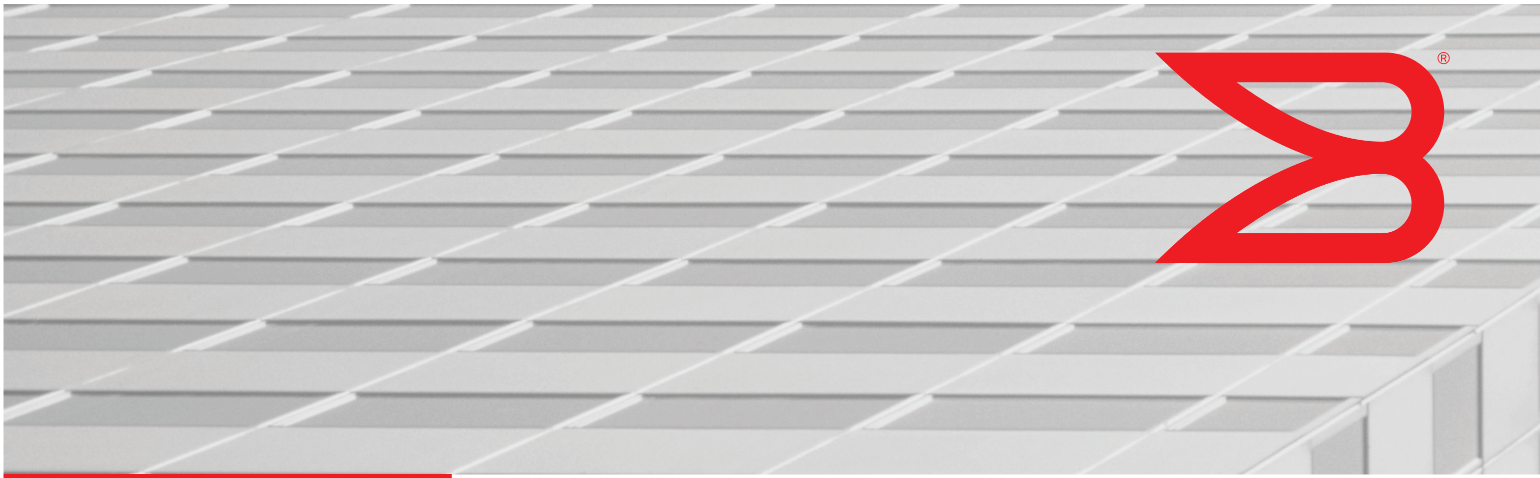
WHITE PAPER



SERVICE PROVIDER

Brocade sFlow for Network Traffic Monitoring

Although both sFlow and NetFlow enjoy widespread industry adoption, sFlow is the better technology for traffic monitoring.

BROCADE

Business critical applications rely heavily on network services. Changes in network usage can alter the performance and reliability of a network, which directly impacts a company's cost of maintaining network services and ability to conduct key business operations. Therefore, monitoring networks is important for the prevention and detection of faults and for improving overall network reliability.

With converged networks that carry different kinds of traffic, the right bandwidth and traffic characteristics have to be observed for each network traffic type. A means of measuring traffic characteristics is therefore important. For a service provider selling premium services, measuring and analyzing traffic characteristics is crucial. For businesses that are building new network infrastructure or IT solutions, capacity planning for new networks is based on historic and projected traffic usage patterns. So measuring traffic characteristics and usage becomes central to capacity planning. It is clear that there is an acute need for traffic monitoring technologies for both enterprises and service providers.

INTRODUCTION

Several different technologies have been employed to monitor network traffic, such as sFlow, NetFlow , Remote Network MONitoring (RMON I and II), and SMON (a set of MIB extensions to RMON). Although both sFlow and NetFlow are used for traffic monitoring, sFlow has many benefits over NetFlow. This paper presents an overview of both sFlow and NetFlow technologies and demonstrates the superiority of sFlow as a traffic monitoring solution over NetFlow. The paper also provides insights into the wide range of solutions that sFlow is capable of supporting.

sFLOW OVERVIEW

sFlow is a packet sampling technology that can be implemented in a broad range of networking devices from Layer 2 switches to high-end core routers. Figure 1 shows the evolution of packet sampling technologies over the past 10 years. Due to the introduction of high-speed networks, packet sampling has become widely recognized as the most scalable, accurate, and comprehensive solution for network monitoring.

