Whitepaper

Multi-Point Correlation for Mobile Operators — Turn Big Data into Competitive Advantage

When it comes to telecommunications services, nothing is simple anymore. Carriers are now transporting new, real-time services—like VoLTE, ViLTE, and others—that are highly sensitive to delay, jitter, and latency. To be successful, carriers must connect these services to their existing tool rail and enable them with both specialist data and analytical tools.

A centralised tool rail can offer many operational efficiency advantages, but it also demands that tools work in different ways. As examples:

- Each tool needs specific traffic types: APM (Application Performance Management) tools need different data than NPM (Network Performance Mangement) tools, CEM (Customer Experience Management) tools may need different data than either APM or NPM tools, and so forth.
- Each tool ingests traffic at a different rate, which is largely dependent on the line rate. interface. Security tools, for instance, often process at much slower speeds than other tool types.
- Each tool has a different throughput rate, largely depending on its processing capability.
- Each tool needs unique traffic pre-processing and can waste cycles pre-processing traffic internally as a software function.
- Each tool conducts high-value, deep-dive processing in specific areas.
- Each tool provides different results based on the same data input due either to unique pre-processing inside the tools or unique non-systemwide timestamps.
- Some tools need to see overlapping copies of the same traffic going to other tools.
- Each tool's upgrade cycle as well as ability to expand for future traffic levels varies. For example, some tools may expand the number of interfaces; others, the number of processors.

Gigamon's FlowVUE® application, which is part of Gigamon's Visiblity Platform, offers a new subscriber-based IP sampling paradigm that helps carriers turn Big Data into manageable data. The application not only enables existing tools to connect to the latest high-speed pipes by providing a representative view of subscriber traffic for diagnostic coverage, but it also enables overlapping traffic samples to be sent to different tools at the same time for multi-dimensional analysis of subscriber behavior and deeper insight into the traffic. By correlating subscriber identity, traffic type, and subscriber quality of experience, service providers can begin to truly understand where network trouble points reside and what their associated causes are.

Operators also gain new operational efficiencies by avoiding the unnecessary traffic and tool dimensioning of over- and under-subscription across a wide set of tools. They can now dimension their tool rail for a specific percentile of the typical busy hour and apply cost savings elsewhere on their network. For example, during the height of the busy hour, they can increase the traffic scaling factor to reduce the number of traffic samples flowing to the connected tools. Conversely, during the non-busy hour, they can decrease the traffic scaling factor to increase the number of samples flowing to the connected tools. Through an individual API link that is unique to each connected tool, they can enable each tool to independently signal the correct traffic scaling factor and form a real-time feedback and control loop.

The benefits are groundbreaking. Operators gain:

- Better network-wide intelligence
- Better tool optimization and processing throughput that can lead to cost savings
- Better resource utilisation for new operational advantages
- And finally, a better competitive advantage in the market place due to improved resource utilisation

Use Case: A Day in the Life of a Subscriber (Multi-point Correlation)

How do the FlowVUE benefits translate to an operator in practical terms? Let's look at a day in the life of Jenny, a typical subscriber.

In the morning, Jenny is riding the train to work while taking an important international VoLTE phone call. Jenny realises that when the train slows down, the call is fine, but when the train speeds up, the call suffers from drop outs. Jenny also happens to be using a newly released handset.

- Since the problem appears to be VoLTE-specific, and likely interoperability related, the carrier can prioritise the new handset as the main issue. By correlating on subscriber identities that have active trouble tickets for VoLTE calls and, in turn, triggering on the specific traffic type coming from the new handset, the carrier can zero in on the problem much faster. This helps to maintain high customer satisfaction while simultaneously reducing active case load for support.

Jenny frequently uses an employer-supplied, trusted, and secure app on her handset. While in a customer meeting, she notices the data on her handset doesn't work very well inside the customer's multi-story office building and she's forced to step out of her meeting to complete the customer quote. To avoid the issue in the future, she is thinking about switching to a different mobile service provider.

- The carrier can detect failed sessions from specific high-value apps, narrow down monitoring to understand which user endpoints have the most problems, and make recommendations back to the subscriber or the endpoint manufacturer. If after rigorous monitoring it's discovered that a certain handset is the cause, the operator can elect to replace only those handsets that are used in locations with problems (thus gaining an operational efficiency). Armed with this new insight, the carrier can also reserve in-building frequency bands for those services that need them most, or those locations that struggle most.

At lunchtime, Jenny is in a popular park listening to music on her handset from her service provider's new music offering. Due to the density of subscribers in the park—everyone's using real-time services—the quality of her service decreases. Disappointed with the performance, she is tempted to switch to an advertising supported OTT (Over-The-Top) service instead.

- By focusing in on Jenny's traffic, the operator can move her to a higher class of service, avoiding the issues at that location. The operator can keep the OTT services on the lowest class of service to make sure there is enough bandwidth for the service Jenny is using. The operator can also downgrade Jenny to a lower rate music codec to eliminate the bandwith problem.

Back at the office, Jenny is using an OTT social media app on her mobile device for work purposes. Currently, her carrier doesn't know what services she uses and is unable to analyse the traffic from her handset. It would, however, like to understand usage models for OTT service offerings so that it can evaluate the possibility of monetizing them.

- By tuning the network to recognise and send only specific OTT traffic to the tool rail, the carrier can minimise the total amount of traffic that needs to be analysed and optimise tool processing throughput. The carrier can do multiple different types of analysis in parallel by sending overlapping samples of traffic to multiple tools in parallel. After the carrier understands what OTT traffic can be monetised, it can then reduce the traffic to just a set of specific OTT types – greatly reducing analytic tool load and related costs.

In the evening, Jenny is using her handset to download a new freeware app from the Internet. Ironically, after downloading the app that was supposed to help her download faster, she starts to get strange messages on her screen. Not only does she notice a stall in downloading activity from her apps, but her battery seems to be drainig faster. Jenny thinks her handset has been hacked.

- Having detected unusual traffic coming from Jenny's device as well as from those of several other customers who downloaded the same app, the carrier requested that the app be removed from third-party app stores, only they have been slow to respond. The carrier decides on a faster solution that allows every handset with the malicious app to forward its traffic—which is part of a brand-new botnet—through a special security screening, which can backlist and block as needed. Since the operator can now pinpoint the malicious traffic type, it can forward only the bad traffic and allow the good traffic to pass unrestricted. The operator gains an operational advantage since it doesn't need security tool bandwidth for all traffic. On top of that, it can send multiple overlapping data samples to different tools to detect many different malicious traffic types in parallel. This can vastly reduce security infrastructure costs as well as the need for continual transport pipe expansion.

About Gigamon

Gigamon provides an intelligent Unified Visibility Fabric™ to enable the management of increasingly complex networks.Gigamon technology empowers infrastructure architects, managers and operators with pervasive visibility and control of traffic across both physical and virtual environments without affecting the performance or stability of the production network. Through patented technologies, centralized management and a portfolio of high availability and high density fabric nodes, network traffic is intelligently delivered to management, monitoring and security systems. Gigamon solutions have been deployed globally across enterprise, data centers and service providers, including over half of the Fortune 100 and many government and federal agencies.

For more information about the Gigamon Unified Visibility Fabric visit: **www.gigamon.com/solutions/service-providers**