

# NetFlow Seminar

*Erick Faul*

*Erick.faul@netqos.com*

# Why NetFlow: The Past

- ◆ NetFlow was developed as an improvement to switching technology. Fundamentally it was a caching technology that improved performance in the presence of long lists (ACL).
- ◆ Cisco Switching Technologies:
  - Process Switching: lookup per packet
  - Fast Switching: lookup first packet, cache lookup
  - NetFlow Switching: additional caching to speed ACLs
  - Cisco Express Forwarding (CEF): FIB replaces cache
- ◆ NetFlow switching has since been replaced by the CEF FIB as the Cisco premiere switching approach.
  - CEF eliminates cache churn with common short-lived flows
  - CEF is less CPU intensive than route-caching

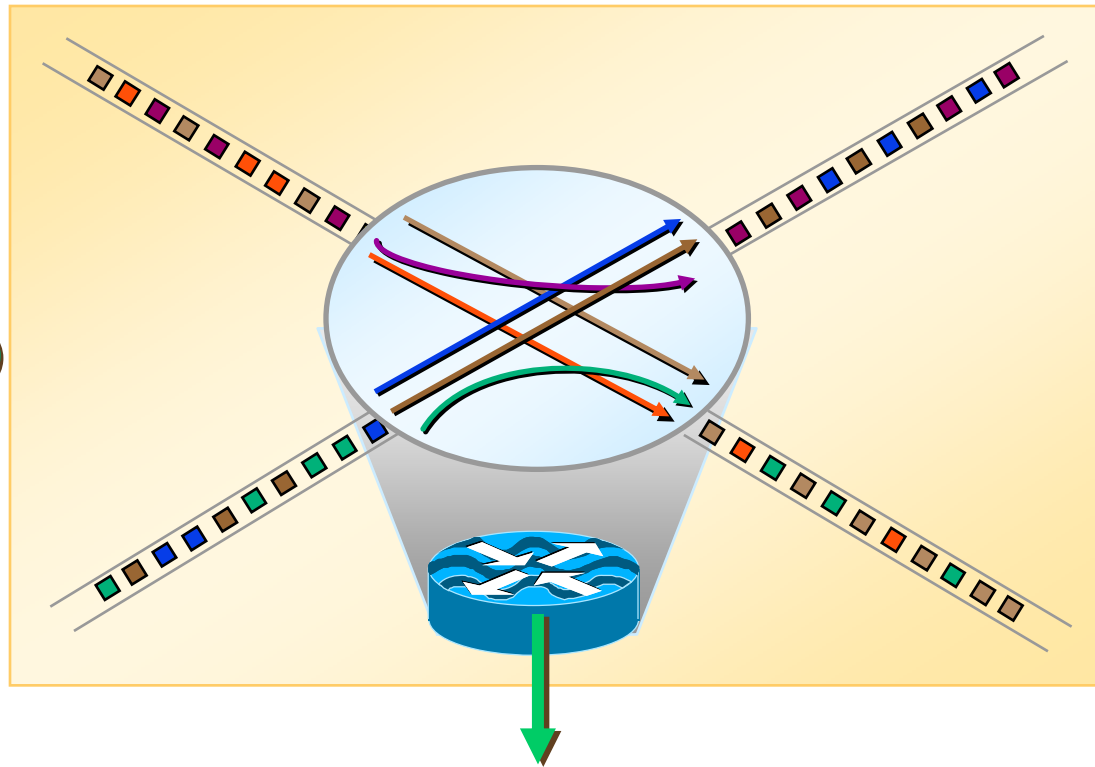
# What is NetFlow Today?

- ◆ What is NetFlow today?
  - Software in Cisco IOS that caches information on Cisco flows to provide
    - Feature acceleration (Policy routing, IP accounting, crypto encryption/decryption-complex ACL etc)
    - Very rich statistical information
      - ⇒ Answers who, what, when, where, how
      - ⇒ Useful for trouble-shooting, capacity planning, security threat detection, accounting, etc

# What is a NetFlow “Flow”?\*

Unidirectional IP stream with unique:

1. Source IP Address
2. Dest. IP Address
3. Source Layer 4 Port
4. Dest. Layer 4 Port
5. Layer 3 IP Protocol
6. Packet Marking (ToS)
7. Input Interface