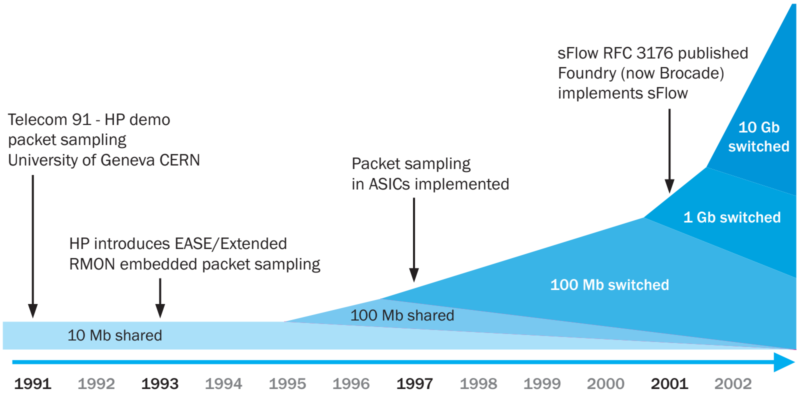


Figure 1.
Packet sampling timelines.

Traditional technologies such as NetFlow have focused on analyzing each packet and embedding traffic monitoring inside routers. This methodology impacts the performance of the router (especially at high traffic speeds) and leads to inaccurate results. sFlow samples packets, but separates traffic analysis from traffic sampling. While the sampling logic is embedded inside the network element (for example, the router or switch), traffic analysis is actually performed on a separate machine (typically a server). This allows for both larger scale and real-time responsiveness.

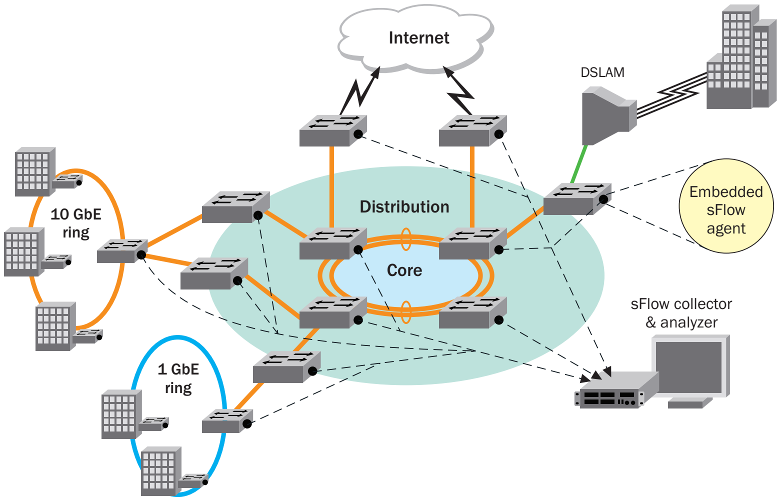


Figure 2.
sFlow data collection and analysis.

The different components of the sFlow system, shown in Figure 2, are the sFlow generator, the sFlow agent, and the sFlow collector.

The sFlow generator is the network element that generates traffic samples. Packet sampling is typically performed in hardware to provide wire-speed performance. The sFlow agent is a software process that runs as part of the network management software within the network element. sFlow agents in routers and switches throughout the network continuously send a stream of sFlow datagrams to a central sFlow collector. Interface counters and flow samples are combined into sFlow datagrams, which require very little processing. Data is packaged into sFlow datagrams, which are immediately sent on the network. This minimizes the load on sFlow agents' memory and processor..

The sFlow collector software analyzes the datagrams received from each sFlow agent and presents a real-time, network-wide view of traffic flows. Several sFlow collector and analyzer software solutions are available both commercially and as freeware software. For a list of available collectors, see http://www.sflow.org/products/collectors.php. The sFlow standard is currently at version 5. For more information, see http://www.sFlow.org..

NETFLOW OVERVIEW

NetFlow is a network protocol developed by Cisco for collecting IP traffic information on Cisco IOS-enabled equipment. It is a Cisco proprietary technology for the collection of traffic data on routers. Special hardware is required for Cisco routers to run NetFlow, and not all Cisco routers are capable of supporting NetFlow.

