Feature Brief

Adaptive Packeting Filtering

Challenges with Traffic Complexity in Enterprise and Service Providers

Traditionally, network management and monitoring was based on classification by Layer 3 IP address (to determine users) and by Layer 4 port (to determine applications). This was a fairly reliable method when users typically had static IP addresses and the applications used well-defined ports. However in today's environment, static IP address assignment is not typical, thanks to DHCP addressing, and certain applications use non-standard ports, including port-hopping, making it nearly impossible to monitor solely on IP address and Layer 4 port information. In addition, as organizations continue to adopt collaborative applications hosted off-premise, a large amount of traffic is encapsulated or tunneled. The overall impact of encapsulated traffic on the tool's bandwidth and compute cycle is significant and has steadily increased, especially within data centers and across geographical networks. Protocol awareness and the ability to look beyond Layer 4 packet information (content awareness) is a core requirement to accurately classify the monitored traffic and distribute it across the monitoring and analytic tools.

Gigamon Solution—Adaptive Packet Filtering

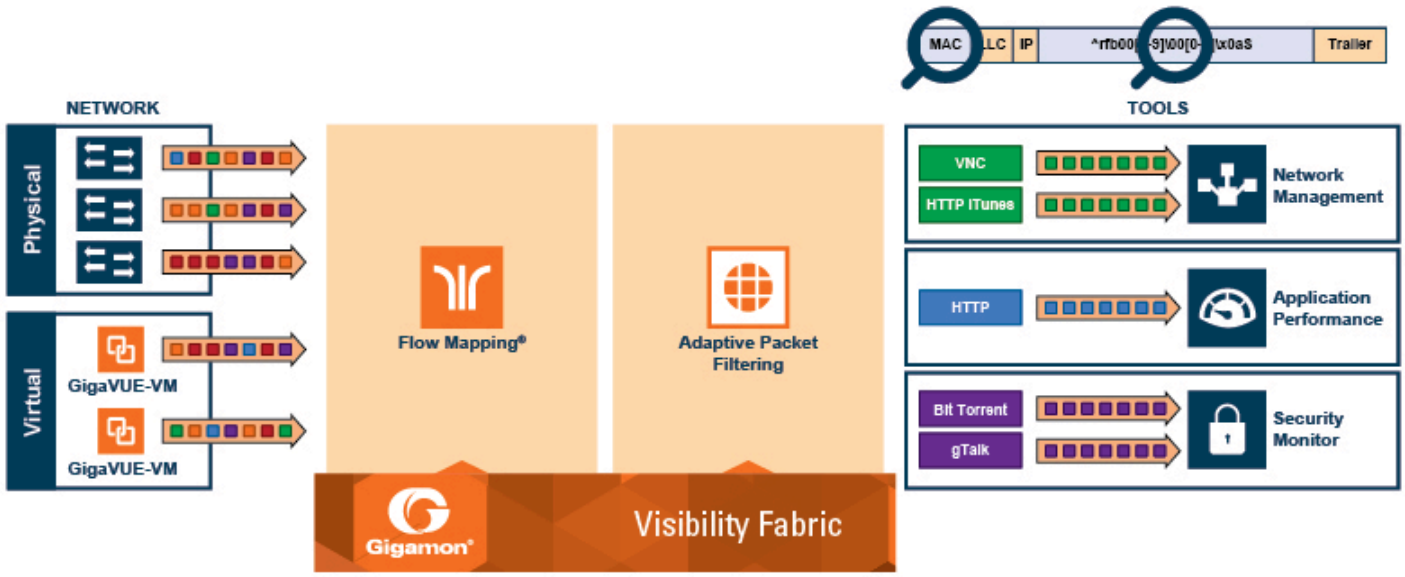
Content-based Filtering

With the traffic complexity introduced by today's network applications, Adaptive Packet Filtering—an optional extension of GigaSMART® technology—provides a powerful filtering engine that identifies content based on signature or patterns across any part of the packet, including the packet payload. These patterns can be as simple as a static string at a user configured offset, or an extremely complex Perl Compatible Regular Expression (PCRE) at a variable offset.

