31, DstAddress = 10.1.3.3, Protocol = udp, SrcPort = 20002, DstPort = 5445, SSRC = 3080896
Policy: inline, Class: inline, Interface: FastEthernet0/0/0, Direction: input

General Statistics:

```

Start Time	Event Lost Count	Event Lost Count	Event Lost Count	Monitor Error	Interface Input	Interface Output
01:21:22	0	0	0	false	Fa0/0/0	Fa0/0/1
01:20:52	0	0	0	false	Fa0/0/0	Fa0/0/1
01:20:22	0	0	0	false	Fa0/0/0	Fa0/0/1
01:19:52	0	0	0	false	Fa0/0/0	Fa0/0/1
01:19:22	0	0	0	false	Fa0/0/0	Fa0/0/1
01:18:52	0	0	0	false	Fa0/0/0	Fa0/0/1
01:18:22	0	0	0	false	Fa0/0/0	Fa0/0/1
01:17:52	0	0	0	false	Fa0/0/0	Fa0/0/1
01:17:22	0	0	0	false	Fa0/0/0	Fa0/0/1
01:16:52	0	0	0	false	Fa0/0/0	Fa0/0/1

```

IP Statistics:

```

Start Time	Byte Count	Packet Count	Byte Rate(Bps)	Packet Rate(pps)	Per Flow Byte Rate Avg(Bps)	Per Flow Byte Rate Min(Bps)	Per Flow Byte Rate Max(Bps)	Per Flow Packet Rate(pps)	Drop Count	Flow Count
01:21:22	NA	NA	7783	NA	7783	7783	7783	NA	NA	1
01:20:52	NA	NA	6882	NA	6882	6882	6882	NA	NA	1
01:20:22	NA	NA	7896	NA	7896	7896	7896	NA	NA	1
01:19:52	NA	NA	7566	NA	7566	7566	7566	NA	NA	1
01:19:22	NA	NA	7629	NA	7629	7629	7629	NA	NA	1
01:18:52	NA	NA	6642	NA	6642	6642	6642	NA	NA	1
01:18:22	NA	NA	7083	NA	7083	7083	7083	NA	NA	1
01:17:52	NA	NA	7144	NA	7144	7144	7144	NA	NA	1
01:17:22	NA	NA	8752	NA	8752	8752	8752	NA	NA	1
01:16:52	NA	NA	7166	NA	7166	7166	7166	NA	NA	1

```

Media Statistics:

```

Start Time	Byte Count	Packet Count	Byte Rate(Bps)	Per Flow Byte Rate Avg(kBps)	Per Flow Byte Rate Min(kBps)	Per Flow Byte Rate Max(kBps)	Media Event Flags
01:21:22	214139	969	7137	7137	7137	7137	Normal
01:20:52	187561	945	6252	6252	6252	6252	Normal
01:20:22	217548	968	7251	7251	7251	7251	Normal
01:19:52	207745	962	6924	6924	6924	6924	Normal
01:19:22	209879	951	6995	6995	6995	6995	Normal
01:18:52	180551	936	6018	6018	6018	6018	Normal
01:18:22	193468	952	6448	6448	6448	6448	Normal
01:17:52	195183	957	6506	6506	6506	6506	Normal
01:17:22	242644	997	8088	8088	8088	8088	Normal
01:16:52	195920	953	6530	6530	6530	6530	Normal

```

RTP Statistics:

```

Start Time	RTP Flow Count	Expected Packet Count	Lost Packet Count	Jitter Avg(usec)	Jitter Min(usec)	Jitter Max(usec)	Fraction Lost Count Avg	Fraction Lost Count Min	Fraction Lost Count Max
01:21:22	1	969	0	6356	35	27480	NA	NA	NA
01:20:52	1	945	0	5081	15	17960	NA	NA	NA
01:20:22	1	968	0	4630	8	18533	NA	NA	NA
01:19:52	1	962	0	4688	21	17781	NA	NA	NA
01:19:22	1	951	0	5020	16	22009	NA	NA	NA
01:18:52	1	936	0	5531	4	17246	NA	NA	NA
01:18:22	1	952	0	4396	20	23369	NA	NA	NA
01:17:52	1	957	0	4361	12	23407	NA	NA	NA
01:17:22	1	997	0	4309	72	22260	NA	NA	NA
01:16:52	1	953	0	5431	66	18701	NA	NA	NA

Figure 8: Historical intervals

Impairment

The policy shown in Figure 3 is also applied to R1 and the impairment device (netem) is configured to delay packets by 100ms, introduce a jitter of 50ms, and a loss of 15%.

```
tc qdisc add dev eth1.3514 root netem delay 100ms 50ms \
distribution normal loss 15%
```

Figure 9: netem command on linux PC to impair traffic exiting eth1.3514

We can validate the impairment by performing pings between R2 and R1:

```
3845-AA0216#ping 10.1.3.130
```



```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.3.130, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 60/110/172 ms
```

Figure 10: Ping between R2 and R1, validating impairment

It is possible to see the different points of view by comparing the outputs at R2 and R1 as shown in Figure 11 and Figure 12.

```
3845-AA0216#show performance traffic status ssrc 3080896
Flow Spec: SrcAddress = 10.1.160.31, DstAddress = 10.1.3.3, Protocol =
udp, SrcPort = 20002, DstPort = 5445, SSRC = 3080896
Policy: inline, Class: inline, Interface: FastEthernet0/0/0, Direction:
input

Flow Status:

...
Common Stats:
Event Lost Count Sum          : 0
Event Lost Count Minimum      : 0
Event Lost Count Maximum      : 0

Media Stats:
Byte Rate Average             : 2883 Bps
Byte Rate Minimum             : 2868 Bps
Byte Rate Maximum             : 2895 Bps
Media Event                   : Media-Normal

RTP Stats:
Payload Type                  : 97
Expected Packet Count         : 8995
Packet Lost Count Sum         : 0
Packet Lost Count Minimum     : 0
Packet Lost Count Maximum     : 0
Inter Arrival Jitter Average  : 6540 usec
Inter Arrival Jitter Minimum  : 0 usec
Inter Arrival Jitter Maximum  : 27430 usec
Fraction Lost Count Average   : 0.00
Fraction Lost Count Minimum   : 0.00
Fraction Lost Count Maximum   : 0.00
```

Figure 11: Observation on R2 (3845-AA0216), before impairment

```
1861-AA0213#show performance traffic status ssrc 3080896
Load for five secs: 3%/0%; one minute: 5%; five minutes: 6%
Time source is NTP, 03:09:02.606 EST Sun Jun 6 2010

Flow Spec: SrcAddress = 10.1.160.31, DstAddress = 10.1.3.3, Protocol =
udp, SrcPort = 20002, DstPort = 5445, SSRC = 3080896
Policy: inline, Class: inline, Interface: FastEthernet0/0, Direction:
input

Flow Status:

IP Stats:
Byte Count                    : 880806
Packet Count                  : 7588
Drop Count                    : 0
Byte Rate Average             : 2936 Bps
Byte Rate Minimum             : 2838 Bps
```

```

Byte Rate Maximum      : 3006 Bps
Packet Rate            : 25 pps
TTL Average            : 58
TTL Minimum            : 0
TTL Maximum            : 58

Common Stats:
Event Lost Count Sum   : 2697
Event Lost Count Minimum : 255
Event Lost Count Maximum : 281

Media Stats:
Byte Rate Average      : 2430 Bps
Byte Rate Minimum      : 2348 Bps
Byte Rate Maximum      : 2486 Bps
Media Event            : Media-Normal

RTP Stats:
Payload Type           : 97
Expected Packet Count  : 9573
Packet Lost Count Sum  : 1989
Packet Lost Count Minimum : 180
Packet Lost Count Maximum : 226
Inter Arrival Jitter Average : 42456 usec
Inter Arrival Jitter Minimum : 0 usec
Inter Arrival Jitter Maximum : 220644 usec
Fraction Lost Count Average : 20.77
Fraction Lost Count Minimum : 18.78
Fraction Lost Count Maximum : 23.10

```

Figure 12: Observation on R1 (3845-AA0216), after impairment

If we compare the metrics side by side, it is obvious that there is problem in between R2 and R1.

R2	R1
RTP Stats:	RTP Stats:
Payload Type : 97	Payload Type : 97
Expected Packet Count : 8995	Expected Packet Count : 9573
Packet Lost Count Sum : 0	Packet Lost Count Sum : 1989
Packet Lost Count Minimum : 0	Packet Lost Count Minimum : 180
Packet Lost Count Maximum : 0	Packet Lost Count Maximum : 226
Inter Arrival Jitter Average : 6540 usec	Inter Arrival Jitter Average : 42456 usec
Inter Arrival Jitter Minimum : 0 usec	Inter Arrival Jitter Minimum : 0 usec
Inter Arrival Jitter Maximum : 27430 usec	Inter Arrival Jitter Maximum : 220644 usec
Fraction Lost Count Average : 0.00	Fraction Lost Count Average : 20.77
Fraction Lost Count Minimum : 0.00	Fraction Lost Count Minimum : 18.78
Fraction Lost Count Maximum : 0.00	Fraction Lost Count Maximum : 23.10

Table 3: Comparison of RTP statistics between R2 and R1

Thresholds and Alarms

The policy (Figure 3) applied in the network included a threshold set to trigger an alarm and report it through syslog if the loss exceeded 10%. With the impairment, this threshold has certainly been crossed (see 'Fraction Lost Count' field values in Table 3) and syslog messages are generated as shown in Figure 13. The 'TCA RAISE' keyword in the message indicates the creation of an alarm.

```

Jun  6 03:24:17.314: %PERF_TRAFFIC_REACT-3-ERRSET: TCA RAISE.
Detailed info: Threshold value crossed - current value 22.49

```

```
Flow info: src ip 10.1.160.31, dst ip 10.1.3.3
          src port 20002, dst port 5445
          ssrc 3080896
Policy info: Policy-map inline, Class inline, Interface FastEthernet0/0,
Direction input
React info: id 1, criteria rtp-lost-fraction, severity error, alarm type
discrete, threshold range (10.00, 100.00]
```

Figure 13: Alarm declared based on loss percentage

When the impairment is removed as shown in Figure 14, the alarm is cleared as well. The 'TCA CLEAR' indicates the clearing of an existing alarm. A history of the measurements is available in the historical intervals, and the record of the alarm is available via syslog.

```
tc qdisc add dev eth1.3514 root netem delay 0ms 0ms distribution normal
loss 0% limit 30000
```

Figure 14: netem command on linux PC to fix impairment of traffic exiting eth1.3514

```
Jun  6 03:29:17.487: %PERF_TRAFFIC_REACT-3-ERRCLEAR: TCA CLEAR.
Detailed info: Threshold value crossed - current value 0.00
Flow info: src ip 10.1.160.31, dst ip 10.1.3.3
          src port 20002, dst port 5445
          ssrc 3080896
Policy info: Policy-map inline, Class inline, Interface FastEthernet0/0,
Direction input
React info: id 1, criteria rtp-lost-fraction, severity error, alarm type
discrete, threshold range (10.00, 100.00]
```

Figure 15: netem command on linux PC to fix impairment of traffic exiting eth1.3514

Flexible Traffic Selection and Policies

Performance-monitor is able to make measurements based on very specific class of traffic. The Cisco Common Classification Policy Language[12] (C3PL) is used for configuring performance-monitor as a whole and the 'class-map'[13] structure is used to select groups of traffic to monitor. This infrastructure allows the operator to select traffic based on combinations of layer-3 and layer-4 fields, DSCP values, deep packet inspection values and many more criteria. Below are several examples of class-maps that use different methods to match various types of traffic:

```
class-map match-all voip
  match protocol rtp audio
!
class-map match-all DSCP-CS5
  match dscp cs5
!
class-map match-all DSCP-EF
  match dscp ef
!
class-map match-all voip-dpi
  match protocol rtp audio
!
class-map match-all telepresence-dpi
  match protocol telepresence-media
!
class-map match-all IPVS-traffic
```

```

match ip dscp cs5
match access-group name fromIPVScamera
!
ip access-list extended fromIPVScamera
permit ip host 10.1.160.28 any

```

Figure 16: class-map examples

The class-maps determine 'what traffic' is monitored, the measurements themselves are determined by the flow records. The performance-monitor flow record is an extension of the flow records available via the Flexible NetFlow (FNF) feature [14]. The flow records allow specific metrics to be collected as well as data aggregation policies to be configured. This same record definition is used in exporting the measured data to NetFlow collectors.

There are two built-in performance traffic flow records but the operator may wish to create their own; mixing, adding, and deleting metrics as necessary. Figure 17 shows the two default flow records and Figure 18 shows the configuration of a completely new performance-monitor flow record.