The NetFlow feature generates NetFlow records in the router. In some routers, the processor captures packets and forwards them in software. In other routers, the processor captures packets in software but packet forwarding is done in hardware. The processor builds a NetFlow cache inside the router. A flow in NetFlow is defined on the basis of the following seven fields of the packet: source IP address, destination IP address, source port (for example, TCP source port), destination port (for example, TCP destination port), IP protocol type, ingress SNMP interface index, and IP type of service (ToS).

For every new packet captured, the processor searches its cache to match the packet to its flow information. When the NetFlow information has to be displayed, the processor works on the NetFlow cache to generate output. In some routers, the processor builds a NetFlow record containing information about multiple flows. This information can be exported from the router via UDP or Stream Control Transmission Protocol (SCTP). NetFlow versions 5, 6, and 7 are the most commonly deployed. Note that after the success of sFlow, NetFlow version 9 was introduced with some packet sampling capabilities in a limited set of routers.

sFLOW VS NETFLOW

In committing to advanced 802.11n wireless technology, network administrators must ensure that every piece of the wireless LAN is both reliable and compatible with the other pieces of the network. The best way to ensure compatibility is to find an equipment provider offering a broad range of wired and wireless networking gear. With the industry's broadest wired and wireless networking portfolio and a long history of delivering business critical connectivity, Brocade® offers all the pieces necessary to deploy a wireless enterprise. The Brocade Mobility portfolio supports the latest draft of the 802.11n standard from IEEE.

Support for All Layers of Networking Stack

sFlow is an industry standard (RFC 3176), which can be used across multiple platforms supporting diverse protocols. The generic format of the sFlow packet allows it to work on all layers of the network stack from Layer 2 to Layer 7. sFlow can be used on switches and routers, but NetFlow works only on IP routers on Layers 3 and 4 of the network stack. Although some recent extensions have been released to support Layer 2 in NetFlow version 9, support for switching technology is mostly incomplete.

Superior Processor and Resource Utilization

The superior sampling technology used by sFlow reduces processor load on routers and switches and provides an accurate representation of the network traffic for monitoring, accounting, billing, network planning, and traffic engineering. Since NetFlow caches information in the router and sometimes also forwards packets in software, it imposes a much higher load on processor and memory resources. Sorting algorithms implemented on the NetFlow cache to match each packet to its NetFlow flow also significantly increases processor utilization rates. For example, CPU utilization could go as high as 70% in some routers for larger numbers of flows. Because of NetFlow's higher processor and memory resource requirements, it cannot be used for higher speed interfaces. Other applications on the router also suffer when NetFlow is enabled because of the resources (memory, CPU, CAM entries and so on). In addition, NetFlow suffers from inaccuracies when there is a high load on the processors.

Real-time Monitoring

sFlow provides accurate statistics in real time. This feature is very helpful in preventing security attacks such as Denial of Service (DoS) and in providing quality of service guarantees. It is also useful to determine historic network load for trending and network planning. Since sFlow does not cache and aggregate flow data or spend time processing data inside the router, the statistics are provided real time. However, NetFlow does not separate processing of data from its export and therefore is not working in real time.

Standards Based

sFlow is a standard defined in RFC 3176. The sFlow.org consortium that develops the sFlow standard includes most of the leading network equipment and network traffic analysis vendors. Most packet-processing ASICs support the sFlow standards. NetFlow, on the other hand, is a proprietary, single-vendor technology. One vendor alone decides on its future enhancements. Although there have been recent efforts to include NetFlow specifications within a standard called IP Flow Information Export (IPFIX), which emphasizes the exporting of flow information, IPFIX suffers from poor vendor adoption and still has most of the deficiencies of NetFlow.

Ease of Configuration

sFlow has superior configuration capabilities and can be configured through SNMP. Sampling rates can be set on every interface. NetFlow, on the other hand, does not support sampling on most versions. Version 9 supports sampling, but only allows a global sampling rate to be set. sFlow is a cheaper technology to develop, since it is supported in ASICs and processed outside the router or switch, and these savings are passed on to customers.

Table 1. Detailed feature comparison between sFlow and NetFlow.

