Extending Network Visibility by Leveraging NetFlow and sFlow Technologies

This paper shows how a network analyzer that can leverage NetFlow and sFlow technologies can provide extended visibility into enterprise networks without added investment.

NETWORK INSTRUMENTS®

Abstract

NetFlow and sFlow® are traffic reporting mechanisms that manufacturers have embedded into enterprise-level switches and routers. This paper describes the strengths and limitations of these technologies, and why combining NetFlow/sFlow reporting mechanisms with a distributed network analyzer is a best practice in network monitoring. Deploying a distributed analyzer that can interpret NetFlow and sFlow reporting streams gives network managers extended visibility without over-extending the IT budget.

Introduction

NetFlow and sFlow are similar to the local public library: everybody lives near one; virtually everyone helped pay for one, but very few people actually use their local branch, other than to check out a book to read now and then. Many are completely unaware that the library has a larger collection of DVDs than most video stores, more varied music than many CD outlets, and often a dedicated research staff that will answer questions on any topic imaginable. And all of these benefits are usually available for free.

NetFlow and sFlow are similarly overlooked. Part of the reason is that, until recently, analysis vendors have viewed these technologies as a competitive threat rather than an opportunity. But now that NetFlow and sFlow support are appearing in commercial analysis tools, IT administrators can better leverage this free visibility lying latent in their switches and routers.

NetFlow and sFlow: Technology Overview

NetFlow and sFlow are standard traffic reporting mechanisms that device manufacturers have embedded into devices such as routers and switches. Unlike SNMP, NetFlow and sFlow are "push" technologies that send periodic reports to designated collectors. Neither NetFlow nor sFlow provide as much detail as most commercially-available remote monitoring probes. However, because these technologies are freely available, they make an attractive alternative where the expense of a dedicated commercial probe is not justified, or simply to extend the visibility of probes already deployed.

NetFlow vs. sFlow

NetFlow is implemented in the router or switch software (typically Cisco IOS or one of its clones). sFlow is implemented in a dedicated hardware chip, thus conserving a device's memory and CPU resources. Both mechanisms send UDP datagrams to a collector that summarize traffic statistics. NetFlow collects data on all routed IP traffic traversing the device; statistics obtained via sFlow is based on packet sampling. Packet sampling conserves resources by only considering a representative sample of traffic (i.e., only 1 in n packets is collected, and by default only a portion or slice of each sampled packet is stored). Although it is possible to collect each sampled packet in its entirety, doing so could overwhelm the resources of the reporting device.

Although flow technologies provide network statistical data, they do not provide the packet-level detail required for complete analysis. It is simply unavailable from these embedded technologies. For example, to perform any type of application analysis or expert analysis, the analyzer must have access to every packet in the conversation, something that only a fully functional network analysis probe can deliver.

