Strategies for Enabling Service Assurance in a Virtualized, Software-Defined World

Network function virtualization (NFV) completely changes how networks are designed, built, and managed. NFV pulls the functions necessary to run networks off of the current proprietary hardware and places it on open-based computer servers that can be deployed where they are needed most. Functions can be deployed and scaled on demand, thus greatly improving infrastructure utilization and significantly bending the network cost curve growth.

Once NFV is in place, software defined networks (SDN) can be deployed to provide an architectural approach that separates the control and data planes of a network. Through programmability, SDN provides greater control of a network, allowing applications and the network to better work together while establishing the infrastructure for a whole new range of cloud services.

When NFV and SDN are used in tandem, providers become liberated from the physical constraints and complexities of current networks. This results in a network that is more scalable, more dynamic by allowing changes in real time, and more cost effective to operate over time. It also provides for greater flexibility for network management, better performance, and better customer service while providing a more agile environment for the introduction of new services and applications. But with all of the benefits, there will be challenges.

Market Drivers and Challenges

The market for software-defined networking is relatively new and it is projected to surge over the next five years as service providers look to bolster service offerings and cut costs. Some of the main market drivers include:

- Optimized equipment and infrastructure costs through consolidation of network functions, while exploiting economies of scale from the IT industry
- Improved scalability resulting from virtualizing, enabling a single platform to be used for different applications and users
- Accelerated time-to-market by shrinking typical innovation cycles for new services and applications
- Expand ed collaboration resulting from open environments, enabling a wide variety of ecosystems and partnerships

Networks of the future will be designed, implemented, and managed radically differently than they are today. Network performance, which was once predictable in a dedicated, hardware-based network appliance, will now be affected in many ways when a new virtual network element is installed. Physical links connecting network equipment today are points of delineation and locations in which data can be accessed for monitoring and troubleshooting. In the future, these become virtual interfaces, connecting functions within software in the same (or different) physical servers. Today's methods and techniques to identify why, where, and who is impacted will change or be adapted.

The transformation towards open solutions, white-box technologies, and virtual network functions creates a significant opportunity to cost effectively and quickly deliver revolutionary services at breakthrough price points. This, in turn, will enable new business models critical to the success of the proposed vision. However, in order to seize these opportunities, operators must overcome a number of significant challenges in the management, monitoring, and assurance of virtualized architecture and services, including:

- **Business processes** — methods and procedures must adapt to hybrid physical and virtual environments
- **Service assurance and support** — migration from a reactive network or service failure response model to a proactive network and service assurance model
- **Service management and service continuity** — the nature of SLA is changing; real-time, contextual, and location-aware assurance and analytic solutions are essential
- **Visibility blind spots** — traffic visibility between physical and virtual networks, and within virtualized physical hosts, will be essential; this requires elastic mediation and correlation capabilities offered by an appropriate service assurance and analytics architecture
- **Complex service chains** — granular application and service awareness will be required for efficient implementation of SDN, Orchestration, and Policy functions and will require external mediation and correlation capabilities.
- **Complex multivendor environments** — whitebox inconsistency compounded with heterogeneous wireline and wireless network environments requires scalable and normalized operations, administration, and maintenance solutions

Enabling the Virtualized Networking Evolution

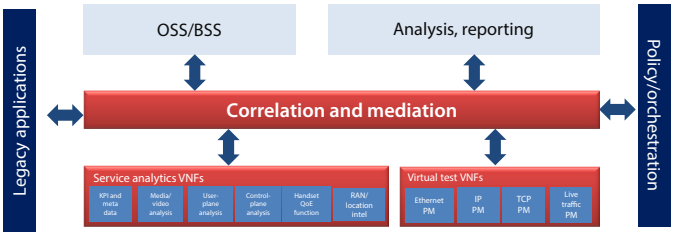
In a virtualized network environment, assurance solutions and processes must a transition from traditional reactive "monitoring" to proactive "real-time intelligence and analytics," tightly integrated with and coupled to the network and services as well as orchestration and policy systems. And, while monitoring-system costs have been growing almost linearly with the growth in network traffic, tomorrow's solutions must break this growth curve by leveraging virtual agents for intelligent network probing, coupled with intelligent analytics and storage. As with all network technology transitions, the legacy technology does not disappear for some years and therefore assurance solutions and processes must deliver an approach supporting both virtualized and non-virtualized environments, enabling a transition from today's networks to future software-defined, orchestrated, virtual networks.

Traffic and application visibility, performance management, mediation, correlation, and real-time analytics are necessary and critical capabilities. These enable dynamic assurance and troubleshooting functions spanning both virtualized and non-virtualized networks while providing a non-linear cost relationship between assurance solutions (delivering monitoring, analytics, testing, and troubleshooting) and traffic levels. Traditional monitoring systems, which store massive amounts of data for post-processed call tracing and analysis, simply do not cost-effectively scale with network traffic growth. The only way for next-generation assurance solutions to break the escalating monitoring cost curve is by implementing new streamlined methodologies for data processing, analysis, and storage.

