

Cisco Netflow

Pittsburgh Area Cisco Users Group (PACUG)

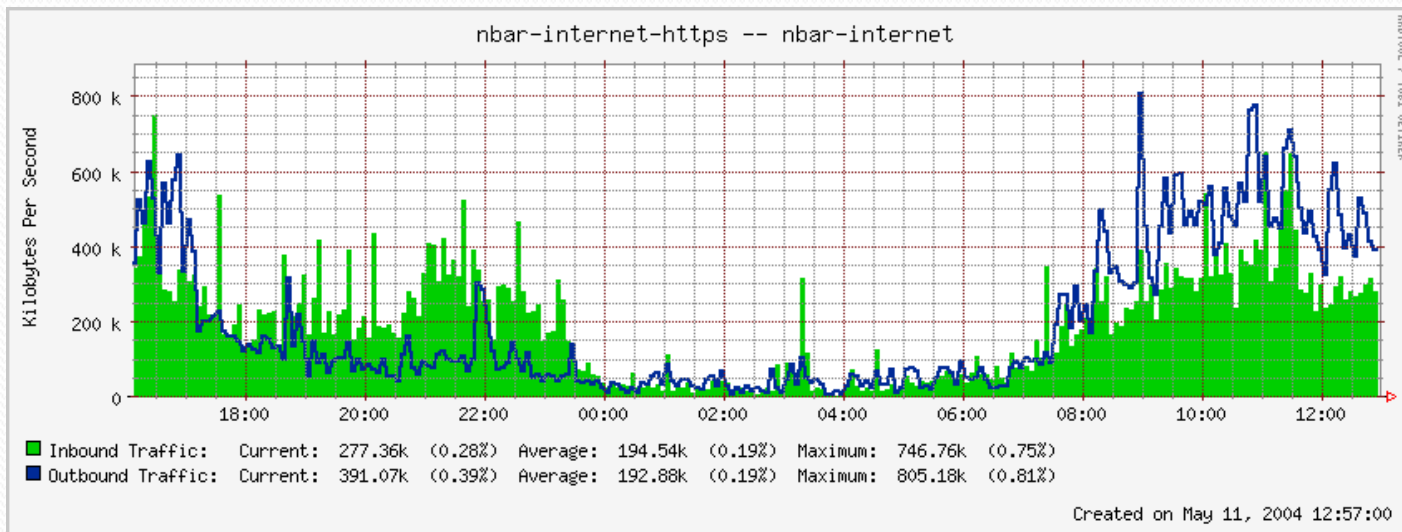
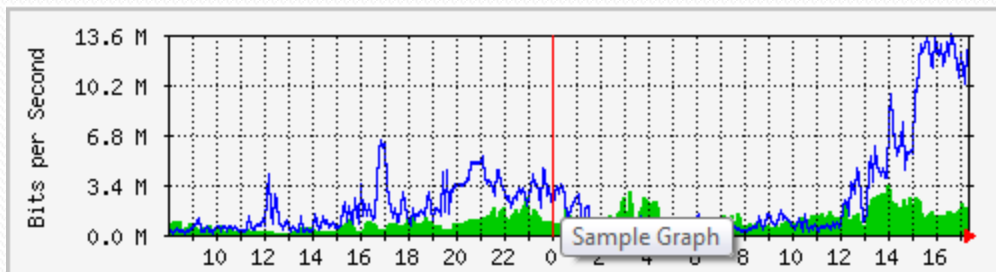
Carl Burkland

November 19, 2008

Bandwidth Monitoring Utilities

- SNMP
 - Query-based “pull method” for collecting data
 - *Lacks detailed IP information and protocol statistics*
 - Utilize MRTG (Multi Router Traffic Grapher)
- Add - NBAR (Network Based Application Recognition) + SNMP
 - Query-based “pull method” Protocol
 - Application Recognition capability with defined SNMP mibs for query (ciscoNbarProtocolDiscoveryMIB (1.3.6.1.4.1.9.9.244))
 - Utilize MRTG (Multi Router Traffic Grapher) –OR—
 - IP NBAR PROTOCOL DISCOVERY

MRTG Graph with and without NBAR



Why Netflow?

