Innovations and Approaches to Traffic Flow Management

Chris Hocker
Consulting Systems Engineer
US Federal/Public Sector
Agenda

• Introduction
• Flexible Netflow
• AVC/NBAR2
• Performance Agent
• Performance Monitor
• IP SLA
• Management
Introduction
Infrastructure

Borderless End-Point/User Services
- Mobility
- Workplace Experience
- Video

Securely, Reliably, Seamlessly: AnyConnect, Mobile Collaboration

Borderless Network Services
- Mobility: Motion
- Green: EnergyWise
- Security: TrustSec
- Application Performance
- Voice/Video: Medianet

Infrastructure
- Switching
- Routing
- Wireless
- Security
- WAAS

Borderless Management and Policy

Application Awareness - Easier service delivery
Next Gen Enterprise
Overall Design

- Business Applications
- Voice and Video traffic
- Data Applications
Flexible Netflow
Cisco IOS NetFlow—What Is It?

- Developed and patented at Cisco Systems in 1996
- NetFlow is the de facto standard for acquiring IP operational data
- Standardized in IETF via IPFIX
- Provides network and security monitoring, network planning, traffic analysis, and IP accounting
- Packet capture is like a wire tap
- NetFlow is like a phone bill

Network World Article—NetFlow Adoption on the Rise
Flexible Netflow (FNF)

- Feature to collect and export network information and statistics
  - Flexibility in defining fields and flow record format
  - Utilize Netflow Version 9 Format
  - UDP-based transport
- Open-standard, can be analyzed by Cisco Insight, Cisco Prime NAM, Cisco Prime Assurance Manager, and 3rd Party Tools
- Consist of data collection (flow monitor) and data export (flow export)
- Is required to collect application info from NBAR2
Flexible NetFlow (FNF)
Multiple Monitors with Unique Key Fields

<table>
<thead>
<tr>
<th>Key Fields</th>
<th>Packet 1</th>
<th></th>
<th>Non Key Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP</td>
<td>3.3.3.3</td>
<td></td>
<td>Packets</td>
</tr>
<tr>
<td>Destination IP</td>
<td>2.2.2.2</td>
<td></td>
<td>Bytes</td>
</tr>
<tr>
<td>Source port</td>
<td>23</td>
<td></td>
<td>Time Stamps</td>
</tr>
<tr>
<td>Destination port</td>
<td>22078</td>
<td></td>
<td>Next-Hop Address</td>
</tr>
<tr>
<td>Layer 3 Protocol</td>
<td>TCP - 6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TOS Byte</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Input Interface</td>
<td>Ethernet 0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Traffic Analysis Cache

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Dest. IP</th>
<th>Dest. I/F</th>
<th>Protocol</th>
<th>TOS</th>
<th>…</th>
<th>Pkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.3.3.3</td>
<td>2.2.2.2</td>
<td>E1</td>
<td>6</td>
<td>0</td>
<td>…</td>
<td>11000</td>
</tr>
<tr>
<td>1.1.1.1</td>
<td>2.2.2.2</td>
<td>E1</td>
<td>6</td>
<td>0</td>
<td>…</td>
<td>11000</td>
</tr>
</tbody>
</table>

Security Analysis Cache

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Dest. IP</th>
<th>Dest. I/F</th>
<th>Input I/F</th>
<th>Sec</th>
<th>…</th>
<th>Pkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.3.3.3</td>
<td>2.2.2.2</td>
<td>E1</td>
<td>E1</td>
<td>101</td>
<td>…</td>
<td>11000</td>
</tr>
</tbody>
</table>

FNF Allows custom monitoring records
Flexible NetFlow (FNF) Configuration Example

1. Configure the Exporter

   ```
   Router(config)# flow exporter my-exporter
   Router(config-flow-exporter)# destination 1.1.1.1
   ```

2. Configure the Flow Record

   ```
   Router(config)# flow record my-record
   Router(config-flow-record)# match ipv4 destination address
   Router(config-flow-record)# match ipv4 source address
   Router(config-flow-record)# collect counter bytes
   ```

3. Configure the Flow Monitor

   ```
   Router(config)# flow monitor my-monitor
   Router(config-flow-monitor)# exporter my-exporter
   Router(config-flow-monitor)# record my-record
   ```

4. Apply to an Interface

   ```
   Router(config)# interface s3/0
   Router(config-if)# ip flow monitor my-monitor input
   ```
Gaining Full Visibility with Flexible Netflow

Flexible NetFlow

- Monitors data from layer 2 thru 7
- Determines applications by combination of port and payload
- Flow information who, what, when, where
- Flexible NetFlow allows your own select of key fields
Identification and Classification
Using FNF

- FNF available on both routers and switches
- Viewable via FNF exports and CLI
Integrated Performance Collection & Exporting

- Integrated performance monitoring available for different type of applications and use cases

Advanced Monitoring

Voice and Video Performance (Performance Monitor)

- 30% of traffic is voice and video

Critical Applications Performance (Performance Agent)

- 40% of traffic is critical applications

Basic Monitoring

What applications, how much bandwidth, flow direction?

