



Gaining Operational Efficiencies with the Enterasys S-Series[®]

Hi-Fidelity NetFlow

Gaining Operational Efficiencies with the Enterasys S-Series

Introduction

Network infrastructures are the bedrock upon which enterprises build, grow and support their businesses; to that end network managers are constantly making decisions that affect critical business activity across the network. Traditional click-and-wait-type applications, such as email, web browsing, and office productivity tools are being joined by real-time communications applications such as voice and video over IP. Today's network managers are faced with significant challenges to optimize application performance, availability and quality of service (QoS) in the face of the explosion in the density and diversity of end systems attaching to the infrastructure.

Network managers need granular visibility into users, devices and applications that are using network bandwidth, as well as events or other disruptions of service. Visibility is crucial as networks become more complex - the ability to measure, quantify and analyze enterprise "application" traffic across the network is critical to assuring service. Initially, in order to gather information on network traffic, enterprises relied on dedicated hardware probes that collected RMON2 statistics. However, in the quest for better network management, increasing numbers of network managers have turned to flow monitoring. NetFlow provides accurate insight into all applications running on the network without the use of probes.

What Is NetFlow

NetFlow is a data collection protocol in switches and routers that provides network administrators with statistics for the amount and type of traffic between IP users in their network. When NetFlow is enabled routers and switches keep track of all inbound conversations on each interface it is enabled on.

NetFlow examines packets based on seven key fields:

- Source IP address
- Destination IP address
- Source port
- Destination port
- Layer 3 protocol type
- Type-of-Service (ToS) byte
- Input logical interface

If two packets match all seven key fields, the switch or router will assign them to the same flow or conversation. Once the conversation has ended or is summarized it is sent to a "NetFlow Collector". A NetFlow management application is used to retrieve the data from the collector for analysis and report generation.

There are multiple versions of NetFlow; the most widely deployed is version 5. However, version 9 is becoming increasingly popular. The Internet Engineering Task Force released a standard called IP Flow Information Export (IPFIX RFC 3917), which is based on NetFlow v9's data export format. Details of the specification are available at <https://datatracker.ietf.org/doc/rfc3917/>

Enterasys S-Series NetFlow Capabilities

Enterasys has implemented NetFlow on our S-Series switches. Version 5 and version 9 are both supported completely free of charge, which is significant since other vendors require expensive dedicated hardware modules or daughter cards and license fees to implement NetFlow. A distinct Enterasys advantage is flow-based ASIC capabilities that collect NetFlow statistics for every packet in every flow without sacrificing CPU or switching performance. The S-Series implementation enables the collection of NetFlow data on both switched and routed frames, allowing S-Series modules in all areas of a network infrastructure to collect and report flow data at gigabit speeds.

A single NetFlow packet can be very large and contains conversation details on up to 24 (NetFlow v9) conversations; because of this most vendors implement statistical sampling techniques, which help to maintain performance. Since sampled NetFlow does not report on every packet the NetFlow records must be adjusted for the effect of sampling - traffic volumes, in particular, are now an estimate rather than the actual measured flow volume. Enterasys provides unsampled NetFlow, and therefore can accurately represent nearly 100% of all IP traffic.

