NetFlow and *nGenius*® Performance Manager

A Powerful Combination

Introduction

While an easily accessible, high-performing and always-available network is essential to a company's business, visibility into its end users, business applications, and on-going traffic is crucial for fine tuning its performance. This paper presents evidence supporting the conclusion that NetScout's *nGenius* Performance Management System offers organizations a superior performance management solution based on NetFlow data sources because of its:

- Scalability
- Advanced application recognition
- Newspaper-style reporting
- Integrated troubleshooting features
- Extensibility to integrate other network traffic data sources through NetScout's CDM™ technology.

What Is NetFlow?

NetFlow-enabled switches and routers from industry-leading vendors track IP flows as they enter an enabled interface of an infrastructure device in the network. NetFlow's ability to reduce data by aggregating exchanges between a source and destination as a conversation session in a single NetFlow datagram record is a recognized value.

NetFlow information is transmitted in UDP datagrams that include a header along with one or more flow records. The UDP NetFlow Export Packet is approximately 1500 bytes and could include up to 50 flow records. NetFlow records are sent to a NetFlow collector by configuring the router or switch with a destination address. The packets are sent with greater frequency depending upon how busy the NetFlow-enabled ports become. Current versions of NetFlow implemented in enterprise networks include NetFlow version 1, 5, 7, 8 and 9. NetFlow v9 can transmit data flow and template records in TCP or SCTP as well as UDP.

NetFlow Datagram

A NetFlow datagram is defined by seven unique keys. These elements define one NetFlow record from another.

1. Source IP address
2. Destination IP addresses
3. Source Port Number (TCP or UDP)
4. Destination Port numbers (TCP or UDP)
5. Layer 3 Protocol Type (such as IP, ICMP)
6. Type of Service (ToS) bits
7. Input logical interface (ifIndex)

NetFlow Versions

Version 1:	Original version of NetFlow
Version 5:	The standard and most commonly deployed
Version 7:	Specific to Cisco Catalyst 6500 and 7600 Series Switches, similar to Version 5, but does not include Autonomous System numbers, interface, TCP Flag and TOS information
Version 8:	Added a choice of eleven aggregation schemes that reduce resource usage
Version 9:	Added a flexible, extensible file export format for easier support of additional fields and technologies such as MPLS, Multicast, and BGP Next Hop

Using NetFlow Information in Enterprise Networks

Using NetFlow as a data source for network management solutions has a number of benefits. It can be cost-effective because the infrastructure product that switches and routes the packets also tracks and produces the NetFlow records, meaning that it scales to the enabled ports and devices in that network. Another NetFlow benefit is that it normalizes many packet exchanges between two endpoint IP addresses into one logical flow-based conversation record, reducing the impact on the network when it is being sent to collectors.

Enterprises use the information collected from NetFlow for a variety of business applications. Some of these include:

- *Usage-Based Billing* – NetFlow records include IP addresses, packet and byte counts, timestamps, Type of Service, and application ports that can be used for interdepartmental billing.
- *Autonomous System Traffic Engineering* – NetFlow records include autonomous system numbers that are needed by ISPs to distinguish each other, and are used by traffic engineers to identify trends in order to intelligently load balance traffic over all their network paths. Autonomous system numbers are available in the Exterior Border Gateway Protocols used by routers – so they are available to routers, but not available "on the wire."
- *MPLS and VPN Traffic Analysis* – MPLS affixes labels to IP traffic for prioritization and path selection, in the process obscures important IP flow information details from many performance instrumentation technologies. IP VPNs can also obscure important flow details by encrypting traffic streams and hiding application information. NetFlow can capture and preserve these important details by having either the ingress or egress edge device generate NetFlow records. In this way, crucial management visibility can be maintained.

nGenius Flow Collectors

NetFlow datagrams, gathered from industry-leading routers and/or switches, are sent to either *nGenius* Probes or to *nGenius* Flow Collectors, NetScout's dedicated high-density NetFlow devices. Both *nGenius* Probes and *nGenius* Flow Collectors map the NetFlow data into the CDM framework for display in the common format views of *nGenius* Performance Manager.