(Flexible Netflow and NBAR/NBAR2)
AVC/NBAR2
AVC - How the Solution works

Deep Packet Inspection

DPI engine (NBAR2) identifies applications using L7 signatures

Perf. Collection & Exporting

ISR G2 & ASR collect application bandwidth and response time metrics, and export to management tool

App Visibility & User Experience Report

Advanced reporting tool aggregates and reports application performance

Management Tool

Use QoS or PfR to control application network usage to improve application performance

Control
AVC Building Blocks

Deep Packet Inspection (NBAR2)

Management

Visibility
- FNF
- IOS
- PA
- BW/Export
- BW/App Experience

Control
- HQoS
- PfR

© 2012 Cisco and/or its affiliates. All rights reserved.
What applications do I have running on my network?

Enable NBAR2 on WAN aggregation, Internet edge, or Branch router.

Users call about application problem, how do I isolate the problem?

Enable IOS PA on branch router and get per-segment network delay.

I want to monitor branch user experiences accessing Oracle application in my Data Center

Enable IOS PA on branch router and monitor transaction time and server delay.

YouTube and BitTorrent are taking over my network

Use NBAR2 and QoS policy to restrict recreational traffic. Mark internal web traffic with higher priority.

Do you have this problem?

What you can do with AVC solution
AVC Sample Monitoring Policy

AVC Monitoring Policy

Enterprise Voice & Video
→ Match enterprise subnet
→ Match RTP traffic

→ Collect Media Performance
→ Collect Traffic Statistics

Enterprise TCP Apps
→ Match datacenter subnet
→ Match TCP

→ Collect ART
→ Collect Traffic Statistics

Enterprise Cloud Apps
→ Match SFDC
→ Match Office 365

→ Collect ART
→ Collect Traffic Statistics

Web Browsing
→ Match HTTP

→ Collect URL Sample
→ Collect Traffic Statistics

Rest of traffic
→ Match any

→ Collect Traffic Statistics
What is An Application?

HTTP
Are these applications?
80

FTP
20/21

POP3
110

IMAP
143

HTTP S
Or just ports?
443

SMTP
25

What about these?

webex
Rhapsody
Gmail
YouTube
RCA
McAfee
talk
BitTorrent
Windows Server Update Services
salesforce.com

© 2012 Cisco and/or its affiliates. All rights reserved.
How to Identify Applications?
Let’s have a look at HTTP…

Layer-4 Non-Application Aware Reporting (Courtesy of Lancope)
How to Identify Applications?
Let’s have a look at HTTP…

Layer-7 Application Aware Reporting (Courtesy of Lancope)
Next Generation NBAR (NBAR2)

- New DPI engine provides Advanced Application Classification and Field Extraction Capabilities from SCE
- Protocol Pack allows adding more applications without upgrading or reloading IOS
Multiple methods to use the engine, depending on need.

Enable NBAR Protocol Discovery at interface level
- All traffic is classified based on protocol.
- Results (packets, bytes, application) are available via CLI and MIB

Invoke ‘match protocol’ CLI in C3PL/MQC (class-map) CLI
- Used in a number of different IOS functions (QoS, performance monitor, IOS FW)
- Results vary depending on IOS function used

Invoke ‘application name/ID’ fields in flexible netflow (FNF)
- Application name/ID is included in NetFlow export reports

PfR NBAR integration via ‘traffic-class application nbar’ CLI
Identification and Classification
Using NBAR/NBAR2

- Apply NBAR/NBAR2 to identify traffic.
- Visualized via FNF exports or NBAR MIB
Flexible NetFlow & NBAR Integration

show flow mon <app_mon> cache
IPV4 SRC ADDR  IPV4 DST ADDR  APP NAME  ...  
==========================================
10.0.1.1         10.0.1.2         nbar rtcp
10.0.1.1         10.0.1.2         nbar ssh
10.0.1.1         10.0.1.2         nbar telnet
10.0.1.1         10.0.1.2         NBAR lunar_light

NBAR = Custom Applications

NBAR application name inclusion in Flexible NetFlow record creates association of application name with flow reporting.

