**Gigamon®**
The Smart Route To Visibility™

Multicasting, TAP and Traffic Aggregation for Telecom Networks

Going beyond VoIP, IPTV or even Triple Play, today's unifying theme is Service-over-IP (SoIP). In other words, all revenue-generating next-generation services (voice, video and data) introduced by carriers now share the common feature that they are simply digitalized traffic carried over IP-based Ethernet.

SoIP will be a source of struggle – not just the obvious market-based struggle between cable providers and telecommunication providers – but a societal-based struggle between expectation and business reality. As SoIP enjoys mainstream deployment, consumers will demand Quality-of-Service that they are accustomed to with traditional medium (i.e., analog telephone and television) in spite of added features and reduced price. Similarly, government will demand unrestricted access for lawful intercept in all manners of digital communications, to be consistent with unrelenting homeland security concerns. In summary, SoIP providers can no longer ignore the harsh business reality of providing a fixed-income service while accommodating ever-growing monitoring demands.

The weapon of choice for service-oriented network monitoring is Deep Packet Inspection (DPI) which are high performance software solutions that run on standard server hardware platforms enabling providers to 1) identify, classify and even selectively block IP traffic to prevent revenue leakage from unauthorized SoIP services, 2) detect and protect against security threats and network anomalies, 3) facilitate wiretapping and reconstruction of relevant digital transactions. For the

technology to work, DPI must be able to unobtrusively acquire production traffic from multiple sources across a redundant Traffic Visibility Network. Recently, instead of using conventional network taps, the Traffic Visibility Fabric has emerged as the "Best Practice" traffic access and network monitoring architecture for cost-effective DPI monitoring. Currently being deployed by several major carriers in nationwide rollouts, TVN has saved tens of millions of dollars for telecom customers by aggregating tapped traffic from multiple network links, separating SoIP from non-SoIP traffic using hardware based packet filters, and regenerating and mapping the aggregated traffic to multiple DPI analyzers in order to optimize traffic load.

Long-Distance Carrier Core Network
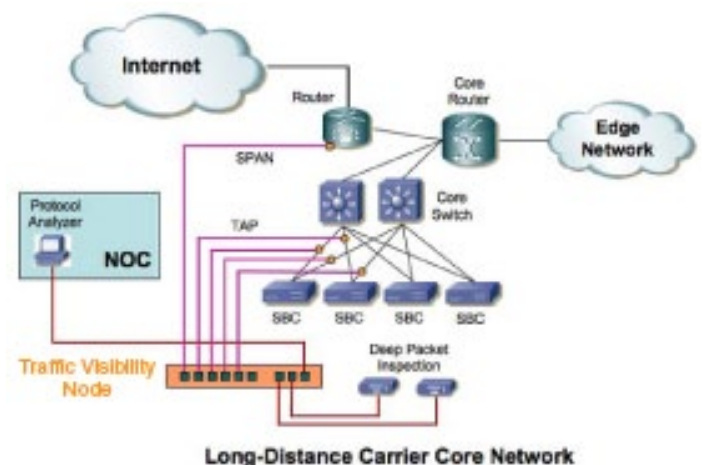
The technical challenge for DPI monitoring is akin to that of searching for pins in a haystack; more precisely, searching for fragments of pins from multiple gigantic haystacks. Recall that

Ethernet was designed for traffic. It was meant for synchronized transmission of traffic broken up into fragments (i.e., packets), where the timing and the temporal order between fragments is not important. So when someone surfs the web making random requests for packets from all over the World, packets will arrive in different order and at different time slots. Some of them don't even arrive at all. The protocol embedded in Ethernet makes allowance for such chaos and diligently reassembles the fragments in proper order and make repeated requests if they are lost. This scheme works for traffic and surprisingly works for voice and video as well in spite of the fact that digital voice and digital video are synchronized traffic, since in this case the order and the timing between the fragments are indeed important.

One reason why Ethernet works even for SoIP is because the pipes that make up the carrier networks are relatively large and under-utilized; therefore SoIP packets typically travel unhindered. Moreover, customers' state-of-the-art fully meshed networks are redunTVNt and parallelized such that there are multiple paths for the packets to travel. On the other hand, when a network engineer has to make an independent measurement of the network's performance as it is utilized for SoIP transmission (in order to ensure SLA, for example) or when a law enforcement officer is given the mandate to track potentially illicit discourse, the fact that SoIP packets are never retransmitted (such that every single packet must be collected) and that there are unlimited paths for them to travel have imposed a huge problem. In other words, how does one comb through multiple haystacks in order to find all of the random fragments (packets) of a pin?