Router sends stats to a collector via UDP

# NetFlow Versions

- ◆ NetFlow v1, v5, v7 are similar
- ◆ NetFlow v1 is the oldest and not frequently used
- ◆ NetFlow v5 adds flow sequence numbers, subnet masks, and AS information to the data in v1
- ◆ NetFlow v7 is only supported in Catalyst 5000/6000 series switches
- ◆ NetFlow v8 supports five aggregation schemes
- ◆ NetFlow v9 supports flexible templates
  - Offload link load – transfer only fields of interest
  - Offload NetFlow collector/harvester processing
  - Flexibility to support future features
  - And still provide useful information...or not

# NetFlow Platform Support

Cisco IOS™ Software Release Version	Supported NetFlow Export Version(s)	Supported Cisco Hardware Platforms
11.1CA, 11.1CC	v1, v5	7200, 7500, RSP7000
11.2, 11.2P	v1	7200, 7500, RSP7000
11.2P	v1	Route Switch Module (RSM), 11.2(10)P and later
11.3, 11.3T	v1	7200, 7500, RSP7000
12.0	v1, v5	1720, 2600, 3600, 4500, 4700, AS5800, 7200, uBR7200, 7500, RSP7000, RSM
12.0T 12.0S	v1, v5	1720, 2600, 3600, 4500, 4700, AS5800, 7200, uBR7200, 7500, RSP7000, RSM, MGX 8800 RPM, BPX 8600
12.0(3)T and later 12.0(3)S and later	v1, v5, v8	1400*, 1600*, 1720, 2500*, 2600, 3600, 4500, 4700, AS5800, AS5300**, 7200, uBR7200, 7500, RSP7000, RSM, MGX8800 RPM, BPX 8650
12.04XE	v1, v5, v8	7100
N/A	v7	Catalyst 5K NetFlow Feature Card (NFFC) Catalyst 6K with MSFC card
12.0(6)S	v8	12000

\*Support for NetFlow Export v1, v5, and v8 on 1600 and 2500 platforms is targeted for Cisco IOS software release 12.0(5)T. NetFlow support for these platforms will not be available in the Cisco IOS 12.0 mainline release.

\*\*Support for NetFlow Export v1, v5, and v8 on AS5300 platform is targeted for Cisco IOS software release 12.0(7)XR.

# Packet Marking Maps to NetFlow TOS Field\*

Marker	Preservation	Value range
IP precedence	Throughout a network	8 values, 2 reserved (0 to 7)
DSCP	Throughout a network	64 values, 32 are standard (0 to 63)
QoS group	Local to a router	100 values (0 to 99)
MPLS experimental bits	Throughout an MPLS network (optionally throughout an entire IP network)	8 values
Frame Relay DE bit	Throughout a Frame Relay network	2 values (0 or 1)
ATM CLP bit	Throughout an ATM network	2 values (0 or 1)
IEEE 802.1Q or ISL CoS	Throughout a LAN switched network	8 values (0 to 7)

# Useful Websites

- ◆ NetFlow
  - [www.cisco.com/go/netflow](http://www.cisco.com/go/netflow)
- ◆ Internet Protocol Flow Information Export (IPFIX) is an IETF Working Group
  - [www.ietf.org/html.charters/ipfix-charter.html](http://www.ietf.org/html.charters/ipfix-charter.html)
- ◆ Cisco IT Case Study
  - [http://www.cisco.com/warp/public/732/Tech/nmp/docs/cisco\\_it\\_case\\_study\\_netflow.pdf](http://www.cisco.com/warp/public/732/Tech/nmp/docs/cisco_it_case_study_netflow.pdf)
- ◆ NetFlow version 9 is the basis for the standard in the IETF Standards Track
  - <http://www.ietf.org/internet-drafts/draft-ietf-ipfix-protocol-07.txt>

A starburst-shaped badge with a jagged orange border and a black background, containing the word "New" in white, slanted text.

