Real Time Topology Based Flow Visualization

John K. Smith  jsmith@referentia.com
Referentia Systems Incorporated

Flocon 2011, Salt Lake City, UT
Agenda

• Flow Visualization Tool Overview
• Visualizations and Design Issues
• Use Cases

NOTE: Networks shown in this presentation are simulated, not actual DoD networks, traffic or addresses.
Beginnings

• **Initial Goal**
  - Network Quality of Service Monitor and Control
  - Tactical Military Networks
  - Easy to use for E3-E5 (Sergeant)

• **Working With**
  - Office of Naval Research
  - U.S. Marines
    - Marine Forces Pacific (MARFORPAC)
    - 3<sup>rd</sup> Marine Expeditionary Force (III MEF)
Tool Overview

- Quality of Service
- Routing Visualizations
- Flow
- Service Level Agreement
- Configuration
- Monitoring
- Historical Analysis
- Visualization

- Network Management
- Network Situational Awareness
- Computer Network Defense
Hand Drawings

Visio Diagrams

- Can’t interactively explore
- No correlation to live network data
- Not always accurate or kept current
Mental Model

- Accuracy and fidelity of the model
- Ability to explore the model
- Interact with the model
Mental Model and Situational Awareness

Network Situational Awareness

Mental Model

1. Perception
2. Comprehension
3. Projection

Information
Router, Switch, IDS/IPS, Sensors

Response/Remediation
Decision Making

Network
DMTF CIM Model

- Very detailed model of network devices and protocols
- Vendor neutral
- Currently we use
  - A simpler subset of CIM
  - Performance and flow data added
Tool Design

- **Java 6 JRE**
  - **Server**
    - Flow
    - QoS
    - Routing
    - IPSLA
    - Configure Engine
    - Monitor Engine
    - SNMPv2/v3, SSH/Telnet, NetFlow/sFlow/JFlow

- **UI**
  - Java Topology Visualization
  - Java Swing Based Libraries

- **Client**

- **API**
  - DB – time series/SQL

- **Cisco Router and Switches**
  - Any Flow enabled device
  - Any RFC 1213 MIB supported device
Topology Based Flow Visualization

- **Flow Collector**
  - Not generator like Argus or YAF
  - Time series storage
  - Netflow v5-v9, sFlow, Jflow
  - Cisco Flexible Netflow setup

- **Flow Visualization**
  - Topology from real networks
    - Discovery
    - Model creation from config
    - Node and edge displays
  - Flow Projection
    - “Real Time” – as real time as NetFlow can be
    - Projection of flows onto topology
What is it for?

- **Network Management**
  - It’s really hard to know what’s going on in a router
  - Let alone across routers in a network
  - Where problem locations are, where to fix

- **Network SA**
  - Knowing how flows are routed
  - Knowing direction, load sharing
  - Flow – Routing – QoS – SLA

- **CND**
  - Doesn’t solve finding needle in haystack problem
  - Doesn’t do pattern analysis
  - Can be used with sensors to alert and monitor events
  - Response planning and actions
  - Compliments forensic analysis
Flow System View

- Panning
- Zooming
- Color Coding
- Aggregation
Flow System View

- Filtering
- Tracing of Flows
- Source and Destination ID
- DNS Resolution
- Historical Replay
- Black Listed IP ID
Device Topology View

- Device Level View
- Process Flows in Real Time
- Updates Display – 10 sec
- Shows IP to IP, Port to Port
- Switching Path
Individual Flow

- Isolation down to particular source
- Aggregation along shared path
- Highlighting of black listed address
- Tunnel to physical interface association
- Indicators for policies such as ACL, QoS, PBR
Device Topology View

- **Table View**
- **Using Flexible Netflow**
  - IPv6
  - MAC, TCP
  - AS Number
  - Next Hop etc
Display Updates and NetFlow Behavior

- **Static display easier, real time* is harder**
- **How long to leave flows displayed**
  - Process flow records as they come in
  - Update/Refresh rate of the display – 10 sec
  - Aging of the flows out of the display
  - Router – active/inactive timer settings

### Table: Flow Behavior

<table>
<thead>
<tr>
<th>Poll</th>
<th>Aging (sec)</th>
<th>Time (min)</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 sec</td>
<td>2 min</td>
<td>40 sec flow</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 min flow</td>
</tr>
</tbody>
</table>

- **Active Timer**: 1 min
- **Inactive Timer**: 10 sec

*Real flow aging times can be adjusted based on network requirements.*
Flow Display and Processing Issues
Flow Display and Processing Issues

- Issues
  - Shear number of flows
  - Efficient storage and retrieval for display
  - Temporal aspect of flows
  - Display layer performance
- Top N or Bottom N Flows
  - Reduce amount of displayed items
  - Aggregation of same flow records
- Merging
  - Merge flows based on attributes
  - DSCP, IP address, Rate, Bytes
  - Match based
- Filtering
  - Basic - src/dst ip, port, dscp etc
  - Advanced – BGP AS, next hop, ..
NetFlow Specific Issues

- **Flow Data**
  - Router sourced or consumed flows
  - Index to interface number mapping, Null/Local
  - Not always correct, MIB issues

- **Differences**
  - ASA vs Router vs Switch
  - Intra VLAN, Layer 3
  - NetFlow and sFlow
  - SNMP based flow

- **Time Related**
  - Flow time outs – active/inactive
  - Flow time stamps

- **NetFlow configuration**
  - Flexible NetFlow
Visualization - Scanning
Visualization - Multicast Traffic
Last Hop Router

- Egress flows not showing
- Traffic shown as going to Null but really router CPU
Visualization - Load Sharing
Visualization - Load Sharing
Visualization - Load Sharing
Interactions with Flows

1) Identify flow visually
2) Create ACL
3) ACL for PBR
Correlating Flow with & QoS and Flow Based Graphs

Investigating Inbound Traffic Spike

- FA0 interface showed spike in flows
- Inbound flow graphed
- Correlated to QoS statistics graph
Flow Layer Visualization
Quality of Service and Ping Visualization
Flow with other Network Visualization

- Service Level Agreement
  - Latency, Jitter, Loss, MOS

- Flow
  - Actual Path, Load Sharing

- Routing
  - Route Path, Asymmetric, Summarization

- Quality of Service
  - Priority, BW, Queues, Drops
Usage: Talisman Saber Exercises US Marines

Scholfield Hawaii
Australia
Okinawa

Marines III MEF
• **Fleet monitoring of operational traffic**  
  - Traffic over satcom  
  - Voice from ship to shore  
• **CND exercise**  
  - Monitoring red team attacks  
  - Working with sensors
Issues and Limitations

• **Not Good At**
  - Showing large quantities of flows
  - Finding needle in hay stack
  - Pattern or algorithm analysis

• **Usage Issues**
  - Access to routers
  - Over WAN usage
  - Flow from multiple routers
  - Bandwidth in monitoring
Summary

• **Future Work**
  • Additional Network SA
  • Distributed Architecture
  • Cisco Flexible Netflow

• **For More Information**
  • jsmith@referentia.com
  • www.actionpacked.com