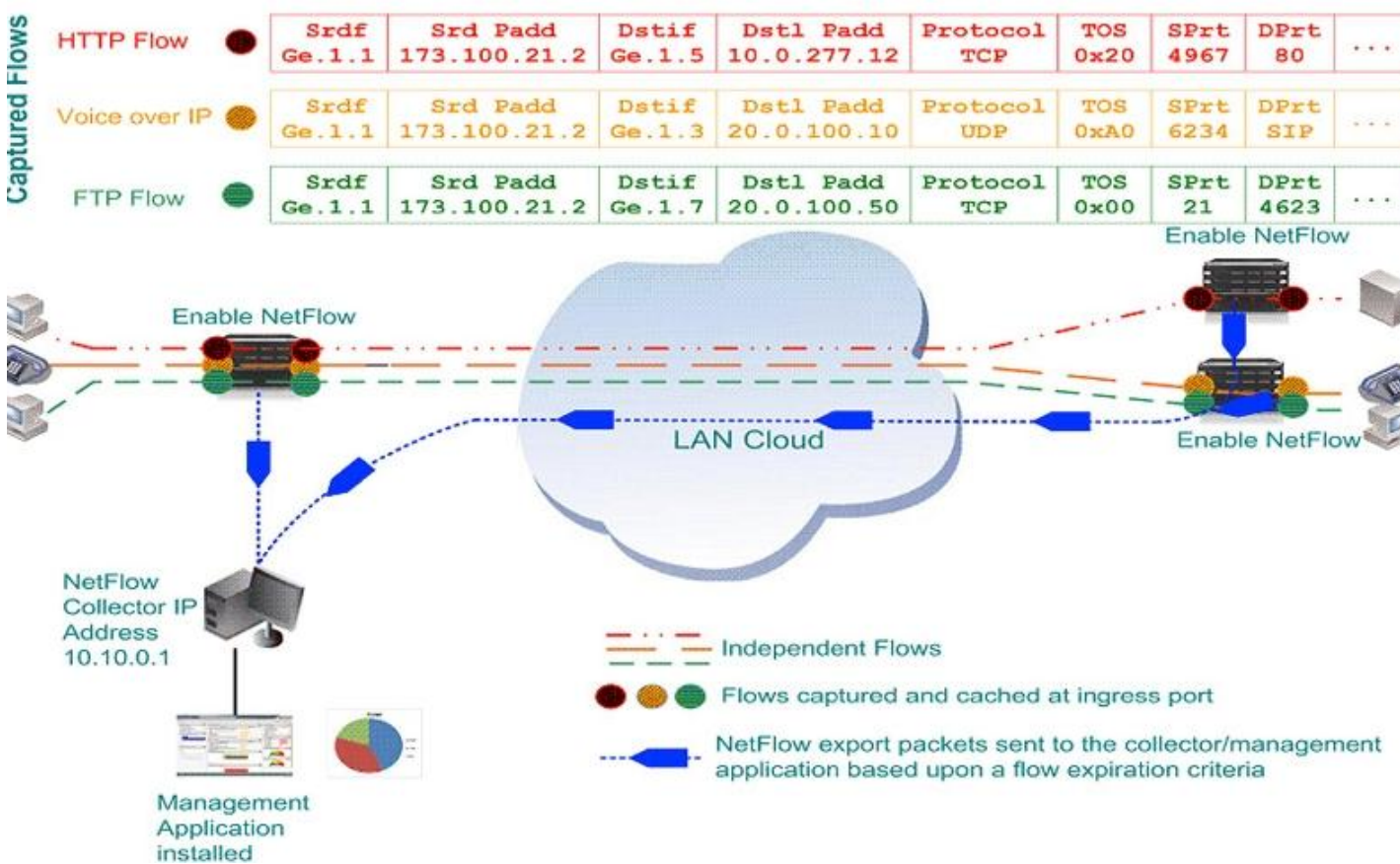
The S-Series flow-based architecture provides a powerful mechanism for collecting real time flow statistics, with reporting capacity that scales with the addition of each I/O module without degradation to switching/routing performance or requiring the purchase of expensive NetFlow monitoring hardware. Enterasys embeds NetFlow capabilities into every ASIC providing our customers with industry-leading value.

The S-Series tracks every packet in every flow, collecting 9,000 flow records per second, per blade on any module. This is an order of magnitude greater NetFlow collection performance than any other NetFlow appliance vendor (over 70,000 flow records per second in a fully populated chassis) and as such can provide network managers with nearly 100% accuracy of who is communicating and with what application across the switch.

Once NetFlow data has been collected an analysis tool is required to examine and correlate the information into detailed reports. A NetFlow collector application correlates the received records and prepares them for use by the NetFlow management application. In some cases the collector and management applications are bundled in a single application. The Enterasys SIEM can be utilized as a NetFlow collector to provide Network Behavioral Analysis Detection (NBAD). This ensures that reconnaissance activities, denial of service attacks and zero-day attacks are detected and remediated before significant damage can occur.

In addition to the Enterasys SIEM the Enterasys Network Management Suite (NMS) can use NetFlow data for troubleshooting, analysis and management. A variety of open-source tools also provide analysis and reporting on NetFlow data provided by S-Series switches.

Profile Your Network Using NetFlow



NetFlow Network Profile Example

The example above shows Enterasys S-Series switches with NetFlow enabled and the subsequent flow data for HTTP, VoIP and FTP traffic. The NetFlow export packets are received by the collector and the usage information for each flow is displayed, thus providing an intuitive view into the network's overall usage. When compared to the use of RMON2 and the deployment of probes, the S-Series provides businesses with significant savings and greatly enhances the operational efficiency of the network and therefore also increases the operational efficiencies of the organization.

