



**October 15, 2009**

## **Gigamon Data Access Networking**

By Ray Horvak

Gigamon is a provider of data access networking products. TR hasn't covered this area much, so a brief tutorial may be in order for those unfamiliar with it.

Contemporary IP-based WANs are quite complex at the enterprise level. They typically comprise many network elements (NEs) such as voice, video and data terminals, multiplexers, switches, routers and gateways. Many of these are addressable and manageable devices that can sense and store data describing their state and level of performance, upload that data along with alerts and alarms to a network management system (NMS) or passively respond to data requests from it, and respond to commands.

The elements generally are managed via a vendor-specific proprietary protocol that includes coding technique, data format, command structure and security mechanisms. Across an IP network, the NEs and NMSs establish and maintain dialogues via the Simple Network Management Protocol (SNMP), which functions at the application layer of the TCP/IP suite. Network engineers and administrators also employ sniffers, aka protocol analyzers, in the form of either hardware or software, to monitor, intercept and log traffic for analysis and diagnostic purposes. In addition to network and application performance monitors in the forms of sniffers or RMON (remote monitoring) probes, there may be forensic recorders that capture traffic associated with a particular IP address range or telephone number, and intrusion detection systems and security monitors looking for indications of breaches or attempts.

Many tools can be deployed to monitor and manage network elements and segments involving large volumes of traffic. These devices are commonly connected to the network via permanent test access ports (TAPs) that create monitoring ports between any two devices for the purpose of collecting in-line data. As TAPs are created through either splitting or replication, they see all data passing over a given segment as though they were in-line. Cisco equipment commonly includes a switched port analyzer (SPAN) that performs roughly the same function but drops corrupted and runt frames. Other

manufacturers use a variety of names such as port mirroring and monitoring. In large and complex networks, the plethora of tools and resulting contention for TAPs and SPAN ports can quickly get out of control.

Gigamon (a contraction of Gigabit and monitor) manufactures data access switches that tap into the core of high-speed Ethernet switches. GigaVue 420 provides 4 ports of 10GE and 20 of 1GE. GigaVue 2404 provides 24 ports of 10GE and 4 of 1GE.

Kevin Jablonski, Senior Director of Business Development, explained the products, applications and benefits. “In a simple many-to-one scenario, data arriving from multiple sources over multiple network ports can be aggregated and delivered to a single tool port. Thereby GigaVue replaces multiple distributed copies of a given tool with a single one in a centralized tool farm. In an any-to-many scenario, traffic arriving at a single network port can be replicated and delivered to multiple destination tool ports. In a more complex many-to-many scenario, data arriving from multiple sources at multiple network ports can be filtered, aggregated and forwarded to different tools connected to tool ports.” Filters can be applied at both network and tool ports. Pre-filters applied to network ports filter bulk inbound data by MAC address, IP address range, VLAN, TCP port number, etc. and pass the outbound traffic to post-filters that fine-tune the object data and deliver it to the specific tool. This allows a variety of tools to analyze and identify data flows at more manageable data rates. In essence, the Gigamon solution can help a smaller number of tools work more efficiently.

According to Jablonski, “Once installed it is a relatively simple matter to access GigaVue via the Citrus web-based GUI or CLI and zero in on information on any network segment at any time with no need for maintenance windows nor associated configuration management issues. The value proposition is that of increased performance and enhanced tool management at reduced cost.”

GigaVue is incorporated into passive monitoring solutions for network security, troubleshooting, application analysis, forensics recording and SOX compliance through partners including ClearSight, Coradient, FireEye, Net scout, Network Instruments, Solera Networks and WildPackets. A channel-focused organization, Gigamon relies on its partners’ distribution channels and maintains direct relationships with select VARs.