```

3845-AA0216#show flow record type performance-traffic default-tcp
Load for five secs: 3%/2%; one minute: 3%; five minutes: 3%
Time source is NTP, 13:53:14.898 EST Sun Jun 6 2010
flow record type performance-traffic default-tcp:
  Description:          VM default TCP record
  No. of users:         0
  Total field space:    44 bytes
  Fields:
    match ipv4 protocol
    match ipv4 source address
    match ipv4 destination address
    match transport source-port
    match transport destination-port
    collect routing forwarding-status
    collect transport round-trip-time
    collect transport event packet-loss counter
    collect interface input
    collect interface output
    collect counter bytes rate
    collect timestamp interval
    collect application media event
    collect monitor event

3845-AA0216#show flow record type performance-traffic default-rtp
Load for five secs: 3%/2%; one minute: 3%; five minutes: 3%
Time source is NTP, 13:53:21.415 EST Sun Jun 6 2010
flow record type performance-traffic default-rtp:
  Description:          VM default RTP record
  No. of users:         1
  Total field space:    76 bytes
  Fields:
    match ipv4 protocol
    match ipv4 source address
    match ipv4 destination address
    match transport source-port
    match transport destination-port
    match transport rtp ssrc
    collect routing forwarding-status
    collect transport packets expected counter
    collect transport packets lost counter
    collect transport event packet-loss counter
    collect transport rtp jitter mean

```

```

collect transport rtp jitter minimum
collect transport rtp jitter maximum
collect interface input
collect interface output
collect counter bytes rate
collect timestamp interval
collect application media bytes counter
collect application media bytes rate
collect application media packets counter
collect application media event
collect monitor event

```

Figure 17: default-top and default-rtp flow records

```

1861-AA0213#conf t
Enter configuration commands, one per line. End with CNTL/Z.
1861-AA0213(config)#flow record type performance-traffic enhan-tcp-rtp
1861-AA0213(config-flow-record)# description basic rtp only stats
1861-AA0213(config-flow-record)# match ipv4 source address
1861-AA0213(config-flow-record)# match ipv4 destination address
1861-AA0213(config-flow-record)# match transport source-port
1861-AA0213(config-flow-record)# match transport destination-port
1861-AA0213(config-flow-record)# match transport rtp ssrc
1861-AA0213(config-flow-record)# collect routing forwarding-status
1861-AA0213(config-flow-record)# collect ipv4 ttl minimum
1861-AA0213(config-flow-record)# collect ipv4 ttl maximum
1861-AA0213(config-flow-record)# collect transport packets lost counter
1861-AA0213(config-flow-record)# collect transport packets lost rate
1861-AA0213(config-flow-record)# collect transport round-trip-time
1861-AA0213(config-flow-record)# collect transport event packet-loss
counter
1861-AA0213(config-flow-record)# collect transport rtp jitter mean
1861-AA0213(config-flow-record)# collect transport rtp jitter minimum
1861-AA0213(config-flow-record)# collect transport rtp jitter maximum
1861-AA0213(config-flow-record)# collect interface input
1861-AA0213(config-flow-record)# collect counter packets
1861-AA0213(config-flow-record)# collect timestamp interval
1861-AA0213(config-flow-record)# collect application media packets
counter
1861-AA0213(config-flow-record)# collect monitor event
1861-AA0213(config-flow-record)#end

```

Figure 18: configuration of a custom performance-monitor flow record

The flow records are placed inside a flow monitor (same as in Flexible NetFlow). The flow monitor allows the association of the flow record with a flow exporter (if the data needs to be exported to a NetFlow collector). The flow monitor may be configured in global configuration mode if it is to be used across different sets of traffic, or it may be configured 'inline' under the policy map as explained below.

The flow monitor (of which the flow record is a part) and the class-maps are brought together with threshold configuration under the performance-monitor policy map. The policy map may be configured 'inline' as shown in Figure 3, or for more complex configurations, or configurations applied to multiple points a global performance-traffic policy-map may be more appropriate.

In Figure 2, the test topology was shown with video surveillance and video based telephony applications being run over the network. In the case of video surveillance, the video traffic may be RTP based or HTTP based depending on the type of client. Additionally, for RTP based video surveillance the cisco IPVS-2500 camera uses a dynamic RTP payload type (PT=96) and a non-

standard video encoding rate (30khz). For the jitter calculation to be accurate we will need to inform the performance-monitor feature of this change. As both video surveillance and IP based video telephony serve different business needs and have different sensitivities the thresholds will be different. The configuration below accomodates these diverse requirements.

```

class-map match-all voice-ef
  match dscp ef
class-map match-all video-conf
  match dscp af41
class-map match-all IPVS-traffic
  match ip dscp cs5
  match access-group name fromIPVScamera
!
ip access-list extended fromIPVScamera
  permit ip host 10.1.160.28 any
!
flow record type performance-traffic enhan-tcp-rtp
  description basic rtp only stats
  match ipv4 source address
  match ipv4 destination address
  match transport source-port
  match transport destination-port
  match transport rtp ssrc
  collect routing forwarding-status
  collect ipv4 ttl minimum
  collect ipv4 ttl maximum
  collect transport packets lost counter
  collect transport packets lost rate
  collect transport round-trip-time
  collect transport event packet-loss counter
  collect transport rtp jitter mean
  collect transport rtp jitter minimum
  collect transport rtp jitter maximum
  collect interface input
  collect counter packets
  collect timestamp interval
  collect application media packets counter
  collect monitor event
!
policy-map type performance-traffic voice-vc-ipvs-1
  class voice-ef
    flow monitor inline
    record default-rtp
    react 1 rtp-jitter-average
      threshold value gt 50000
      alarm severity alert
      action syslog
    react 2 rtp-lost-fraction
      threshold value gt 10.00
      alarm severity alert
      action syslog
  class IPVS-traffic
    flow monitor inline
    record enhan-tcp-rtp
    monitor parameters
      interval duration 10
    monitor metric rtp
      clock-rate 96 30000
    react 1 rtp-lost-fraction
      threshold value gt 2.00
      alarm severity alert
      action syslog

```

```

class video-conf
  flow monitor inline
  record default-rtp
  react 1 rtp-lost-fraction
  threshold value gt 2.00
  alarm severity alert
  action syslog
  react 2 rtp-jitter-average
  threshold value gt 50000
  alarm severity alert
  action syslog
!
interface FastEthernet0/0
ip address 10.1.3.130 255.255.255.128
ip ospf 1 area 0
service-policy type performance-traffic input voice-vc-ipvs-1
service-policy type performance-traffic output voice-vc-ipvs-1

```

Figure 19: Complex performance-monitor policy

Mediatrace

With mediatrace, the operator can request information from the nodes along the path that particular flow is taking (or would have taken). The nature of the request can be very general, such as the interface names involved in the forwarding of the flow, and names of the routers. However, the data presented in a single screen back to the operator can also be very flow specific. For example, mediatrace can dynamically configure and query the performance-monitor feature on a per node basis to generate per flow loss, jitter and latency type of information. In the topology in Figure 1, the operator is able to make a request on R1 the loss information regarding the CTS flow. Mediatrace is able to dynamically discover the nodes along the path, and gather performance-monitor information from both R1 and R2 and output the data in a single, seamless report.

Quick Mediatrace

As mentioned earlier, mediatrace is able to follow a particular flow's path and gather various layers of information. Mediatrace can be executed from the IOS exec or periodically via configuration.

The example in Figure 20 shows a mediatrace hop poll execution that only does path discovery. The trace is run on a router (VXR-AA0310) upstream of R2 and we are able to not only see that R2 and R1 are in the path, but also the ingress and egress interfaces on the mediatrace enabled routers. Analysis of the TTL field tells us that the hops at ttl=254 and ttl=253 are grey areas for mediatrace reporting. However, the response also demonstrates that the mediatrace packet is able to traverse grey areas and end to end support is not required.