- Find out
 - WHO?
 - Source / Destination IP address of traffic flow
 - WHAT?
 - Source / Destination Protocol of traffic flow
 - WHEN?
 - Timestamp

Netflow Facts

- Netflow – Developed by Cisco

Version	Description
v1	First try
v5	Most used version
v6	Added Encapsulation information - not supported by Cisco
v7	Added Catalyst Switch information
v8	Added router-based Netflow aggregation
v9	Template Based, allowing many combinations
IPFIX	v10; IETF Standardized NetFlow 9 w/ Enterprise fields

- IETF Standard being developed – based on Cisco Netflow v9 (very soon!)
 - Internet Protocol Flow Information eXport (IPFIX)
- Other vendor implementations
 - Juniper Networks - Jflow or cflowd
 - Huawei Technology - NetStream
 - Alcatel-Lucent - cflowd

Versions 5 & 9

Version 5

- Gateway Protocol (BGP) autonomous system information
- Flow sequence numbers

Version 9

- Layer 2 information, new security detection information, IPv6, Multicast, MPLS
- Almost any information can be exported from a router or switch
- 3rd party applications – no need to redevelop applications with changing technology
- Modularity - New features can be added to NetFlow more quickly, without breaking current implementations.
- V9 is capable of handling requirements for future implementations

Netflow Components

- **Exporter** – sends flow data to Collector in UDP / SCTP packets
 - Cisco Routers
 - Limited Catalyst switch support
 - Cisco ASA 5580 – security events
- **Collector** – receives and stores Netflow records for review / action
 - Cisco NetFlow Collector (NFC)
 - **Plixer Scrutinizer (demo tonight)**
 - Managewise NetFlow Analyzer
 - **Solarwinds NetFlow Traffic Analyzer (demo tonight)**
 - NetQoS ReporterAnalyzer
 - NTOP (GNU) – NMON (Commercial)

What can Netflow see?

Ingress / Inbound

- IP-to-IP packets
- IP→ to → Multiprotocol Label Switching (MPLS) packets
- Frame Relay-terminated packets
- ATM-terminated packets

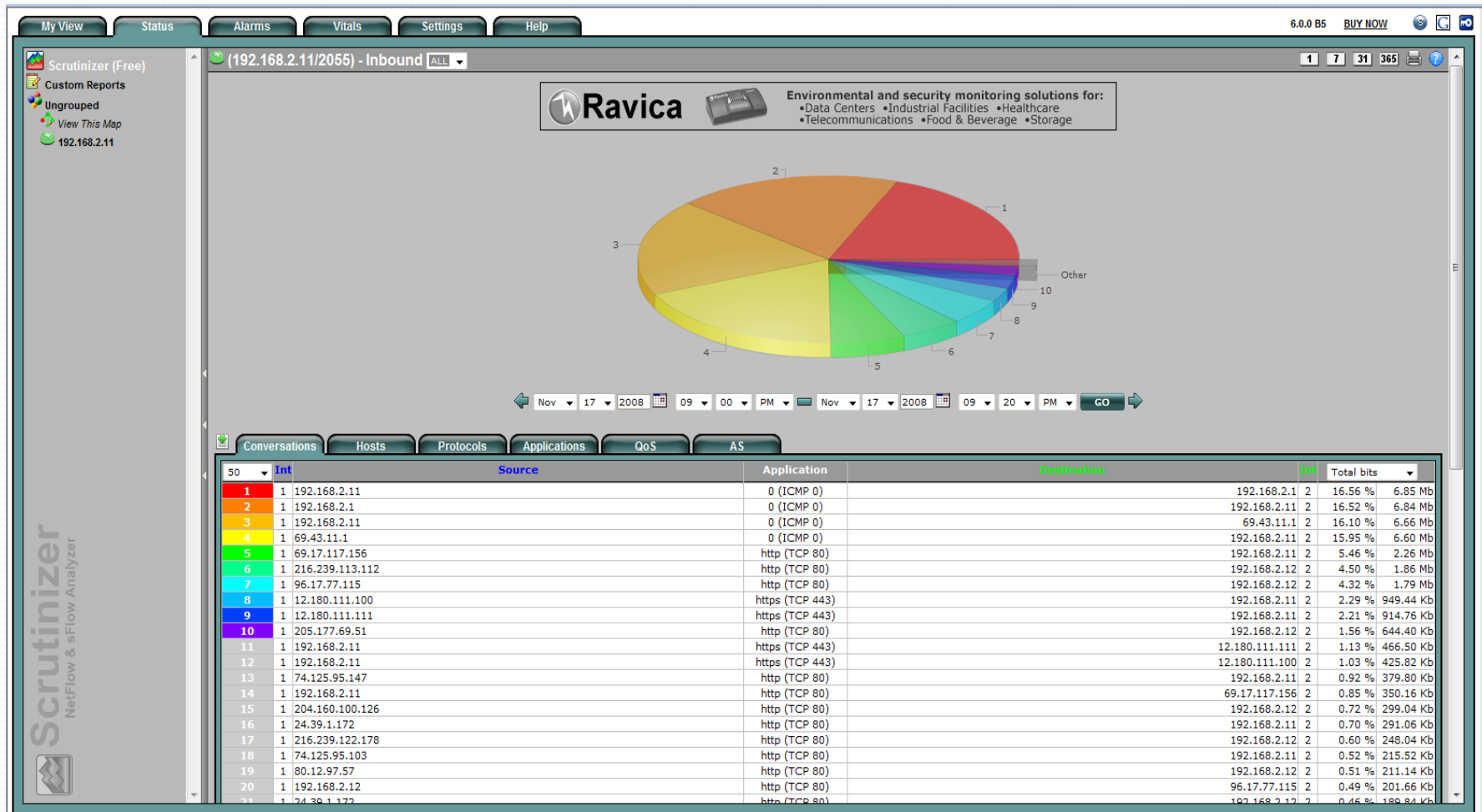
Egress / Outbound

- IP traffic
- Multiprotocol Label Switching (MPLS)→ to →IP packets.