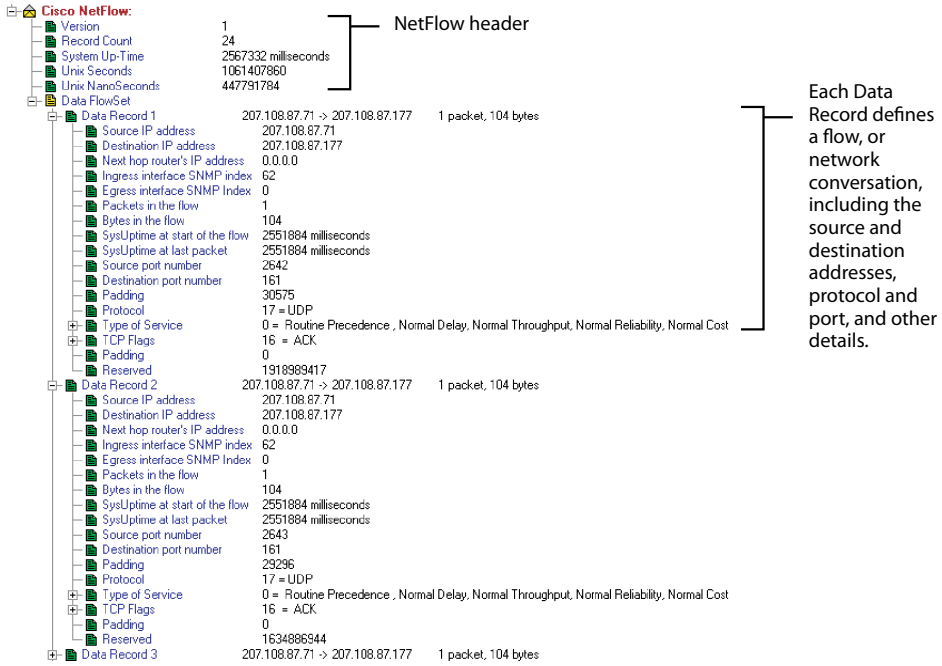
Data Collected by NetFlow and sFlow

The UDP datagrams sent by NetFlow and sFlow contain various network traffic statistical counts coupled with some administrative header information. To illustrate the structure of a NetFlow or sFlow report stream, you can capture and decode the datagrams with a protocol analyzer.

NetFlow records data per "flow," a flow being the traffic stream passing between a pair of addresses on a particular port.

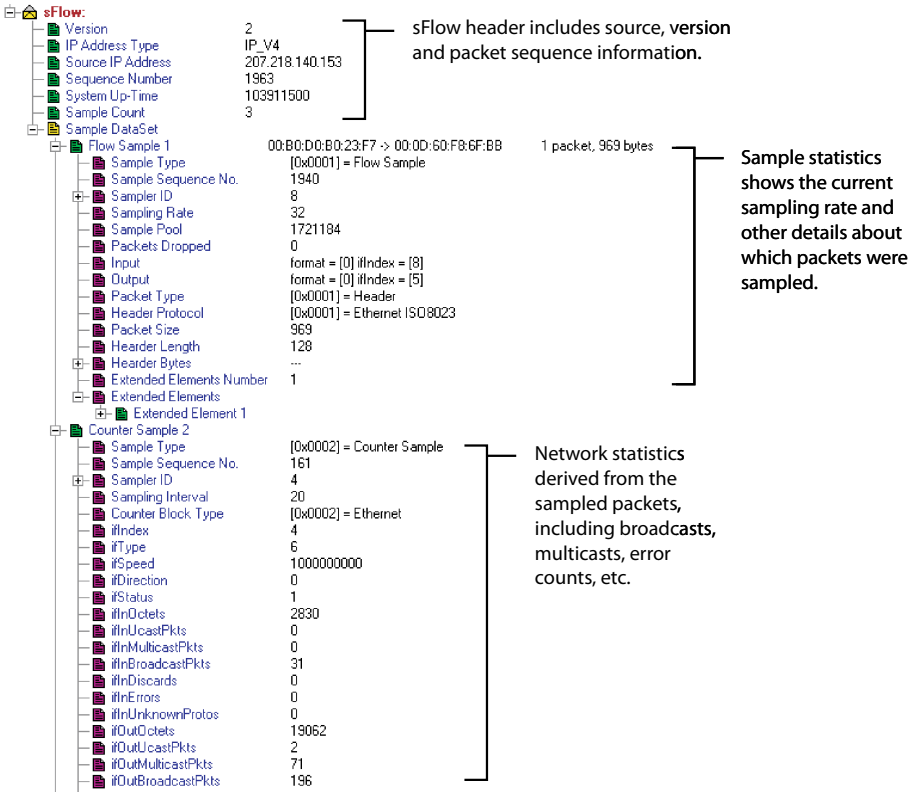
NetFlow Datagram Example

(Decode provided by Network Instruments' Observer®)



An sFlow agent, in addition to passing the sampled packet slices to the collector, also passes datagrams that carry aggregate network information:

sFlow Datagram Example *(Decode provided by Network Instruments' Observer)*



Leveraging NetFlow and sFlow

How can you take advantage of NetFlow and sFlow reporting? There are a number of ways to access the data reported by these technologies:

- With NetFlow, you can query for data directly through the administrative interface of the router or switch. This capability is more for setup and internal troubleshooting purposes; manually looking at the NetFlow stream from multiple devices is obviously not a practical mechanism for monitoring an enterprise network.
- You can use dedicated tools, both open-source and commercial, to monitor NetFlow/sFlow reporting streams. Any of these dedicated NetFlow/sFlow monitors may be adequate for smaller shops located on a single local network; managing larger networks with multiple remote sites requires real integration with the analysis solution to be truly practical (See below).
- You can use select commercial analyzers with truly integrated support for NetFlow or sFlow agents. This is by far the most attractive option for the enterprise, as detailed below.

