Device Instrumentation Examples:

IP SLAs & NetFlow

Presented by Emmanuel Tychon
Technical Marketing Engineer

TU Dresden, January 17th 2007
Cisco IOS IP SLAs
## Today’s Multimedia QoS Requirements (Examples)

<table>
<thead>
<tr>
<th>Traffic Type</th>
<th>Maximum Packet Loss</th>
<th>Maximum One-Way Latency</th>
<th>Max. Jitter</th>
</tr>
</thead>
<tbody>
<tr>
<td>VoIP (land line quality)</td>
<td>1 %</td>
<td>120 ms</td>
<td>30 ms</td>
</tr>
<tr>
<td>Video-conferencing</td>
<td>1 %</td>
<td>200 ms</td>
<td>50 ms</td>
</tr>
<tr>
<td>Streaming video (one way video)</td>
<td>2 %</td>
<td>5 s</td>
<td>N/A (assuming the receive buffer is large enough)</td>
</tr>
</tbody>
</table>

### How to measure?
Architecture Overview

IP SLAs is a feature to test the network metrics and to validate SLAs.

IPSLA Sender

IPSLA-Test

IPSLA Responder

Router

IP Host

Targets

Management (optional)
IPSLA Operation with Responder [1/2]
UDP Jitter Operation

- Measures the delay, delay variance (jitter) and packet loss by generating periodic UDP traffic.
- Measures: per-direction jitter, per-direction packet-loss and round trip time.
- Detect and report out-of-sequence and corrupted packets.
- One-way delay requires Cisco IOS® 12.2(2)T or later and clock synchronization between source and destination.
- Always requires IPSLA responder.
- Starting Cisco IOS 12.3(4)T, the operation can measure MOS and ICPIF scores for VoIP.
UDP Jitter - Measurement Example

Each packet contains STx, RTx, ATx, dx and the source can now calculate:

**JitterSD** = (RT2-RT1)-(ST2-ST1) = i2-i1

**JitterDS** = (AT2-AT1)-((RT2+d2)-(RT1+d1)) = i4-i3
UDP Jitter Operation (Example)

- Simulating G.711 VoIP call.
- Use RTP/UDP ports 16384 and above, the packet size is 172 bytes (160 bytes of payload, 12 bytes for RTP header).
- Packets are sent every 20 milliseconds (default interval).
- Marked with DSCP value of 8 (TOS equivalent 0x20).
- Runs every minute (default frequency)

```
ip sla 1
    udp-jitter 10.0.0.2 16384 num-packets 1000
    request-data-size 172
    tos 20
ip sla schedule 1 start-time now
```

\[
\begin{align*}
A &= 20 \text{ ms} \\
B &= 20 \text{ s} \ (1000 \times 20 \text{ ms}) \\
C &= 40 \text{ s} \ (60 \text{ s} - 20 \text{ s})
\end{align*}
\]
NetFlow
What is NetFlow?

NetFlow Subinterface Support  
Egress NetFlow Accounting  
MPLS Egress NetFlow  
NetFlow v9  
MPLS Egress NetFlow Accounting  
MPLS Aware NetFlow  
NetFlow aggregation  
NetFlow Data Export  
NetFlow Dynamic Top Talkers CLI  
NetFlow Input Filters  
NetFlow TOS-based Router Aggregation  
NetFlow Layer 2 for Security Monitoring  
NetFlow MIB and Top Talkers  
NetFlow Data Export version 8  
NetFlow Top Talkers CLI

NetFlow Support per Vlan  
Maximum Mask Aggregate Output NetFlow  
NetFlow Multicast Support  
NetFlow Policy Routing  
NetFlow Reliable Export (SCTP)  
NetFlow Bridged Flow Statistics  
Random Sampled NetFlow  
NetFlow Data Export – Sampled  
NetFlow Export of BGP Next Hop  
NetFlow Multiple Export  
NetFlow export with BGP AS  
NetFlow for IPv6 unicast Traffic  
Flexible NetFlow  
NetFlow Input Filters with multi-sampling rates  
NetFlow Data Export version 5  
Sampled NetFlow  
NetFlow Top Talkers  
NetFlow Minimum Prefix Mask for Router- based Aggreg
Version 5 Flow Format

Flow Keys

- Packet Count
- Byte Count
- Source IP Address
- Destination IP Address
- Start sysUpTime
- End sysUpTime
- Source TCP/UDP Port
- Destination TCP/UDP Port
- Input ifIndex
- Output ifIndex
- Next Hop Address
- Source AS Number
- Dest. AS Number
- Source Prefix Mask
- Dest. Prefix Mask
- Type of Service
- TCP Flags
- Protocol
- Routing and Peering
- From/To Application
- Usage
- Time of Day
- Port Utilization
- QoS
Flexible NetFlow
High Level Concepts and Advantages

- Flexible NetFlow feature allows user configurable NetFlow record formats, selecting from a collection of fields:
  - Key
  - Non-key
  - Counter
  - Timestamp