Enterasys provides industry-leading ROI and reduced operational costs by embedding NetFlow services into S-Series switches; the value is best described by the following statements:

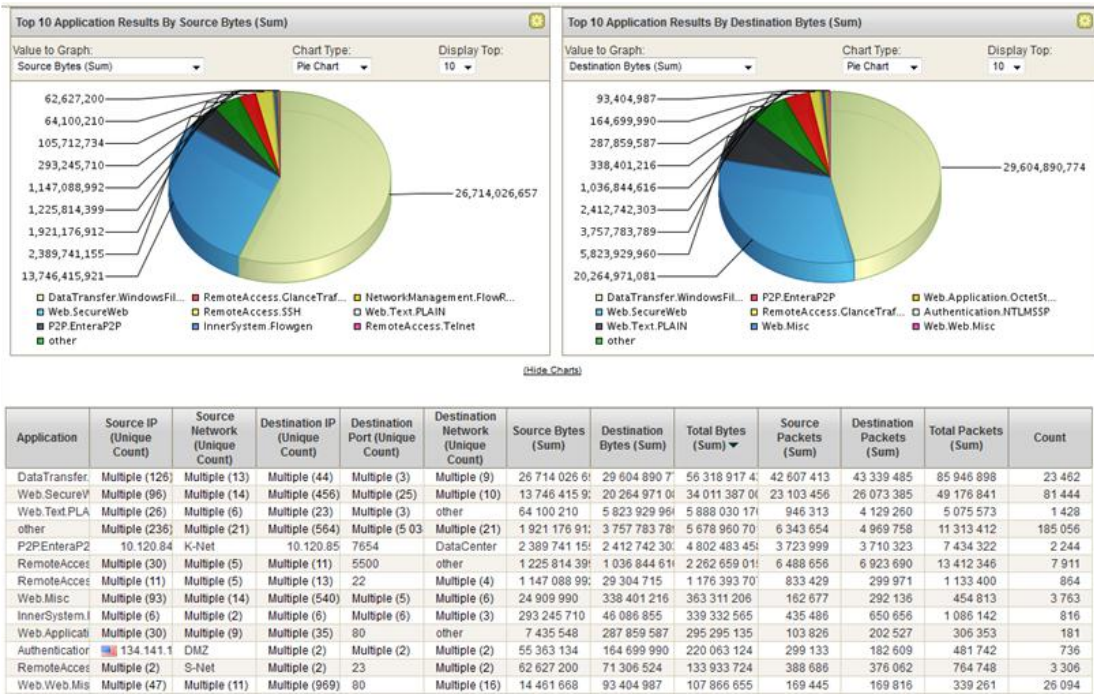
- **No capital investment** - the S-Series provides full NetFlow support free of charge, in contrast to the significant costs associated with purchasing, deploying and maintaining large numbers of probes required to cover all or part of the network.
- **Low deployment costs** - Configuring NetFlow on the S-Series is simply the matter of enabling a few global and interface commands; probe solutions by contrast require extensive configuration, detailed planning and significant deployment and maintenance costs.
- **Complete data source** - the S-Series provides hi-fidelity NetFlow, automatically measuring and reporting on all IP traffic; most probe solutions require that each probe be configured for each monitored traffic type.
- **No life cycle maintenance** - S-Series NetFlow support is provided at no additional cost in every S-Series module; probes require costly licenses, software upgrades and probe upgrades to cater for network bandwidth increases.
- **Lower operational costs** - By implementing S-Series switches, operational costs are lowered as network managers and administrators save the time needed to configure and maintain large numbers of third party probe devices.