Reporting Example (Cisco Prime Assurance)
Flexible NetFlow
NBAR2 Integration – Field Extraction

- NBAR extracts fields from flows and exposes it into Flexible NetFlow
- HTTP Fields (Hostname and URL) planned in 15.2(4)M and IOS XE 3.7.0S

```
show flow mon <app_mon> cache
IPV4 SRC ADDR   IPV4 DST ADDR   APP NAME       Hostname         URL … …
===============  ==============  =============  ===============  ===========
10.0.1.1         10.0.1.2       nbar http     www.google.com   /news
```

```
router(config)# flow record HTTP_record
router(config-flow-record)# match ipv4 source address
router(config-flow-record)# match ipv4 destination address
router(config-flow-record)# match application name
router(config-flow-record)# match application http hostname
router(config-flow-record)# match application http URL
```
Enable enterprise application monitoring and management

### Custom Enterprise Application

<table>
<thead>
<tr>
<th>App</th>
<th>Server</th>
<th>URI</th>
<th>BW</th>
<th>Resp. Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payroll</td>
<td>server1.example.com</td>
<td>-</td>
<td>2M</td>
<td>100ms</td>
</tr>
<tr>
<td>Doc. Management</td>
<td>server2.example.com</td>
<td>/doc</td>
<td>1M</td>
<td>250ms</td>
</tr>
<tr>
<td>Software Rep.</td>
<td>server2.example.com</td>
<td>/software</td>
<td>5M</td>
<td>30sec</td>
</tr>
</tbody>
</table>

- **Today:** NBAR supports custom app by port or values in payload
- **New:** Custom application match on HTTP URL
- Configuration through PAM
- Recognize custom app for reporting and for QoS policy

**Cisco Prime Assurance**

ASR1K: XE 3.8S
ISR G2: 15.2(4)M1
PAM 2.0
IPv6 Application monitoring

- Configure traffic statistics collection for IPv4 and IPv6 protocols
- IPv6 application reporting with Flexible NetFlow

```
interface Gi1/1
  ip nbar protocol-discovery [ipv4|ipv6]

flow record app_record
  match ipv6 source address
  match ipv6 destination address
  match application name

# sh flow monitor APPIIPv6  cache format table

<table>
<thead>
<tr>
<th>IPV6 SOURCE ADDRESS</th>
<th>IPV6 DESTINATION ADDRESS</th>
<th>APPL NAME</th>
</tr>
</thead>
</table>
```
Performance Agent
Monitor Branch End User Experiences
IOS Performance Agent (PA)

Key Features
Extend Application Response Time (ART) to remote sites
Interact with NBAR2
Standard NFv9 export
In-box metric aggregation reduces number of flow records sent across WAN

Benefits
Visibility into application performance across WAN
Quantify user experience through ART
Troubleshoot application performance
Track service levels for application delivery
PA separates application delivery path into multiple segments

- Server Network Delay (SND) is typically the WAN Delay
# List of Metrics reported by IOS PA

## Traditional FNF Metrics
- Application ID (from NBAR2)
- Client/Server Bytes
- Client/Server Packets
- Source MAC Address
- Input/Output Interface
- IP DSCP

## ART Metrics
- CND - Client Network Delay (min/max/sum)
- SND – Server Network Delay (min/max/sum)
- ND – Network Delay (min/max/sum)
- AD – Application Delay (min/max/sum)
- Total Response Time (min/max/sum)
- Total Transaction Time (min/max/sum)
- Number of New Connections
- Number of Late Responses
- Number of Responses by Response Time (7-bucket histogram)
- Number of Retransmissions
- Number of Transactions
- Client/Server Bytes
- Client/Server Packets

## WAAS Express Metrics
- Input/Output Bytes
- WAAS Connection Mode
  - TFO, TFO/LZ, TFO/DRE, TFO/LZ/DRE
- Input/Output DRE Bytes
- Input/Output LZ Bytes
Understand IOS PA ART Metrics Calculation

- **Response Time (RT)**
  \[ t(\text{First response pkt}) - t(\text{Last request pkt}) \]

- **Transaction Time (TT)**
  \[ t(\text{Last response pkt}) - t(\text{First request pkt}) \]

- **Network Delay (ND)**
  \[ \text{ND} = \text{CND} + \text{SND} \]

- **Application Delay (AD)**
  \[ \text{AD} = \text{RT} - \text{SND} \]
Performance Monitor
Performance Monitor (PerfMon)
What is the goal?