Combining NetFlow data with *nGenius* Performance Manager analysis capabilities extends the conversation information and yields top hosts or "top talkers," application recognition and utilization, QoS levels, autonomous system numbers and alarming. The resulting rich traffic information supports challenging network management tasks that include real-time monitoring, in-depth troubleshooting, and historical reporting.

NetFlow data resident in enterprise networks can be a valuable source in performing more than network and application performance management disciplines. The *nGenius* Flow Collector deployed with the standard *nGenius* Flow Director enables users to export the original NetFlow datagrams for use by other consumers of the data, such as billing services, or for industry-standard security and intrusion detection systems.

Customer Story – Insurance Company

A Northeast-based, nationwide insurance company has a number of business units for different categories of insurance policies such as car insurance or life insurance. They also have developed custom applications for policy administration. They use the *nGenius* Flow Collector to collect NetFlow Datagrams from all remote sales offices for Traffic Accounting purposes. While they do not use the information for direct billing, they have found it to be an excellent way to demonstrate how each business unit's activity affects expensive bandwidth resources.

Leveraging CDM Technology to Monitor NetFlow

NetScout's CDM™ architecture provides the underlying structure for collecting and managing NetFlow information and mapping it to the powerful real-time and historical analysis views and reports available in *nGenius*® Performance Manager.

Application Conversations & Talkers
As described in the table "NetFlow Datagrams", each NetFlow record details an IP-based conversation. When an *nGenius* Flow Collector receives a NetFlow datagram it decodes the Flow record and fills in the CDM tables with the basic conversation-layer details, that is, IP source and destination address and well-known TCP or UDP port information for the application in use. The *nGenius* Flow Collector populates the application-layer conversation tables from the NetFlow records. The ability to see who is talking to whom in the network, at what time of the day and which applications are the primary benefits of the conversation information. Many enterprises and government agencies find this conversation-level detail of how valuable network resources are being consumed very useful.

What distinguishes the *nGenius* Flow Collector from other solutions is its ability to gain even greater traffic insight by applying NetScout's CDM technology. Once the *nGenius* Flow Collector populates the conversation tables and subsequent "Talkers" tables from the NetFlow records, it can perform real-time and historical analysis and supply views of Top Talkers or Top Hosts in the network, helping many IT organizations quickly identify abusers of network bandwidth.

Conversation and Talkers information, provided at an application layer for views into the well-known TCP/UDP applications in use at the time, is valuable information for IT organizations. They can, for example, find out that Lotus Notes is the top host in their network, or that a Telnet conversation consumed the most bandwidth yesterday. Having these details available can reduce troubleshooting and capacity planning time and effort.

NetScout's Common Data Model Architecture provides a structure for collecting and displaying up to seven categories of network and application information:

- Statistics – basic network usage information such as traffic utilization, packets, bytes, bits sent and received, and throughput.
- Errors – network errors such as CRC errors
- Packet Trace – packet capture and decode analysis across any network topology
- Alarms – threshold alarms based on configurable events for overall segment utilization or for application utilization in a segment
- Conversations – the source and destination addresses that identify who is talking to whom in networked applications
- Talkers – analysis of top hosts utilized for networked applications
- Response Time – a mechanism that analyzes conversation details for determining, in milliseconds, the responsiveness of particular networked applications

This information is collected from three primary categories of data sources:

- Standard SNMP data sources, such as MIBII and Frame Relay MIB, provide statistics and error information
- NetFlow-enabled data sources, such as infrastructure routers and switches, provide IP conversation information.
- *nGenius* Probe data sources, provide statistics, errors, packet trace, alarms conversations, talkers, and response time.

Statistics and Utilization

The *nGenius* Flow Collector identifies the interface port speeds of the NetFlow-enabled devices, which enables the *nGenius* Performance Management solution to populate the CDM statistics tables. The *nGenius* solution uses these tables to calculate total packets and utilization for the infrastructure ports. Organizations can use this information for two purposes:

- *Real-time troubleshooting* – With views of utilization per port, IT staff can quickly identify under- and over-utilized ports and drill down to discover the applications, users, and conversations contributing to that activity.
- *Historical reporting and trending* – Most and least utilized ports are displayed in automated daily, weekly, and monthly *nGenius* Newspapers to help IT staff make informed traffic engineering and capacity planning decisions.

