ProCurve Networking
HP Innovation

More From Your Network

Introduction to sFlow

Holger Hasenaug, Technical Consultant
HP ProCurve Networking
CCIE#6343

hp invent

The Big Network Challenges

ProCurve Networking
HP Innovation

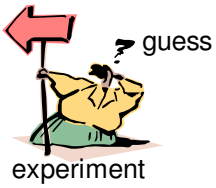
- Is network performance slowing down or becoming congested?
- What is the current network usage and what has it been historically?
- Are worms and viruses propagating in my network?
- Why is a server slow or inaccessible? Is it the network?
- Are my network resources being misused?
- Which users and applications are driving network traffic?
- Who is running P2P in my network?

2

How to control what you don't measure?

ProCurve Networking HP Innovation

control decisions based on guesswork



Run around with a protocol analyzer during an emergency which only delivers data from small parts of the network

Business productivity impacted by slow resolution to network problems

3

What is sFlow?

ProCurve Networking HP Innovation

- sFlow is a "Statistical Sampling Technology" – an Open Standard, RFC 3176
- HP–patented and proven technology (over 15 years) that employs "Statistical Packet Sampling" and SNMP data to monitor network flows in a network formerly known as HP EASE, XRMON
- sFlow delivers L2-L4 network-wide traffic flow information with wire-speed network performance

4

What does sFlow provide?

ProCurve Networking HP Innovation

A comprehensive and detailed visualization of all traffic flows across the network

- Real-time and historical traffic analysis and accounting - *network-wide*
- MAC IPv4, IPv6, IPX, AppleTalk, ICMP, TCP, UDP, URL (L2-L7)
- Input/output port, VLAN, priorities, subnets, full AS path, BGP communities & preferences

Wire-speed traffic monitoring on every port

- Embedded hardware-based packet sampling in ASICs
- Accurate at all speeds: 10/100/1000, 10 Gigabit
- Scalable to 10s of thousands of ports

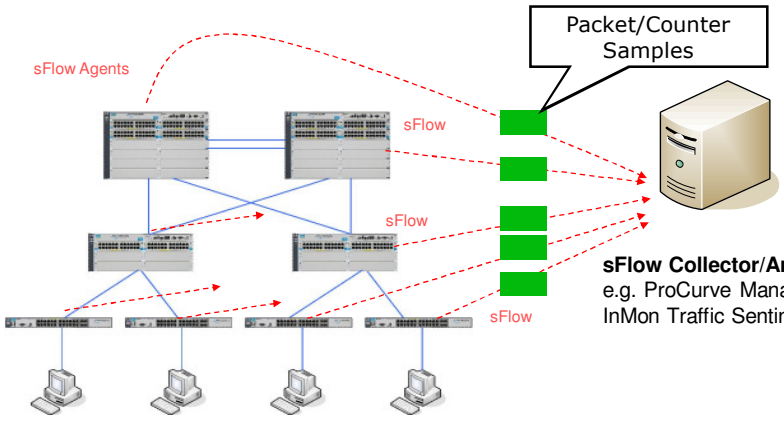
Monitoring without impact on switch and network performance

- Minimal CPU and memory impact
- Minimal use of network bandwidth
- No SNMP polling

5

sFlow Components

ProCurve Networking HP Innovation



Always-on, real-time measurements from every port sent to a single sFlow collector forms central, network-wide view

Provides network visibility for administrators to make informed decisions

6

Hot Buttons for an Enterprise

ProCurve Networking HP Innovation

Performance and fault management

- ✓ Network and service congestion control
- ✓ Troubleshoot network performance problems

Security management

- ✓ Identify and defend against DoS Attacks
- ✓ Network-wide security surveillance
- ✓ Identify policy violations

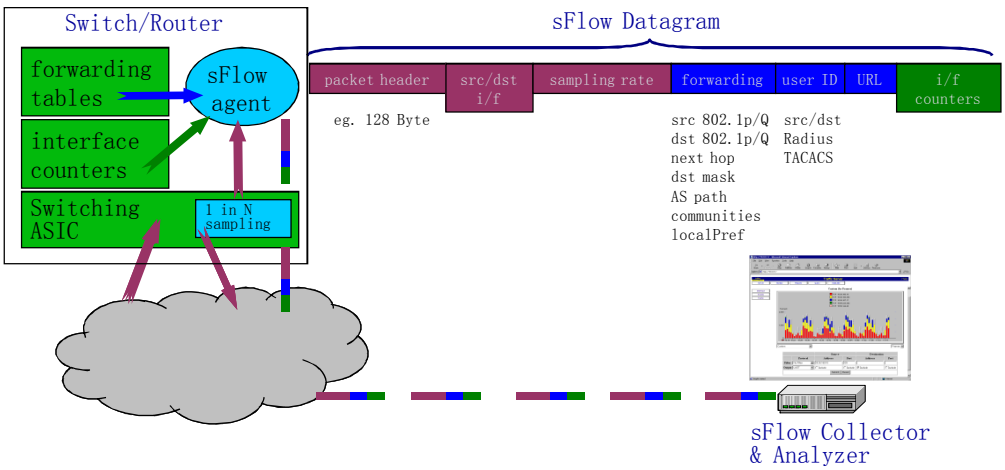
Capacity planning

- ✓ Reporting based on network-wide traffic flows including:
  - VLANs
  - IP subnets or addresses
  - IP Services (TCP and UDP)