- Native RTP and TCP Analysis
  - **Visibility**: Network nodes are able to discover & validate RTP, TCP and IP-CBR traffic on hop by hop basis
  - **SLA**: À la carte metric (loss, latency, jitter etc.) selections, applied on operator selected sets of traffic
  - **Troubleshooting**: Allows for fault isolation and network span validation
Performance Monitor
Position vs FNF and IP SLA

Active Monitoring

Router 1
IPSLA Sender

Active Probing

IPSLA Responder
Router 2

Passive Monitoring

Flexible Netflow

Flow Record

Enhanced RTP and TCP metrics reporting
Filtering and classification (based on existing C3PL model)

PerfMon

Flow Record
New Metrics
Performance Monitor 1.0 - IOS 15.1(3)T

- Variety of network centric metrics added.
- More metrics and protocols coming

<table>
<thead>
<tr>
<th>Metric/Data Value</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>transport rtp ssrc</td>
<td>RTP</td>
</tr>
<tr>
<td>application media packets counter (long)</td>
<td>All</td>
</tr>
<tr>
<td>application media bytes counter (long)</td>
<td>All</td>
</tr>
<tr>
<td>application media bytes rate</td>
<td>All</td>
</tr>
<tr>
<td>application media packet rate</td>
<td>All</td>
</tr>
<tr>
<td>transport packets lost counter</td>
<td>RTP</td>
</tr>
<tr>
<td>transport packets expected counter</td>
<td>RTP</td>
</tr>
<tr>
<td>transport packets lost rate</td>
<td>RTP</td>
</tr>
<tr>
<td>counter bytes rate</td>
<td>All</td>
</tr>
<tr>
<td>transport event packet-loss counter</td>
<td>TCP, RTP</td>
</tr>
<tr>
<td>transport round-trip-time</td>
<td>TCP</td>
</tr>
<tr>
<td>transport rtp jitter maximum</td>
<td>RTP</td>
</tr>
<tr>
<td>transport rtp jitter minimum</td>
<td>RTP</td>
</tr>
<tr>
<td>transport rtp jitter mean</td>
<td>RTP</td>
</tr>
<tr>
<td>application media packets rate variation</td>
<td>IP-CBR</td>
</tr>
<tr>
<td>application media event</td>
<td>-</td>
</tr>
<tr>
<td>counter packets dropped</td>
<td>All</td>
</tr>
</tbody>
</table>
New Metrics
Performance Monitor 2.0 - IOS 15.2(2)T

- Additional audio/video metrics
- More emphasis on TCP metrics

<table>
<thead>
<tr>
<th>Metric/Data Value</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>RTP payload type</td>
<td>RTP</td>
</tr>
<tr>
<td>IPv6 support</td>
<td>(all new and existing metrics)</td>
</tr>
<tr>
<td>Flexible NetFlow (FNF) field imports</td>
<td>all</td>
</tr>
<tr>
<td>TCP Max Segment Size</td>
<td>TCP</td>
</tr>
<tr>
<td>TCP min/max/avg Window Size</td>
<td>TCP</td>
</tr>
<tr>
<td>Client/server bytes</td>
<td>TCP</td>
</tr>
<tr>
<td>Client/server packets</td>
<td>TCP</td>
</tr>
<tr>
<td>Out of order bytes</td>
<td>TCP, RTP</td>
</tr>
<tr>
<td>Out of order packets</td>
<td>TCP, RTP</td>
</tr>
</tbody>
</table>
Perf-mon: Wide Applicability

- Tested with:
  - Cisco EX90, MXP1700, Polycom, Cisco TelePresence (1xxx, 3xxx), CUVA, CP-9971, CP-7985, CP-7960 (audio only),
  - Cisco Video Surveillance Cameras, WebEx (HTTPS), IPTV (VLC)
  - Just plain web transactions (wget)
Performance Monitor (PerfMon)
NetFlow Export