But beware of some commercial network analysis vendors that stretch the definition of NetFlow/sFlow support. In reality, they merely provide separate, dedicated NetFlow/sFlow monitors (as described in the second bullet item above). They are often physically separate devices that do not share look-and-feel or data with the standard analysis engine.

Why Coupling NetFlow/sFlow with Distributed Analysis is Best

NetFlow and sFlow by themselves do not scale particularly well. Directing all of the reporting streams to a central console generates excessive (and unsecured) traffic. Redirecting the reporting streams so that you or someone else can look at the data from another site isn't practical at many organizations where administrative access to routers and switches is limited.

Also, as mentioned earlier, neither NetFlow nor sFlow provide packet-level visibility (sFlow only allows sampling of packet slices). This type of visibility (and the sophisticated reports and analysis that comes with it) requires an advanced network analyzer.

Integrating these two technologies delivers multiple benefits:

- **Consolidation, compression, and encryption of the reporting streams:** Both NetFlow and sFlow send multiple streams of clear text, which is inefficient and can be a security issue. One commercial product that mitigates these problems is Network Instruments® Observer®. Observer consolidates and compresses NetFlow/sFlow reporting streams, and encrypts the communication.
- **Increased administrative flexibility:** Access to the data stream is no longer locked in the router or switch: it can be controlled via the probe's administrative interface. There are two problems with having to administer traffic reporting through the device:

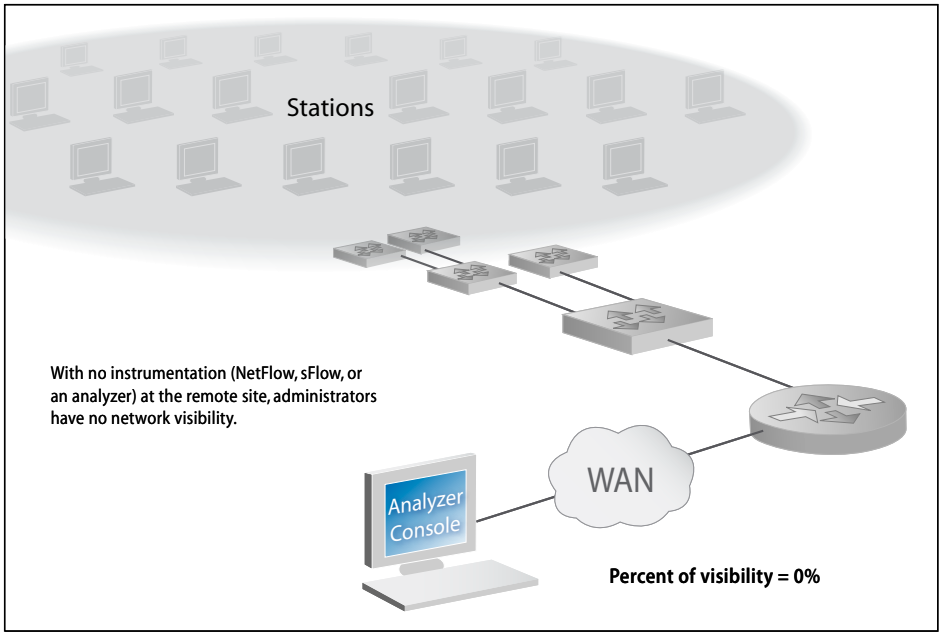
1) access to device administration is limited in most enterprises, and 2) the targeting capabilities of NetFlow/sFlow are limited; NetFlow, for example, allows you to specify only two target collectors. By making a distributed probe the target, you can then administer the probe, and if it is a Network Instruments' Expert Probe, you can create multiple, virtual probe instances to extend the availability of the NetFlow/sFlow analysis to dozens of users if necessary.

- **Apply sophisticated monitoring features to NetFlow/sFlow data:** Network Instruments' Observer, for example, allows you to store NetFlow/sFlow-derived data in long-term archival reports (Network Trending). It also allows you to set alarms that trigger an automated notification when various network conditions are reported by NetFlow or sFlow, such as the appearance of a protocol or IP address.
- **Reduce training costs:** By showing the NetFlow- or sFlow-derived data in the same reporting format displayed by a standard probe, the IT staff does not have to learn multiple user interfaces to access the same type of information from different points of visibility.