# NetQoS ReporterAnalyzer™

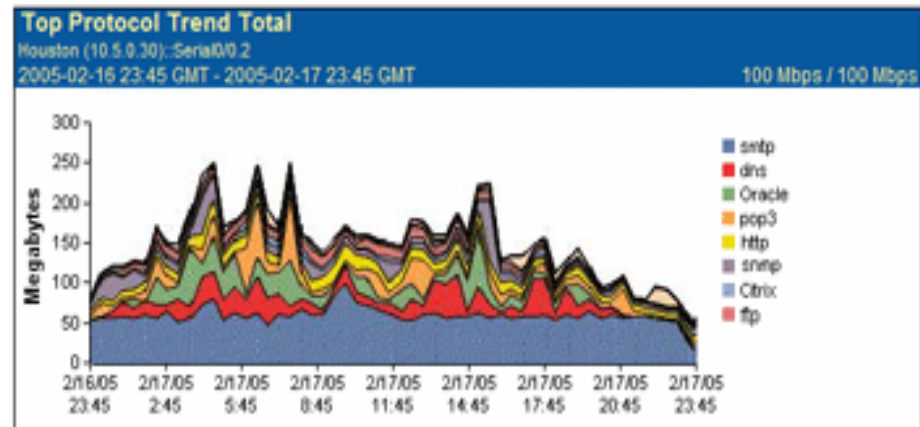
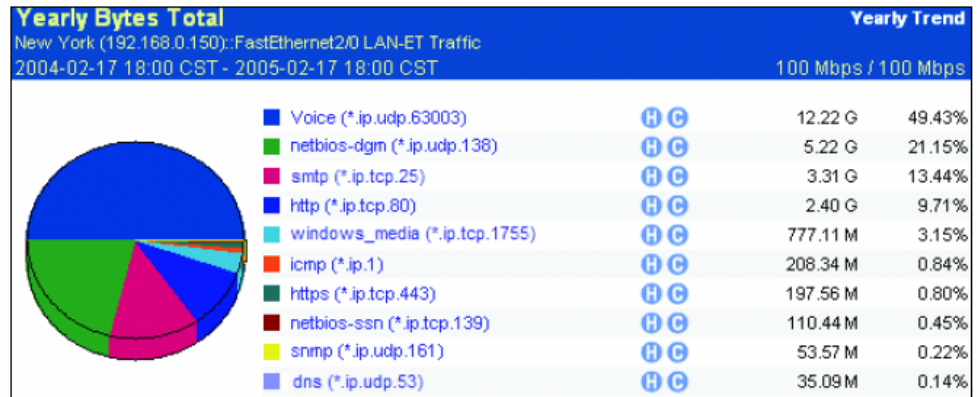
*The Standard for Flow-Based  
Reporting*

# What Can ReporterAnalyzer Tell You?

- ◆ 1. Capacity Planning
  - When traffic has exceeded 80% utilization on a particular link.
  - If increasing capacity will solve the problem on a link.
  - Any links that can be downgraded to save money.
  - Applications, hosts and conversations that are taking up bandwidth.
- ◆ 2. Troubleshooting
  - How a virus is affecting your network - which links and hosts.
  - Real-time identification and monitoring of unwanted traffic.
- ◆ 3. Traffic Analysis
  - Applications that are using excessive bandwidth, who is using them and when.
  - Workday-only traffic for the month.
  - The amount of web traffic in one region vs. another region.

# Troubleshoot Network Issues Rapidly

- ✓ Gain visibility into all interfaces, applications, hosts and conversations for the entire network
- ✓ Create flexible reports to meet your specific needs
- ✓ Leverage your existing infrastructure using NetFlow



***“We use NetQoS to give us the overall health of the network so we can be proactive, not just reactive.”  
– ChevronTexaco Global Network Architecture Team***

# Features

- ◆ View rate, volume and utilization measurements by application, host, and conversation.
- ◆ Virus Scan Wizard to quickly report and alert on potential viruses.
- ◆ Real-time reports and alarms for every interface on the network.
- ◆ Scheduled reports to automatically run and be emailed.
- ◆ Application defined by a combination of ports, IP addresses, and ToSes.
- ◆ Aggregate network traffic by business units, geography, IP subnets, etc.
- ◆ Customize time periods to support workday reporting.

# Standard Reports

- ◆ Real-time reports for protocol, host, conversation and ToS.
- ◆ Host and conversation distribution by protocol.
- ◆ Trend plots for protocols, hosts and conversations.
- ◆ Traffic rates, utilization, and volumes for protocols, hosts and conversations.
- ◆ Eight-hour, daily, weekly, monthly, yearly or customizable time periods.

# Custom Reports

- ◆ Custom reports enable groupings by interface, protocols and/or subnets - allowing you to view data in the ways and at the levels you need.
- ◆ For instance, you can create reports:
  - Based on various traffic measurements, report formats, data resolutions and specific time periods.
  - Broken down by interface, host, conversation and protocol/application.

# Analysis

- ◆ Specific thresholds may be created to trigger a real-time alarm when network traffic reaches a certain level.
- ◆ Threshold violations can be viewed in a calendar plot for a high level view, or as a complete listing of all violations for a detailed view.