Feature	NetFlow	sFlow
Packet capture	No	Partially
Sampling packets	Partially	Yes
Industry standard	No	Yes
Protocols		
- Packet headers	No	Yes
- Ethernet/802.3	No	Yes
- IP/ICMP/UDP/TCP	Yes	Yes
Layer 2		
- Input/Output interface	Yes	Yes
- Input/Output priority	No	Yes
Layer 3		
- Source subnet/prefix	Yes	Yes
- Destination subnet/prefix	Yes	Yes
- Next hop	Yes	Yes
BGP4		
- Source peer AS	Partially	Yes
- Destination peer AS	Partially	Yes
- Communities	No	Yes
- AS path	No	Yes
MPLS		
- Tunnel name	No	Yes
- VC (name, ID, CoS)	No	Yes
- FEC information (type, length, etc.)	No	Yes
Real-time data collection	Partially	Yes
Configuration		
- Configurable without SNMP	Yes	Yes
- Configurable via SNMP	No	Yes
- Set sampling rate per interface	No	Yes
Low cost	No	Yes
Scalable (switch IFS/collector)	No	Yes
Wire speed	Partially	Yes

In summary the benefits of sFlow include:

- **Accuracy**. Because sFlow is implemented in hardware at wire speed, a high degree of accuracy is achieved.
- **Unified technology.** Users can obtain detailed information from Layer 2 through Layer 7 on all flows. Protocols such as IP and MPLS, are supported.
- **Scalability.** Since sFlow has a low impact on the router/switch performance, all speeds of links (10 Gigabits per second (Gbps) and above) can be monitored. The sFlow technology also scales to monitor tens of thousands of flows over several hundred ports on the router or switch.
- **Deployment ease.** sFlow can be easily deployed on existing networks, and configuring sFlow is simple. Several vendors offer sFlow collector software that can create accurate network views.
- **Minimal network load.** sFlow is non-intrusive in a network. The sFlow packet overhead is less than 0.02% for a 10 Gigabit Ethernet (GbE) link even with aggressive sampling rates.
- **Real time.** Since sFlow is sampled in hardware, changes in flow rates are reflected in real time in the flow statistics.

BROCADE sFLOW FEATURES

Brocade understood the power of sFlow early and was one of the first to implement it. Brocade switches and routers support sFlow version 5. With extensive experience in building high-density routers and switches with large numbers of high-speed interfaces, Brocade has pushed the envelope with a scalable and mature implementation of the sFlow technology. The following innovations by Brocade enhance the richness of the technology:

- **Increased accuracy of sampling.** Within given sampling rates, the Brocade processor randomizes the capturing of packets. This ensures that sampling is more accurate and comprehensive in capturing flow information.
- **Highly scalable.** Brocade's scalable architecture reduces processor overhead to a minimum, which allows for packet capture at very high rates. Sampling rates as high as 1 in 512 packets on 10 GbE interfaces have been achieved with minimal impact to the functioning of the switch or router.
- **Optimized data export.** To ensure the best performance, Brocade switches and routers can stagger the durations for exporting sFlow information. The export durations are configurable to ensure maximum scalability.
- **VPN endpoint monitoring.** Service provider networks that use Virtual Leased Lines (VLL), Virtual Private LAN Service (VPLS), and Virtual Routing and Forwarding (VRF) technologies enjoy the benefits of using the sFlow technology to monitor their L2/3 VPN endpoints. MPLS Virtual Circuit and tunnel on endpoint interfaces can be monitored via sFlow.
- **Flow monitoring.** Network administrators can achieve fine grained flow monitoring on Brocade routers and switches by isolating a single flow among millions of flows.
- **Ease of configuration.** Brocade makes sFlow configuration even easier by allowing both per-port sampling configurations and global sampling configurations to be applied to all ports.
- **Distributed sFlow Agents.** To increase sFlow performance and scalability, Brocade high-end routers and switches implement sFlow agents on the interface modules. This architecture isolates the sFlow agent to the interface modules, which enables high performance without diluting resources from the rest of the system.

APPLICATIONS OF BROCADE SFLOW

Network administrators can use Brocade's sFlow technology to examine current and historic network usage trends or to understand why the performance of a network is slowing down. They can find out if the network is the problem when a server is slow or inaccessible. They can detect worms and viruses propagating in a network and help understand if network resources are being misused. They can graph top users and applications that drive network traffic and analyze different protocols running in the network.

