

DATA ACCESS NETWORKING FOR ENHANCED SECURITY, MONITORING & MAINTENANCE

(Article previously published in www.convergedigest.com, November 20, 2006)

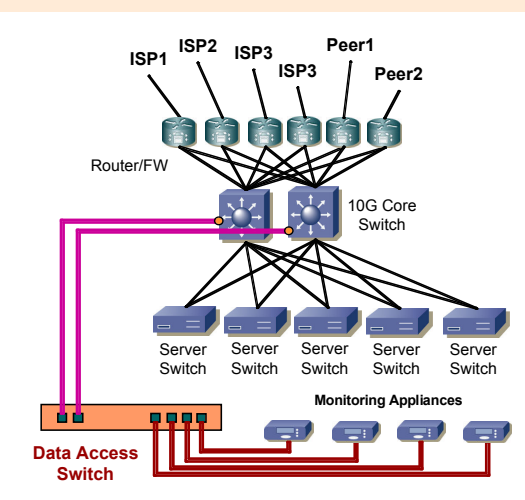
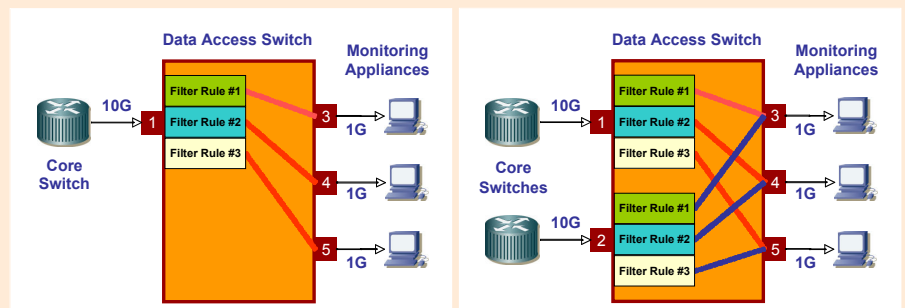
It is now clear that Internet has finally lived up to its potential. The ongoing Internet boom (aka Web 2.0) is delivering a refreshing wave of moneymaking services, successfully transforming the World Wide Web from a collection of static portals to a dynamic interactive medium ideally suited for commerce, advertising, grass-root content creation, as well as on-demand multimedia consumption.

Besides the critical mass in broadband adoption and wireless accessibility, an important enabling factor for Web 2.0 is the commoditization of high speed networking technology. Whereas in 2000, service providers struggled with deploying expensive 100-Meg Fast Ethernet switching technology, today they have nearly all transitioned to Gigabit Ethernet to remain competitive. As the trend continues, the year 2007 will emerge as the year of 10 Gigabit. Few customers are willing to be left behind and most are already moving feverishly to transition their core network to 10-Gig in order to enjoy additional cost savings and substantial performance gains.

One technical challenge of deploying 10-Gig core network has not changed, which is to provide a cost-effective and comprehensive solution to monitor mission-critical traffic at full line-rate in order to ensure network integrity including performance, security and compliance. Unfortunately, for the near future, 10-Gig monitoring tools will not be readily available, and even if they were, would be too expensive or simply incapable of working at true line-rate except in short bursts. One can throttle the 10-Gig traffic down to a level digestible by 1-Gig tools by filtering, but obviously that would compromise the objective of providing comprehensive monitoring since theoretically 90% of the traffic could be lost.

Gigamon's GigaVUE Data Access Switch, which is designed specifically for out-of-band network monitoring, can accommodate multiple bit-mask filtering rules at each ingress port (both 1-Gig and 10-Gig). Using these multi-rule multi-dimensional pre-filters, 10-Gig traffic can be "mapped" to multiple load-sharing 1-Gig analyzers, with each tool analyzing a specific VLAN range, port number or IP subnet according to the specific filter rule, thereby performing comprehensive monitoring at

10 Gigabit rate without oversubscribing any single Gigabit tool. On the other hand, whether it is Gigabit or 10 Gigabit, mission critical core network are almost always tiered, meshed and fully redundant. Therefore, high availability network architecture dictates that multiple 10-Gig links are deployed between parallel switches to improve reliability. In summary, in order to provide comprehensive monitoring, multiple 10-Gig data streams would have to be mapped simultaneously and aggregated so that each tool gets a logical slice of the total traffic. Finally, since mapping filters are hardware based, latency is negligible and full line-rate performance is guaranteed.



Shown here is a typical web-centric customer data center running a 10-Gig core. To support the tremendous amount of web traffic (on the order of tens of millions of page views per week), it is not uncommon to have ten or more 1-Gig links to the Internet (to ISP's and peering sites). Furthermore, total traffic can be increasing at 30% per quarter. A scalable solution is therefore desperately needed to match customer's growth.

At the core of the network, servers are organized in clusters, each serving a specific business function ranging from online shopping, credit verification, merchandize delivery and product support, upload and download of music, picture, podcast and video, various online activities including search, chat, email, blog, etc. Each server switch is connected to the core switches using two 10-Gig redundant links, which are themselves connected to the Internet through multiple 1-Gig redundant links.

A large number of best-of-breed monitoring tools from multiple vendors are deployed including web analytical tools to track real-time user experience and to enable internal charge-back to various business functions, database security tools to prevent leakage of confidential information, forensic data storage to proactively and retroactively examine attacks and abuses, etc., all of which compete for out-of-band data access. With the

Data Access Switch, the 10-Gig traffic streams mirrored from the two core switches are captured and aggregated. Mapping filters based on IP address range corresponding to the server switches are used to segregate the total traffic into different logical groupings such that each appliance is responsible for monitoring of traffic belonging to one or several specific business functions. In summary, using a Data Access Switch with multi-rule mapping feature to share the load among multiple parallel processing Gigabit tools, 10-Gig network can be monitored comprehensively and cost-effectively. Moreover, the Data Access Switch acts as the virtualization layer between the network and the tools. It is the building block for a flexible Data Access Network (DAN) that enables engineers to deploy monitoring tools at will. Moves, adds, and changes can be performed without requiring any physical changes or exerting load to the production network. Speed change (1G-to-10G or 10G-to-1G) and media conversion (copper-to-optical, multimode-to-single mode) can be easily accommodated.