An NFV Reality Check

Authored by

Sponsored by

Introduction

The traditional IT operational model is highly manual and very hardware centric. As a result, IT infrastructure services have historically been both expensive to provide and slow to respond to new requirements. Over the last few years, the pressure that virtually all IT organizations have felt to reduce cost and to be more responsive to new business requirements has driven both the adoption of new technologies, such as server virtualization, and the adoption of new ways of delivering IT services, such as cloud computing.

This white paper is part of a five-part series of white papers and webinars that describe the journey that IT organizations must take to go from the traditional highly manual, hardware centric IT operational model to an operational model that is highly automated, software centric and which reduces both the cost of IT infrastructure services as well as the time it takes to implement those services. This white paper will focus on a key component of that journey: Network Function Virtualization (NFV). NFV is a key component of that journey because the goal of NFV is to enable service providers to greatly simplify their operations and to reduce both CAPEX and OPEX by having all of the network functions they use available as virtual appliances that can be easily provisioned and integrated regardless of the vendor who provided the application or the hypervisor(s) on which it runs. In addition, while the term NFV is used in the context of service providers, similar concepts apply to enterprise IT organizations.

The previous white papers in this series, *The Mandate for a Highly Automated IT Function*[1]; *The Promise and the Reality of a Software Defined Data Center*[2]; and *An SDN Reality Check*[3] described some of the components of the journey to a new IT operational model. The primary goal of this white paper is to provide a reality check on NFV relative to its current ability to provide greater agility and elasticity. To achieve that goal, this white paper will describe the status of NFV development and adoption. The white paper will also identify the role of automation in a software defined network and will describe how NFV is related to DevOps and how that relationship is one more factor that is driving change in terms of the way that network organizations need to think about network service delivery.

---

[1] http://www.qualisystems.com/white_papers/the-mandate-for-a-highly-automated-it-function-2/

[2] http://ashtonmetzler.com/QS%20Paper%202%20V3%200%20(1).pdf

[3] http://ashtonmetzler.com/SDN%20Reality%20Check.pdf

Network Function Virtualization: The Enterprise Perspective

As described below, the initial push to get started with NFV came from services providers such as AT&T and Deutsche Telekom and service providers are still some of the primary drivers of NFV. While there are differences in areas such as the scale and the extent of the enabling technologies, enterprises face many of the same challenges that drove the service providers to initiate NFV. For example, the typical network is comprised of numerous L4 – L7 services such as:

- Application Delivery Controllers (ADCs);
- Firewalls;
- Intrusion Detection Systems/Intrusion Protection Systems (IDS/IPS);
- WAN Optimization Controllers (WOCs);
- Authentication, Authorization and Accounting (AAA) systems.

In a traditional data center implementing these L4 – L7 services is cumbersome and time consuming as it requires acquiring the requisite network appliances and cabling them together in the correct order. Since each appliance has its own unique interface, configuring these appliances is an error-prone task. In addition, IT organizations have two alternatives relative to sizing these appliances. They can either size the appliances for the peak application load or they can resize the appliances on a regular basis to account for shifts in the traffic load. The first alternative results in stranded capacity and the second alternative results in an increase in the amount of manual labor that is required.

The Open Networking Foundation[4] (ONF) is the group most closely associated with the standardization of SDN. SDN overcomes the challenges of implementing L4 – L7 services by implementing two closely related techniques that offer to enterprise IT organizations functionality that is similar to what NFV offers to service providers. Those techniques are service insertion and service chaining. The phrase *service insertion* refers to the ability to dynamically steer traffic flows to a physical or virtual server[5] that provides one of the L4 – L7 services that were listed above. The phrase *service chaining* refers to the ability to dynamically steer traffic flows through a sequence of physical or virtual servers that provide the same type of L4 – L7 services.

As discussed in *An SDN Reality Check,* SDN moves management functions out of the hardware and places them in controller software that runs in a virtual machine or on a physical server. A standardized configuration protocol between the controller and network devices replaces proprietary device configuration languages. As a result, entire service chains can be provisioned

[4] https://www.opennetworking.org/

[5] While it is possible to steer traffic to either a physical or a virtual appliance, the primary focus of service chaining is on services provided by virtual appliances.

and constantly reconfigured from the controller. In that scenario, the chance for error is much smaller since the controller software has an overall view of the network which reduces the chance for inconsistent device configurations.

Network Function Virtualization: The Role of ETSI

NFV is being driven primarily by telecommunications service providers to meet their specific requirements. Their interest in NFV stems from the fact that in the current environment, telecommunications and networking software is being run on three types of platforms:

- Industry standard servers running Linux or Windows;
- Virtual appliances running over hypervisors on industry standard hardware servers;
- Proprietary hardware appliances.