What Defines a Flow?

- Source IP address
- Destination IP address
- Source port for UDP or TCP, (zero for other protocols)
- Destination port for UDP/TCP, type & code for ICMP, (zero for other protocols)
- IP protocol
- Ingress interface
- IP Type of Service

Plixer Scrutinizer



Solarwinds Real-time Netflow Analyzer

SolarWinds Real-time NetFlow Analyzer - 192.168.2.11 - Interface 1

File Edit Tools View Help

Period: 5 min Display: Top 5 Refresh rate: 5 Units: Kilobits Monitor More NetFlow Interfaces Stop Flow Capture Refresh

Views

- Applications
 - AVM USB Remote Architecture (2066/UDP)
 - Domain Name Server (53/UDP)
 - GROOVE (2492/TCP)
 - http protocol over TLS/SSL (443/TCP)
 - mpshrv (1261/TCP)
 - MSL License Manager (1464/TCP)
 - NETBIOS Name Service (137/UDP)
 - Post Office Protocol - Version 3 (110/TCP)
 - QNTS-ORB (1262/TCP)
 - Unknown
 - World Wide Web HTTP (80/TCP)
- Conversations
- Domains
- Endpoints
- Protocols

Inbound Traffic

Traffic Analysis for Applications

Application	Protocol	Total Traffic	Total Packets	Traffic Percentage
http protocol over TLS/SSL (443)	TCP	488.4 Kb	1612	90%
Post Office Protocol - Version 3 (110)	TCP	37.1 Kb	117	7%
61459	TCP	8.3 Kb	17	2%
63589	UDP	6.2 Kb	7	1%
World Wide Web HTTP (80)	TCP	5.4 Kb	31	1%

Outbound Traffic

No data available for

Application	Protocol	Total Traffic	Total Packets
-------------	----------	---------------	---------------

Related Links

- [Monitor NetFlow v9, J-flow, sFlow >](#)
- [Analyze Historical NetFlow Reports >](#)
- [Download More Free Tools >](#)
- [Get Support From SolarWinds Community >](#)

SolarWinds Real-time NetFlow Analyzer - Microsoft Internet Explorer 13 m 8 sec 0%

Will it increase resource utilization?

- Short answer – **Yes**
- Especially if Netflow is supported in software!
- Impact not as large if classification of the flows is done in hardware

What is the typical impact?