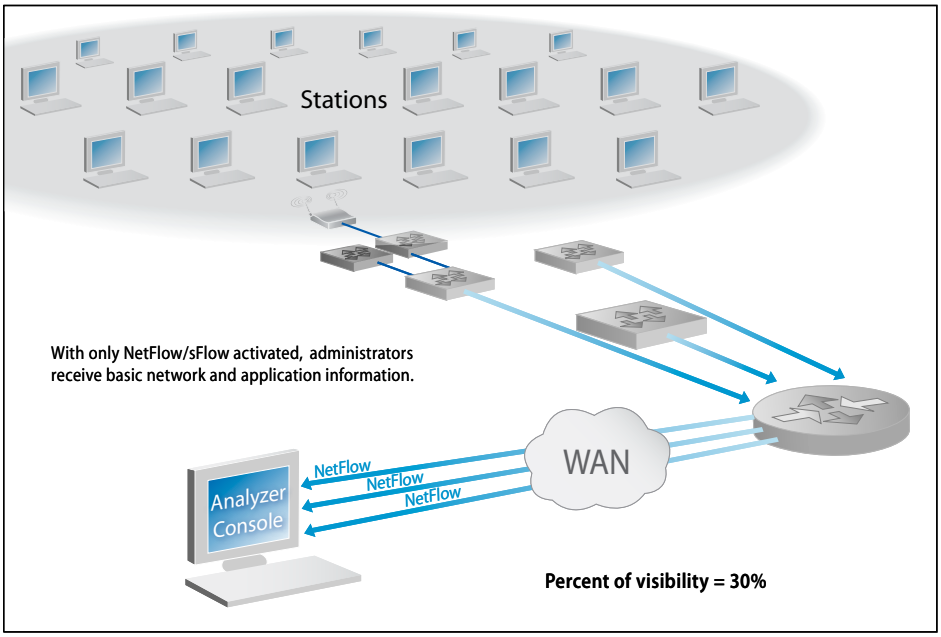
NetFlow/sFlow+Distributed Analysis=Total Visibility

The following diagrams illustrate how NetFlow/sFlow and analyzers work together to give the IT administrator total visibility into a remote segment.

No Probe, no NetFlow, no sFlow



NetFlow and sFlow activated



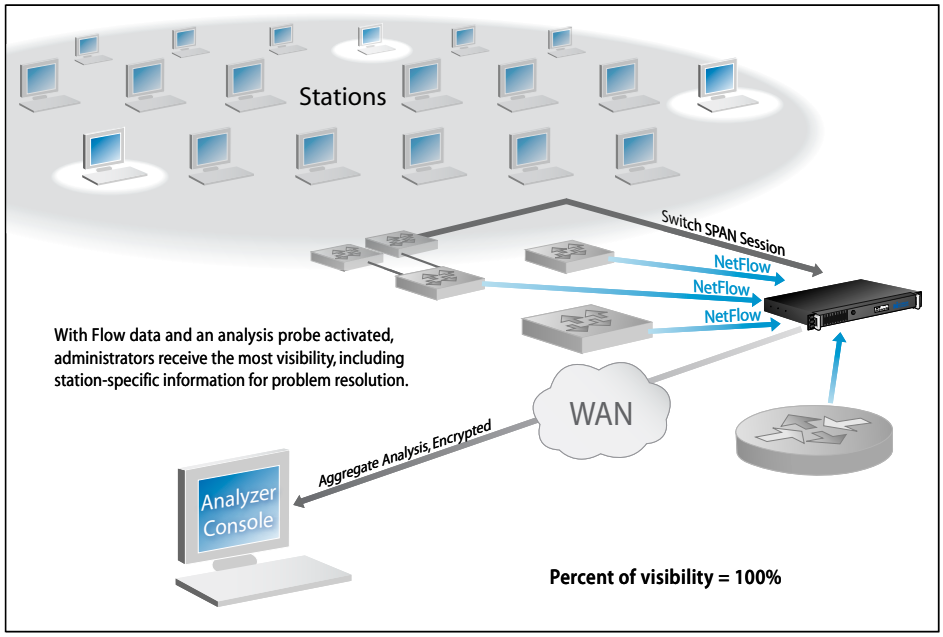
With NetFlow and sFlow enabled on the devices that support it, the administrator has limited visibility. In particular, the administrator can see:

- Which stations are generating the most traffic
- What applications are running on the network by protocol and port number
- Internet connections
- VLAN usage statistics
- Type of Service (ToS), also called Precedence or Quality of Service (QoS).

