Application Note: MPLS Stripping

Eliminating Blind Spots and Enhancing Monitoring in presence of MPLS using Phantom HD

Multiprotocol Label Switching (MPLS) is a highly scalable, protocol agnostic, data-carrying mechanism that has received broad market attraction in service provider networks. Now, enterprises are increasingly connecting the distributed and extended enterprise via MPLS-based Wide Area Networks (WANs) or deploying their own private MPLS networks. MPLS brings the benefits of circuits to packet-based IP communications, providing consolidation, control, and network resiliency. MPLS simplifies the network, reduces cost, and enables network convergence with greater control and resiliency for the enterprise.

MPLS operates at a layer that is generally considered to lie between traditional definitions of layer 2 (data link layer) and layer 3 (network layer), and thus is often referred to as a "layer 2.5" protocol. But the benefits of MPLS comes with a price tag of reduced visibility of monitoring and security tools that were not designed to handle "layer 2.5" protocols.

Many network monitoring, analysis, and security tools are either unable to handle or have limitations when handling MPLS traffic. Those tools were designed without thinking about the increasing adoption of MPLS in large organizations' networks. Thus, the presence of MPLS protocols in the packet streams can restrict and even limit the ability of monitoring and security tools to perform requested (and required) filtering and load balancing tasks.

Phantom HD Eliminates MPLS-Generated Blind Spots

By using a dedicated hardware solution that was purpose-built to bridge converged networks, Net Optics addresses the need to eliminate the blind spots created by MPLS.

Net Optics Phantom HD is a key component for building a comprehensive, consolidated monitoring infrastructure for both network management and security. It simplifies and extends the range of data monitoring visibility across converged physical and virtual networks. Phantom HD can be deployed in data networks, as well as in digital voice and video networks. The appliance supports and streamlines elimination of monitoring port contention and minimizes the number of tools needed to optimally monitor and manage the network.

Phantom HD is the bridge between the evolving network routing technologies and traditional tools. Providing high-throughput tunneling support, the appliance encapsulates and de-capsulates transport tunneling protocols (GRE, R-SPAN). In addition, Phantom HD can strip other protocol headers including MPLS, VN-Tag, VXLAN and Fabric Path. It also handles fragmentation and defragmentation of packets that might become fragmented during the tunnel encapsulation process.

Phantom HD is optimized to aggregate and de-capsulate traffic from different sources, including Phantom Virtualization Taps, Switch SPAN ports and other regular taps.

When terminating GRE tunnels, Phantom HD aggregates the resulting raw traffic and sends it at the rate of 10 Gbps to the tools of choice in a user's physical instrumentation layer for inspection and analysis.

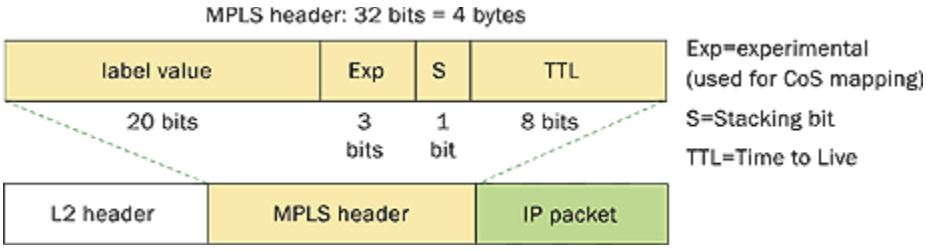
When originating GRE tunnels, Phantom HD can encapsulate raw traffic from both virtual and physical devices and send it at a 10 Gbps rate to remote destinations for processing.

MPLS Labels

In an MPLS network, data packets are assigned labels. Packet-forwarding decisions are made solely on the contents of this label, without the need to examine the packet itself. MPLS operates at a layer that is generally considered to lie between traditional definitions of layer 2 (data link layer) and layer 3 (network layer), and thus is often referred to as a "layer 2.5" protocol. This protocol was designed to provide a unified data-carrying service for both circuit-based clients and packet-switching clients and to supply a datagram service model. MPLS can be used to carry many different kinds of traffic, including IP packets and native ATM, SONET, and Ethernet frames.

MPLS works by prefixing packets with an MPLS header containing one or more labels. This is called a label stack. Each label stack entry contains four fields:

- 20-bit label value
- 3-bit Traffic Class field for QoS (Quality of Service) priority (experimental) and ECN (Explicit Congestion Notification)
- 1-bit bottom-of-stack flag. (If set, this signifies that the current label is the last in the stack.)
- 8-bit TTL (time to live) field



Label Stacking

By packaging multiple labels into a stack, MPLS routers and switches can use more than one label on top of the packet to route that packet across the network. In fact, some MPLS applications actually need more than a single label in the label stack to forward the packets. One example includes MPLS VPN, which puts two labels in the stack.

Monitoring Limitations of MPLS Networks

Identifying Application and Network Traffic over MPLS is an issue, since the MPLS header is between the Ethernet and IP headers. This means that existing network infrastructure tools, which only pre-filter based upon fixed-offsets, can't be used because the headers and data after the Ethernet header are no longer at their standard offset. For example, the IP Header starts at byte-offset 18 when MPLS is present as opposed to byte-offset 14 without MPLS.

The Solution: MPLS Stripping

Net Optics Phantom HD provides the ability to strip MPLS labels from packets, enabling non-MPLS-capable network monitoring tools to monitor packets. The device's logic was build in such a way that a simple MPLS strip command can be used to strip MPLS labels from packets. By using other Phantom HD features such as VLAN tagging, it is possible to add specific VLAN tags to packets. In this way, monitoring tools can handle differently those packets that formerly contained MPLS tags.