NetFlow Applications

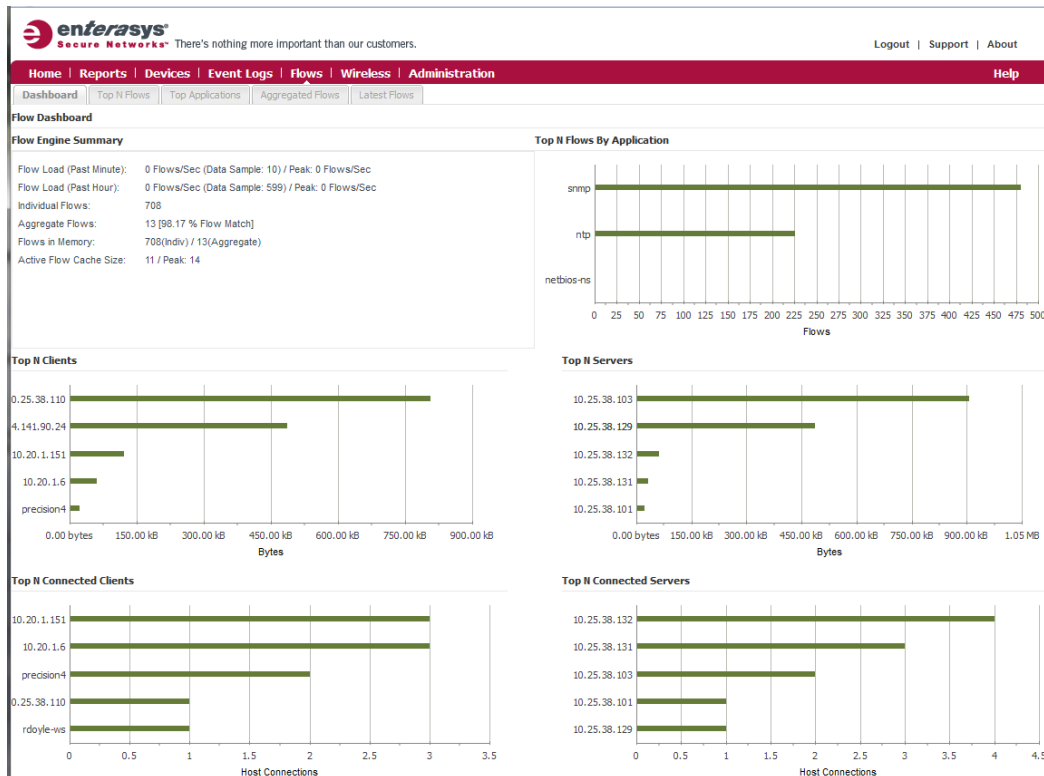
When NetFlow statistics are baselined and trended historically, the information gathered is used to understand traffic patterns, plan for growth, optimize for efficiency, and analyze network behavior to secure the network. NetFlow is also used by some enterprises as a billing, accounting or audit method for IT services chargeback. The result is clear visibility of top talkers, top receivers and top applications in use on the network. NetFlow contains details that can be used for forensic-like data mining, and it provides a wealth of information regarding the traffic traversing enterprise networks, which when reported on correctly can provide details for:

- Characterization of the applications that are utilizing the traffic
 - What applications are running on the network?
 - Who are my top talkers?
 - What percentage of traffic are they?
- Understanding of who is originating and receiving the traffic
 - How many users are on the network at any given time?
 - How long do my users surf the internet?
 - Where do they go? And where did they come from?
- Distinguishing traffic utilization by device
 - Examining the amount of traffic per port
- Efficient and non disruptive network maintenance
 - When will upgrades affect the least number of users?
- Service level monitoring and reporting
 - Are users staying within an Acceptable Usage Policy (AUP)?
 - Is VoIP traffic receiving the required QoS?
- Network wide security monitoring
 - Watch and alert for DoS attacks like smurf and fraggle from anywhere

The following screenshot from the Enterasys SIEM shows the use of NetFlow data to identify the Top Applications by Destination and Source.



Enterasys NMS uses NetFlow data to simplify troubleshooting, problem resolution and network management. The dashboard below from Enterasys NMS OneView shows information on the Top Applications, Top Clients, Top servers, Top Connected Clients and Top Connected Servers.



Enterasys NMS can also use NetFlow information to simplify access control and prioritizations provisioning. Once a flow is identified at either the network or interface level a simple right click on the flow will open a dialogue box to create a rule that will permit, deny or prioritize the flow.

The screenshot shows the Enterasys NMS interface with the 'Flows' tab selected. A table of network flows is displayed, and a 'Create Policy Rule' dialog box is open over it.