```

VXR-AA0310#mediatrace poll path-specifier source 10.1.160.31 destination
10.1.3.3 hops
Started the data fetch operation.
Waiting for data from hops.
This may take several seconds to complete...
Data received for hop 0
Data received for hop 1
Data received for hop 2
Data fetch complete.
Results:
Data Collection Summary:
  Request Timestamp: 16:13:41.153 EST Sun Jun 6 2010
  Request Status: Completed

```

```

Number of hops responded (includes success/error/no-record): 3
Number of hops with valid data report: 3
Number of hops with error report: 0
Number of hops with no data record: 0
Detailed Report of collected data:
  Number of Mediatrace hops in the path: 3

  Mediatrace Hop Number: 0 (host=VXR-AA0310, ttl=255)
    Ingress Interface: None
    Egress Interface: Gi0/3

  Mediatrace Hop Number: 1 (host=3845-AA0216, ttl=252)
    Ingress Interface: Fa0/0/0
    Egress Interface: Fa0/0/1

  Mediatrace Hop Number: 2 (host=1861-AA0213, ttl=251)
    Ingress Interface: Fa0/0
    Egress Interface: V11000

```

Figure 20: mediatrace hop poll

Mediatrace System Poll

A deeper example follows in Figure 21, where a system poll is executed. In a system poll not only is the node, and interface discovery performed, but statistics from the interfaces are also gathered. Mediatrace uses SNMP internally to gather this information from the router, and the 'snmp community' IOS configuration command needs to be applied. In this example we can see that 1861-AA0213 on Fa0/0 has received some errors.

```

VXR-AA0310#mediatrace poll path-specifier source 10.1.160.31 destination
10.1.1.3.3 system
Started the data fetch operation.
Waiting for data from hops.
This may take several seconds to complete...
Data received for hop 0
Data received for hop 1
Data received for hop 2
Data fetch complete.
Results:
Data Collection Summary:
  Request Timestamp: 15:56:15.046 EST Sun Jun 6 2010
  Request Status: Completed
  Number of hops responded (includes success/error/no-record): 3
  Number of hops with valid data report: 3
  Number of hops with error report: 0
  Number of hops with no data record: 0
Detailed Report of collected data:
  Number of Mediatrace hops in the path: 3

  Mediatrace Hop Number: 0 (host=VXR-AA0310, ttl=255)
    Metrics Collection Status: Success
    Ingress Interface: None
    Egress Interface: Gi0/3
    Metrics Collected:
      Collection timestamp: 15:56:15.042 EST Sun Jun 6 2010
      Octet input at Ingress (Bytes): NOT COLLECTED
      Octet output at Egress (MB): 1596.446327
      Pkts rcvd with err at Ingress (pkts): NOT COLLECTED
      Pkts errored at Egress (pkts): 0
      Pkts discarded at Ingress (pkts): NOT COLLECTED

```



```

Pkts discarded at Egress (pkts): 0
Ingress i/f speed (bps): NOT COLLECTED
Egress i/f speed (mbps): 1000.000000

Mediatrace Hop Number: 1 (host=3845-AA0216, ttl=252)
Metrics Collection Status: Success
Ingress Interface: Fa0/0/0
Egress Interface: Fa0/0/1
Metrics Collected:
  Collection timestamp: 15:56:15.056 EST Sun Jun 6 2010
  Octet input at Ingress (MB): 2421.417393
  Octet output at Egress (MB): 2423.802672
  Pkts rcvd with err at Ingress (pkts): 0
  Pkts errored at Egress (pkts): 0
  Pkts discarded at Ingress (pkts): 0
  Pkts discarded at Egress (pkts): 0
  Ingress i/f speed (kbps): 100000.000
  Egress i/f speed (kbps): 100000.000

Mediatrace Hop Number: 2 (host=1861-AA0213, ttl=251)
Metrics Collection Status: Success
Ingress Interface: Fa0/0
Egress Interface: V11000
Metrics Collected:
  Collection timestamp: 15:56:15.064 EST Sun Jun 6 2010
  Octet input at Ingress (MB): 3464.474746
  Octet output at Egress (MB): 3462.522579
  Pkts rcvd with err at Ingress (pkts): 8
  Pkts errored at Egress (pkts): 0
  Pkts discarded at Ingress (pkts): 0
  Pkts discarded at Egress (pkts): 0
  Ingress i/f speed (kbps): 100000.000
  Egress i/f speed (kbps): 100000.000

```

Figure 21: mediatrace system poll

Mediatrace and Performance-Monitor

Finally, in the mediatrace integration with performance-monitor we are able to gather flow specific statistics. For the flow specific statistics, additional information such as the IP protocol and layer-4 ports need to be specified. If a performance-monitor data profile is not selected, a default one based on the IP protocol is used. In the example in Figure 22, mediatrace automatically requests RTP metrics from the nodes along the path. Mediatrace is able to help correlate data from across a path on to a single screen. Analysing the output we see that all through the path there are no drops and that jitter has been steadily increasing along the path but in the end is negligible.

```

VXR-AA0310#mediatrace poll path-specifier source 10.1.160.31 port 20000
destination 10.1.3.3 port 24584 ip-protocol udp perf-traffic
Started the data fetch operation.
Waiting for data from hops.
This may take several seconds to complete...
New periodical session with global session id (74769259) is added. Active
session number is (1).
Data received for hop 0
Data received for hop 1
Data received for hop 2
Data fetch complete.
Results:
Data Collection Summary:

```

```
Request Timestamp: .17:09:33.317 EST Sun Jun 6 2010
Request Status: Completed
Number of hops responded (includes success/error/no-record): 3
Number of hops with valid data report: 3
Number of hops with error report: 0
Number of hops with no data record: 0
Detailed Report of collected data:
  Number of Mediatrace hops in the path: 3

  Mediatrace Hop Number: 0 (host=VXR-AA0310, ttl=255)
  Metrics Collection Status: Success
  Ingress Interface: None
  Egress Interface: Gi0/3
  Metrics Collected:
    Flow Sampling Start Timestamp: .17:09:01.093 EST Thu Jun 6 1940
    Loss of measurement confidence: FALSE
    Media Stop Event Occurred: FALSE
    IP Packet Drop Count (pkts): 0
    IP Byte Count (Bytes): 299600
    IP Packet Count (pkts): 1498
    IP Byte Rate (Bps): 9986
    Packet Drop Reason: 0
    IP DSCP: 34
    IP TTL: 62
    IP Protocol: 17
    Media Byte Rate Average (Bps): 8988
    Media Byte Count (Bytes): 269640
    Media Packet Count (pkts): 1498
    RTP Interarrival Jitter Average (usec): 556
    RTP Packets Lost (pkts): 0
    RTP Packets Expected (pkts): 1493
    RTP Packet Lost Event Count: 0
    RTP Loss Percent (%): 0.00