7

sFlow in Operation

ProCurve Networking HP Innovation



8

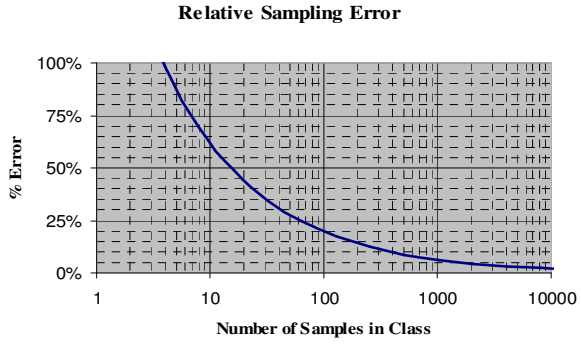
Statistical Model for Packet Sampling

ProCurve Networking HP Innovation

Estimating Traffic per Protocol

Total number of frames = N
Total number of samples = n
Number of samples in class = c
Number of frames in the class estimated by:

$$N_c = \frac{c}{n} \cdot N$$

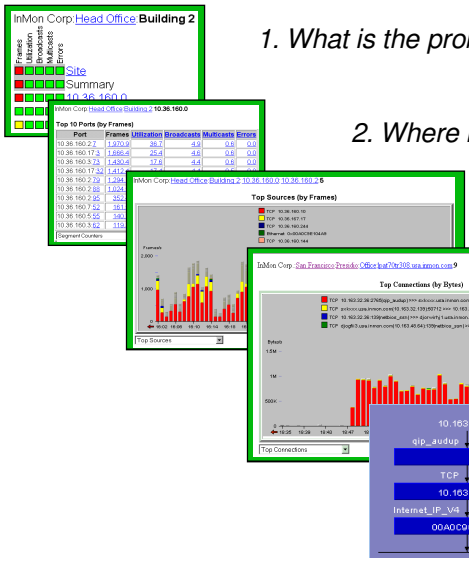


$$\%error \leq 196 \cdot \sqrt{\frac{1}{c}}$$

9

InMon Traffic Server – Drill Down

ProCurve Networking HP Innovation

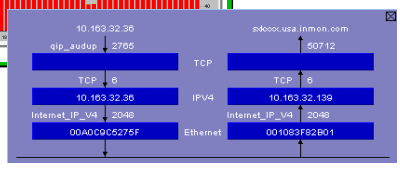


1. What is the problem

2. Where is the problem?

3. Who is causing the problem?

4. What are they doing?

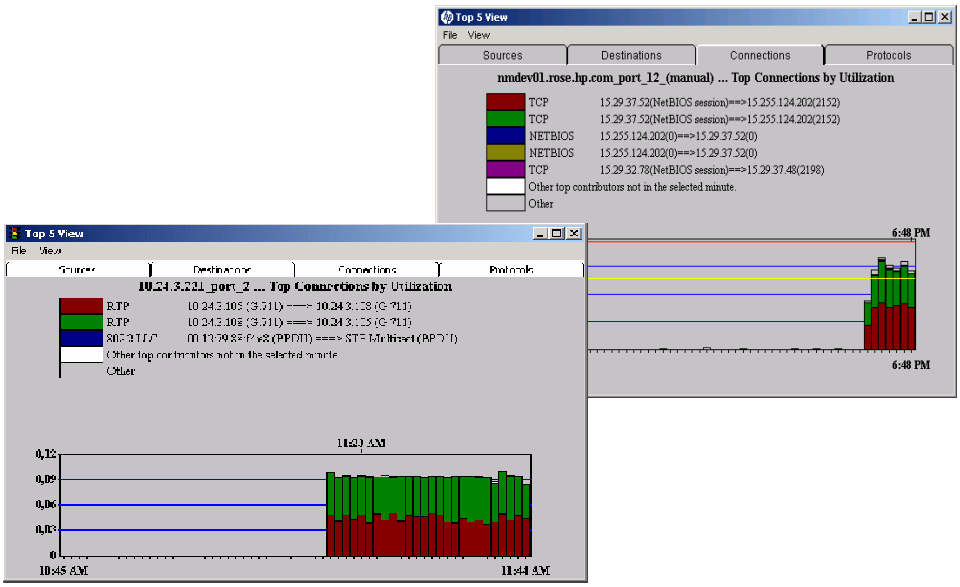


5. Full connection details

10

HP ProCurve Network Manager

ProCurve Networking
HP Innovation



11

sFlow example used for virus and DoS detection

ProCurve Networking
HP Innovation

Detection

- Alerts from security sensors in the switch and third party security appliances:
  - Virus Throttling **(built-in the switch)**
  - sFlow **(built in the switch)**
  - 3rd party security appliance support
  - Alert suppression

