Solution Brief

GigaSMART De-Duplication

Key Benefits

- ✓ Eliminate redundant information currently feeding your network and security tools
- ✓ Gain improved value and performance from existing tools by deferring future upgrades
- ✓ Free tool storage and processing resources used to handle redundant packets in the traffic stream
- ✓ Improve tool performance, capacity, efficiency and reliability
- ✓ Increase the time tools spend on packet analysis while reducing time spent de-duping packets
- ✓ Gain more accurate performance analysis
- ✓ Reduce false positive results for error reporting metrics, including packet retransmissions
- ✓ Reduce load due to elimination of duplicate packet storage
- ✓ Boost speed and accuracy of forensics analysis and malware detection

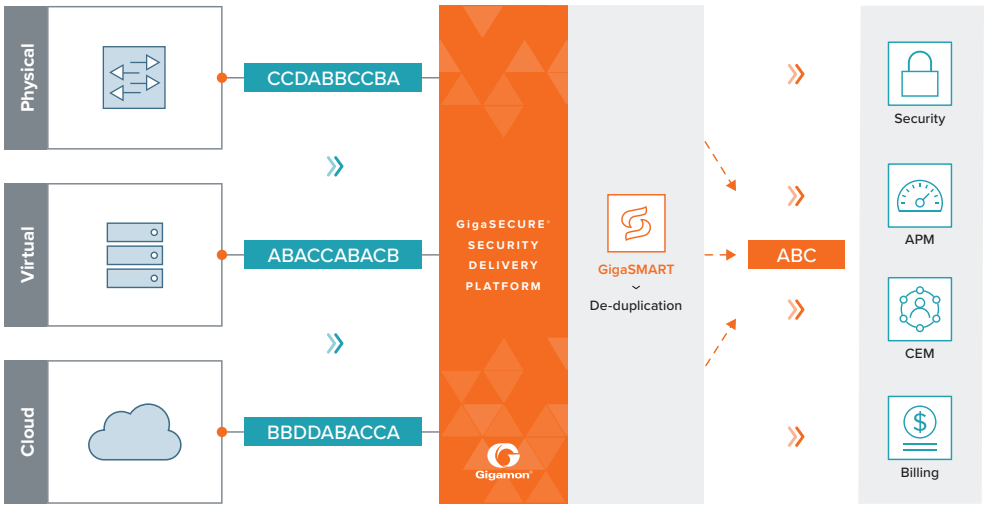
Challenges with Tap and Aggregation

Gigamon customers use tap and aggregation solutions to gain 100% visibility into network traffic and to achieve effective application, network and security monitoring, and analysis. This results in the elimination of blind spots and improved understanding of application performance, network utilization, and security threats. However by their nature, tap and aggregation solutions collect packets from multiple points along a network path, resulting in duplicate copies being sent to your tools for analysis. Duplicates can also be caused by inter-VLAN communication, incorrect switch configuration or unavoidable SPAN/mirror port configurations.

Since today's networks are already transporting traffic volumes at much higher rates than most tools can handle, analysis tools cannot easily handle the processing drain of up to 40% of duplicate packets on incoming feeds. This drain on network processing is a real challenge needing an effective solution.

The impact of duplicate packets can create many challenges including:

- Distorted results when evaluating application or network performance, leading to improper performance diagnosis and artificially elevated packet and byte counts
- Duplicate packets can be misinterpreted by analysis tools, resulting in false positives for problems that don't exist
- Reduced retention periods of data on forensic recorders due to the storage allocated to de-duplicate traffic
- Inaccurate flow data in NetFlow/IPFIX reports



Tool optimization for physical, virtual, and cloud visibility with GigaSMART De-duplication

Gigamon Solution—Duplicate Packet Removal with GigaSMART

The GigaSMART De-duplication application identifies and eliminates duplicate packets and sends an optimized feed to the tools. It offloads the deduplication task from the tools, allowing you to centralize the deduplication function and feed multiple tools with the same feed. GigaSMART De-duplication significantly improves the performance of connected tools, allowing them to analyze increased volumes of aggregated traffic on the network without increasing tool capital expenditure.

GigaSMART De-duplication is robust, accurate and customizable. It allows you to tune duplicate detection to improve accuracy and effectiveness. For example, you can specify whether two packets that are identical except for IP TOS or TCP Sequence number are considered duplicates. In addition, the detection window is configurable between 10-50,000 µs.

Expected packet changes due to forwarding, including source and destination MAC addresses, are taken into consideration. The application also supports service chaining so that you can send the de-duplicated traffic stream to the GigaSMART NetFlow application for optimized NetFlow generation and export.

3272-01 08/18

Gigamon®

3300 Olcott Street, Santa Clara, CA 95054 USA | +1 (408) 831-4000 | www.gigamon.com