Flows	Client Address	Server Address	Server Port	Protocol	Last Seen Time	Duration	Rate	Packets	Bytes	Sensor IP	Input Interface	Output Interface
90	10.20.1.6	10.25.38.101	snmp	UDP	09:39:17	1m 56s	0.226	90	26 K	10.25.38.103	ge.2.1	ge.2.2
45	10.20.1.151	10.25.38.131	snmp	UDP	09:39:12	1m 17s	0.117	45	9 K	10.25.38.103	vlan.0.556	vlan.0.600
54	10.20.1.151	10.25.38.132	snmp	UDP	09:39:12	54s	0.290	54	16 K	10.25.38.103	vlan.0.556	vlan.0.600
125	10.25.38.132	madc2fr	ntp	UDP	09:39:01	2m 34s	0.080	125	12 K	10.25.38.103	vlan.0.600	vlan.0.556
125	madc2fr	10.25.38.132	ntp	UDP	09:39:01	2m 33s	0.080	125	12 K	10.25.38.103	vlan.0.556	vlan.0.600
9	rdoyle-ws	10.25.38.129	snmp	UDP	09:38:37	8m 39s	1	2784	534 K	10.25.38.103	vlan.0.556	vlan.0.600
17	10.25.38.110	10.25.38.103	snmp	UDP	09:38:06	30m 55s	0.438	7491	613 K	10.25.38.103	vlan.0.556	vlan.0.556
46	10.20.1.151	10.25.38.103	snmp	UDP	09:37:46	10m 15s	0.178	544	109 K	10.25.38.103	vlan.0.556	vlan.0.556
79	10.20.1.6	10.25.38.131	snmp	UDP	09:36:40	790ms	20	79	16 K	10.25.38.103	vlan.0.556	vlan.0.600
88	10.20.1.6	10.25.38.132	snmp	UDP	09:36:40	880ms	29	88	26 K	10.25.38.103	vlan.0.556	vlan.0.600
52	precision4	10.25.38.131	snmp	U				10 K	10.25.38.103	vlan.0.556	vlan.0.600	
52	precision4	10.25.38.132	snmp	U				15 K	10.25.38.103	vlan.0.556	vlan.0.600	
1	rdoyle-ws	10.25.38.129	netbios-ns	U				0.2 K	10.25.38.103	vlan.0.556	vlan.0.600	

The 'Create Policy Rule' dialog box contains the following text and controls:

- Check the box below to include the IP address in the created rule and select a policy domain from the drop down list. Enter all or part of the domain name to find a matching domain.
- UDP/TCP Include IP Address
- Domain:
- Buttons: Create, Cancel

To make the NetFlow data easier to understand and more useful Enterasys NMS can filter the NetFlow data by metrics such as flows by count, top clients, top servers, etc.

The screenshot shows the Enterasys NMS interface with the 'Flows' tab selected. A table of network flows is displayed, and a filter menu is open over it.

Flows	Client	Server Port	Protocol	Last Seen Time	Duration	Rate	Packets	Bytes	Sensor IP	Input Interface	Output Interface
116	madc2fr		UDP	09:29:22	2m 24s	0.079	116	11 K	10.25.38.103	vlan.0.556	vlan.0.600
116	10.25.38.132		UDP	09:29:22	2m 24s	0.079	116	11 K	10.25.38.103	vlan.0.600	vlan.0.556
82	10.20.1.151		mp	09:27:40	820ms	29	82	24 K	10.25.38.103	vlan.0.556	vlan.0.600
82	10.20.1.151		mp	09:27:16	1m 52s	0.213	82	24 K	10.25.38.103	ge.2.1	ge.2.2
74	10.20.1.151		mp	09:27:40	740ms	20	74	15 K	10.25.38.103	vlan.0.556	vlan.0.600
50	10.20.1.151		mp	09:29:12	54s	0.269	50	15 K	10.25.38.103	vlan.0.556	vlan.0.600
48	precis		mp	09:26:11	2m 52s	0.054	48	9 K	10.25.38.103	vlan.0.556	vlan.0.600
48	precis		mp	09:26:11	57s	0.243	48	14 K	10.25.38.103	vlan.0.556	vlan.0.600
42	10.20.1.151		mp	09:29:12	1m 17s	0.109	42	8 K	10.25.38.103	vlan.0.556	vlan.0.600
42	10.20.1.151		mp	09:25:46	9m 14s	0.179	495	99 K	10.25.38.103	vlan.0.556	vlan.0.556

The filter menu is open, showing the following options:

- Top Flows By Flow Count
- Top Applications by Flow Count
- Top Applications by Packets
- Top Applications by Bytes
- Top Clients By Flow Count
- Top Clients By Packets
- Top Clients By Bytes
- Top Servers By Flow Count
- Top Servers By Packets
- Top Servers By Bytes
- Most Connected Clients
- Most Connected Servers

NMS OneView provides port level granularity for NetFlow data. Using the PortView interface a network manager can easily isolate the NetFlow data for a single port. This provides a detailed look at the applications being used by a user or endstation.

