Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 13, Issue 8

The critical role of Active Assurance in the context of SDN and NFV

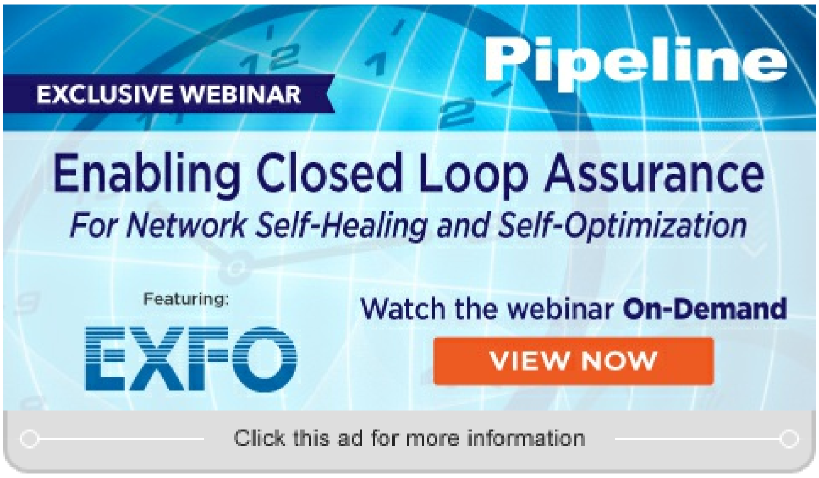
By: Claudio Mazzuca

The transition from traditional networks to virtualized networks is well underway, driven by the promise of SDN and NFV. These networking tools have the power to dramatically change the way services are created and managed, but how will these changes impact the way service providers manage their customers' Quality of Experience (QoE)? The answer lies in a fundamental shift away from traditional network monitoring to a more dynamic, software based real-time service assurance solution architecture.

Fundamentals of virtualization

Why the move to virtualization?

Traditional networks were built to address specific service needs/requirements and scaled to address the anticipated capacity. In other words, a traditional network was purpose-built for a specific service or set of services. Developing new services or scaling the network to handle more services than expected involved lengthy, expensive planning and engineering projects, often lasting 9 months or more, to ensure the new service could be fit into the existing network without impacting the existing services.



According to a recent **report**, most service providers, some more aggressively than others, are developing strategies to transition to virtualized networking. Fueled by the success of Enterprise Data Center virtualization along with advances in Software Defined Networking (SDN), these service providers are looking to fundamentally change the way services are created and managed; to become more agile and responsive to their customers ever-changing needs while at the same time driving OPEX and CAPEX out of their bottom line.

Software Defined Networking (SDN) is a concept that has been around for many years. Its fundamental premise is the separation of the control plane from the data plane to allow for centralized, dynamic management of network resources in response to changes in the network state (i.e., load-balancing to overcome congestion in the network or bandwidth augmentation to address increased bandwidth utilization on a critical link).

Network Function Virtualization (NFV) is the evolution of data center virtualization into the service provider network. Purpose-built hardware platforms, such as routers or NIDs, are disaggregated into their basic functional elements and each functional element implemented in software as virtual network function (VNF) running in one or more virtual machines on commercial off-the-shelf (COTS) servers. By combining, or chaining, these VNFs in software, an entire network can be built without any purpose-built hardware at a much lower cost. And since the network is entirely software based, NFV allows the service provider to efficiently manage their network resources by deploying them only where needed or justified and new services can be added without additional capital investment.

But the real value to the service provider comes when you combine SDN with NFV. In doing this, service providers are now able to leverage the value of NFV (service agility and operational efficiency) with the value of SDN (rapid spooling up services on demand, secure segregation of functions and improved asset utilization) to build virtualized networks where new services can be created by simply adding new VNFs. Services can now be rapidly deployed by creating a chain of VNFs between the desired endpoints, and the network continuously optimized to ensure sufficient resources are always available to address the service requirements.

Finally, a key element to unlocking the full value of virtualized networks is automation. Massively scalable networks, built in software and continuously optimized simply cannot be managed effectively by humans. Automation unlocks a whole new dimension in service management that is not possible in traditional networks. Not only can services be created, deployed and monitored autonomously, but they can be managed by the customer themselves. On-demand service creation or modification can be handled in real-time, through a customer portal without the need for manual intervention by the service provider. The network itself will handle everything from resource allocation, service instantiation, service testing and billing - and all in near real-time.

There is, however, a risk associated with this new paradigm. While the general trend is toward automated, customer managed service creation, customers are becoming less willing to accept sub-par quality of service. Self-service does not mean best effort. Service providers need to meet or exceed customer expectations from day one or else risk losing them to the competition.