Some applications of Brocade sFlow include:

- **Network outages.** sFlow can monitor thousands of ports in a network to accurately pinpoint reasons for network outages or why traffic on a server is slow.
- **Traffic monitoring.** sFlow provides real-time statistics of traffic on the network, including bandwidth used, protocols, connections, and more.
- **Network planning** Historic traffic usage trends can be used to determine network capacities for planning purposes.
- **Intrusion detection** sFlow can help recognize network-based attacks.
- **Profiling routes.** Traffic flow rates for each route can be determined.
- **Accounting and billing.** For billing purposes, sFlow can provide detailed statistics about applications in use on the network.

EXAMPLES OF BROCADE SFLOW SOLUTIONS

the following sections present examples of Brocde sFlow solutions in representative customer scenarios.

Closed-Loop Network Visibility for Video Monitoring

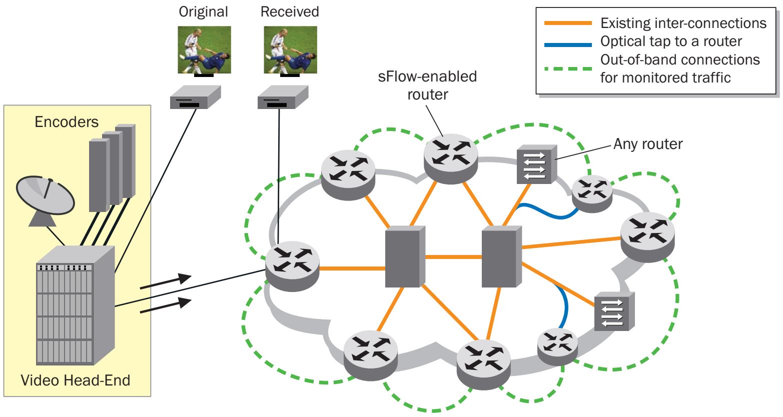


Figure 3. sFlow in a closed-loop network for video networks.

sFlow technology can be used in monitoring video feeds at Network Operations Centers (NOCs) for latencies, jitter, and other traffic characteristics in real time to allow network operators to quickly isolate problems in the network. If the received video feed differs in quality from the original feed, the network operator sFlow can help isolate the faulty network elements. Corrective action can also be taken at the policy-enforcing engines of the network in response to deviations from desired traffic characteristics.

sFlow routers can be connected to collectors either in-band or out-of-band. Standalone management software is used for closed-loop analysis to verify video flows in real time. Collectors analyze the received sFlow feed for the required traffic characteristics. Thus, sFlow provides a reverse feedback path between the location being monitored and the NOC. With the Brocade sFlow solution, the sample rate can be as aggressive as 1 in 512 packets offering real-time responsiveness to faults or degradation in service.

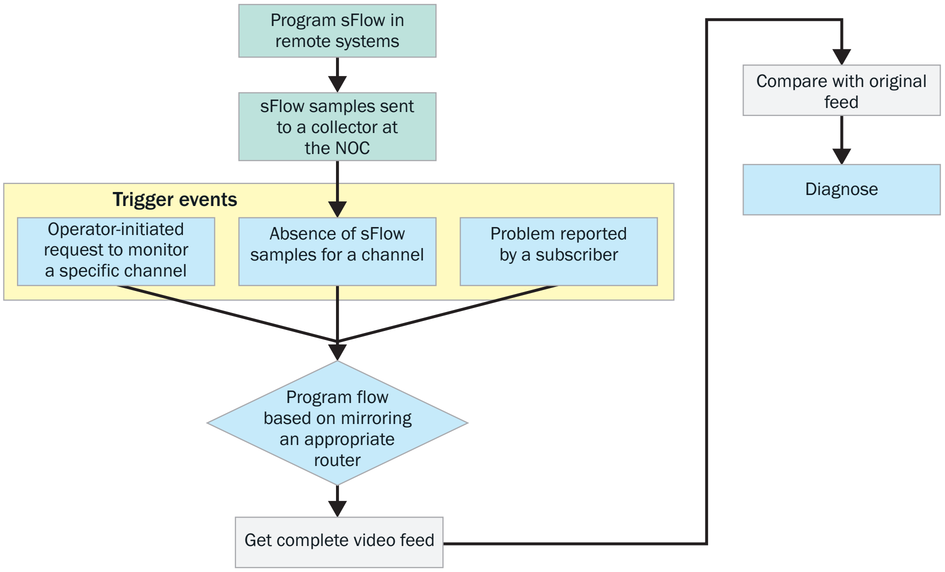

Program sFlow in remote systems
sFlow samples sent to a collector at the NOC
Trigger events
Operator-initiated request to monitor a specific channel
Absence of sFlow samples for a channel
Problem reported by a subscriber
Program flow based on mirroring an appropriate router
Get complete video feed
Compare with original feed
Diagnose

Figure 4. Faults in video networks.

