Traffic Monitoring using sFlow®

With the ever-increasing reliance on network services for business critical applications, the smallest change in network usage can impact network performance and reliability. This has a direct impact on the ability to conduct key business functions and on the cost of maintaining network services.

By providing unprecedented visibility into network usage and active routes of even today's high-speed and complex networks, sFlow provides the data required to effectively control and manage network usage, ensuring that network services provide a competitive advantage.

Examples of the applications of sFlow data are:

- Detecting, diagnosing, and fixing network problems
- Real-time congestion management
- Understanding application mix (e.g. P2P, Web, DNS etc) and changes
- Usage accounting for billing and charge-back
- Audit trail analysis to identify unauthorized network activity and trace the sources of denial-of-service attacks
- Route profiling and peering optimization
- Trending and capacity planning.

sFlow is a sampling technology that meets the key requirements for a network traffic monitoring solution:

- **sFlow provides a network-wide view** of usage and active routes. It is a scalable technique for measuring network traffic, collecting, storing, and analyzing traffic data. This enables tens of thousands of interfaces to be monitored from a single location.
- **sFlow is scalable**, enabling it to monitor links of speeds up to 10Gb/s and beyond without impacting the performance of core internet routers and switches, and without adding significant network load.
- **sFlow is a low cost solution**. It has been implemented on a wide range of devices, from simple L2 workgroup switches to high-end core routers, without requiring additional memory and CPU.
- **sFlow is an industry standard** with a growing number of vendors delivering products with sFlow support.

A brief history of packet sampling

Packet sampling has been used to monitor network traffic for over ten years (see **Figure 1**). Hewlett-Packard first demonstrated network-wide monitoring using packet sampling of the University of Geneva and CERN networks at Telecom '91. This was followed up with the introduction of networking products with embedded packet sampling capability - HP Extended RMON - in 1993.

However, broad acceptance of this technique is only just starting, driven by the introduction of higher speed networks and the transition from shared to switched networks.

Packet based sampling as an embedded network traffic monitoring technique is now compelling. In a switched environment, the most effective place to monitor traffic is within the switch/router, where all the traffic will be seen. Traditional probes will only have a partial view of traffic.

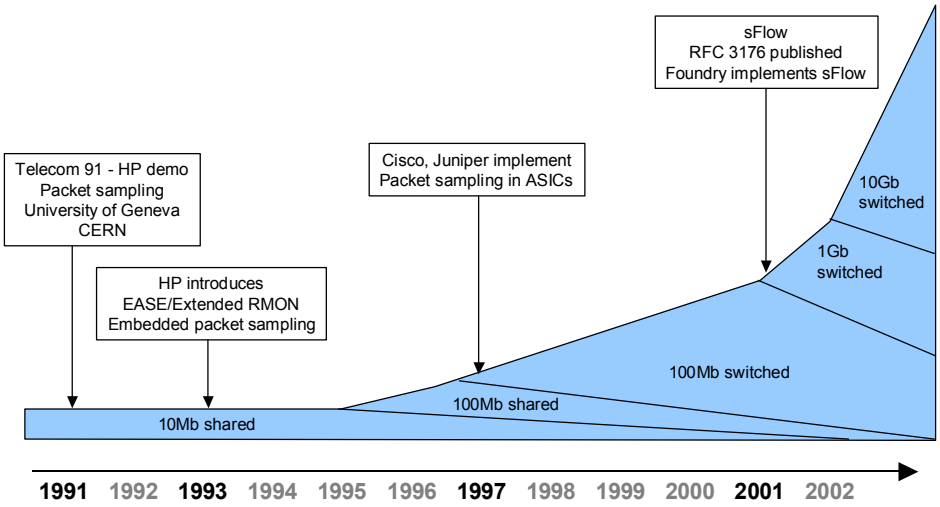

Figure 1 *History of Packet Sampling*

However, a traffic monitoring solution embedded within a switch or router must not impact forwarding performance. Switches and routers with embedded sFlow sampling technology have been available since 2001. This solution provides detailed and quantitative traffic measurements, at gigabit speeds, gives insight into forwarding decisions, and does not impact forwarding or network performance.

What is sFlow?

sFlow is a multi-vendor sampling technology embedded within switches and routers. It provides the ability to continuously monitor application level traffic flows at wire speed on all interfaces simultaneously.