Fundamentals of service assurance and analytics in NFV/SDN

Whether the network is a traditional network or a virtual network, there is only one true measure of success – Customer Satisfaction, and the revenue growth this will bring. In the end, the customer doesn’t care about the technology used to deliver their service; they only care that their service delivers what was promised. In fact, the shift to virtualized networks makes this even more critical since automated, dynamic service creation means customers can change providers very easily. Customer retention becomes solely dependent on the customer Quality of Experience (QoE), which the ITU-T has defined as, the “*overall acceptability of an application or service, as perceived subjectively by the end-user*".

So how will service providers manage their customers’ QoE in a virtual network where the service is built in software and the network is constantly changing to optimize performance? It turns out, this can be done using many of the same tools used in traditional networks, but adapted to software, or Virtual Network Function (VFN) applications, that are dynamically instantiated when and where needed.

Traditionally, service providers have focused on the notion of Quality of Service (QoS) to understand and manage their customers service performance. The ITU-T defines QoS as the "*totality of characteristics of a telecommunications service that bear on its ability to satisfy stated and implied needs of the user of the service*", and for a traditional network, this was an acceptable way to manage the customer QoE. Traditional networks had fixed, well defined architectures for service mapping and this meant that service assurance, or QoE, could be closely tied to network performance since there was essentially a one-to-one mapping of service flow to network architecture.

Virtualized networks, on the other hand, break this relationship. In the virtual network, service routing is continually being optimized to address impairments, such as congestion or equipment failure. As such, it is impossible to predict with any certainty how the service is being mapped through the network at any one time, meaning there are no obvious places to measure QoS in the traditional sense. Service providers need to focus on QoE from a different perspective – it needs to become an essential part of the service, rather than part of the network.

Fundamentals of Service Assurance:

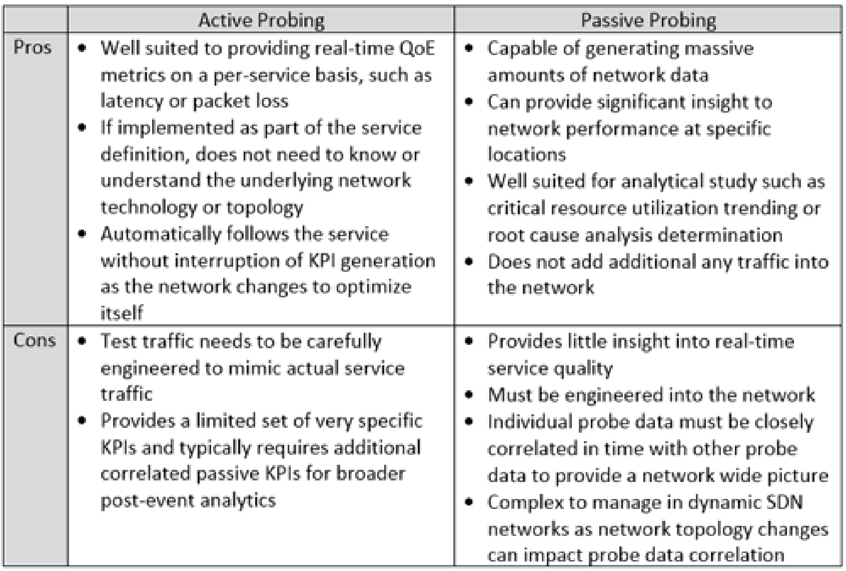
Service assurance relies on two different measurement techniques to understand service performance; passive probing and active probing, and each brings its own value.

Passive probes monitor traffic flows as they traverse the network and generate KPIs or alarms accordingly. As the name suggests, these probes do not impact the services themselves or generate test traffic in the network. This kind of probing can be as simple as reading port level statistics available through SNMP MIBs, or may involve making a copy of the traffic (tapping the physical link or using a mirror port on a switch) and storing it for analysis (often by an external system or even manually by an engineer). Passive probes are engineered into the network at key points to provide very detailed information at that point to derive a wide range of information. For example, TCP headers contain information that can be used to derive network topology, identify services and operating systems running on networked devices, and detect potentially malicious probes. However, all of this requires network traffic to be present and a significant amount of computing and storage resources before any benefit can be realized.

Active probes, on the other hand, work by inserting synthetic test traffic into the network and observing how the network, service or other elements respond. By inserting synthetic test traffic into the service flow, the active probe can measure the performance of the service, end-to-end and in real-time, generating service level metrics such as latency, jitter, and packet loss. Because active probes are essentially a part of the service traffic, they do not need to be engineered into the network. Rather, they can be inserted at some point in the service flow without any knowledge of the service path. Active probing is ideal for generating real-time performance data on specific services with or without the need for customer traffic.