Netflow Performance Analysis

Figure 4. Cisco 2600 Router

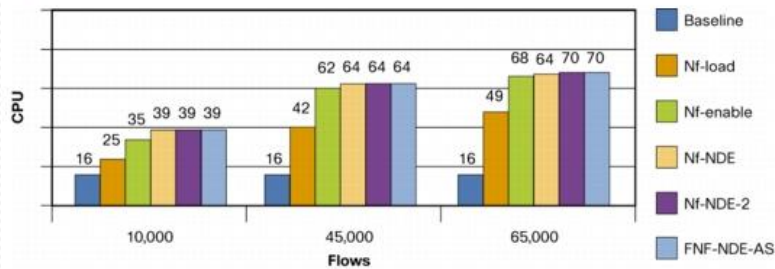


Figure 6. Cisco 2851 Router

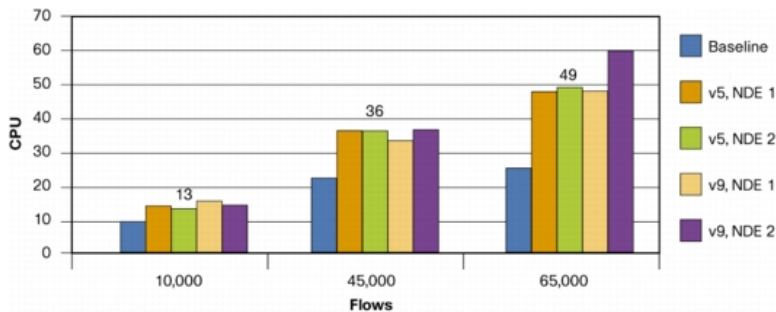
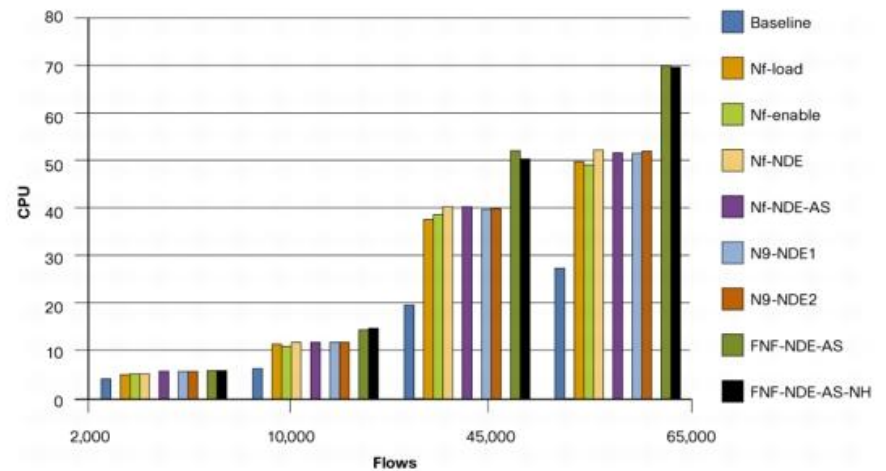


Figure 5. Cisco 2811 Router



Mnemonic	Description
NF-load	Netflow enabled initially - no traffic
NF-enable	Netflow enabled - no Netflow Data Export Defined (NDE)
NF-NDE	v5 Netflow enabled - 1 Netflow Data Export Defined (NDE)
NF-NDE2	v5 Netflow enabled - 2 Netflow Data Exports Defined (NDE)
Baseline	No Netflow enabled - baseline performance
NF-NDE-AS	v5 Netflow enabled - 1 Netflow Data Export Defined (NDE) + BGP AS
N9-NDE1 / v9 NDE1	v9 Netflow enabled - 1 Netflow Data Export Defined (NDE)
N9-NDE2 / v9 NDE2	v9 Netflow enabled - 1 Netflow Data Export Defined (NDE)
FNF-NDE-AS-NH	Flexible Netflow + 1 Netflow Data Export Defined (NDE) + BGP Next Hop
FNF-NDE-AS	Flexible Netflow + 1 Netflow Data Export Defined (NDE) + BGP AS

How can I limit resource impact?

- Sampled Netflow
 - deterministic sampling - select every Nth packet
 - time based sampling - select packet every N milli-seconds
 - random sampling - select one out of N packet
- Aggregation Cache
 - Limits volume of Netflow export data
 - Reduces workload on Netflow collector
 - Provides greater scalability in larger routers

Does my device support Netflow?

Catalyst Switches

- Catalyst 4000 series: SUP IV, SUP V & SUP V10 10GE
 - Supervisor I, II, II Plus - NO SUPPORT FOR NETFLOW
 - Supervisor IV supports NetFlow Export w/ optional Netflow Daughter Card (IOS 12.1.(19)EW, V1, V5 and V8)
 - Supervisor V supports NetFlow Export w/ optional Netflow Daughter Card (IOS 12.2(25)SG, V1, V5 and V8)
 - Supervisor V-10GE has built-in NetFlow support (IOS 12.2(25)EW, V5 and V8)
- Catalyst 6500 series: SUP 1, SUP 2, SUP 720
 - Supervisor 1 & 2 – netflow in software
 - Supervisor 720 – dedicated TCAM for Netflow

Routers

- Most routers support Netflow after version 12.0 – check [IOS Feature Navigator](#)

Wait! – What do I do if my device does not support Netflow export?

- SPAN + Netflow Probe
 - Download and install netflow probe to a machine with 2 network interface cards (nProbe)
 - One NIC will listen to traffic and the other will export the data received to the Netflow collector
 - Span source port of interest to switchport connected to the listening NIC

How can Netflow be leveraged beyond Network monitoring?

- Network Planning
 - Growth – More Bandwidth?
 - Change in application behavior – Adjust QOS policy?
- Security Monitoring / Denial of Service Prevention
 - Unauthorized traffic
 - Worms
- Accounting and Billing
 - Departmental Chargeback
 - ISP Customer Billing based on data usage
- Traffic Engineering
 - ISP with BGP AS data

Useful Links

- [Cisco Netflow Main Page](#)
- [Cisco Netflow Overview](#)
- [Cisco Netflow Applications](#)
- [Netflow Commercial Applications](#)
- [Freeware Netflow Software](#)
- [nProbe](#)
 - [Online store to purchase nProbe](#)
 - [Configuring nProbe](#)
- [NBAR with MRTG](#)
- [Netflow Performance Data](#)