Feature Details – Content-based Filtering or Masking

- Filtering Based on Packet Contents beyond Layer 2/Layer 3/ Layer 4 Headers Including: URLs, patterns in BitTorrent packets, etc., as well as enable basic application identification such as applications running on non-standard ports (HTTP, FTP, SSH)
- Flexible Engine: Option to custom define signatures and reuse across multiple forwarding rules
- Masking Actions based on matching a search patterns and obfuscating the pattern
- Flexible Actions: Filter and drop, or filter and forward to specific tools
  - Session awareness - filter/forward/drop the whole session

Figure 1: Content-based filtering



With the flexibility offered by adaptive packet filtering, IT operators can:

- Identify and mask credit card numbers and social security numbers across user-level transactions
- Identify and mask phone numbers exchanged across SIP packets
- As part of HTTP transactions: filter on URLs or patterns in the user-agents, PCRE-anchors to identify packets
- As part of HTTPS transactions: identify HTTPS on non-standard TCP ports and forward to a tool port
- Filter on DNS queries for specific URLs
- Filter on source and destination addresses in FCoE packets
- Filter custom applications (e.g., identify and filter control traffic vs. data traffic)

Encapsulation Awareness

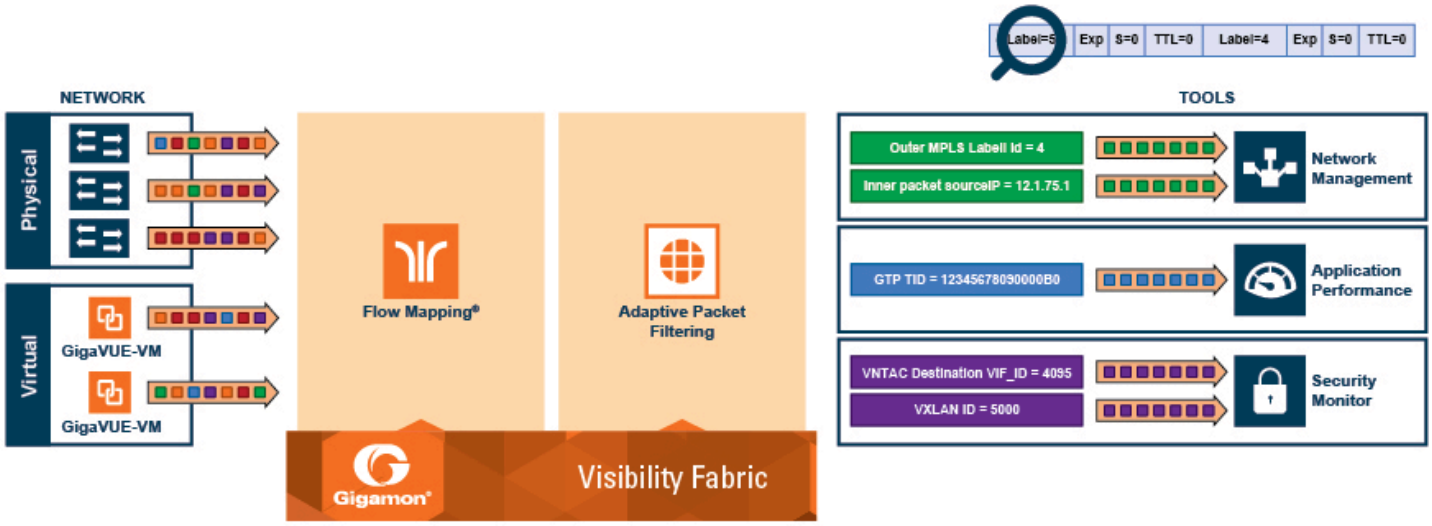
In order to complement the mobility brought about by the virtualized server infrastructure, network virtualization overlays like VXLAN, VN-Tag, and NVGRE are being designed and implemented in data centers and enterprise environments. Across service provider environments, huge volumes of traffic are being tunneled over GTP. The Gigamon Visibility Fabric™ offers the option to strip out or remove these headers, thus providing visibility to monitoring tools that do not understand these overlays and encapsulation protocol. And now with adaptive packet filtering, this capability is further enhanced where operators have the option of making forwarding decisions based on the encapsulation and inner packet contents.