- Advantages:
  Tailor a cache for specific applications, not covered by existing 21 NetFlow features
  Better scalability since flow record customization for particular application reduces number of flows to monitor

Different NetFlow configuration:
- Per subinterface
- Per direction (ingress/egress)
- Per sampler
- Etc.
Flexible NetFlow
Multiple Monitors with Unique Key Fields

Traffic

Key Fields
- Source IP: 3.3.3.3
- Destination IP: 2.2.2.2
- Source Port: 23
- Destination Oort: 22078
- Layer 3 Protocol: TCP - 6
- TOS Byte: 0
- Input Interface: Ethernet 0

Non-Key Fields
- Packets
- Bytes
- Timestamps
- Next Hop Address

Packet 1

Key Fields
- Source IP: 3.3.3.3
- Destination IP: 2.2.2.2
- Input Interface: Ethernet 0
- SYN Flag: 0

Non-Key Fields
- Packets
- Timestamps

Traffic Analysis Cache

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Dest. IP</th>
<th>Source Port</th>
<th>Dest. Port</th>
<th>Protocol</th>
<th>TOS</th>
<th>Input I/F</th>
<th>...</th>
<th>Pkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.3.3.3</td>
<td>2.2.2.2</td>
<td>23</td>
<td>22078</td>
<td>6</td>
<td>0</td>
<td>E0</td>
<td>...</td>
<td>1100</td>
</tr>
</tbody>
</table>

Security Analysis Cache

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Dest. IP</th>
<th>Input I/F</th>
<th>Flag</th>
<th>...</th>
<th>Pkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.3.3.3</td>
<td>2.2.2.2</td>
<td>E0</td>
<td>0</td>
<td>...</td>
<td>11000</td>
</tr>
</tbody>
</table>
Configure a User-Defined Flow Record

**Configure the Exporter**
Router(config)#flow exporter my-exporter
Router(config-flow-exporter)#destination 1.1.1.1

**Configure the Flow Record**
Router(config)#flow record my-record
Router(config-flow-record)#match ipv4 icmp type
Router(config-flow-record)#match ipv4 icmp code
Router(config-flow-record)#collect counter bytes

**Configure the Flow Monitor**
Router(config)#flow monitor my-monitor
Router(config-flow-monitor)#exporter my-exporter
Router(config-flow-monitor)#record my-record

**Configure the Interface**
Router(config)#int s3/0
Router(config-if)#ip flow monitor my-monitor input
## Flexible Flow Key

<table>
<thead>
<tr>
<th>IPv4</th>
<th>Routing</th>
<th>Transport</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP (Source or Destination)</td>
<td>Payload Size</td>
<td>Destination Port</td>
</tr>
<tr>
<td>Prefix (Source or Destination)</td>
<td>Packet Section (Header)</td>
<td>TCP Flag: ACK</td>
</tr>
<tr>
<td>Mask (Source or Destination)</td>
<td>Packet Section (Payload)</td>
<td>Source Port</td>
</tr>
<tr>
<td>Minimum-Mask (Source or</td>
<td>TTL</td>
<td>ICMP Code</td>
</tr>
<tr>
<td>Destination)</td>
<td></td>
<td>ICMP Type</td>
</tr>
<tr>
<td>Protocol</td>
<td>Options</td>
<td>TCP Flag: ECE</td>
</tr>
<tr>
<td>Fragmentation Flags</td>
<td>Version</td>
<td>TCP Flag: FIN</td>
</tr>
<tr>
<td>Fragmentation Offset</td>
<td>Precedence</td>
<td>TCP Flag: PSH</td>
</tr>
<tr>
<td>ID</td>
<td>DSCP</td>
<td>TCP ACK Number</td>
</tr>
<tr>
<td>Header Length</td>
<td>TOS</td>
<td>TCP Header Length</td>
</tr>
<tr>
<td>Total Length</td>
<td></td>
<td>TCP Sequence Number</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCP Flag: RST</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCP Window-Size</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UDP Message Length</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCP Source Port</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UDP Source Port</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCP Destination Port</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UDP Destination Port</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCP Urgent Pointer</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Flexible Flow Non-Key

- Any of the potential “key” field: will be the value of the first packet in the flow

- Plus

<table>
<thead>
<tr>
<th>Counters</th>
<th>Timestamp</th>
<th>IPv4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bytes</td>
<td>sysUpTime First Packet</td>
<td>Total Length Minimum</td>
</tr>
<tr>
<td>Bytes Long</td>
<td>sysUpTime First Packet</td>
<td>Total Length Maximum</td>
</tr>
<tr>
<td>Bytes Square Sum</td>
<td></td>
<td>TTL Minimum</td>
</tr>
<tr>
<td>Packet</td>
<td></td>
<td>TTL Maximum</td>
</tr>
<tr>
<td>Packet Long</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>