  Mediatrace Hop Number: 1 (host=3845-AA0216, ttl=252)
  Metrics Collection Status: Success
  Ingress Interface: Fa0/0/0
  Egress Interface: Fa0/0/1
  Metrics Collected:
    Flow Sampling Start Timestamp: .17:09:01.107 EST Thu Jun 6 1940
    Loss of measurement confidence: FALSE
    Media Stop Event Occurred: FALSE
    IP Packet Drop Count (pkts): 0
    IP Byte Count (Bytes): 299400
    IP Packet Count (pkts): 1497
    IP Byte Rate (Bps): 9980
    Packet Drop Reason: 0
    IP DSCP: 34
    IP TTL: 59
    IP Protocol: 17
    Media Byte Rate Average (Bps): 8982
    Media Byte Count (Bytes): 269460
    Media Packet Count (pkts): 1497
    RTP Interarrival Jitter Average (usec): 553
    RTP Packets Lost (pkts): 0
    RTP Packets Expected (pkts): 1492
    RTP Packet Lost Event Count: 0
    RTP Loss Percent (%): 0.00

  Mediatrace Hop Number: 2 (host=1861-AA0213, ttl=251)
  Metrics Collection Status: Success
  Ingress Interface: Fa0/0
  Egress Interface: V11000
  Metrics Collected:
    Flow Sampling Start Timestamp: .17:09:01.141 EST Thu Jun 6 1940
```

```

Loss of measurement confidence: FALSE
Media Stop Event Occurred: FALSE
IP Packet Drop Count (pkts): 0
IP Byte Count (Bytes): 299400
IP Packet Count (pkts): 1497
IP Byte Rate (Bps): 9980
Packet Drop Reason: 0
IP DSCP: 34
IP TTL: 58
IP Protocol: 17
Media Byte Rate Average (Bps): 8982
Media Byte Count (Bytes): 269460
Media Packet Count (pkts): 1497
RTP Interarrival Jitter Average (usec): 725
RTP Packets Lost (pkts): 0
RTP Packets Expected (pkts): 1492
RTP Packet Lost Event Count: 0
RTP Loss Percent (%): 0.00

```

Figure 22: mediatrace performance-monitor poll using default RTP profile

Flexible Mediatrace Configuration

The mediatrace poll exec command allows for a quick way to do a one time request along a path. There is some flexibility in that the operator can select which major type of data is being requested: path discovery, interface level or the pre-configured performance-monitor records. In the case of the performance-monitor data retrieval requests some parameters (for example RTP clock rate may also need to be specified).

Mediatrace configuration is done in a hierarchical manner employing modular configurations as shown in Figure 23 below. It should be noted that the mediatrace poll exec command is basically a macro that dynamically creates a one time mediatrace session that is run a single time. The poll command makes use of mediatrace profiles, session params as well as path specifiers although sometimes not directly.

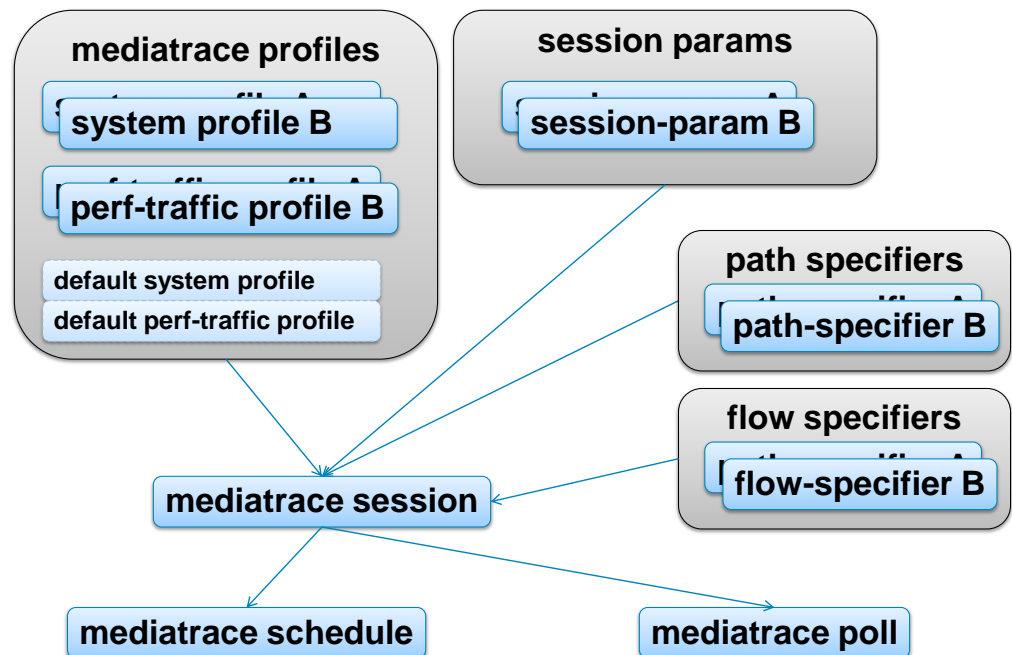


Figure 23: mediatrace configuration and execution model

The path specifier tells mediatrace which path (which set of nodes to query). It is expressed in terms of an IP flow (ip src, ip dest, etc.) description. The more information that is provided (for example when layer-4 addresses are used as part of the multipath selection algorithm [15]), the more accurate is mediatrace's ability to follow the same path as the target flow. The mediatrace path specifiers guide the 'where to monitor' element of deployment design.

Mediatrace flow specifiers define the 'what to monitor'. Similarly to the filters in the performance-monitor class-map the flow specifier can be very specific (for example a 5-tuple) or more generic such as a DSCP classification. As the path specifier is in terms of a flow description, by default the path specifier is also the flow specifier. Examples of path and flow specifiers can be found below in Figure 24.

```
mediatrace path-specifier 160.28to3.15 destination ip 10.1.3.3
 source ip 10.1.160.28
!
mediatrace flow-specifier IPcamera.2.XP1
 source-ip 10.1.160.28 source-port 5002
 dest-ip 10.1.3.15 dest-port 3576
```

Figure 24: mediatrace path and flow specifiers

Mediatrace profiles define the 'what information' to measure and gather from the path. This is broken down into two main areas: system profiles and performance-monitor profiles. System profiles gather information that is not flow specific. Examples of system profile data options include CPU, memory and interface metrics. The mediatrace system poll command by default gathers interface statistics as seen in Figure 21. The performance-monitor profile interacts with the performance-monitor module in the nodes along the path. Mediatrace can dynamically configure a performance-monitor policy to gather flow specific statistics. Performance traffic profiles can describe groups of statistics based on TCP or RTP metrics. Additionally, performance-monitor mediatrace profiles can configure the manner of measurement by allowing the configuration of the monitor interval as well as RTP clock-rates. An example of a mediatrace profile can be found in Figure 25.