Source Address	Source Port	Destination Address	Destination Port	Protocol	Last Seen Time	Duration	Rate	Packets	Bytes	Sensor IP	Input Interface
10.20.1.6	55911	10.25.38.101	snmp	UDP	09:54:17	10ms	16	1	0.16 K	10.25.38.103	ge.2.1
10.25.38.101	snmp	10.20.1.6	55911	UDP	09:54:17	10ms	42	1	0.42 K	10.25.38.103	vlan.0.600
10.25.38.101	snmp	10.20.1.6	55911	UDP	09:51:17	10ms	42	1	0.42 K	10.25.38.103	vlan.0.600
10.20.1.6	55911	10.25.38.101	snmp	UDP	09:51:17	10ms	16	1	0.16 K	10.25.38.103	ge.2.1
10.25.38.101	snmp	10.20.1.6	55911	UDP	09:48:17	10ms	42	1	0.42 K	10.25.38.103	vlan.0.600
10.20.1.6	55911	10.25.38.101	snmp	UDP	09:48:17	10ms	16	1	0.16 K	10.25.38.103	ge.2.1
10.25.38.101	snmp	10.20.1.6	55911	UDP	09:45:17	10ms	42	1	0.42 K	10.25.38.103	vlan.0.600
10.20.1.6	55911	10.25.38.101	snmp	UDP	09:45:17	10ms	16	1	0.16 K	10.25.38.103	ge.2.1
10.25.38.101	snmp	10.20.1.6	55911	UDP	09:42:17	10ms	42	1	0.42 K	10.25.38.103	vlan.0.600
10.20.1.6	55911	10.25.38.101	snmp	UDP	09:42:17	10ms	16	1	0.16 K	10.25.38.103	ge.2.1
10.25.38.101	snmp	10.20.1.6	55911	UDP	09:42:17	10ms	42	1	0.42 K	10.25.38.103	vlan.0.600
10.25.38.101	snmp	10.20.1.6	55911	UDP	09:39:17	10ms	42	1	0.42 K	10.25.38.103	vlan.0.600
10.20.1.6	55911	10.25.38.101	snmp	UDP	09:39:17	10ms	16	1	0.16 K	10.25.38.103	ge.2.1
10.20.1.6	55911	10.25.38.101	snmp	UDP	09:38:16	660ms	0.247	1	0.16 K	10.25.38.103	ge.2.1
10.25.38.101	snmp	10.20.1.6	55911	UDP	09:38:16	660ms	0.633	1	0.42 K	10.25.38.103	vlan.0.600
10.20.1.6	55911	10.25.38.101	snmp	UDP	09:33:16	680ms	0.240	1	0.16 K	10.25.38.103	ge.2.1
10.25.38.101	snmp	10.20.1.6	55911	UDP	09:33:16	660ms	0.633	1	0.42 K	10.25.38.103	vlan.0.600
10.20.1.6	55911	10.25.38.101	snmp	UDP	09:30:16	660ms	0.247	1	0.16 K	10.25.38.103	ge.2.1
10.25.38.101	snmp	10.20.1.6	55911	UDP	09:30:16	640ms	0.653	1	0.42 K	10.25.38.103	vlan.0.600
10.25.38.101	snmp	10.20.1.6	55911	UDP	09:27:16	670ms	0.624	1	0.42 K	10.25.38.103	vlan.0.600
10.20.1.6	55911	10.25.38.101	snmp	UDP	09:27:16	670ms	0.243	1	0.16 K	10.25.38.103	ge.2.1
10.20.1.6	55911	10.25.38.101	snmp	UDP	09:24:16	450ms	0.362	1	0.16 K	10.25.38.103	ge.2.1
10.25.38.101	snmp	10.20.1.6	55911	UDP	09:24:16	440ms	0.950	1	0.42 K	10.25.38.103	vlan.0.600
10.20.1.6	55911	10.25.38.101	snmp	UDP	09:21:16	660ms	0.247	1	0.16 K	10.25.38.103	ge.2.1
10.25.38.101	snmp	10.20.1.6	55911	UDP	09:21:16	660ms	0.633	1	0.42 K	10.25.38.103	vlan.0.600
10.20.1.6	55911	10.25.38.101	snmp	UDP	09:18:16	690ms	0.236	1	0.16 K	10.25.38.103	ge.2.1
10.25.38.101	snmp	10.20.1.6	55911	UDP	09:18:16	690ms	0.606	1	0.42 K	10.25.38.103	vlan.0.600