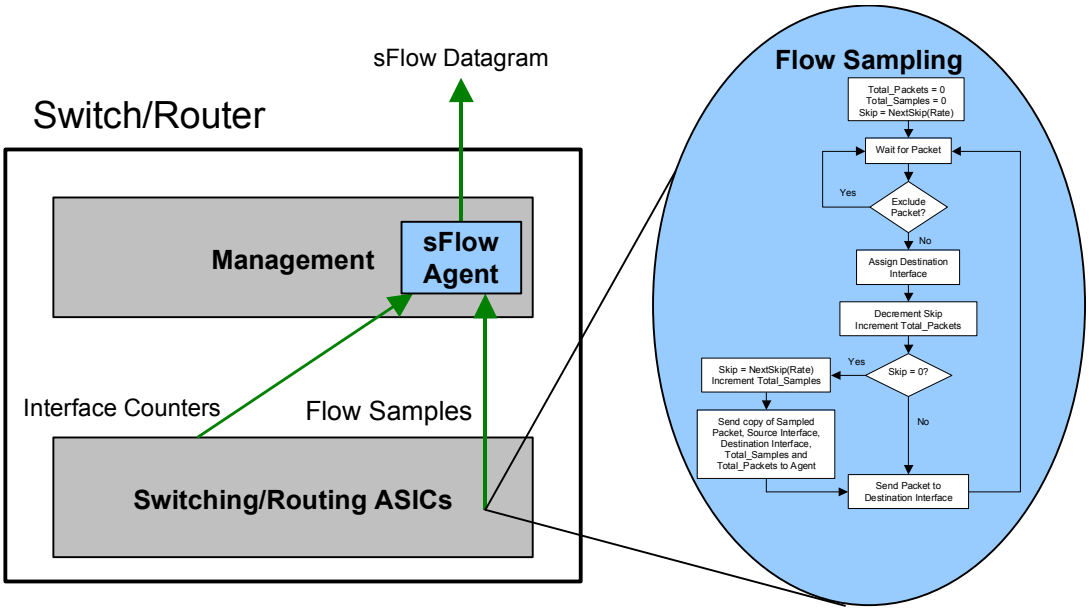

Figure 2 *sFlow Agent Embedded in Switch/Router*

The sFlow Agent is a software process that runs as part of the network management software within a device (see **Figure 2**). It combines interface counters and flow samples into sFlow datagrams that are sent across the network to an sFlow Collector. Packet sampling is typically performed by the switching/routing ASICs, providing wire-speed performance. The state of the forwarding/routing table entries associated with each sampled packet is also recorded.

The sFlow Agent does very little processing. It simply packages data into sFlow Datagrams that are immediately sent on the network. Immediate forwarding of data minimizes memory and CPU requirements associated with the sFlow Agent.

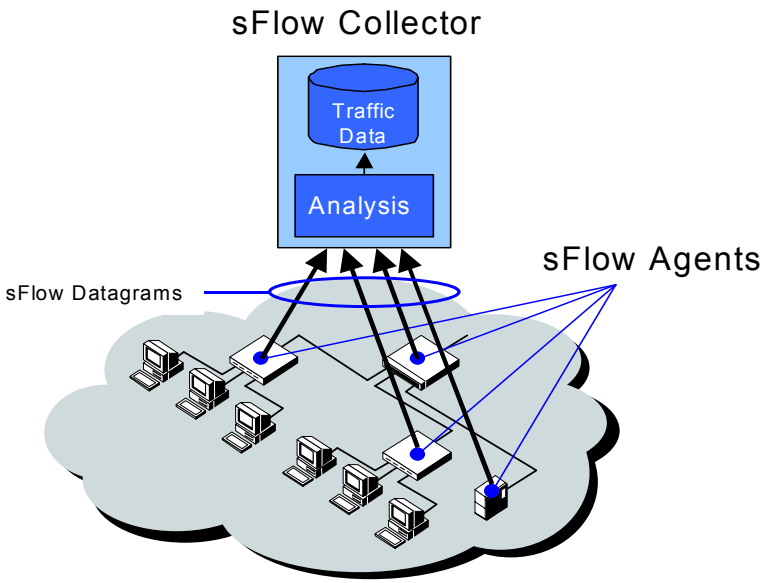

Figure 3 *sFlow Agents and Collector*

Figure 3 shows the basic elements of the sFlow system. sFlow Agents throughout the network continuously send a stream of sFlow Datagrams to a central sFlow Collector where they are analyzed to produce a rich, real-time, network-wide view of traffic flows.

sFlow monitoring of high-speed, routed and switched networks has the following properties:

- **Accurate** Because sampling is simple enough to be performed in hardware, it operates at wire speed. In addition, the sFlow system is designed so that the accuracy of any measurement can be determined. Other traffic flow measurement technologies "clip" under heavy loads resulting errors that are difficult to quantify.
- **Detailed** Complete packet header and switching/routing information permits detailed analysis of L2-L7 traffic flows.
- **Scalable** The sFlow system is scalable in both the size and speed of the network it can monitor. sFlow is capable of monitoring networks at 10Gbps, 100Gbps and beyond. Thousands of devices can be monitored by a single sFlow Collector.
- **Low Cost** The sFlow Agent is very simple to implement and adds negligible cost to a switch or router.
- **Timely** The sFlow Collector always has an up to the minute view of traffic throughout the entire network. Timely information is particularly important if the traffic data is needed to provide real-time controls. For example to manage quality of service or to defend against a denial of service attack.