This capability provides historical reports for most and least utilized segments, enterprise wide, as determined from all data sources. Other solutions may offer most utilized NetFlow segments, or most utilized MIB II segments, however, using information from all the data sources to calculate these reports, *nGenius* Performance Manager provides the broadest and most complete analysis of top utilized segments available.

Identifying Complex Applications from NetFlow
NetFlow supports IP and its well-known TCP and UDP-based applications, for example Lotus Notes, HTTP or Telnet. These applications are identified by their well-known TCP or UDP ports and are recognized by most NetFlow collectors, including the *nGenius* Performance Management Solution. However, there are a number of applications that are more complex in nature, such as SAP or Exchange, which can be transported on multiple ports. Other collection tools are unable to differentiate ports, and when tracking these types of activity, label them as TCP Other or UDP Other.

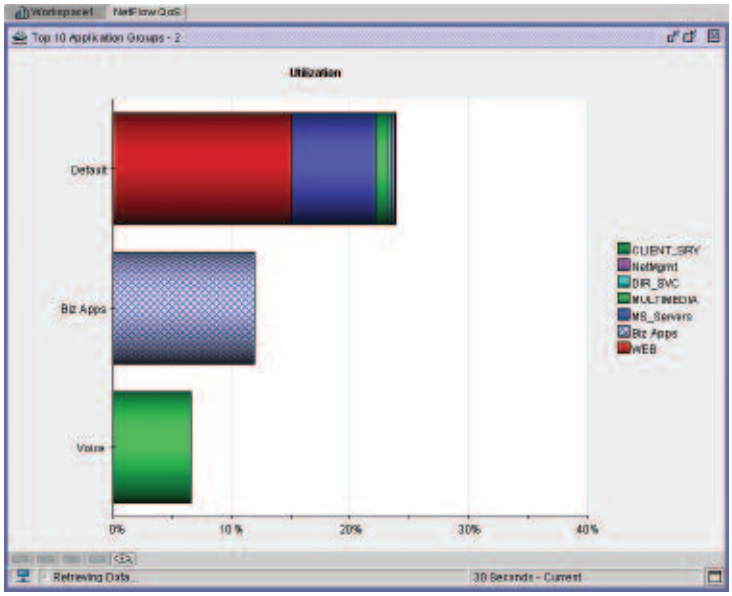
NetScout's CDM Port can recognize these complex applications. For example, the range of ports used by SAP can be configured and assigned to a single CDM Port number for monitoring and tracking purposes. The *nGenius* Solution can then recognize related flow data that would otherwise have been labeled "TCP Other" or "UDP Other," and properly classify it as SAP. Further, the aggregate SAP activity can now be tracked, monitored, and reported against, including all talkers and conversations, providing an important system-wide view of all activity which contributes to making more informed decisions about capacity planning and troubleshooting.

Autonomous System Numbers
NetFlow records are tracked with Autonomous System (AS) numbers. AS numbers are unique identifiers for telecommunications providers globally, assigned to that particular provider or ISP. They are found in Border Gateway Protocols used by routers and are thus available for inclusion in NetFlow records, but are not available "on the wire." The *nGenius* Solution collects this information from each NetFlow record, which is particularly useful to ISPs in distinguishing among themselves for billing purposes or to traffic engineers in establishing trends of network activity for more informed load balancing.

Customer Story – Regional Service Provider

An Asian-based regional service provider was experiencing network challenges in tracking traffic flows and router load in their core. They needed to identify individual customers' business applications as well as anomalous traffic patterns. Simultaneously, they needed to resolve a number of customer challenges – evaluation of the user experience, individual customer link utilization, and utilization by application. They deployed *nGenius* Probes in the regional core of the customer-facing part of the network for identifying all applications and response-time analysis. They used *nGenius* Flow Collector to collect NetFlow datagrams from distributed routers for traffic engineering and basic customer activity monitoring. By monitoring traffic based on the AS number in NetFlow datagrams, they could easily track partner carriers and adjust bandwidth demand.

The real-time screen from *nGenius* Performance Manager shows the network configured to deliver Voice in one class of service, business-critical applications in the second class and all other applications in a default, best effort class. Viewing all the QoS classes in the same screen makes it quick and easy to discover and rectify mis-configurations.