If faults occur in the network, the network manager can view a full replica of the video stream to compare with the original stream. A policy management system reacts to “network events” and applies pre-defined policies such as requesting a full replica of the video stream.

Examples of these network events are the absence of sFlow packets for a certain duration, an operator-initiated operation, or a subscriber-reported problem. The policy manager activates the replication of the video stream through Access Control List (ACL)-based mirroring. Routers can also encapsulate the mirrored traffic into a point-to-point Virtual Leased Line which is set up in advance, to transport the video stream to the NOC.

In addition to monitoring networks, many transit providers use Brocade sFlow in other ways. For instance, Amsterdam Internet Exchange (AMS-IX) uses Brocade's scalable sFlow solutions to effectively monitor high-speed network interfaces and to bill customers based on bandwidth usage. AMS-IX uses its own collector software to analyze sFlow data. For more information, visit http://www.ams-ix.net/technical/sflow.html.

Benefits. The Brocade sFlow solution for video monitoring has several advantages. First, the solution provides a real-time, network-wide service visibility with no performance degradation. sFlow datagrams have been shown to contribute to less than 0.02% of overhead on 10 GbE interfaces.

Second, the sFlow implementation is easy to integrate into an existing infrastructure. By tuning the sFlow sample size, the solution adapts to different traffic loads. IP-based diagnostic tools such as traceroute can be used in conjunction with sFlow without degrading existing services.

Finally, the monitoring infrastructure offers high reliability. The out-of-band sFlow datagram network, including mirrored traffic, is not affected by outages to the core infrastructure. The MPLS Layer 2 VPN infrastructure has built-in resiliency. Multi-location monitoring using multiple sFlow collectors ensures that monitoring is unaffected by collector downtime. Mirrored traffic and sFlow traffic can also be sent to a different NOC for troubleshooting offering additional resiliency.

MPLS VPN networks

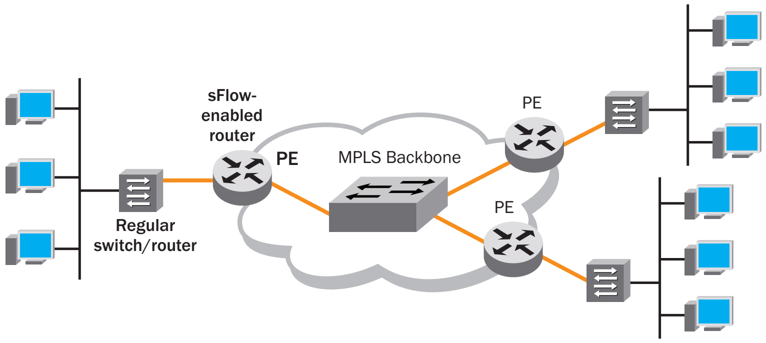


Figure 5.
sFlow in MPLS VPN (VPLS) networks.

MPLS VPN technologies such as VLL and VPLS are popular among business customers that connect different campuses through an MPLS backbone. However, MPLS solutions also make traffic analysis more challenging, because conventional technologies such as SNMP offer only aggregate traffic statistics. Aggregated statistics have limited utility in monitoring individual VPN endpoints. Service providers require the following features to monitor Layer 2 and Layer 3 VPNs:

- Monitoring of network performance, availability, and security
- Trending and traffic analysis per VPN endpoint
- Comprehensive VPN information for troubleshooting and planning
- Identification of the Virtual Circuit (VC) that carries a high traffic load
- Traffic trending and threat detection on a per-VC basis