Is one better than the other? Do you need both? Well, it really depends on what you're trying to do. In a traditional network, where the physical network was closely aligned to the service requirements, passive probing was adequate for managing the majority of services since networking metrics like bandwidth utilization or errored frames provided sufficient insight into service performance to allow network operations teams to manage issues as they arose – albeit, not in real-time. Active probing was typically reserved for high revenue services with performance based SLAs since violations of the service agreement could cost the service provider significant money or worse, the customer itself.

In a virtualized network, driven by SDN and NFV principals and fully automated to drive out OPEX and enable massive scale, continuous access to real-time service and network performance metrics is essential. The entire network operates as a closed loop control system where the feedback mechanism is service performance [See reference]. Passive probing is ideally suited for gathering massive amounts of historical network data and storing it for deep troubleshooting and analysis. Active probing, on the other hand, is ideally suited for creating real-time performance information on a service level, and for this reason, active probing is critical for virtualized networks.



	Active Probing	Passive Probing
Pros	• Well suited to providing real-time QoE metrics on a per-service basis, such as latency or packet loss • If implemented as part of the service definition, does not need to know or understand the underlying network technology or topology • Automatically follows the service without interruption of KPI generation as the network changes to optimize itself	• Capable of generating massive amounts of network data • Can provide significant insight to network performance at specific locations • Well suited for analytical study such as critical resource utilization trending or root cause analysis determination • Does not add additional any traffic into the network
Cons	• Test traffic needs to be carefully engineered to mimic actual service traffic • Provides a limited set of very specific KPIs and typically requires additional correlated passive KPIs for broader post-event analytics	• Provides little insight into real-time service quality • Must be engineered into the network • Individual probe data must be closely correlated in time with other probe data to provide a network wide picture • Complex to manage in dynamic SDN networks as network topology changes can impact probe data correlation

Table 1 - Active versus Passive probes

Service Assurance in a Virtual Network

Since services in a virtual network are implemented in software and dynamically routed through the virtual network to address changing network conditions, this implies only the service endpoints are fixed. How the service is mapped through the network is indeterminate, so predicting where to place physical probes, active or passive, is difficult. Fortunately, there is a simple solution to this problem. By implementing the probes as VNFs, service assurance becomes part of the service itself, rather than a function of the network. This is a fundamental shift in the way service providers think about service assurance. No longer is it an afterthought added to address high revenue services, rather it becomes an essential part of all services. And it’s not just for ongoing service assurance either; it also applies to service activation testing. In the fully- automated virtual network, services will be created and tested before being handed over to the customer, in minutes rather than days, and all without human intervention. And once up and running, these same services are monitored constantly to ensure they continue to meet the service requirements – and when they don’t, the network automatically adjusts itself to fix the issue.

Closed Looped Assurance with Active Probes

As mentioned, a primary factor in the success of virtualized networks is automation - the ability of the network itself to make decisions on 1) how and where to build new services and 2) how to continually optimize the virtual network to address changes in the network state. This ability will rely heavily on analytics to drive this process and the analytics will only be a good as the information being fed to it.

For certain, longer term planning activities like bulk capacity upgrades or data center expansions, information from passive probing systems may be sufficient as this information is well-suited to historical trend and predictive needs analysis. But for decisions involving the performance of services in the virtual network or optimization activities to address network congestion or facility failures, real-time metrics are required and these will only come from active probing. Deployed appropriately, the active probes can provide the analytics engine with a complete view of performance from three key dimensions – customer, service and network. This multi-dimensional 3D view allows for a greater understanding of the entire network state and, therefore, better optimization decisions. Only by continuously feeding real-time QoE metrics back into the decision making systems will service providers be able to exceed their customers service expectations.

How EXFO delivers this solution

Smarter service assurance is the foundation for smarter network success. EXFO provides a clear, three-phase path for transitioning with confidence to NFV/SDN deployment and operationalization.

Our service assurance solutions for physical, hybrid and virtualized infrastructures deliver high performance and reliability at the network, service and subscriber levels. Our real-time 3D analytics, test orchestration, and active and passive monitoring offer unprecedented agility, efficiency, automation and end-to-end visibility. Together, we will make sure the virtual and the physical behave as expected—and deliver results as promised.

Phase One - ***Virtualizing***
Make sure your migration to virtualization is done right, without negative impacts to subscribers or your bottom line. We fully assure the performance of physical, hybrid and virtual infrastructures, and the services they deliver throughout their entire lifecycles.

Phase Two - ***Automating Operations***
Make sure the automation of your services deployment increases ROI, efficiency, performance and deployment speed. We make it possible to automate your operations without risking reliability.

Phase Three - ***Complete Integration of Service Assurance in DevOps***
Make sure you reach your goals of optimized operational efficiency, agile service creation and increased revenue. We make it possible by enabling closed-loop automation through real-time analytics and test orchestration.