Pipeline
Knowledge Is Power

www.pipelinepub.com **Volume 6, Issue 3**

Improving Network Monitoring

By Dan Pocek

Proactive traffic monitoring becomes more complicated in a high-capacity, converged network for a number of reasons. First, converged networks are exacerbating what I will call the fire hose problem, or the fact that tools are trying to monitor a specific traffic type that is traversing the network in an increasing larger pipe of mixed voice, video, and data traffic. This is like filling a water glass with a fire hose as the traffic arrives at the monitoring tool and “overwhelms” it; as data rates increase, this problem grows exponentially. Second, network tunneling, or the encapsulation of data within public and private network infrastructure, has become widespread in today’s corporate networks, driven by a need to securely transport sensitive data and leverage public networks. This is not welcome news for monitoring tools such as protocol analyzers and transaction recording solutions that are already struggling to keep up with converged network data flows. These tools now must also find a way to access and process complicated tunnels. This article looks at these two issues in greater detail and evaluates the solutions that attempt to address them.

Converged networks are carrying a combination of voice, video, and data at increasingly higher speeds. This presents a problem for monitoring tools that are designed to monitor a specific application, service, or suite of services since most of these tools only need access to a small fraction of the data in a high-speed line. The process of isolating the service of interest for each tool can exhaust the resources of the monitoring equipment, leaving fewer resources for higher-level processing. A VoIP monitoring tool, for example, must first find and target the VoIP traffic within a large converged pipe before it can begin to measure Quality of Service and other metrics and key performance indicators that provide valuable information about how the service is performing.

Currently, Switch Port for Analysis (SPAN) ports or Test access point (TAPS) can be deployed for connecting to monitoring systems. SPAN ports replicate or mirror only certain traffic, dropping corrupt packets. TAPS duplicate all traffic on a link and forward it to the monitoring port without introducing delay, or changing the content or structure of the data. While SPAN ports and/or optical TAPs are used to provide access to monitoring tools, neither approach solves the fire hose problem. Using SPAN ports on a router provides a fairly straightforward approach to providing access and can even offer some level of traffic aggregation, assuming the router platform is lightly utilized. However, this approach is not reliable since these processing functions are contingent upon the amount of resources not being utilized for other, higher-priority router tasks. Furthermore, the primary function of a router is not to provide monitoring access, so burning SPAN ports on these platforms for this purpose can quickly become cost-prohibitive. Optical TAPs, on the other hand, eliminate the cost issues related to SPAN ports, but have their own restrictions. Most importantly, they do not have their own processing resources and therefore do not alleviate the monitoring equipment's burden of too much data, nor do they provide traffic aggregation functionality. Additionally, they drain optical power from the network.

A smarter solution comes in the form of optimizing traffic prior to monitoring equipment. Here, the term "optimization" is an umbrella term for link aggregation, packet/service filtering, interface/protocol translations, and other tactics intended to streamline the data for specific monitoring needs. These devices can be used to front-end multiple tools that are monitoring different services, sending only the data of interest to each tool. Consequently, tools are able to become more efficient and require less up-front processing resources, allowing them to focus on what they do best, such as measuring the Quality of Service of VoIP traffic. Another added benefit of this monitoring access solution is that the life of a monitoring tool is lengthened since these products can also perform filtering and interface translations as data speeds increase and protocols change. Figure 1 below shows a data access configuration where one of these devices accesses converged network traffic and directs it to specific tools for higher-level processing.

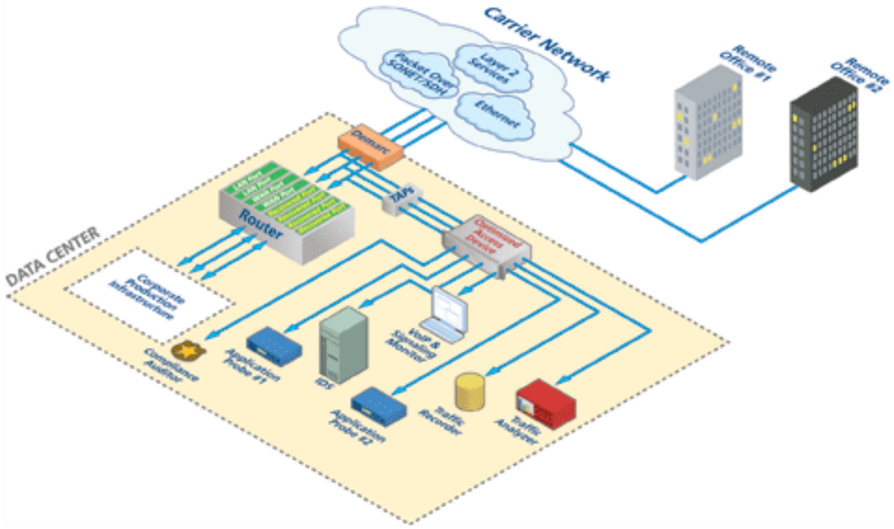

Figure 1

The increase in tunneled protocols within converged networks complicates monitoring strategies even further. The Generic Routing Encapsulation (GRE) protocol, for example, is a widely used tunneling protocol that creates a virtual point-to-point link between routers and remote points in an IP network through IP tunnels. GRE has created a void in network monitoring strategies because many probes or tools cannot remove its tunnel header. The result is that GRE data is often not monitored, which is problematic because network administrators need a comprehensive view of the network in order to effectively anticipate and troubleshoot problems. Furthermore, monitoring the GRE protocol is even more necessary since network resources are easily wasted due to its stateless nature. Resources are wasted because an application on the near end of a transmission will continue to use network resources even when the application on the far end is no longer available.

Today, network administrators solve this tunneling problem by positioning monitoring tools behind the access router so that the tunnels are already stripped off of the payload. While this solution does eliminate the issues related to tunnels, it introduces several new complications. First and foremost, it raises doubts as to whether the data was compromised before or after the router. It also masks issues relative to WAN network performance. In order to monitor all network traffic, tools and probes need to be equipped to identify and process all data, whether it is traversing the network as IP or GRE.

While several flavors of solutions are available in the market today that address one or the other of the problems discussed above, only a few combine the valuable functionalities of optimized access and tunnel identification/processing. Network administrators looking for a fool-proof monitoring strategy need to consider not only the new and improved monitoring tools available today, but also monitoring access optimizers that empower these tools to be more comprehensive and cost-effective.