Without a probe, however, some important features are missing:

- NetFlow does not capture any actual packets, and sFlow only captures a slice of each packet it collects, which is only a fraction of the total number of packets traversing the device.
- Certain types of deep analysis are impossible without access to every packet on the wire: for example, application response time analysis, and "ladder chart" graphical displays of network conversations (sometimes called "connection dynamics") are unavailable.
- NetFlow and sFlow reports generate multiple, unsecured data streams across the network or WAN link. As we will see in the next diagram, using a probe at the remote site to collect the data is more efficient and secure.

sFlow and NetFlow provides extended visibility, probe delivers detailed drill-down



For continuous visibility of every packet on the remote network, you would need to deploy multiple probes to continuously collect SPAN sessions from each switch. This is usually not practical or desirable. Combining NetFlow/sFlow reporting with a probe gives you the best of both worlds:

- For continuous monitoring of aggregate network statistics, NetFlow and sFlow are adequate, especially if they report to a local probe that provides network trending and alarm notifications. For example, with such a system, you can trigger a notification when certain protocols appear, or when any one station consumes a threshold percentage of network traffic.
- When NetFlow/sFlow monitoring indicates a problem, you can direct a SPAN session from the relevant segment to the probe deployed onsite for packet capture and drill-down analysis.
- Some distributed analyzers (such as Network Instruments' Observer) store NetFlow and sFlow information in an extremely compact form, which means the system can store data for very long-term trend analysis. This type of historical information can be crucial for planning network upgrades and establishing baseline usage patterns.

Also note that a single, encrypted probe/console link over a WAN link is preferable to sending multiple, unsecured data streams over a WAN link.

Using a Remote Probe + NetFlow/sFlow to Manage a Remote Network

So, how does all this work in practice? Here are a few typical network problems, and how they would be detected and solved using a combination of NetFlow/sFlow for broad monitoring, and a Network Instruments Expert Probe for detailed drill down:

- The sFlow Top Talkers reports from the access layer show that there is a station generating a wildly disproportionate share of network traffic. Suspecting a malware infection, the administrator directs a SPAN session from the relevant switch to the Expert Probe, and activates the hacker/virus triggers and alarms. Suspicions are confirmed. The administrator calls the user to schedule a spyware/adware/virus sweep as soon as possible.

- Users are complaining about slow Internet access. NetFlow reports from the router show an unusually large volume of high-port (>9000) TCP traffic, which almost certainly points to Bittorrent. Using the Expert Probe to analyze a SPAN session of the core switch's connection to the router, the administrator filters for high-port TCP traffic. Sure enough, the new hire's workstation is the culprit. The administrator calls the offending user and gives him a short refresher course on corporate Internet usage policy.
- VoIP users at the remote site are complaining of poor voice quality. NetFlow/sFlow reports a complete absence of any traffic with Type of Service (ToS) set to 5 (in other words, high-priority VoIP traffic). The solution is to reconfigure the call manager at the remote site to use the appropriate ToS setting.

In short, NetFlow/sFlow gives a broad view of problems that might be affecting the network, while precise diagnosis requires capturing every relevant packet on the wire with the probe.

Conclusion

Managing large networks that span multiple locations is never easy or cheap. Every monitoring tool requires hardware resources, and even open-source and device-embedded tools such as NetFlow and sFlow have setup and maintenance costs. But by deploying the correct level of monitoring where it is needed, you can have comprehensive visibility without breaking the IT budget.

Leveraging NetFlow and sFlow technologies with a distributed analyzer (such as Network Instruments' Expert Observer and probes) offers the best of both worlds:

- NetFlow/sFlow-provided broad visibility for network trending and the "30,000-foot" view.
- Access to every packet on the wire when necessary, accomplished by directing a SPAN session to the probe.

NetFlow/sFlow technologies, when used alone, are inefficient and not secure. By leveraging distributed analysis infrastructure to integrate NetFlow and sFlow reporting, you can not only gain free visibility, but enhance the security and scalability of NetFlow and sFlow.

Corporate Headquarters
Network Instruments, LLC • 10701 Red Circle Drive • Minnetonka, MN 55343 • USA
toll free (800) 526-7919 • telephone (952) 358-3800 • fax (952) 358-3801
www.networkinstruments.com

European Headquarters
Network Instruments • 7 Old Yard • Rectory Lane • Brasted, Westerham • Kent TN16 1JP • United Kingdom
telephone + 44 (0) 1959 569880 • fax + 44 (0) 1959 569881
www.networkinstruments.co.uk