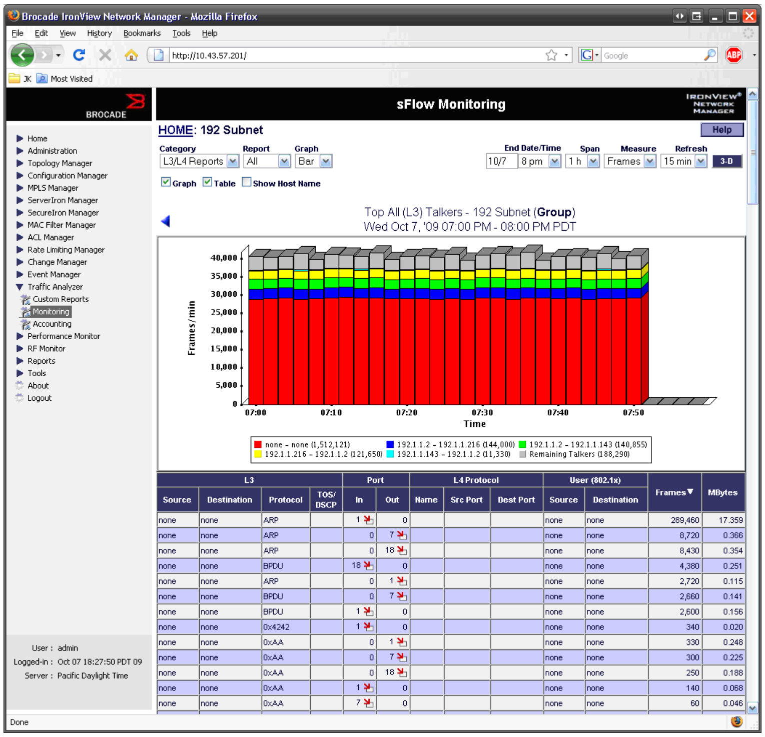
Brocade sFlow technology can provide the solution. Brocade routers at the provider edge (PE) offer sFlow version 5 with VPN endpoint sampling capabilities. PE routers are connected to collectors at NOCs that analyze sFlow datagrams. Collectors can perform analysis and trending on every VC instance with standalone sFlow collection and monitoring tools available for MPLS traffic analysis. Collectors can detect abnormal traffic patterns and excess traffic usage. The sFlow data analysis can aggregate information based on many fields in the flow. Examples of data provided include traffic trends (peak rate, jitter, latency, etc.) per Virtual Circuit, high bandwidth users per Virtual Circuit and/or MAC address, and traffic totals based on multiple parameters.

Benefits. Service providers reduce business risk and increase quality of services they offer by deploying the Brocade sFlow solution. The sFlow solution for MPLS VPN networks is easily deployed with very low overhead on PE routers. Real-time monitoring of critical business services provides quick detection of traffic anomalies. The solution helps service providers maintain the strict Service Level Agreements (SLAs) associated with their platinum customers. For instance, they can rate limit top talkers on a link. They can also perform trending analysis and offer higher bandwidth or price services to their top talkers. The comprehensive network visibility and flexible reporting provided by Brocade sFlow improves fault detection and correction capabilities.

NETWORK MANAGEMENT

The capabilities of Brocade sFlow are more powerful when coupled with the Brocade Ironview® Network Manager (INM). The INM sFlow collector allows a seamless integration with the powerful sFlow capabilities described above. Brocade INM can be used to both monitor traffic patterns with enhanced collector capabilities and also create actions in response to specific events, as described in the closed-loop networking monitoring example above.

Monitoring



User : admin
Logged-in : Oct 07 18:27:50 PDT 09
Server : Pacific Daylight Time

HOME: 192 Subnet

Category: L3/L4 Reports | Report: All | Graph: Bar | End Date/Time: 10/7 8 pm | Span: 1 h | Measure: Frames | Refresh: 15 min

☑ Graph ☑ Table □ Show Host Name

Top All (L3) Talkers - 192 Subnet (**Group**)
Wed Oct 7, '09 07:00 PM - 08:00 PM PDT

🟥 none – none (1,512,121)
🟦 192.1.1.2 – 192.1.1.216 (144,000)
🟩 192.1.1.2 – 192.1.1.143 (140,855)
🟨 192.1.1.216 – 192.1.1.2 (121,650)
▨ 192.1.1.143 – 192.1.1.2 (11,330)
⬜ Remaining Talkers (188,290)