```
mediatrace profile perf-traffic test
 metric-list rtp
  clock-rate 96 30000
 admin-params
  sampling-interval 10
```

Figure 25: mediatrace profile

The mediatrace session-params container describes information about the mediatrace session itself. Configuration parameters here are related to how many historical buckets of data to keep in memory, what the response timeout is etc. An example of a mediatrace session-params config can be found in Figure 26

```
mediatrace session-params cam2xp1
 response-timeout 3
 history data-sets-kept 10
```

Figure 26: mediatrace session-params configuration.

Finally, the path-specifier, session-params and profiles are brought together in a mediatrace session configuration. While individual elements can be used with the mediatrace poll command, if there is a need to run mediatraces in succession and keep a historical record, the mediatrace

session is the best mechanism. An example of a mediatrace session can be found in Figure 1. All that is needed after this is to schedule the session (in configuration mode), by configuring the start time, recurrence and lifetime.

```
mediatrace 1
description cam2XP1
path-specifier 160.28to3.15
session-params cam2xp1
profile perf-traffic test flow-specifier IPcamera.2.XP1
```

Figure 27: mediatrace session configuration

```
mediatrace schedule 1 start-time now
```

Figure 28: mediatrace session scheduling

Once the mediatrace session is scheduled, the data is available via the 'show mediatrace session data' command structure. An example is shown in Figure 31 below. The format should be familiar as it is the same format as used in mediatrace poll. Note that the first mediatrace run was not able to gather the performance-monitor statistics due to the fact that the monitor-interval on the nodes had not completed and was not available. The next run (bucket index 2) at 21:23:40.577 does in fact have the statistics: from the monitor interval ending at 21:22:40.513.

```
VXR-AA0310#show mediatrace session data 1
Session Index: 1
Global Session Id: 102992555
Session Operation State: Active
Bucket index: 1
Data Collection Summary:
  Request Timestamp: 21:21:40.577 EST Sun Jun 6 2010
  Request Status: Completed
  Number of hops responded (includes success/error/no-record): 3
  Number of hops with valid data report: 0
  Number of hops with error report: 0
  Number of hops with no data record: 3
Detailed Report of collected data:
  Last Route Change Timestamp:
  Route Index: 0
  Number of Mediatrace hops in the path: 3

  Mediatrace Hop Number: 0 (host=VXR-AA0310, ttl=255)
  Metrics Collection Status: Fail (19, No statistic data available
for reporting)
  Ingress Interface: None
  Egress Interface: Gi0/3
  Metrics Collected:

  Mediatrace Hop Number: 1 (host=3845-AA0216, ttl=252)
  Metrics Collection Status: Fail (19, No statistic data available
for reporting)
  Ingress Interface: Fa0/0/0
  Egress Interface: Fa0/0/1
  Metrics Collected:

  Mediatrace Hop Number: 2 (host=1861-AA0213, ttl=251)
  Metrics Collection Status: Fail (19, No statistic data available
for reporting)
  Ingress Interface: Fa0/0
  Egress Interface: V11000
  Metrics Collected:
Bucket index: 2
```

```
Data Collection Summary:
  Request Timestamp: 21:23:40.577 EST Sun Jun 6 2010
  Request Status: Completed
  Number of hops responded (includes success/error/no-record): 3
  Number of hops with valid data report: 3
  Number of hops with error report: 0
  Number of hops with no data record: 0
Detailed Report of collected data:
  Last Route Change Timestamp:
  Route Index: 0
    Number of Mediatrace hops in the path: 3

  Mediatrace Hop Number: 0 (host=VXR-AA0310, ttl=255)
  Metrics Collection Status: Success
  Ingress Interface: None
  Egress Interface: Gi0/3
  Metrics Collected:
    Flow Sampling Start Timestamp: 21:22:40.513 EST Thu Jun 6 1940
    Loss of measurement confidence: FALSE
    Media Stop Event Occurred: FALSE
    IP Packet Drop Count (pkts): 0
    IP Byte Count (KB): 13657.177
    IP Packet Count (pkts): 9912
    IP Byte Rate (Bps): 455239
    Packet Drop Reason: 0
    IP DSCP: 40
    IP TTL: 62
    IP Protocol: 17
    Media Byte Rate Average (Bps): 448631
    Media Byte Count (KB): 13458.937
    Media Packet Count (pkts): 9912
    RTP Interarrival Jitter Average (ms): 25345
    RTP Packets Lost (pkts): 0
    RTP Packets Expected (pkts): 9912
    RTP Packet Lost Event Count: 0
    RTP Loss Percent (%): 0.00

  Mediatrace Hop Number: 1 (host=3845-AA0216, ttl=252)
  Metrics Collection Status: Success
  Ingress Interface: Fa0/0/0
  Egress Interface: Fa0/0/1
  Metrics Collected:
    Flow Sampling Start Timestamp: 21:22:40.574 EST Thu Jun 6 1940
    Loss of measurement confidence: FALSE
    Media Stop Event Occurred: FALSE
    IP Packet Drop Count (pkts): 0
    IP Byte Count (KB): 13626.173
    IP Packet Count (pkts): 9890
    IP Byte Rate (Bps): 454205
    Packet Drop Reason: 0
    IP DSCP: 40
    IP TTL: 59
    IP Protocol: 17
    Media Byte Rate Average (Bps): 447612
    Media Byte Count (KB): 13428.373
    Media Packet Count (pkts): 9890
    RTP Interarrival Jitter Average (ms): 25355
    RTP Packets Lost (pkts): 0
    RTP Packets Expected (pkts): 9890
    RTP Packet Lost Event Count: 0
    RTP Loss Percent (%): 0.00

  Mediatrace Hop Number: 2 (host=1861-AA0213, ttl=251)
  Metrics Collection Status: Success
  Ingress Interface: Fa0/0
```

```

Egress Interface: V11000
Metrics Collected:
  Flow Sampling Start Timestamp: 21:22:40.547 EST Thu Jun 6 1940
  Loss of measurement confidence: FALSE
  Media Stop Event Occurred: FALSE
  IP Packet Drop Count (pkts): 0
  IP Byte Count (KB): 13640.573
  IP Packet Count (pkts): 9900
  IP Byte Rate (Bps): 454685
  Packet Drop Reason: 0
  IP DSCP: 40
  IP TTL: 58
  IP Protocol: 17
  Media Byte Rate Average (Bps): 448085
  Media Byte Count (KB): 13442.573
  Media Packet Count (pkts): 9900
  RTP Interarrival Jitter Average (ms): 25345
  RTP Packets Lost (pkts): 0
  RTP Packets Expected (pkts): 9900
  RTP Packet Lost Event Count: 0
  RTP Loss Percent (%): 0.00

```

Figure 29: Observation on R2 (3845-AA0216), before impairment

Appendix A: Initial Configuration

```

1861-AA0213#sh run
Building configuration...