Adaptive packet filtering enables the capability to filter on specific encapsulation protocol parameters including GTP tunnel ID, VXLAN ID, and VN-Tag src/dst vif ID to name just a few. In addition, operators also have the capability of looking beyond the encapsulation protocols into the original (encapsulated) packet, to filter on source/destination IP or Layer 4 port numbers. With fragmentation awareness, Gigamon's Adaptive Packet Filtering function can ensure that all IP fragments associated with the filtered packet is always forwarded to the same tool to enable a complete view of the traffic stream for accurate analytics.

Feature Details – Encapsulation Awareness

- Intelligent Filtering across Advanced Encapsulation Headers including: VXLAN ID, ERSPAN ID, GRE Key, VN-Tag src/dst vif ID, list ID, VLAN ID in QinQ, MPLS labels and GTP tunnel ID
- Inner Packet Filtering of Encapsulated Flows
  - Layer 2 Headers including Ethertype, src/dst MAC addresses, and VLAN IDs (across QinQ)
  - Layer 3 Headers including src/dst IPv4/IPv6 addresses, IP Version, IP Fragmentation, TOS, DSCP, TTL, and IPv6 Flow Labels
  - Layer 4 Headers including src/dst Ports and TCP Flags
- Match across One or a Combination of Filtering Parameters
  - Supported across five layers of encapsulation
  - Support for GigaSMART operations in combination with adaptive packet filtering

Figure 2: Encapsulation awareness



With encapsulation awareness enabled by Adaptive Packet Filtering, operators have multiple options to act on the packet including:

- Filter on encapsulation header parameters, Layer 2 – 4 parameters in the outer or inner headers (up to 5 layers of encapsulation) and in any combination. For example:
  - Forward traffic specific to a subset of VXLAN IDs
  - Distribute traffic based on MPLS label values
- In combination with header stripping and/or tunnel decapsulation:
  - Decapsulate a header or terminate a tunnel and then make forwarding decisions based on the original packet
  - Implement "conditional" header stripping, based on encapsulation header parameters or inner/outer packet contents
- Forward a subset of traffic "as-is" to monitoring tools that need these encapsulations for analysis
- Alternatively strip out the outer headers/encapsulations and distribute traffic to monitoring tools that do not require these outer headers for analysis
- Since adaptive packet filtering is implemented as a second level map, operators can also implement overlapping rules where
  - A copy of the traffic can be distributed across a group of monitoring tools
  - A refined subset from the same incoming stream is distributed across a different set of tools

Key Benefits

- Enhance Visibility into Tunneled Application Flows
  - Apply security across overlay networks
  - Granular control over traffic flows to monitoring tool infrastructure
- Comply with Privacy and Regulatory Requirements
  - Obscure sensitive user data before it is stored by capture tools
- Optimize Monitoring Tool Rails
  - Enable selective reduction in traffic to monitoring tools
  - Enhanced tool performance with reduced traffic loads
- Offload Basic Application Identification to the Visibility Fabric
  - Identify applications based on one or more combinations of packet contents, ports and/or URLs
  - Visibility into flows tunneled over HTTP/S

About Gigamon

Gigamon solutions have been deployed globally across enterprise, data centers and service providers, including over half of the Fortune 100 and many government and federal agencies.
For more information about the Gigamon Unified Visibility Fabric™ visit: **www.gigamon.com**

3098-03 04/15

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