TVN is often described as the distributed "Traffic Socket" for comprehensive out-of-band network monitoring. The Gigamon® GigaVUE® Traffic Visibility Node which is the building block of TVN is like a vacuum cleaner that sucks up the hay wherever they might exist, filters out metal fragments that possess characteristics which would materialize into a pin, and presents these relevant pieces to the DPI analyzer in order to recreate the original puzzle. The diagram on the top shows a commercial

SoIP network. This is the core network typical of a long distance carrier which has a number of redundant core switches that manage traffic in and out of the SBC (Session Border Controller) and core routers that manage signaling and SoIP traffic that goes out to other switch centers (edge networks) or to the Internet. If one were to attach a DPI analyzer directly to the network, the amount of traffic would be so overwhelming that it will easily oversubscribe the tool. Moreover, so many individual tools would have to be deployed in order to fully capture all of the relevant packets from disparate critical locations across the network that no customer can ever cost-justify such a deployment.

Instead, telecom customers use a number of passive network taps to tap all of the redunTVN optical Gigabit links connecting the SBC to the switch, copy and filter the traffic using the GigaVUE Traffic Visibility Node either to extract RTP (voice) or RTCP (signaling) packets, regenerate and map (i.e., load balance) the aggregate to multiple DPI analyzers. In addition, GigaVUE can accept SPAN port traffic from the routers to monitor outgoing traffic. Finally, for troubleshooting purpose, a protocol analyzer remotely located at the central NOC can be connected to the Traffic Visibility Node, which would be shared among the switching centers (supporting the highly skilled network engineers).

Cable Provider Edge Network
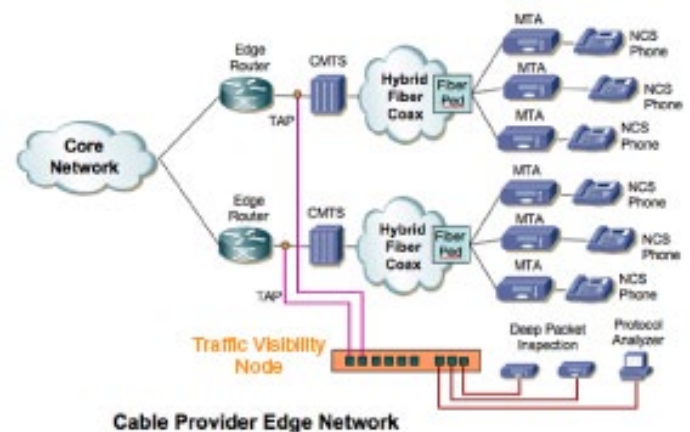
Besides the core, telecom customers also deploy Traffic Visibility Fabric at the edge (see bottom picture) where basically the same

connectivity functions are performed at the neighborhood hubs, passively tapping all of the Gigabit copper links that connect the CMTS (Cable Modem Termination Systems) to the edge routers, and aggregating, regenerating and filtering SoIP traffic for DPI monitoring. In summary, network monitoring using DPI analyzer is a mission critical application that is tailor-made for the best practice Traffic Visibility Fabric architecture, using the GigaVUE Traffic Visibility Node to aggregate traffic from multiple taps, regenerate and filter aggregate traffic both at the core and the edge, and as usual is saving substantial amount of money for our telecom customers.

About Gigamon

Gigamon provides intelligent Traffic Visibility Networking solutions for enterprises, data centers and service providers around the globe. Our technology empowers infrastructure architects, managers and operators with unmatched visibility into the traffic traversing both physical and virtual networks without affecting the performance or stability of the production environment. Through patented technologies, the Gigamon GigaVUE portfolio of high availability and high density products intelligently delivers the appropriate network traffic to security, monitoring or management systems. With over seven years experience designing and building intelligent traffic visibility products in the US, Gigamon serves the vertical market leaders of the Fortune 1000 and has an install base spanning 40 countries.

For more information about our Gigamon products visit:

www.gigamon.com