nGenius Packet Flow Switch Family for Traffic Aggregation

Technology advances in major data center environments have led organizations to establish strategic monitoring architectures to efficiently move packet flow data from the network layer to the monitoring layer. The addition of a network monitoring fabric helps IT groups achieve greater visibility while extending the investments made in network performance, application performance, security and compliance monitoring devices.

Traffic aggregation is one of several deployment scenarios for the nGenius® packet flow switch family. As a part of many data center and core network monitoring architecture strategies, the nGenius switch offers intelligent filtering and aggregation capabilities to replicate and load-balance network traffic from several network points and simultaneously delivers targeted traffic flows to the required monitoring device(s) for in-depth analysis.

With the nGenius switch in place, IT organizations can improve their pervasive visibility across the service delivery environment, improve end-device performance and reduce the time to deploy additional monitoring devices as other needs arise. Ultimately, this enables the efficient and cost-effective sharing of rich packet-flow data across the full complement of management and security tools, today and tomorrow.

Challenges Addressed by nGenius Packet Flow Switch Family

Optimizing scalability and end-device performance are important considerations when delivering packet-flows from the network to monitoring tools. Variations in network traffic loads, different monitoring needs across environments, plus growth in network traffic volume, infrastructure speeds and complexity, make assuring optimal tool load difficult, when using traditional approaches for access. Under-utilization of tool capacity can lead to significant waste in IT resources and reduced return on investment in the valuable monitoring infrastructure. On the other hand, overloading the tool can cause incomplete or even inaccurate analysis, thus reducing the efficacy and dependability of the tool.

Using the nGenius packet flow switch family, IT organizations can evolve the aggregation and delivery of packet-flows to monitoring tools to deliver improvements in tool efficiency and effectiveness. Deploying the nGenius packet flow switch enables IT organizations to streamline the delivery of traffic aggregation from several points in the network to a single, or several, monitoring, performance management, and security tools. Additionally, the granular filtering and advanced packet conditioning capabilities of the nGenius switch help assure delivery of the right information to the right tool in order to avoid end-device overload.

nGenius Packet Flow Switch Family

The nGenius packet flow switch family mediates access to traffic traversing strategic network links, and provides intelligent targeting and aggregation of IP traffic from multiple network connections. The switches in the nGenius family offer a variety of features to meet the unique demands of different environments and purposes. Whether requirements are high performance, high-density scalability, line-rate packet de-duplication, choices of time-stamping protocols, or intelligent traffic processing, there is an nGenius switch to meet the needs for delivering transparent, selective, and efficient packet-flow access to the attached monitoring devices. Using the nGenius switch family, IT architects can assure high accuracy for deployed monitoring applications including performance management for voice, video, and data, security analysis, and forensics. Additionally, the nGenius switch family enables IT organizations to expand and scale packet-flow access across the entire enterprise while optimizing the load on the various monitoring tools used.

Key features of the nGenius packet flow switch family that aid in traffic aggregation scenarios include massive scalability, high performance, high density, rich interface support spanning 1, 10, 40 and 100 GbE, and, depending on the situation, the flexibility of configuring any port for either ingress from the network or egress to a monitoring tool. Another critical feature for aggregation uses is built-in, sophisticated, filtering and conditioning functions at layers 2/3/4 for creating refined packet-flow forwarding streams that optimize end-device performance.

The nGenius packet flow switch family is built to match the scale of the underlying network today and for years to come. The nGenius switch family delivers industry-leading

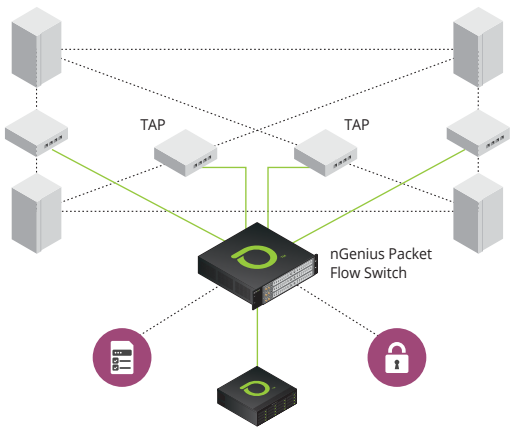

Figure 1: nGenius packet flow switch aggregates valuable packet-flow data from multiple visibility points and delivers the aggregated flows with high flexibility and configurability to the InfiniStream appliance and other monitoring devices.

