NETSCOUT nGenius Packet Deduplication

NETSCOUT nGenius® 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, Full 10G line-rate deduplication for each port, 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 tools for the purpose of monitoring, analyzing, and recording.

When accessing data from networks, duplicates of 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 IP Packet Deduplication

Causes

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
- Overlapping during traffic capture and aggregation

Effects

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

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 packet flow switch (PFS) packet deduplication feature provides a configurable, line-rate, real-time, and multiple 10G capability for removing duplicate packets before forwarding them on to the monitoring, analysis, or recording tools.

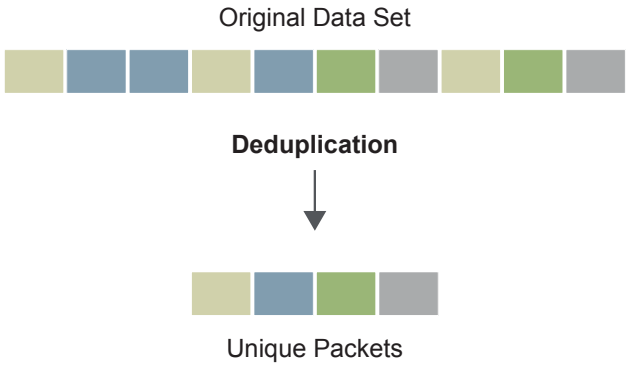

Figure 1: Act of Packet Deduplication.

Key Capabilities

The Packet Deduplication feature has the following key capabilities:

- Full line-rate deduplication at up to 2500G per PFS
- Selective packet deduplication
- Deduplication based on keyed secure hash
- Configurable duplicate packet tracking time window
- No added delay to initial unique packet
- Discarding all subsequent duplicates of any packet
- Selective operation as a Span (ingress), Monitor (egress), or Service (intermediate) function, per port
- Presentation of metrics associated with duplicate packets
- Enable/disable the feature, as desired

Deduplication Benefits: Enhanced Performance

The following summarizes the benefits of de-duplicating packets in the PFS layer:

- Substantially reduces the volume of traffic sent to the tools
- Increases tool efficiency and reduces errors on the monitoring tool
- Closes security holes that exist in other implementations

User Interface

The graphical user interface (GUI) controls each port and the application window for counters. The command line interface (CLI) and application programming interface (API) provide the same support.

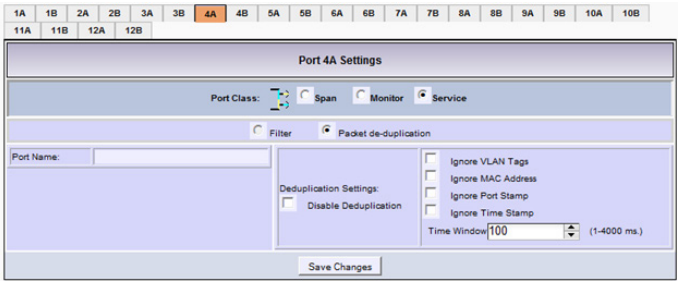

Figure 2: Deduplicate Port Settings.

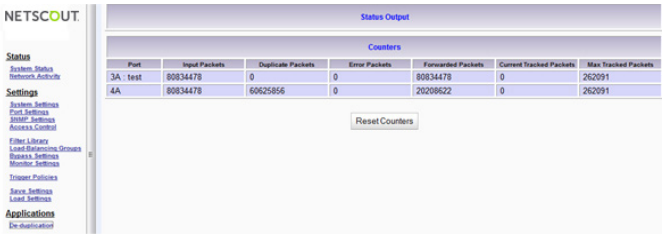

Figure 3: Deduplicate Application Window.

All the capabilities of the User Interface are also available through the CLI commands.

Product Support

Deduplication is currently supported on the PFS 4204/VB420 and PFS 6010/VB6000 platforms.

Refer to the "Advanced Packet-processing Engine" technical brief for more details on the platforms.

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

© 2016 NETSCOUT SYSTEMS, INC. All rights reserved. NETSCOUT, nGenius, InfiniStream, Sniffer, nGeniusONE, ASI, Adaptive Service Intelligence and the NETSCOUT logo are registered or pending trademarks of NETSCOUT SYSTEMS, INC. and/or its affiliates in the United States and/or other countries ("NETSCOUT"). All other brands and product names and registered and unregistered trademarks are the sole property of their respective owners. Use of this product is subject to the NETSCOUT SYSTEMS, INC. ("NETSCOUT") End User License Agreement that accompanies the product at the time of shipment or, if applicable, the legal agreement executed by and between NETSCOUT and the authorized end user of this product ("Agreement"). NETSCOUT reserves the right, at its sole discretion, to make changes at any time in its technical information, specifications, service, and support programs.