NetFlow in Action

Example 1

Problem: After baselining network performance, a company implements a VoIP solution at its corporate headquarters, confident that their infrastructure can handle the load. However, end users begin to complain about poor and sometimes unavailable VoIP service.

Analysis: The network manager had already enabled NetFlow version 9 across the network infrastructure. The network is heterogeneous at the network edge with switches from multiple vendors; however, Enterasys S-Series products are installed at the distribution and core layers of the infrastructure. Using Plixer's Scrutinizer NetFlow analysis tool, the network manager is able to determine that VoIP traffic is not swamping the available bandwidth and has been assigned a "First Class" quality of service (QoS) level. This ToS (Type of Service) value gives voice the highest priority within the network. Upon further investigation it was determined that the company's CRM application had also been configured with a "First Class" quality of service and it was that application causing degradation to the VoIP performance.

Solution: In this example, the use of NetFlow on S-Series switches discovered the improperly configured application ToS levels that directly impacted VoIP usage. This configuration error was corrected and performance of the VoIP application across the network returned to the required service levels and users no longer encountered poor or unavailable VoIP calls.

Example 2

Problem: A large higher education institution spent many years monitoring their campus networks using appliance-based solutions. They placed traffic monitoring appliances throughout the campus wherever they thought they might have traffic anomalies such as viruses and denial of service attacks, and monitored the network to identify problems. However, the appliance approach didn't scale to their 30,000 port environment due to the large number of devices that would be needed. The network controller didn't want that many appliances to manage and maintain. The challenge was finding a product that would be able to collect large numbers of flows at line rate.

Solution: The customer decided to use port mirroring and remote port mirroring to direct traffic to central locations for flow monitoring. The campus network had many security devices at its boundaries to protect against attack from outside. The biggest challenge came at the beginning of the semester when new students arrived on campus and connected their laptop PCs to the network. The result was a multitude of attacks coming from inside the network, and the customer needed a highly scalable monitoring solution to pinpoint the origin of the internal attacks. The solution was the Enterasys S-Series. The customer selected the S-Series as it differentiated itself from competitive solutions for the following reasons:

- The S-Series was very cost effective in comparison to a solution built with many dozens of appliances
- Operational costs were far lower based on many fewer devices throughout the campus
- The S-Series flow-based ASICs utilized NetFlow to monitor traffic at line rate on every port
- 100% of the incoming traffic could be monitored so every event or attack could be captured
- The S-Series supported a high density of Gigabit and 10 Gigabit Ethernet ports that allowed the monitoring of extremely large volumes of traffic
- The S-Series had very large port buffer memory, which allowed it to perform extremely well when monitoring high volumes of traffic.

Conclusion

Network managers are under increasing pressure to align the IT infrastructure to the goals and requirements of the business. In today's rapidly changing environment with large complex networks, the only way to achieve these goals is to provide comprehensive visibility into the network's operational behavior. Enterasys S-Series NetFlow is the ideal tool to optimize enterprise network performance, management and security. The result is the network is better, faster, cheaper and more reliable by using NetFlow with Enterasys than with any other vendor. For more detailed information on and how to configure NetFlow on Enterasys products, please refer to the [Enterasys NetFlow Configuration Guide](#) and for more information on Enterasys and our products go to www.enterasys.com.

Contact Us

For more information, call Enterasys Networks toll free at 1-877-801-7082, or +1-978-684-1000 and visit us on the Web at enterasys.com



Thought Leadership
Patented Innovation

© 2010 Enterasys Networks, Inc. All rights reserved. Enterasys Networks reserves the right to change specifications without notice. Please contact your representative to confirm current specifications. Please visit <http://www.enterasys.com/company/trademarks.aspx> for trademark information.



Delivering on our promises. On-time. On-budget.