Current configuration : 6044 bytes
!
! Last configuration change at 14:17:01 EST Sat Jun 5 2010 by aa
! NVRAM config last updated at 19:46:53 EST Thu Jun 3 2010 by aa
!
version 15.1
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
!
hostname 1861-AA0213
!
boot-start-marker
boot system flash flash:c1861-adventerprisek9-mz.151-1.16.PI14
boot-end-marker
!
!
logging buffered 4096
logging console informational
enable password lab
!
aaa new-model
!
!
aaa authentication login default group tacacs+ line
aaa authentication enable default group tacacs+ enable
aaa authorization console
aaa authorization exec default group tacacs+ if-authenticated
aaa authorization commands 1 default group tacacs+ if-authenticated
aaa authorization commands 15 default group tacacs+ if-authenticated
aaa authorization configuration default group tacacs+
aaa accounting commands 15 default
  action-type stop-only
  group tacacs+
!
!
!
!
!
!
!
!

```

```
aaa session-id common
!
clock timezone EST -5 0
clock summer-time EST recurring
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
crypto pki token default removal timeout 0
!
!
!
dot11 syslog
no ip source-route
ip cef
!
!
!
!
ip dhcp pool site-1000-vlan-1000
 network 10.1.3.0 255.255.255.128
 default-router 10.1.3.1
 dns-server 10.1.160.6
 domain-name medianet.cisco.com
 option 150 ip 10.1.1.18
!
ip dhcp pool s1000-cts1k-1
 host 10.1.3.5 255.255.255.128
 hardware-address 001d.a238.a680
 default-router 10.1.3.1
 dns-server 10.1.160.6
 domain-name medianet.cisco.com
 option 150 ip 10.1.1.18
!
ip dhcp pool s1000-7970-cts1k-1
 host 10.1.3.4 255.255.255.128
 client-identifier 0100.2290.5983.a4
 default-router 10.1.3.1
 dns-server 10.1.160.6
 domain-name medianet.cisco.com
 option 150 ip 10.1.1.18
!
ip dhcp pool ipc-zz0140
 host 10.1.3.7 255.255.255.128
 client-identifier 0100.1de5.ea78.08
 default-router 10.1.3.1
 dns-server 10.1.160.6
 domain-name medianet.cisco.com
 option 150 ip 10.1.1.18
!
ip dhcp pool s1000-7961-zz0103-1
 host 10.1.3.6 255.255.255.128
 client-identifier 0100.235e.18ee.3c
 default-router 10.1.3.1
 dns-server 10.1.160.6
 domain-name medianet.cisco.com
 option 150 ip 10.1.1.18
!
ip dhcp pool medianet-tme-aakhter-2
 host 10.1.3.8 255.255.255.128
 client-identifier 0100.1125.ce94.f3
 default-router 10.1.3.1
 dns-server 10.1.160.6
 domain-name medianet.cisco.com
 option 150 ip 10.1.1.18
!
ip dhcp pool s1000-7985-zz0103-1
 host 10.1.3.9 255.255.255.128
 client-identifier 0100.5060.03aa.87
 default-router 10.1.3.1
 dns-server 10.1.160.6
 domain-name medianet.cisco.com
 option 150 ip 10.1.1.18
!
ip dhcp pool s1000-7942-zz0103-1
 host 10.1.3.10 255.255.255.128
 client-identifier 0100.1d45.2d54.e8
 default-router 10.1.3.1
 dns-server 10.1.160.6
 domain-name medianet.cisco.com
 option 150 ip 10.1.1.18
 class class-default
!
ip dhcp pool medianet-tme-aakhter-3
 host 10.1.3.3 255.255.255.128
```



```

client-identifier 0100.016c.c9eb.48
default-router 10.1.3.1
dns-server 10.1.160.6
domain-name medianet.cisco.com
option 150 ip 10.1.1.18
!
!
ip dhcp pool s1000-7961-zz0
client-identifier 0100.1d45.2d54.e8
default-router 10.1.3.1
dns-server 10.1.160.6
domain-name medianet.cisco.com
option 150 ip 10.1.1.18
!
!
ip dhcp class class-default
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
!
voice-card 0
!
!
!
license udi pid C1861-SRST-C-F/K9 sn FHK115028GK
archive
log config
hidekeys
username lab password 0 lab
!
!
ip ftp username anonymous
ip ftp password nobody@cisco.com
!
!
!
!
!
!
!
!
interface Loopback0
ip address 10.10.2.13 255.255.255.255
ip ospf 1 area 0
!
interface FastEthernet0/0
description GSR46-AA0402::Fas 0/2/1/3
ip address 10.1.3.130 255.255.255.128
ip ospf 1 area 0
load-interval 30
speed 100
full-duplex
!
interface Integrated-Service-Engine0/0
no ip address
shutdown
!
interface FastEthernet0/1/0
description MANSW-AA0299::Fas 0/16
switchport access vlan 10
!
interface FastEthernet0/1/1
description DATSW-AA0498::Gig 1/28
switchport access vlan 1000
spanning-tree portfast
!
interface FastEthernet0/1/2
!
interface FastEthernet0/1/3
description to TC 1/9
switchport access vlan 1000
spanning-tree portfast

```

```

!
interface FastEthernet0/1/4
!
interface FastEthernet0/1/5
!
interface FastEthernet0/1/6
!
interface FastEthernet0/1/7
description to DATSW-AA0298 Gig 1/3
switchport access vlan 1000
spanning-tree portfast
!
interface FastEthernet0/1/8
!
interface Vlan10
description MANSW-AA0299::Fas 0/16
ip address 10.27.2.13 255.255.0.0
ip flow ingress
ntp broadcast client
!
interface Vlan1000
description Site-1000
ip address 10.1.3.1 255.255.255.128
ip ospf 1 area 0
!
router ospf 1
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
logging esm config
logging 10.27.0.1
access-list 99 permit 10.1.3.15
!
!
!
!
snmp-server community public RO
snmp-server community private RW
snmp-server ifindex persist
snmp-server enable traps flowmon
!
tacacs-server host 10.27.150.201 key none
!
!
!
control-plane
!
!
!
voice-port 0/0/0
!
voice-port 0/0/1
!
voice-port 0/0/2
!
voice-port 0/0/3
!
voice-port 0/1/0
!
voice-port 0/1/1
!
voice-port 0/1/2
!
voice-port 0/1/3
!
voice-port 0/4/0
auto-cut-through
signal immediate
input gain auto-control
description Music On Hold Port
!
!
!
mgcp fax t38 ecm
!
!
!
!
banner exec ^C^[0;ROUTER^C
!
line con 0
exec-timeout 0 0
password lab

```

```

no modem enable
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
line vty 0 10
  exec-timeout 0 0
  password lab
  logging synchronous
  transport preferred none
  transport input all
  exec prompt timestamp
!
exception data-corruption buffer truncate
end

```

Figure 30: 1861-AA0213 initial configuration

```

3845-AA0216#sh run
Building configuration...

