Free is Not Always Cheap—Getting the Most Out of Cisco's NetFlow

By Drew Robb

SOMETIMES YOU CAN FIND A GREAT DEAL IN TERMS OF INITIAL OUTLAY. You could probably get a 1970 station wagon for next to nothing. Of course you wouldn't get much in terms of performance or reliability, and the old gas hog would be expensive to run and maintain.

That was the case with the initial iterations of Cisco Systems, Inc.'s NetFlow technology which provides a metering base for other applications. Cisco included it with its routers and switches, so the price was right, but it also developed a reputation for being difficult to deploy and a performance hog. But that is no longer the problem it once was.

"NetFlow Version 9 has many improvements in functionality and performance," says J. Jeffrey Nudler, Senior Analyst at Boulder, Colorado's Enterprise Management Associates, working in the areas of availability, configuration and performance management. "Perhaps the most significant is that in this version both ingress and egress data are collected. This enables much more granular analysis and effective functionality, be it accounting or failure diagnosis."

The product still, however, requires a third party tool to analyze the data provided. In this article we will take a look at both what NetFlow provides, as well as several products companies can use to analyze NetFlow's data output.

HISTORY LESSON

Cisco created NetFlow to assist customers in areas such as network monitoring, traffic analysis/planning; and usage accounting/billing. It utilizes Cisco's Internetwork Operating System (IOS) which drives Cisco's routers and some of its switches. It involves two elements: a properly configured device generating data and a data collector. Administrators can activate NetFlow on a router by typing in:

```
#ip flow-export destination<ip address> <port number>
#ip flow-export source <interface# or vlan>
#ip flow-export version 5 peer-as
```

Next, configure the collector to listen on the correct UDP port (2055 is the default).

Once that is completed the torrent begins. A single 20 megabit interface creates about 1GB of data daily. NetFlow increases traffic by about 2 percent of the current utilization, so each 100Mb pipe (assuming it is half utilized) streams 1Mb of data to the collector every second. If you have 100 such devices in the network, you need a system capable of aggregating, analyzing and reporting on that much data. But by doing so administrators can spot which are the top applications and users, and which users are communicating with which applications.

Not all network gear supports NetFlow version 9, including some of Cisco's older products.

"NetFlow's improvements come at a price of incompatible data structure with previous versions," says Nudler. "So far very few vendors have made their product NetFlow version 9 compatible due to this stumbling block."

The upcoming Internet Protocol Flow Information eXport (IPFIX) from an Internet Engineering Task Force (IETF) Working Group (www.ietf.org/html.charters/ipfix-charter.html) will standardize flow export and broaden the number of products supported. It is based on NetFlow 9, so will cover products using IOS, but also will include products from Enterasys, Extreme Networks, Foundry Networks, Juniper Networks, Nortel, Riverstone Networks, and others.

Neither NetFlow nor IPFIX replace existing management protocols or tools, but supplement existing monitoring and reporting functions.

"The IPFIX standard is in the process of being verified by the IETF community," says Nudler. "When it becomes a ratified standard, EMA anticipates a number of new vendors entering the NetFlow analysis market giving users greater functionality choices."

ANALYSIS OPTIONS

Once an organization chooses to implement NetFlow or IPFIX, it has several options for analyzing the information generated.

"The Collector contains a voluminous amount of data that has to be processed and analyzed," says Nudler. "Depending on the functionality sought from this Collector-stored data, the sophistication of data extraction and analysis can vary. It is possible to have a home grown application to process NetFlow data, however the economics of this depend on the specific environment resources."

Companies looking for a commercial, rather than home grown application can select from a variety of products including NetQoS, Inc.'s (Austin, Tex.) ReporterAnalyzer; Crannog Software's (Dublin, Ireland) NetFlow Tracker; NetScout Systems Inc.'s (Westford, Mass.) nGenius Performance Manager; AdventNet, Inc.'s (Pleasanton, Cal.) NetFlow Analyzer 4; and Plixer International, Inc.'s (Somersworth, NH) Scrutinizer. Let's take a look at a couple of these in action—one in the enterprise class and one that fits more at the low to mid-range.

NetQoS built its ReporterAnalyzer appliance to meet the needs of large organizations. It has a starting price of around $25,000 and is sold primarily to Global 2000 organizations such as Cisco, Chevron, Hewlett-Packard and Verizon. The technology was developed by NetQoS CTO Dr. Cathy Fulton when she was working as a consultant

for oil and gas services firm Schlumberger, which needs to connect its 60,000 employees working in 80 countries. As such, it is designed for managing widely distributed networks.

"Companies with few geographically dispersed locations typically would not benefit from ReporterAnalyzer's full capabilities, since the product is designed to monitor traffic across network links," says CEO Joel Trammel.

But they don't need to fully implement the product on the entire network before they start to benefit from it.

"The vast majority of enterprise network gear supports NetFlow or the upcoming IPFIX standard that we support," he continues. "One of the benefits our customers like is that they only need to turn on NetFlow on a few key switches and routers in order to start using ReporterAnalyzer, so they are leveraging their existing Cisco or other investment."

