
University of Colorado Boulder

Network Management and Automation

Integrated Traffic Monitoring (ITM) and NetFlow

Levi Perigo, Ph.D.
University of Colorado Boulder
Department of Computer Science

Review

Integrated Traffic Monitoring (ITM) and NetFlow

- **Method of tracking flow patterns across interfaces on a network device (router)**
- **Inbound and outbound (ingress/egress)**
- **Sent to NetFlow 9 over UDP 9996**
  - External data collector
  - Internal "top traffic" collector
    - ***Analyzing traffic flow patterns and displaying them in a graph***

Why NetFlow?

- **You need network situational awareness but full packet capture doesn't scale**

- **Problems with full PCAP:**
  - Storage requirements
  - PII Issues
  - Difficult to search

Why NetFlow?

- **Minimal storage requirements**
- **Quick large scale analysis**
- **Distributed systems**
- **Historic querying**
- **Setting baselines**
- **Anomaly detection**

ITM

- **By monitoring traffic flows, decisions can be made on:**
  - Traffic engineering
  - Traffic profiling
  - Security measures
  - QoS
- **Standardized methodology for:**
  - Recording
  - Analyzing
  - Viewing
- **Smart decisions for optimal network configurations**

Traffic Engineering

- **Manipulating routed traffic based on captured traffic flow patterns**
  - (Using paths that wouldn't be selected through standard routing procedures)

- **Reviewing traffic flow data, traffic engineering can be used per network basis**
  - Understanding beginning-to-end traffic trends
    - ***Load distribution across multiple paths or reroute traffic to a preferred path***

Traffic Profiling

- **Analyzing where traffic is entering and leaving the network**
  - Network traffic trends
- **Traffic flow sorted by:**
  - Interface
  - Ingress/egress
  - Time
  - Protocol
  - Source/destination
- **Overall view of the network**
  - Heavy traffic flow = additional network resources
    - ***Present and future networks (design)***

Security

- **Monitoring traffic on the network**
  - Obtains a baseline
  - Reveals anomalies
    - ***Virus***
  - Changes in network behavior
  - What is “normal”

Quality of Service (QoS)

- **Heaviest traffic flows**

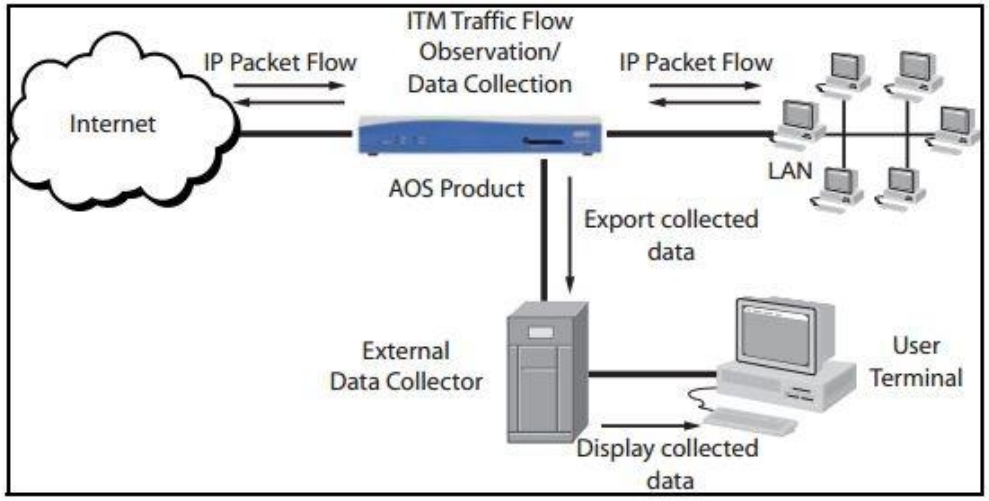
- **Prioritization of traffic**
  - What type of traffic
    - ***IP addresses***
    - ***Protocols***
    - ***Interfaces***

ITM Implementation

- **Can be distributed or single server**
  - Distributed better for large network
  - Single server better for single gateway deployments

ITM Process

- **Capture traffic flow data**
- **Send to external data collector/analyzer (flow cache)**
- **Uses software to analyze it and display to terminal**



Traffic Flow Data Criteria

- **Traffic is grouped; Similar traffic = flow**
  - Traffic flow type: ingress/egress
  - Interface crossed
  - Source IP
  - Destination IP
  - Type of Service (ToS) – IPP, DSCP, PHB
  - Protocol type
  - Source port
  - Destination port