Current configuration : 3391 bytes
!
! Last configuration change at 19:45:44 EST Thu Jun 3 2010 by aa
! NVRAM config last updated at 19:45:45 EST Thu Jun 3 2010 by aa
!
version 15.1
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
!
hostname 3845-AA0216
!
boot-start-marker
boot system flash flash:c3845-adventerprisek9-mz.151-1.16.PI14
boot-end-marker
!
!
logging buffered 4096
logging console informational
enable password lab
!
aaa new-model
!
!
aaa authentication login default group tacacs+ line
aaa authentication enable default group tacacs+ enable
aaa authorization console
aaa authorization exec default group tacacs+ if-authenticated
aaa authorization commands 1 default group tacacs+ if-authenticated
aaa authorization commands 15 default group tacacs+ if-authenticated
aaa authorization configuration default group tacacs+
aaa accounting commands 15 default stop-only group tacacs+
!
!
!
!
!
aaa session-id common
!
clock timezone EST -5 0
clock summer-time EST recurring
!
dot11 syslog

```

```
ip source-route
!
ip cef
!
!
!
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
voice-card 0
!
!
!
!
!
!
!
crypto pki token default removal timeout 0
!
!
!
!
license udi pid CISCO3845-MB sn FOC12223L8D
archive
  log config
  hidekeys
username lab password 0 lab
!
redundancy
!
!
ip ftp username anonymous
ip ftp password nobody@cisco.com
!
!
!
!
!
!
!
interface Loopback0
  ip address 10.10.2.16 255.255.255.255
  ip ospf 1 area 0
!
interface GigabitEthernet0/0
  description to MANSW-0299 Fa0/10
  ip address 10.27.2.16 255.255.0.0
  duplex auto
  speed auto
  media-type rj45
  ntp broadcast client
!
interface GigabitEthernet0/1
  description to CISCO ASA eth0/1
  ip address 192.168.1.2 255.255.255.0
  shutdown
  duplex auto
```

```

speed auto
media-type rj45
!
interface FastEthernet0/0/0
description DATSW-AA0298::Gig 1/44
ip address 10.1.162.2 255.255.255.0
ip nbar protocol-discovery
load-interval 30
duplex auto
speed auto
!
interface FastEthernet0/0/1
description DATSW-AA0298::Gig 1/43
ip address 10.1.3.129 255.255.255.128
ip nbar protocol-discovery
ip ospf 1 area 0
duplex auto
speed auto
!
interface GigabitEthernet2/0
ip address 1.1.1.1 255.0.0.0
ntp broadcast client
!
router ospf 1
redistribute bgp 5003 subnets
!
router bgp 5003
bgp log-neighbor-changes
network 10.1.3.0 mask 255.255.255.0
network 10.10.2.13 mask 255.255.255.255
redistribute ospf 1
neighbor 10.1.162.1 remote-as 101
no auto-summary
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
ip flow-cache timeout active 1
ip flow-export version 9
ip flow-export destination 10.27.12.41 9995
!
!
logging esm config
logging 10.27.0.1
!
!
!
!
snmp-server community public RO
snmp-server community private RW
snmp-server ifindex persist
!
tacacs-server host 10.27.150.201 key none
!
!
control-plane
!
!
!
!
!
!
!
!
!
!
banner exec ^C^[]0;3845-AA0216^C

```

```

!
line con 0
  exec-timeout 0 0
  password lab
line aux 0
line 130
  no activation-character
  no exec
  transport preferred none
  transport input all
  transport output pad telnet rlogin lapb-ta mop udptn v120
line vty 0 10
  exec-timeout 0 0
  password lab
  transport preferred none
  transport input all
!
exception data-corruption buffer truncate
scheduler allocate 20000 1000
end

```

Figure 31: 3845-AA0216 initial configuration

Appendix B: Performance Traffic Configuration

REFERENCES

- [1] "Medianet - Cisco Systems" Available: <http://www.cisco.com/web/solutions/medianet/index.html#~three>.
- [2] "Cisco WAN Bridge" Available: <http://code.google.com/p/wanbridge/>.
- [3] "netem | The Linux Foundation" Available: <http://www.linuxfoundation.org/collaborate/workgroups/networking/netem>.
- [4] "VideoLAN - VLC media player - Open Source Multimedia Framework and Player" Available: <http://www.videolan.org/vlc/>.
- [5] "packETH - ethernet packet generator" Available: <http://packeth.sourceforge.net/>.
- [6] "Net-SNMP" Available: <http://www.net-snmp.org/>.
- [7] "Syslog server | Syslog-ng" Available: <http://www.balabit.com/network-security/syslog-ng/>.
- [8] "TFTPD32 : a opensource TFTP server/service for windows : TFTP server" Available: <http://tftpd32.jounin.net/>.
- [9] "Kiwi Enterprises - Kiwi Syslog Server Overview" Available: <http://www.kiwisyslog.com/kiwi-syslog-server-overview/>.
- [10] "IANA RTP Parameters" Available: <http://www.iana.org/assignments/rtp-parameters>.
- [11] "Cisco IOS Network Management Configuration Guide, Release 12.4T - Web Services Management Agent [Cisco IOS Software Releases 12.4 T] - Cisco Systems" Available: http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cfg_wsma_ps6441_TSD_Products_Configuration_Guide_Chapter.html.
- [12] "Cisco Common Classification Policy Language [Support] - Cisco Systems" Available: http://www.cisco.com/en/US/docs/routers/access/cisco_router_and_security_device_manager/24/software/user/guide/C3PL.html.
- [13] "Cisco IOS Quality of Service Solutions Command Reference - A through C [Support] - Cisco Systems" Available: http://www.cisco.com/en/US/docs/ios/qos/command/reference/qos_a1.html#wp1013312.
- [14] "Cisco IOS Flexible NetFlow Technology White Paper [Cisco IOS NetFlow] - Cisco Systems" Available: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6555/ps6601/ps6965/prod_white_paper0900aecd804be1cc.html.
- [15] "Configuring a Load-Balancing Scheme for Cisco Express Forwarding Traffic [Cisco IOS and NX-OS Software] - Cisco Systems" Available: http://www.cisco.com/en/US/docs/ios/ipswitch/configuration/guide/cef_load_balancng.html.

FOR MORE INFORMATION

For more information about Medianet and Enterprise Medianet please visit:

<http://www.cisco.com/web/solutions/medianet/index.html>

http://www.cisco.com/web/solutions/medianet/ent_medianet.html

or contact your local account representative.

Within the enterprise, the network is primarily a business utility that enables the company to better provide business services. In that light, the monitoring and validation of network's performance for service level agreements (SLAs) is a critical part of supporting the business.

The performance-monitor feature monitors RTP (used for audio and video streams) and TCP traffic for loss, delay and jitter. Per application thresholds and alerts can be set for violations against SLAs.



Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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.

©2006 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0609R)