L3				Port		L4 Protocol			User (802.1x)		Frames▼	MBytes
Source	Destination	Protocol	TOS/ DSCP	In	Out	Name	Src Port	Dest Port	Source	Destination		
none	none	ARP		1	0				none	none	289,460	17.359
none	none	ARP		0	7				none	none	8,720	0.366
none	none	ARP		0	18				none	none	8,430	0.354
none	none	BPDU		18	0				none	none	4,380	0.251
none	none	ARP		0	1				none	none	2,720	0.115
none	none	BPDU		0	7				none	none	2,660	0.141
none	none	BPDU		1	0				none	none	2,600	0.156
none	none	0x4242		1	0				none	none	340	0.020
none	none	0xAA		0	1				none	none	330	0.248
none	none	0xAA		0	7				none	none	300	0.225
none	none	0xAA		0	18				none	none	250	0.188
none	none	0xAA		1	0				none	none	140	0.068
none	none	0xAA		7	0				none	none	60	0.046

Figure 6. Brocade INM sFlow monitoring.

The screen capture in Figure 6 shows the Brocade INM traffic analyzer interpreting sFlow datagrams. A graph shows the number of frames per second received from the analyzed traffic. A list of most active flows (top talkers) is also displayed. The rich information offered by sFlow such as the source and destination port, TOS/DSCP, number of frames, and number of bytes is displayed conveniently for the network engineer.

The traffic manager can build custom reports based on flow parameters meeting certain criteria for better search capabilities. It also has accounting capabilities.

Event Processing

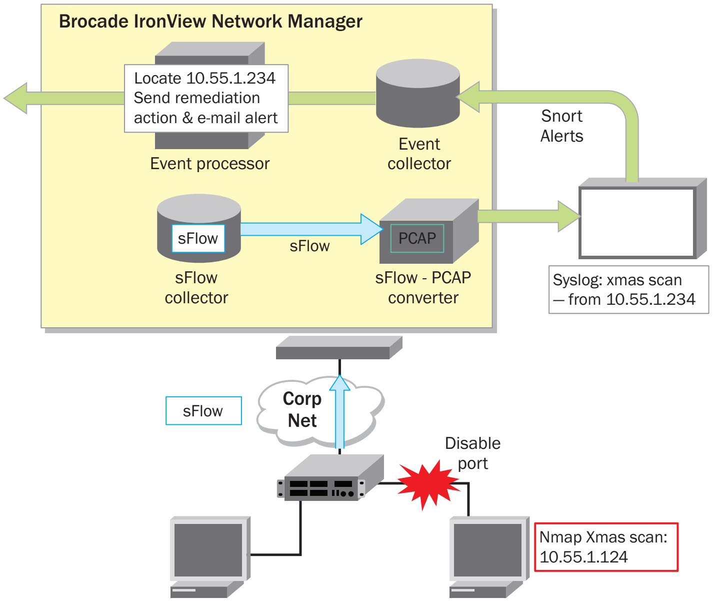


Figure 7.
Brocade INM actions for sFlow data.

Custom rules can be built into Brocade INM to take remedial action on alerts created by analyzing sFlow data patterns. As previously described, sFlow datagrams can be analyzed for security threats such as DoS and worm attacks. For instance, in Figure 7, traffic from source IP 10.55.1.124 contains errant flows based on a Snort analysis of sFlow data. This event has been configured to trigger an action and an alert via e-mail to the network administrator. The specific action in this case is to disable the port to which the errant station is connected.

Brocade INM's seamless integration with sFlow offers both monitoring and event processing and provide a powerful set of capabilities ranging from monitoring to accounting to security attack detection and prevention.

CONCLUSION

sFlow, which is a standards-based monitoring technology, is far superior to NetFlow, which is a proprietary technology. Brocade sFlow technology enables a highly scalable and easy-to-use sFlow implementation. It has been proven to work with hundreds of interfaces over thousands of flows and with aggressive sampling rates. When deployed in networks, Brocade sFlow technology can accurately monitor networks, provide real-time data on network quality/health, and save money by maintaining business continuity.

Corporate Headquarters
San Jose, CA USA
T: +1-408-333-8000
info@brocade.com

European Headquarters
Geneva, Switzerland
T: +41-22-799-56-40
emea-info@brocade.com

Asia Pacific Headquarters
Singapore
T: +65-6538-4700
apac-info@brocade.com

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.