Using sFlow

Using sFlow to continuously monitor traffic flows on all ports gives network-wide visibility into the use of the network. This visibility replaces guesswork, fundamentally changing the way that network services are managed.

Troubleshooting Network Problems

Any use of a network generates traffic. Consequently, problems are often first observable in abnormal traffic patterns. sFlow makes these abnormal traffic patterns visible with sufficient detail to enable rapid identification, diagnosis, and correction.

Controlling Congestion

By monitoring traffic flows on all ports continuously, sFlow can be used to instantly highlight congested links, identify the source of the traffic, and the associated application level conversations. sFlow provides the necessary information to determine effective controls, for example which traffic to rate control or prioritize or where to provision more bandwidth.

Security and Audit Trail Analysis

Gartner estimates that 70% of security incidents that actually cause loss to enterprises involve insiders, while service providers and other organizations are constantly bombarded with various other (external) attacks. A comprehensive security strategy involves protecting the network from external and internal misuse and information assets from theft.

Since attacks and security threats will come from unknown sources, effective security monitoring requires complete network surveillance, with alerts to suspicious activity. sFlow provides this blanket audit trail, for the whole network.

The continuous network-wide surveillance and route tracing information provided by sFlow allows internal and externally sourced security threats and attacks to be rapidly traced and controlled.

When sFlow is used to build a detailed traffic history a baseline of normal behavior is established, from which anomalies can be detected and suspicious activity identified.

By giving visibility into real-time and historical network-wide usage, sFlow can be used to prevent intentional attacks, minimize unintentional mistakes, and protect information assets.

Route Profiling

Since sFlow contains forwarding information, it can be used to profile the most active routes and the specific flows carried by these routes.

Understanding the routes and flows makes it possible to optimize routing - improving connectivity and performance, and choosing the most cost effective peering partners.

Accounting and Billing for Usage

Detailed network usage information is needed to fairly charge for network services and to recover the costs of providing value-added services. sFlow data can be used to account and bill for network usage, by customer. It can also be used to provide customers with an itemized breakdown of their total traffic, highlighting top users and applications. This information gives the customer confidence in the fairness of the charges and allows them to control costs.

Availability

sFlow solutions consist of:

- **Network equipment** equipped with sFlow Agents, which monitor network traffic and generate sFlow data.
- **Software applications** that receive and analyze sFlow data.

sFlow has been implemented on a wide range of network switches and routers, from affordable L2 workgroup switches to high-end core routers. A number of software applications take advantage of the sFlow network traffic monitoring capability in these switches. These applications provide a variety of solutions including congestion control and troubleshooting, route profiling, audit trail security analysis, and accounting for billing. A full list of sFlow solutions can be found on sFlow.org.

sFlow.org

sFlow.org is an international, multi-vendor, and end-user forum. It promotes the benefits of sFlow sampling technology for monitoring and managing traffic in complex networks, and drives the widespread adoption of sFlow by end users, network equipment vendors, and software application developers.

The sFlow.org web site is the authoritative source for information on sFlow, specifications, latest developments, and products that support sFlow.

The sFlow specification has been published as RFC 3176. Source code for the sFlow agent and basic traffic analysis tools are freely available.

Appendix A: Comparison of sFlow with other technologies

The following table compares the advanced features of sFlow with current solutions based on RMON and Cisco NetFlow®. RMON (4 Groups) refers to the four basic functions from RMON (Statistics, History, Alarms, Events) that are often embedded in switch interfaces. RMON II refers to full implementations of RMON II, these are typically provided in the form of an add-in card or a hardware probe.

	RMON (4 groups)	RMON II	NetFlow®	sFlow®
Packet Capture	N	Y	N	P
Interface Counters	P	P	N	Y
Protocols				
Packet headers	N	P	N	Y
Ethernet/802.3	N	Y	N	Y
IP/ICMP/UDP/TCP	N	Y	Y	Y
IPX	N	Y	N	Y
Appletalk	N	Y	N	Y
Layer 2				
Input/output interface	N	N	Y	Y
Input/output priority	N	N	N	Y
Input/output VLAN	N	N	N	Y
Layer 3				
Source subnet/prefix	N	N	Y	Y
Destination subnet/prefix	N	N	Y	Y
Next hop	N	N	Y	Y
BGP 4				
Source AS	N	N	P	Y
Source Peer AS	N	N	P	Y
Destination AS	N	N	P	Y
Destination Peer AS	N	N	P	Y
Communities	N	N	N	Y
AS Path	N	N	N	Y
Real-time data collection	Y	Y	P	Y
Configuration				
Configurable without SNMP	N	N	Y	Y
Configurable via SNMP	Y	Y	N	Y
Low Cost	Y	N	N	Y
Scalable (switch interfaces/collector)	P	N	N	Y
Wire-speed	Y	P	P	Y

N	Feature not supported
P	Feature partially supported. Either the feature is incomplete or can only be enabled by disabling other features.
Y	Fully supported