QoS Monitoring

As one of the seven key distinguishing pieces of information, NetFlow records include the Type of Service bits used to prioritize applications within a particular Quality of Service class. For example, when organizations implement a QoS policy and want to prioritize voice traffic over revenue applications, and revenue applications over web surfing, they use ToS. The *nGenius* solution identifies the ToS bits and categorizes traffic with its associated QoS class. This allows granular views of a NetFlow interface to be displayed simultaneously with all the QoS levels discovered in that segment. Further, it can identify and track the applications assigned within each QoS level. This level of detail lets IT quickly uncover configuration errors, whether they are QoS levels that should not exist or applications that may have been assigned to a wrong QoS class.

nGenius Performance Manager Analysis

Long-Term Reporting

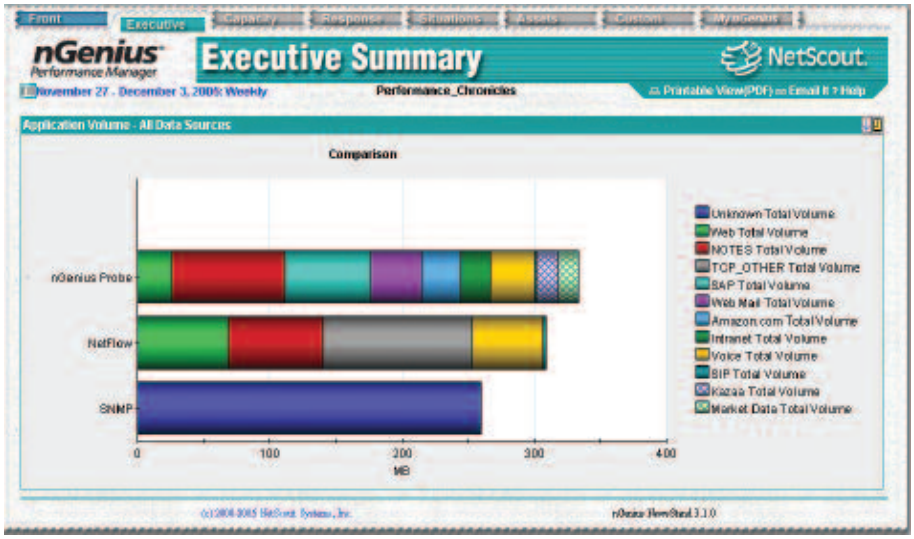
The *nGenius* Performance Manager collects data from the *nGenius* Flow Collectors for historical reporting via the *nGenius* NewsPaper, a custom report that users can disseminate to other users remotely via a web-based repository called a NewsStand. NewsPapers are composed of sections and articles (categories and reports) that contain information relating to network performance. The categories include: Executive Summary, Capacity Planning and Predictive Analysis (Situations To Watch). Automated daily, weekly, and monthly, NewsPapers can be tailored for specific audiences such as separate NewsPapers for a company's North American, European, and Asian IT departments or for IT, Finance, and other business units.

The Executive Summary section provides a high-level view of activity either enterprise wide or by area of the network such as the WAN. From articles published in this section, organizations can quickly identify top applications and busiest ports. This lets companies making substantial investments in particular applications, SAP for instance, see how widely deployed and utilized it is throughout the network.

The Capacity Planning section of the *nGenius* NewsPaper is where NetFlow statistics offer significant value. *nGenius* Performance Manager software provides trended data for applications, hosts, and conversation utilization with an integrated baseline of activity. The data link, network, and application-layer activities are automatically trended in long term NewsPapers as well as in real time views in the *nGenius* Performance Manager console. Specific hosts can be trended for historical analysis as well. The "Situations to Watch" section further helps in this regard by looking at growing trends in the network and making predictions against segments and circuits.

Use of Other CDM Data Sources

An additional element *nGenius* Performance Manager provides is the ability to bring in statistics from other SNMP standard devices. Industry standard routers, switches, and DSU/CSUs that support MIBII, miniRMON, or the Frame Relay MIB contribute significant details to capacity planning. *nGenius* Performance Manager collects packets, bytes, bits and errors, sent and received by network infrastructure products for a broader, more complete view of enterprise-wide network activity. Combined with the statistics gathered from the *nGenius* Flow Collectors and *nGenius* Probes, the capacity planning reports in *nGenius* NewsPapers have a broad, rich analysis of the network's most utilized and least utilized segments and ports by including data from all sources. Overall, IT organizations can better focus their traffic engineering activities with network-wide, trended information from as many data sources as available.