- NetFlow based metrics export from network
  Can be based on flows, or aggregations of flows, etc.
  Variety of uses: capacity planning, troubleshooting, baselining, etc.
- 14+ NMS application vendors engaged!
  Plixer Scrutinizer, SevOne SevOneNMS
  ActionPacked LiveAction (configuration also planned)
• Metrics can be tested against thresholds to trigger actions
  Multi-level Alarm Raise/Clear, SNMP Traps, Syslog, embedded scripts, automatic mediatrace,
  Radar: Path adaptation (PfR)
Sample Config to Monitor RTP Traffic

```
flow exporter pam
    destination 10.35.89.61
    transport udp 9991
!
flow monitor type performance-monitor medianet-perf-mon-monitor
    record default-rtp
    exporter pam
!
class-map match-any rtp-traffic
    match protocol rtp
!
policy-map type performance-monitor medianet-perf-mon
    class rtp-traffic
        flow monitor medianet-perf-mon-monitor
            react 1 transport-packets-lost-rate
            threshold value ge 5.00
            action syslog
!
interface GigabitEthernet0/0
    service-policy output wan-qos
!
service-policy type performance-monitor input medianet-perf-mon
service-policy type performance-monitor output medianet-perf-mon
```
IP SLA
IP SLA: Measuring Network Paths

**Uses**
- Availability
- Network Performance Monitoring
- VoIP Monitoring
- Service Level Agreement (SLA) Monitoring
- Network Assessment
- Multiprotocol Label Switching (MPLS) Monitoring
- Trouble Shooting

**Measurement Metrics**
- Latency
- Packet Loss
- Network Jitter
- Dist. of Stats
- Connectivity

**Operations**
- Jitter
- FTP
- DNS
- DHCP
- DLSW
- ICMP
- UDP
- TCP
- HTTP
- LDP
- H.323
- SIP
- RTP
- RADIUS
- Video

**Source**
- Defined Packet Size, Spacing COS and Protocol
- Cisco IOS Software
- IP SLA

**Destination**
- Cisco IOS Software
- IP SLA

**MIB Data**
- Active Generated Traffic to Measure the Network

**IP SLA Jitter responder supported on CTS**
IPSLA Video Operation
Embedded Traffic Simulator

- IPSLA known in industry for jitter, ICMP, etc. probes
- Most probes measure experience without affecting user traffic (hopefully)
- Need traffic to stress test network
- IPSLA VO provides
  - Realistic representation of arbitrary video (RTP) traffic
    - Packet sizes, burstiness, traffic rate, etc.
  - pre-packaged profiles:
    - IPTV, Video Surv, CTS
  - Extensible via data file
  - Custom profile generation from packet capture
Management
NBAR Protocol Discovery MIB
Traffic Classification and Real-Time Statistics

• Automatically uses all PDLMs
  Run protocol discovery instead of specifying individual protocols

• Provides statistics per application recognized by NBAR via SNMP:
  Bit rate (bps), Packet counts, Byte counts
  Includes statistics for traffic identified with user-defined custom application classification

• Enable or disable protocol discovery per interface

• Configure and view multiple top-n tables listing protocols by bandwidth usage

• Configure thresholds and configure notifications when these thresholds are crossed
Reports - NetFlow & MIB

- **NetFlow** based metrics **export** from network
  
  Can be based on **flows**, or **aggregations of flows**, etc.  
  Variety of uses: **capacity planning**, **troubleshooting**, **baselining**, etc.

- Historical interval reports available on box via **WSMA, MIB, mediatrace, and CLI**
CBQoS MIB

- IOS QoS collects vital information regarding health of QoS classes
- Pre and Post bytes, drops, etc
- Same class names from different routers can be compared
- ‘snmp mib persist CBQoS’
- RFC 3289 (DiffServ MIB) 15.2(4)M
Cisco Prime Assurance

**Cisco Prime™ Assurance:**
- Centralized service assurance Dashboard
- Reporting and trends
- Network readiness assessment
- Network abstraction
- Provides northbound APIs

**Cisco Prime Network Analysis Module (NAM):**
- Packet and flows analysis
- Application response time
- Voice quality metrics
- Operates standalone and with Cisco Prime Assurance

![Diagram showing network infrastructure and components](image.png)
## AVC Management

<table>
<thead>
<tr>
<th>Company</th>
<th>Product</th>
<th>Use Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco</td>
<td>PAM</td>
<td>Network and App Monitoring. Control GUI (future)</td>
</tr>
<tr>
<td>Gomez &amp; DynaTrace</td>
<td></td>
<td>APM combined with App-aware Network Monitoring</td>
</tr>
<tr>
<td>InfoVista</td>
<td>5View</td>
<td>App-aware Network Monitoring</td>
</tr>
<tr>
<td>LiveAction</td>
<td></td>
<td>Control (QoS) GUI, App-aware Network Monitoring</td>
</tr>
<tr>
<td>Scrutinizer</td>
<td></td>
<td>App-aware Network Monitoring</td>
</tr>
</tbody>
</table>

**Others:** Living Object, Insight, CA
Thank you.