scalability reaching thousands of 1/10 GbE ports and hundreds of 40 and 100 GbE ports. The nGenius switch family includes:

- **nGenius 3900 series packet flow switch** – modular, high-density, resilient, 1/10/40/100 GbE switch with unified management capability.
- **nGenius 6010 series packet flow switch** – scalability (6Tbps throughput), highest port density, advanced packet conditioning, in a chassis-based 1/10/40/100 GbE switch for reliable, cost-effective support of high speed links and large data center environments.

Traffic Aggregation Use Cases and Deployment Scenarios

Traffic aggregation is one of several deployment scenarios for the nGenius packet flow switch family for many-to-one or many-to-many delivery of filtered or unfiltered traffic flows from strategic points in the network to one or more monitoring devices, such as the InfiniStream® appliance.

Network Traffic Aggregation: The nGenius packet flow switch enables IT organizations to aggregate either all packet-flows from low traffic volume links or select packet-flows from high traffic volume links and deliver to one or more high-performance monitoring tools. IT operations can better manage and control traffic aggregation with sophisticated layer 2/3/4 filtering and packet conditioning to deliver the right information to the right tool in any of the following example scenarios:

- Traffic aggregation from several low speed network links (e.g. 1 GbE) and delivery to a 10 GbE monitoring device - e.g., InfiniStream appliance. In specific scenarios, by using the source port tagging capability of the nGenius switch, administrators can assure the distinction of traffic based on origin when analyzed using a monitoring system, like the nGeniusONE™ Service Assurance platform.
- Targeted monitoring of a specific business critical application across network layers and locations. For instance, the IT operations team can selectively monitor a critical customer resource management (CRM) application residing in a specific VLAN by using the nGenius switch to aggregate traffic from multiple visibility points, filtering for the VLAN assigned to the CRM system, and delivering to a designated monitoring tool, like a compliance tool.
- Extracting only the relevant traffic from high speed core links before delivering to each monitoring tool. An IT administrator can filter traffic based on VLAN or other L2/3/4 information to direct unified communications (UC) traffic to a UC monitoring tool, HTTP traffic to a malware detection tool, etc. In other cases, leverage line-rate packet de-duplications for efficient traffic aggregation.
- Using packet slicing to reduce the burden on a monitoring device and extend its longevity in face of growing traffic volumes.

A strategic monitoring architecture design that includes the nGenius packet flow switch results in more pervasive visibility as well as better end-device performance. Further, time to visibility is reduced by having the nGenius switch in place as access to critical packet flow data is readily available when other monitoring needs arise.

Benefits - Traffic Aggregation with nGenius Packet Flow Switch Family

- Aggregates monitoring across multiple visibility points to enhance the efficacy of performance management, service delivery management, and other monitoring strategies.
- Enhances tool utilization and, by extension, the return on investment in the monitoring infrastructure.
- Facilitates any-to-any connectivity from multiple network connection points enabling network staff to direct the right information to the right device(s) at the right time.
- Improves end device performance, and ultimately extends its useful life, with sophisticated filtering and aggregation of packet-flow traffic.
- Improves operational efficiency and agility by reducing the time to deploy additional monitoring devices and simplifying connectivity provisioning.
- Integration with the nGeniusONE platform greatly simplifies the architecture of a performance management system, reduces vendor complexity, and lowers overall total cost of ownership.
- Improve ROI of overall monitoring strategies.

NETSCOUT

Americas East
310 Littleton Road
Westford, MA 01886-4105
Phone: 978-614-4000
Toll Free: 800-357-7666

Americas West
178 E. Tasman Drive
San Jose, CA 95134
Phone: 408-571-5000

Asia Pacific
17F/B
No. 167 Tun Hwa N. Road
Taipei 105, Taiwan
Phone: +886 2 2717 1999

Europe
One Canada Square
29th floor, Canary Wharf
London E14 5DY, United Kingdom
Phone: +44 207 712 1672

NETSCOUT offers sales, support, and services in over 32 countries.

For more information, please visit www.netscout.com or contact NETSCOUT at 800-309-4804 or +1 978-614-4000