



Masking

- Eliminate processing and storage bottlenecks
- Enhance security of network tools
- Help pinpoint critical network performance issues
- Easily filter based on network source information

Masking

- Conceal private traffic including financial and medical information
- Empower network monitoring tools to perform their task and maintain PCI and HIPAA compliance
- Enable more traffic storage in an analysis application

Network Port Labeling

- Add labels to the packets indicating the ingress port
- Easily identify where a packet is coming from
- Enhance the efficiency of your network monitoring tools by eliminating the potential of duplicate traffic streams

Time Stamping

- Add Packet time stamps at line rate for subsequent analysis
- Enables troubleshooting of application response times jitter and latency

Packet Slicing

- Reduce packet size to increase processing and monitoring throughput
- Optimize the deployment of forensic recorder tools

Stripping

- Eliminate the need for monitoring tools to decipher protocols associated with MPLS labels, and VLAN tags
- Allow easy filtering, aggregation, and load-balancing of packets with headers removed

IP Tunneling

- Encapsulate and forward packets to monitoring tools between networks on separately routed paths
- Enable routing of data from lights-out data centers to central monitoring facilities

De-duplication

- Relieve tool processing resources in asymmetrical networks by only forwarding a packet once
- Remove packet duplication caused by inter-VLAN communication or incorrect switch configuration

Product Description

The GigaSMART blade enables an entirely new way to enhance monitoring tools, allowing tools to perform analysis more efficiently and accurately.

A networking industry first, the GigaSMART blade significantly enhances the capabilities of the Gigamon GigaVUE-2404 device, creating the ability to modify packets at line-rate, and add valuable information through the GigaSMART network appliances including packet slicing, masking, network port labeling, and time stamping.

Network monitoring tools can now perform more efficiently by eliminating unwanted content with the packet slicing module.

Masking allows network security teams to hide confidential information like passwords, financial accounts, or medical data allowing companies to meet SOX, HIPAA and PCI compliance regulations. Organizations can also add source or timing information at the point of collection with the network port labeling capabilities.