White Paper

The Importance of Monitoring Newly Virtualized Functions & Testing Using NFV Techniques

Prepared by

Sterling Perrin
Senior Analyst, Heavy Reading
www.heavyreading.com

on behalf of

www.jdsu.com

January 2015
Introduction

Progress in network functions virtualization (NFV) is accelerating rapidly, in no small part driven by the 2012 formation of the ETSI NFV Industry Specification Group (ISG) to move the technology forward. The work is led by large Tier 1 network operators globally, including AT&T, BT, China Mobile, Verizon, NTT and Telstra, among others – a heavyweight lineup that commands attention throughout the supply chain.

NFV completely changes how networks are designed, built and managed. It pulls the functions necessary to run networks off of the current proprietary hardware and places them on open-based computer servers that can be deployed in data centers, close to where they are needed most. As operators and their suppliers move from proofs of concept (PoCs) to trials and real-world deployments, monitoring and testing challenges are beginning to rise to the forefront. While PoCs and demonstrations may be compelling, virtualized functions can’t be deployed commercially if not effectively assured.

This white paper analyzes the importance of monitoring and testing in NFV networks, with a focus on how these functions themselves must also evolve and adapt to the new era of virtualization.

Drivers for Deploying NFV

In 2013, Heavy Reading conducted several extensive network operator surveys aimed at understanding the drivers for and inhibitors to wide-scale NFV adoption. Hardware cost savings (including savings from running virtualized servers at higher utilization) and faster (and less costly) upgrades or additions of functions were identified as the dominant drivers based on these interviews. For some operators, lower-cost maintenance (one aspect of OSS) was seen as a major benefit, especially where a large volume of distributed devices that require manual maintenance are currently deployed.

Operators have also indicated a number of triggers that might lead them down the network virtualization path. These include:

- CPU-intensive functions with low throughput
- Functions running on multi-functional boxes
- Functions already running in an x86 server environment
- Non-critical functions
- Functions running on boxes nearing end-of-life
- Functions that can be virtualized without impact on OSS
- New functions or applications

Driven by the ETSI NFV ISG, there has been an explosion of PoCs and field trial activity over the past year. The ETSI NFV PoC framework requires PoCs to include at least two vendors and at least one service provider/network operator, thus ensuring through its structure vendor interoperability and service provider relevance. As of January 2015, the ETSI NFV website lists 30 PoCs in some phase of execution, with many already having been publicly demonstrated at multiple industry events over the past year.
Challenges for NFV in Production Networks

The telecom industry is reaching a point where, with the concepts identified and demonstrated, operators are beginning to move to field trials – and in some cases, actual commercial deployments – of services based on NFV. As they deploy NFV, service providers are facing a new set of challenges in assuring, monitoring, managing and testing services and equipment that are newly virtualized.

End-user concerns revolve around performance and service quality, not delivery methods. The added burden on network operators is to ensure that the quality and performance in their virtualized environments is equivalent to that of their legacy physical environments. If quality and performance cannot be maintained, the overall value proposition of NFV unwinds quickly.

In a virtualized network environment, assurance solutions and processes must 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. Assurance solutions must also span multiple services, including Ethernet/IP, video and mobile.

Figure 1 shows the primary challenges faced by testing in NFV networks, as identified by suppliers.

![Figure 1: Challenges Faced by the NFV Testing Market, 2015-2017](image)

Below, we take a deeper look at the main challenges service providers must overcome in the management, monitoring and assurance of virtualized network architecture and services:

- **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 is necessary.
• **Service management and service continuity**: The nature of service-level agreements (SLAs) 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**: White-box inconsistency, compounded with heterogeneous wireline and wireless network environments, requires scalable and normalized operations, administration and maintenance solutions.

---

**Benefits of NFV for Network Testing & Monitoring**

**Speed**

One of the key promises of NFV – for operators as well as their customers – is the ability to deploy services in minutes, as opposed to weeks or months. Applying the same NFV techniques to network test and service assurance enables network operators to test on demand. Instead of waiting to dispatch a technician equipped with specialized equipment, operators can deploy test instances to verify network performance and resolve customer complaints in minutes.

Coupled with speed is an increase in overall testing agility. NFV, by its definition, dictates a migration from fixed services and fixed services definitions to a dynamic environment in which service parameters and characteristics (service chains) can be modified frequently. In the NFV environment, virtual machines are spun up and down based on service needs. NFV testing can match the agile speed of the network in order to adapt to service changes in real time.

**Scale**

Historically, monitoring and network test systems costs have grown almost linearly with the growth in network traffic, but this trend is not sustainable. Traditional monitoring systems store massive amounts of data for post-processing, call tracing and analysis, but do not cost-effectively scale with network traffic growth. New methodologies for monitoring and troubleshooting must be introduced in order to break the traditional linear relationship between network traffic and network monitoring growth.

Software-based agents and new data collection methodologies enable operators to break this linear relationship. As operators increasingly deploy compute resources in all parts of their networks, virtualized test and monitoring functions allow operators to dramatically increase the number of network test points – giving them dramatically increased network visibility at an acceptable cost.

**Migration to Software-Based Agents**

A migration to software-based agents is key to achieving goals of speed and scale in NFV networks as discussed above. Additionally, performance visibility blind spots
get created as physical functions get virtualized as software and share a common pool of network resources. Software agents eliminate these blind spots by providing visibility and can be deployed on demand or as part of complex service chains.

Compatibility of software-based agents with field instruments, microprobes and other existing physical network elements and devices is critical for operators that need to span both their virtual and legacy physical networks. 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. Such hybrid networks are expected to be the norm for nearly all network operators for the foreseeable future.

**Openness**

Openness is central to NFV (and SDN) as network operators look to integrate network equipment from multiple suppliers and coordinate and deliver services across multiple layers of the OSI stack. Open architecture and interface support is critical to the testing and monitoring of NFV networks as well. Open monitoring and testing products are crucial to enable real-time insight needed for dynamically orchestrated networks. Open interfaces at multiple levels allow network operators to integrate assurance-solution components into various systems, and open APIs are required at the collection, mediation and reporting layers, among others.

The above benefits can be realized in applying NFV techniques across a wide variety of test functions, as illustrated in Figure 2.

---

**Figure 2: Applying NFV Techniques to Test Functions**

![Figure 2](source: JDSU)
Conclusions

There is no question that NFV – along with the related but distinct trend of SDN – will radically transform how telecom networks are built and operated and how communications services are delivered. With 30 ETSI PoCs defined and early commercial deployments commencing, that process is underway now.

By leveraging high-volume standard servers and IT virtualization, NFV accomplishes several goals. NFV supports multi-versioning and multi-tenancy of network functions and allows use of a single physical platform for different applications, users and tenants. It also enables new ways to implement resilience, test and diagnostics, service assurance and security surveillance. Additionally, it facilitates innovation toward new network functions and services that are only practical in a pure software network environment.

Traffic and application visibility, performance management, mediation, correlation and real-time analytics are necessary and critical capabilities. These capabilities 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.

As NFV moves from PoCs to field trials and commercial introductions, the spotlight will increasingly be on how monitoring and testing functions adapt to the newly virtualized world. Successful monitoring and testing products will deliver speed, scale, openness and compatibility with legacy physical networks.