The full benefit, however, comes once the entire network is activated. Tool manufacturer Black & Decker Corporation, for example, has a network servicing 300 sites in 50 countries. It uses NetFlow and ReporterAnalyzer to monitor traffic passing through 800 interfaces, and gain visibility into which applications are running on the network. As a result, the company was able to track down several applications that were consuming excessive quantities of bandwidth and scale them back.

"It's a simple, distributed, scalable way to do network engineering," says John Schnelle, Black & Decker's manager of network architecture and network management systems. "We gave administrators in the field read-access which saves us a lot of trouble calls."

ChevronTexaco started using NetFlow and ReporterAnalyzer to help integrate the IT resources of Chevron Corporation and Texaco, Inc. following their merger in 2001.

"Outside the core network, we didn't have a good way to monitor the health of the network, says Don Mendel, Senior Global Network Architecture Team Leader. "We had RMON probes on the core links, but we still had 250 or so links to the outer networks for which we had no current helpful information. Visibility of the total network was limited."

With ReporterAnalyzer in place, ChevronTexaco was able to locate a single user who was consuming half the network resources at a location in Washington, and eliminate a planned $3000 per month T-1 line in California by finding the actual cause of a slowdown. (The circuit was found to be only running at 2 percent of capacity so the problem wouldn't have been solved by throwing more bandwidth at it.)

"People were always calling up asking, what happened last Thursday? Why was the network so slow? And we didn't have the ability to get that kind of data," says Mendel. "Now, NetQoS gives us the immediate state of our network, when and how we need it."

ReporterAnalyzer is an ideal product for companies such as Black&Decker or ChevronTexaco. Plixer, on the other hand, created a smaller, a less expensive alternative for companies who don't need a product that scales as large or who don't require as extensive a feature set. NetQoS offers greater SNMP support than Plixer and has a distributed harvester technology to aggregate data from over 100 NetFlow routers and switches. It also saves data for a full year, while Plixer's Scrutinizer only does so for thirty days. Such factors are certainly required if you are a large enterprise with a global network spanning hundreds of sites. In addition, Scrutinizer currently relies on its integration with WhatsUp Pro from www.ipswitch.com or Orion from www.solarwinds.net to provide the historical data. This is all integrated in NetQoS.

Many organizations, though, will be able to get by with a lower-level tool. Scrutinizer Professional, for example, which monitors a single switch or router, costs $995. Scrutinizer Enterprise, which collects data from multiple devices and unlimited interfaces, runs $3995. The State of Maine's Office of Information Technology (OIT), for example, provides all IT services to 13,000 State employees at 650 sites. The network contains about 500 switches linking a mix of 10/100/1000 fiber, T-1 lines, 56K frame relay circuits over collapsed ATM, Sonet, and a Gigabit/10-Gigabit backbone. Recently it began using Scrutinizer to monitor its WAN traffic.

"Due to the massive quantities of data it was not practical to develop a tool in-house," says Duncan Bond, OIT data network analyst. "We have been using another product, but Scrutinizer gives us a much more intuitive and direct front-end into NetFlow statistical data."

It is currently configured to report on about a third of the WAN equipment, but eventually it will cover the rest.

"Once IPFIX is ratified and supported on all our switches, we'll collect and report data on our Layer 3 switches as well," he explains. "At that point, Scrutinizer will report on 100 percent of our routed infrastructure."

When network administrators notice a utilization problem, they use Scrutinizer to drill down to determine what is causing the bottleneck.

"Most of the time we don't need to know how the network is being used, only how much," Bond says. "Occasionally, we have to know how it's being used and that's when Scrutinizer is essential. Rather than having to insert an RMON probe or a protocol analyzer to get the information, the data's already there so we can react much faster."

This came in handy when one agency was converting from Novell File Services to Microsoft's Active Directory. The OIT received a call from the agency reporting extremely slow progress. A quick look at Scrutinizer found that many devices were downloading large amounts of data from a server in a different city.

"The technicians had inadvertently put in the wrong server address to pull updates from," says Bond. "Knowing this, the agency quickly reconfigured and the conversion went smoothly."

SIZE OR FEATURES

While NetQoS and Plixer both offer NetFlow analysis products, they are not in direct competition any more than an eighteen wheeler and a Corvette are. True, they are both vehicles, but one is designed for moving heavy loads, while the other zips around mountain roads. You wouldn't want to try use the wrong vehicle for the wrong job. And so it is with NetFlow management software. Although NetQoS targets large global companies and Plixer smaller ones, Nudler emphasizes that it is not the size of the organization, but its technical requirements that determine which product is the best fit.

"NetFlow data can be used for a number of different IT management aspects," he says. "Hence the issues of the organization's management requirements rather than size (given equal technical product capability) should be the primary consideration."

NaSPA member Drew Robb is a Los Angeles based writer who focuses on technology issues.