Response

- Location based response
  - Policy can be configured by location
- Multiple response options
  - Alert administrator
  - Put attacker in a VLAN
  - Limit bandwidth of attacker's port
  - MAC lockout, Block port
  - Remotely mirror suspect traffic to IDS/IPS/UTM
  - Chain of response actions
    - if one response fails go to next one on a list

HP ProCurve
Network Immunity Manager

12

sFlow support of vendors

ProCurve Networking HP Innovation

Network Equipment:	sFlow Collectors:
AlaxalA Networks	Arbor Networks
Alcatel-Lucent	Cetacea Networks
Allied Telesis	Foundry Networks
Comtec Systems	Genie Network Resource Management Inc.
Extreme Networks	Hewlett-Packard
Force10 Networks	Infosim Networking Solutions AG
Foundry Networks	InMon Corp.
HP ProCurve Networking	Klir Technologies
Hitachi	Lancope
NEC	Mazu Networks
	NetScout
	NetUP
	Network Instruments
	netZentry
	NitroSecurity
	ntop.org
	Plixer
	pmacct
	Q1Labs
	QoSmetrics
	RetiCorp Networks
	Tavve
	Wireshark

13

Summary on sFlow

ProCurve Networking HP Innovation

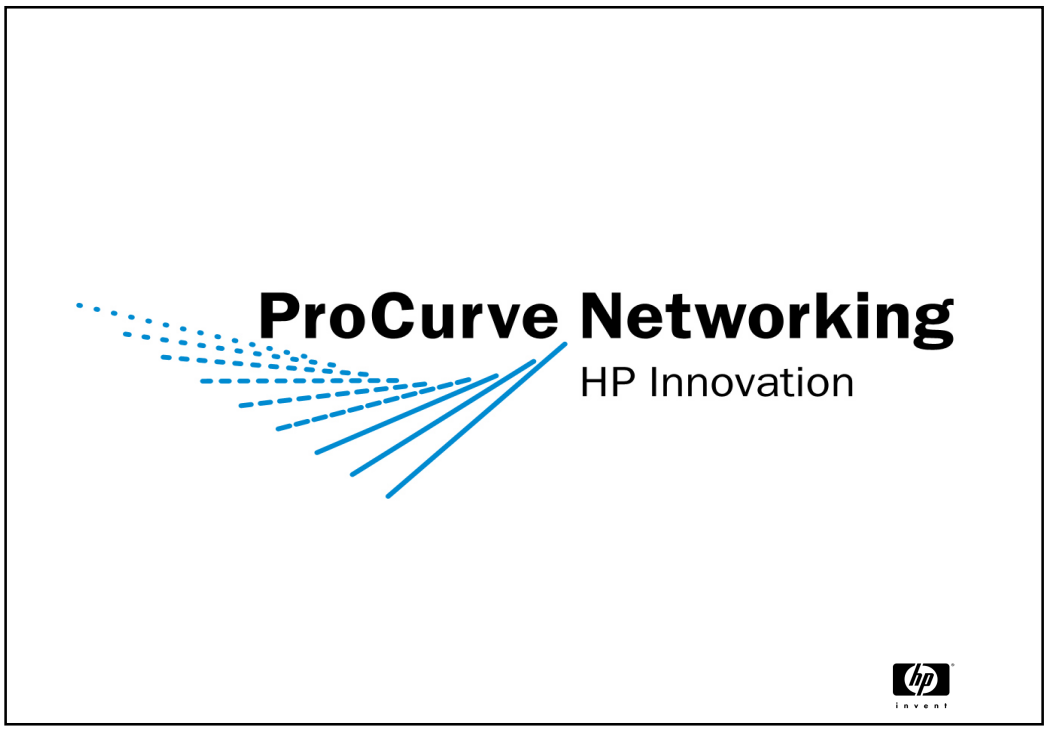
sFlow provides:

- Troubleshooting Network problems
- Controlling Congestion
- Security Analysis
- Accounting and Billing for Usage

A *comprehensive* visualization of *all* end-to-end traffic across the network(s) with minimal network impact and minimal device performance impact.

Further information on http://www.sflow.org

14


ProCurve Networking
HP Innovation
invent