The NewsPapers in *nGenius* Performance Manager display analyzed information from NetFlow, *nGenius* Probes and SNMP data sources side by side. Viewing application and utilization details for all network intelligent data sources improves capacity planning and decision making processes.

Scalability and Flexibility

The *nGenius* Flow Collector combined with the *nGenius* Performance Manager scales to fit different network environments in a number of critical areas. It can accommodate NetFlow-enabled devices and ports from small, concentrated campus deployments to large, distributed global deployments. This is accomplished through the flexibility in *nGenius* Performance Manager whether it is configured as a single centralized server, scalable bundled server, or as a centralized global server with as many distributed local servers as the network requires. Distributing the NetFlow collection with local servers regionally, such as North America, Europe and Asia for global organizations, or Northeast, South and West for US-based companies, reduces the impact of additional traffic on the network of these large distributed enterprises.

The *nGenius* Performance Management solution collects and aggregates statistics from all these distributed NetFlow-enabled ports to provide enterprise-wide analysis. For intelligent capacity planning and infrastructure decisions, both IT organizations and their business counterparts need to see the most utilized and least utilized ports as well as the busiest applications which requires that data from all distributed servers be included in the analysis.

Customer Story – Entertainment Company

A Midwest-based company that manages golf courses was migrating from a Frame Relay WAN to an MPLS network with VPNs to encrypt their traffic. With this change, they were also going from a hub and spoke architecture to a meshed network design so all the locations could communicate directly with each other, avoiding the inefficiency of everything coming into the central site first. The challenge was to do all this and not lose the visibility into the application and conversation detail that previously existed.

They determined it would be too expensive to re-instrument every remote location to match their previous SLA-managed Frame Relay service offering. However, they could use NetFlow and strategically deployed *nGenius* Probes to provide the best visibility at a cost-effective price. *nGenius* Flow Collectors gathered NetFlow data from all the remote locations getting a perspective on communications between locations while *nGenius* LAN Probes with site monitoring enabled at the hub site viewed traffic from the sites coming into headquarters. *nGenius* Performance Manager brought it all together with real-time screens and historical reports with aggregated views and analysis.

Solution Benefits

The *nGenius* Performance Management System offers a significant value to organizations that use NetFlow as part of their network and application performance monitoring solution. Some of the benefits users can derive by deploying *nGenius* Performance Manager in combination with *nGenius* Flow Collectors include:

- Real-time views and analysis of NetFlow data for effective troubleshooting of end-user and application problems enterprise wide.
- Displays of multiple NetFlow-enabled devices and ports simultaneously for quickly pinpointing over- and under-utilized ports.
- Rich, application recognition applied to NetFlow collected records by the CDM Port for complex applications like SAP and Exchange to uncover trends in the performance of these critical business applications and services
- Drilldowns on NetFlow ports to view applications, talkers, and conversations in use for identifying who contributes to high port utilization and for highlighting misuse of network resources
- Conversation details that are made available to other consumers of NetFlow records, for applications such as usage-based billing solutions
- Long-term reports of application activity based on NetFlow records for helping traffic engineers properly size network segments and establish contracts with service providers for WAN services.
- Collection of information from multiple data sources for viewing and displaying in a common format real-time graphs and historical reports of *nGenius* Performance Manager.

Conclusion

IT organizations in corporations and government agencies alike are continuously challenged to efficiently deliver business critical applications enterprise wide. Detailed monitoring and tracking of applications and users is essential in optimizing the performance of the networks they run on. NetScout's *nGenius* Performance Management System, in combination with rich NetFlow data offer the right combination of scalability, advanced application recognition, newspaper-style reporting, integrated troubleshooting, and support of multiple network management data sources. This is the type of expert information that IT departments need in order to provide high-quality business services to their users. Accept nothing less!

For more information on this topic and others like it

CLICK HERE

or visit www.netscout.com

NetScout Systems, Inc.
Corporate Headquarters
310 Littleton Road
Westford, MA 01886 USA
Telephone (978) 614-4000
Fax (978) 614-4004
Web: www.netscout.com

CC-0220-06