Real-time intelligence and analytics providing correlated media, location, user plane, and control-plane analysis preempt and prevent service disruption, and enable meaningful integration of SDN, orchestration, NFV, and policy domains. This is a fundamental architectural shift required by next-generation assurance and performance management systems. Network operators can no longer tolerate performance insight delivered in 5 to 30 minute windows.

Whereas legacy assurance implementations are typically reactive in nature, focused primarily for troubleshooting, truly effective solutions will provide real-time contextual awareness and information related to performance, state, function, context, location, amongst other details. Different organizations require different analytics and performance visibility for a wide variety of needs. Supporting a wide variety of agents delivers specific service, application, and intelligence adaptable to the needs of different stakeholders.

VNF solution suites can provide service activation, performance monitoring, and troubleshooting functions. Whenever practical, physical probes should be replaced by orchestrated software agents that can be deployed on demand or as part of complex service chains, tightly coupled with NFV managers and orchestrators. Virtual test functions and VNF management implemented with open interfaces enables seamless integration orchestration by diverse controllers, and feeds into various real-time analytics and operational support systems.



NFV correlation and mediation architecture

Key capabilities of an effective and efficient assurance solution that can be virtualized include:

- Real-time KPIs/performance data — a fundamental architectural change/capability of new assurance solutions. As networks become increasingly more dynamic, orchestrated, and performance tuned to suit the needs of applications, service level agreements (SLAs) themselves will become real-time and application-aware. With more dynamic, less-deterministic networks, operators cannot wait 15-30 minutes for performance insight as they did in the past, but instead require instantaneous insights.
- Location and context aware — systems must provide location-sensitive and application-aware performance information. Because subscribers will access services and applications over a variety of devices and networks, a clear picture into the interaction between subscriber, network, and application is necessary in order to both optimize the customer experience and increase service monetization opportunities. For instance, by understanding precisely the high-value customer experience, combined with the ability to notify network policy systems when and where SLA violations are occurring, allows orchestrator/policy controllers to implement proactive corrective action.
- Fully orchestrated solution leveraging the NFV infrastructure — in virtualized environments, traditional probing approaches are impractical and orchestrated software agents must replace probes. Software agents eliminate blind spots by providing visibility into the virtual layer and can be deployed on demand or as part of complex service chains for end-to-end service continuity.
- Streamlined data processing — traditional monitoring systems, which store massive amounts of data for post processing, call tracing, and analysis, simply do not cost-effectively scale with network traffic growth. New methodologies for stream-lined monitoring and troubleshooting must be introduced. This approach will break the traditional linear relationship between network traffic and monitoring growth, providing instead a scalable and extensible monitoring and assurance architecture.
- Multiple applications under one orchestrated solution — In the mobile broadband environment, different departments within a network operator organization need different analytics and performance visibility for a wide variety of needs. New solutions must support a wide variety of agents serving the needs of multiple service domains (for example, video, Ethernet/IP, MPC/EPC) managed by a VNF manager. Following the ETSI NFV definitions, this is tightly coupled with the NFV orchestrator and NFV infrastructure manager. This multi-service solution reduces the number of needed integration points for network orchestrators.
- Open interfaces — to support the integration of critical performance data into multi-vendor systems (including but not limited to policy servers, active and assignable inventory databases, and service design and creation systems), an open platform is crucial to enable real-time insight needed for dynamically-orchestrated networks. Following the ETSI NFV architecture model, open interfaces at multiple levels in the solution hierarchy (for example, at collection, mediation, and reporting), allows network operators to easily integrate assurance-solution components into various systems.
- Extensible across hybrid environments — bridging visibility and management between physical and virtual networks is a crucial need. Subscriber access and service delivery will span physical and virtual networks for the foreseeable future. Real-time monitoring and assurance strategies bridging these two domains are necessary in order to deliver consistent customer experience. assurance-solution.

Summary and Conclusion

With the introduction of virtualized networks, network operators will face many new challenges to ensure that customers continue to receive a high quality of service experience. Next-generation assurance solutions will be required with virtualized architectures that are both open and flexible.

In addition, by virtualizing some of the functions which are today implemented in external instrumentation and discrete probes, a next-generation solution will provide a cost-effective and scalable architecture for deploying, testing, and monitoring network resources. By normalizing test, activation, monitoring, and assurance functions, the operational price/complexity associated with managing and extending Ethernet/IP services to the network edge can be reset. The approach spans physical and virtual networks in multivendor environments, and is compatible with field test instruments (which are already widely used by network operators), microprobes, and other existing network elements and devices.

JDSU

North America	Toll Free: 1 855 ASK-JDSU	(1 855 275-5378)
Latin America	Tel: +1 954 688 5660	Fax: +1 954 345 4668
Asia Pacific	Tel: +852 2892 0990	Fax: +852 2892 0770
EMEA	Tel: +49 7121 86 2222	Fax: +49 7121 86 1222

www.jdsu.com/nse

30175917 000 0814 SERVICEASSURANCENFV.AN.MAA.AE August 2014