Packet Deduplication in the Packet Flow Switching Layer

The NETSCOUT® packet deduplication capability removes packet duplicates and provides a substantial reduction in the volume of traffic to the tools. This provides an increase in tool efficiency, a reduction in errors on the monitoring tool, and a closure of security holes that exist in other implementations. The deduplication capability includes selective packet deduplication, keyed secure hash for identifying duplicates, configurable duplicate packet tracking time window, discard of all subsequent duplicates of any packet within the specified time window, and the generation of duplicated traffic statistics.

Background

Packet deduplication technology removes duplicated packets from network traffic that are being forwarded to the analytic tools for the purpose of monitoring, analyzing, and recording. When accessing data from networks, duplicate packets are often captured and aggregated together. Without the duplicate packets being identified and removed first, the tools will alarm on the duplicates or produce compromised data and results.

Problems with Packet Duplication

The following are common causes of duplicate packets in monitoring traffic:

- Planned redundancies in network and monitoring design leads to duplicate packets, such as multiple SPAN ports on a network switch, and SPANs and/or TAPs at various points across a network
- TCP packet retransmission despite the original packet not being lost but instead just delayed
- Traffic capture and aggregation

If duplicated packets in the monitoring traffic does not get deduplicated, the following are likely to take place:

- Monitoring and analysis tools may report false positive errors
- Recording of data, e.g. voice and video, may be compromised
- Additional bandwidth is needed for backhauling traffic to monitoring applications
- Duplicate packets can overload monitoring tool, resulting in packet drops

To avoid these unwanted effects, the monitoring tools need to deduplicate packets themselves before performing analysis of the traffic, which results in the following:

- Consumption of bandwidth on the monitoring tool port
- Consumption of valuable processing resources on monitoring tools resulting in a decrease of actual processing bandwidth

Solution: nGenius Packet Flow Switch Deduplication Capability

The NETSCOUT deduplication capability removes packet duplicates and provides a substantial reduction in the volume of traffic to the tools. This provides an increase in tool efficiency, a reduction in errors on the monitoring tool, and a closure of security holes that exist in other implementations.

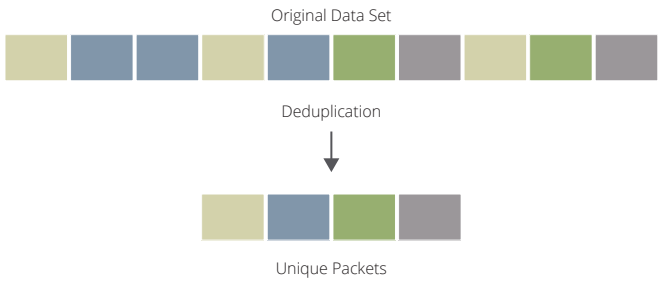

Figure 1: Packet Deduplication.

Architecture

There are two approaches that users can select from for their monitoring fabric infrastructure, being the traditional integrated software and hardware versus the disaggregated hardware and software options.

The advantage of the nGenius Packet Flow Systems (PFS) solutions is that the deduplication itself can be performed by any of the products, regardless of the architecture. It is only if and when a user needs to deduplicate the monitored traffic, for one or more monitoring applications, that the decision of which architecture to adopt may become important, depending on requirements. Figure 2 and Figure 3 show examples of the two architectural approaches using the nGenius PFS family.

Integrated Architecture Deployments

nGenius 3900, 4200, and 6000 series packet flow switches offer fully integrated custom hardware architecture where the packet deduplication for the traffic is conducted in the integrated advanced hardware.

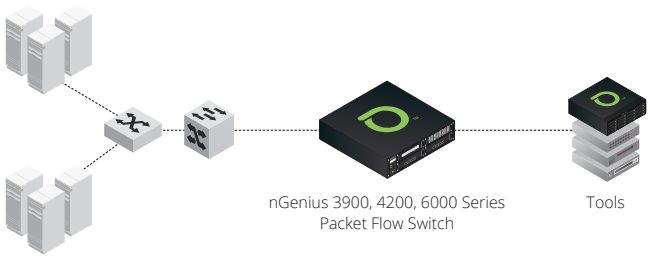

Figure 2: Integrated Hardware & Software with Packet Flow Switch.

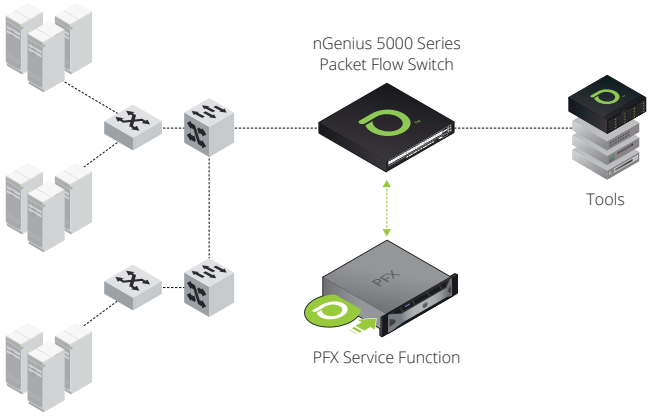

Figure 3: Disaggregated Architecture with PFX for packet deduplication.

Disaggregated Architecture Deployments

The nGenius Packet Flow eXtender (PFX) software is key in the disaggregated approach for performing packet deduplication. In visibility network deployments with nGenius 5000 series packet flow switch, where packet deduplication capability is required, PFX can be added to perform the packet deduplication.

Key Capabilities

- Selective packet deduplication
- Deduplication based on keyed secure hash
- Configurable duplicate packet tracking time window
- Discarding all subsequent duplicates of any packet
- Presentation of metrics associated with duplicate packets
- Enable/disable the deduplication feature, as desired

Solution Benefits

- Substantially reduces the volume of traffic sent to the tools, improving their efficiency
- Eliminates duplication-related errors on the monitoring tool
- Reduces wastage on data recording and storage devices and costs

Product Support

Deduplication is supported on the following products without an additional license:

- nGenius 3900 series packet flow switch
- nGenius Packet Flow eXtender (PFX)
- nGenius 4200 series packet flow switch
- nGenius 6000 series packet flow switch

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us