IXIA NET TOOL OPTIMIZER® ADVANCED FEATURE MODULE (AFM)

DATA SHEET

RELIABLE AND INTELLIGENT PACKET PROCESSING

For better network security and higher profits, enterprises today need complete and efficient access to the data that traverses their networks. Yet privacy compliance mandates strict control of corporate data and customer personally identifiable information (PII).

The Ixia Net Tool Optimizer (NTO) Advanced Feature Module (AFM) processes packets at line rate and prepares data for analysis by security and monitoring tools. It delivers advanced functions like real-time packet de-duplication, timestamping, and masking of personally identifiable information (PII). With AFM, enterprises can look deeper into their networks while maintaining compliance to privacy regulations and delivering higher security for their corporate and customer data.

ZERO-LOSS: BECAUSE EVERY PACKET COUNTS

Ixia's primary competitive differentiator with AFM is its predictable, accurate, and lossless performance. The AFM architecture ensures that no data is lost under any conditions by dedicating high performance hardware to the advanced packet processing. Ixia's solution always delivers the full 160Gbps of traffic no matter the configuration or network conditions.

Other vendors' products often use software-based approaches to try to deliver similar functionality, but their solutions max out at 40Gbps or less. Even then, third-party testing from Tolly[i] demonstrated that those products are unable to meet their advertised performance rating or guarantee steady results as network conditions change.

HIGHLIGHTS

- Protects monitoring tools and helps them operate more effectively with all redundant packets removed, at full line rate with no loss
- Gives monitoring tools every packet they need, even when aggregate bandwidth exceeds port capacity
- Boosts tool performance and keeps sensitive user data secure by removing payload data from the monitored network traffic
- Removes PII, such as credit card or social security numbers, before providing the data to analysis tools
- Enables tools to analyze encapsulated traffic by removing VLAN or QinQ, GTP, MPLS, VNTag, VxLAN, FabricPath, ERSPAN, and L2GRE/NVGRE headers from the packet stream
- Terminates L2GRE tunnels from vTap and delivers plain Ethernet traffic to tools
- Enables tools that cannot process GTP header information to analyze the tunneled packets
- Allows latency-sensitive monitoring tools to know, with nanosecond resolution and accuracy, when a packet traverses a particular point in the network

KEY FEATURES

- **Packet De-Duplication –** Packet duplicates occur in visibility networks when a packet traverses multiple taps or SPAN ports that generate multiple copies of the same packet. De-duplicating packets reduces the amount of redundant data sent to analysis tools, directly improving tool efficiencies and preserving tool integrity. Flexible configuration parameters allow ignoring specific headers and controlling whether the deduplication window is packet- or time-based (Up to 1/2 second for 10/40G and 1 second for 1G).
- **Extended Burst Protection –** Deep buffering allows monitoring tools to see every packet, even under microburst conditions where aggregate bandwidth temporarily exceeds port capacity. This condition commonly occurs when traffic from a high-speed network is adapted to feed a lower-speed tool. Ixia's extended burst protection allows data flow from higher-speed, bursty traffic to 1G tools.
- **Packet Trimming –** Many monitoring tools, especially legacy ones, only need to analyze packet headers. In other monitoring applications, regulatory compliance requires tools remove sensitive data from captured network traffic. The AFM can remove payload data from the monitored network traffic, which boosts tool performance and keeps sensitive user data secure.
- **Protocol Stripping –**Monitoring tools, legacy or even modern ones, cannot analyze traffic encapsulated inside of an unsupported protocol. The AFM enables tools to monitor all required data by removing VLAN or QinQ, GTP, MPLS, VxLAN, VNTag, FabricPath, ERSPAN, and L2GRE/NVGRE headers from the packet stream.
- **L2GRE Tunnel Termination –** Many virtual taps, including Ixia's Phantom vTap, will originate VM traffic in L2GRE encapsulation. AFM can terminate the L2GRE tunnel so plain Ethernet traffic can be directed to tools for processing; hence removing the burden of tunnel termination from the attached tools.
- **Data Masking –** Network operators commonly need to remove PII, such as credit card or social security numbers, before providing the data to analysis tools. The AFM removes the data from the packet in real-time and replaces it with a fixed-field value before forwarding to security and monitoring tools.
- **Timestamping –** Network operators require high-accuracy timestamps on packets to correlate events with other device logs in low-latency financial data centers and to correlate traffic events across a WAN. AFM can insert a high-accuracy timestamp into every packet at ingress. Timestamp sources include local, NTP, and PTP (7300).
- **Double Your Ports –** Network operators need more density to address the space and power constraints of modern data centers. Ixia's innovative Double Your Ports (Simplex) feature enables the ports on an AFM module to be logically divided into two interfaces: one that connects to the network tap, and the other that connects to the security or monitoring tool. This configuration allows users to potentially double the number of active ports in use without adding any new hardware.

[i] http://tolly.com/Docdetail.aspx?Docnumber=216100