Traffic Flow Sampling & Filtering

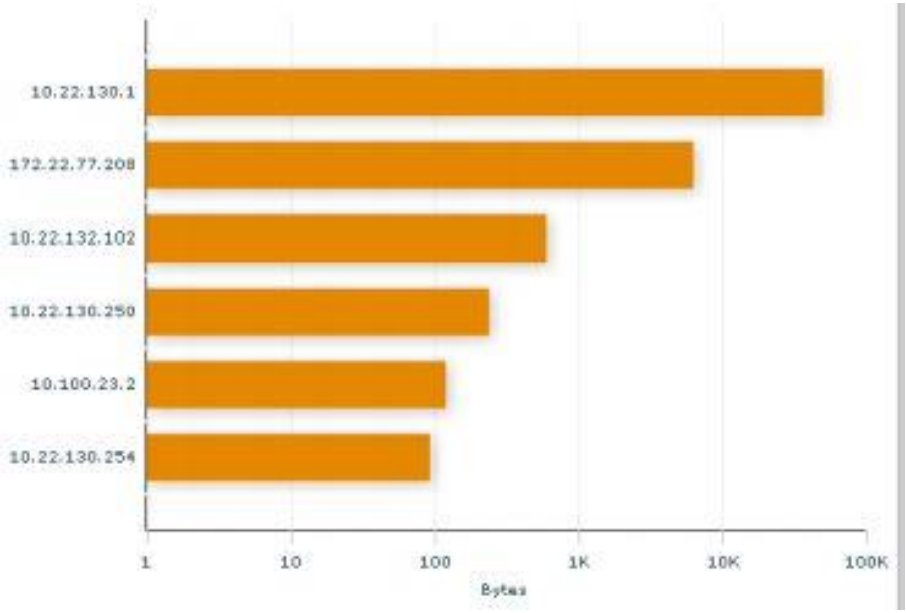
- **Sampling – reduces amount of flow data**
  - Minimizing memory/CPU
  - 1/100 packets (random or fixed)
- **Filtering**
  - ACL
- **Sample and Filter**

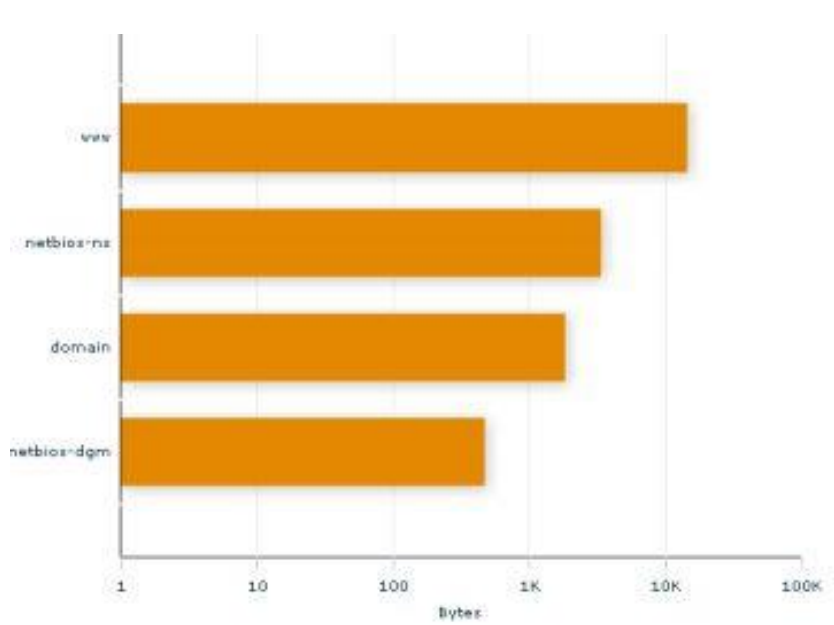
Traffic Flow Data Export

- **Flow records are sent via a “template”**
- **Template describe type/length of headers and what to expect**
- **Templates sent “periodically” due to UDP**

Ingress Data Template	Egress Data Template
ToS Bits	ToS Bits
Packets in a Flow	Packets in a Flow
Bytes in a Flow	Bytes in a Flow
Input Interface	Input Interface
System Up Time of First Packet	Output Interface
System Up Time of Last Packet	Next Hop IP Address
Flow Direction	System Up Time of First Packet
	System Up Time of Last Packet
	Flow Direction

Top Talkers


10.22.130.1
172.22.77.208
10.22.132.102
10.22.130.250
10.100.23.2
10.22.130.254
1
10
100
1K
10K
100K
Bytes


www
netbios-ns
domain
netbios-dgm
1
10
100
1K
10K
100K
Bytes

External Data Collectors

- **Commercial**
  - IBM: Netcool
  - IdeaData: Traffic and Security Analysis
  - SolarWinds
  - Fluke

- **Freeware / Open Source**
  - PNDA
  - Flow-Viewer
  - Plixer – Scrutinizer
  - SiLK
  - NTOP

Network-Based Application Recognition Overview (NBAR/NBAR2)

- **Intelligently classifies and enforces QoS policies**

- **Protocol Discovery**
  - One week initial runtime
    - ***When new Internet applications arrive (streaming)***

- **Benefits**
  - Prioritization
  - Reduce WAN expenses
  - Improve Web response
  - Improve VPN performance (classify early)

Network Design

- **Gather existing documentation and query**
- **Network audit**
  - NetFlow
  - NBAR
  - IP SLA
  - SPAN
- **Traffic analysis**

Big Data Analysis (BDA)

- **Platform for Network Data Analytics (PNDA)**
- **ITM & Netflow**
- **Data lake**
- **Look for trends**
- **Make trend-based, intelligent network decisions**
  - Like what?

Questions?