Telecommunications service providers feel that they can greatly simplify their operations and reduce expense if all network functions were available as virtual appliances that can be easily provisioned and integrated regardless of the vendor who provided the appliance or the hypervisor(s) on which it runs. In order to bring this vision to fruition, an Industry Specifications Group for Network Functions Virtualization (NFV ISG) was formed under the auspices of the European Telecommunications Standards Institute (ETSI). Their vision for the transition from hardware appliances of today to a fully virtualized appliance environment is depicted in Figure 1.

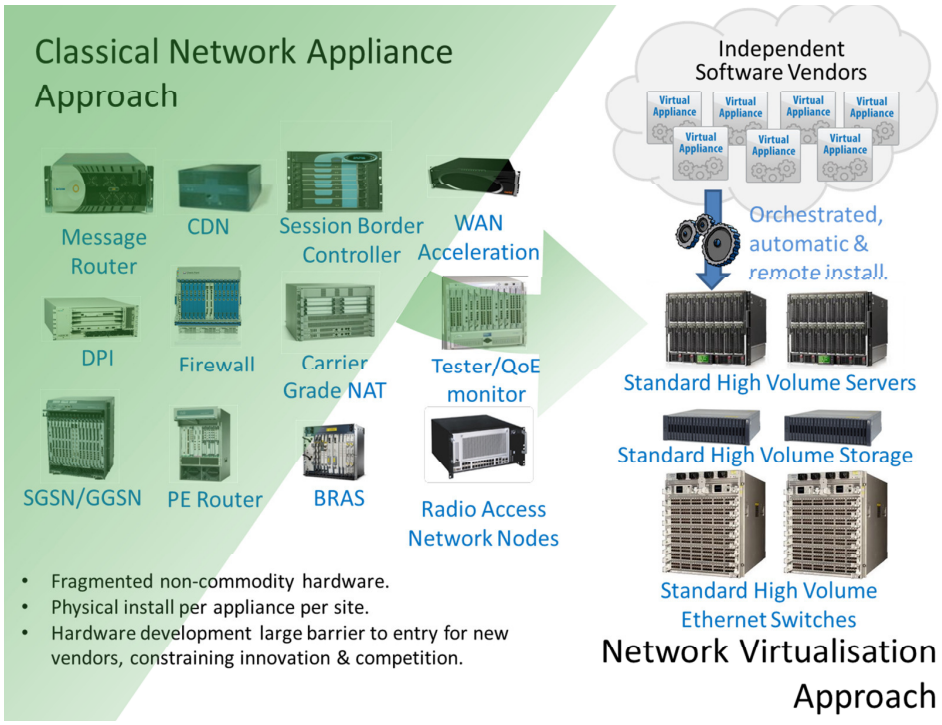

Figure 1: The Virtualization of Network Appliances **Source: NFV ISG**

The approach that the NFV ISG is taking is that the virtualization of network functionality is applicable to any data plane packet processing and control plane function in both fixed and mobile networks. As shown in Figure 1, examples of these functions include:

- Switching elements;
- Tunneling gateway elements: IPSec/SSL VPN gateways;
- Traffic analysis: DPI, QoE measurement;
- Service Assurance, SLA monitoring, Test and Diagnostics;
- Application-level optimization: ADCs, WOCs;
- Security functions: Firewalls, virus scanners, intrusion detection systems;
- Multi-function home routers and set top boxes;
- Mobile network nodes.

The initial members of the ETSI NFV ISG were service providers such as AT&T, Deutsche Telekom and NTT. Its membership[6] has since grown and now includes a number of equipment vendors. As pointed out in *Network Functions Virtualization: Network Operators Perspectives on Industry Progress*[7], "Although ETSI is a Standards Development Organization (SDO), the objective of the NFV ISG is not to produce standards. The key objectives are to achieve industry consensus on business and technical requirements for NFV, and to agree on common approaches to meeting these requirements. The outputs are openly published and shared with relevant standards bodies, industry fora and consortia to encourage a wider collaborative effort. The NFV ISG will collaborate with other SDOs if any standardization is necessary to meet the requirements."

The first meeting of the ETSI NFV ISG group was held in January 2013 and a number of smaller working groups were created in April 2013. In October 2013, ETSI published a set of high level reference documents that are described below. These documents are openly available on the ETSI website[8]:

- **NFV Terminology** document is a common repository for terms used within the NFV ISG documents and seeks to bridge the language gap between the software and networking industries.
- **NFV Requirements** document describes the high level business and technical requirements for an NFV framework including service models.
- **NFV Architectural Framework** document describes the high-level functional architecture and design philosophy for virtualized network functions and the underlying virtualization infrastructure.

6 http://portal.etsi.org/NFV/NFV_List_members.asp

7 http://portal.etsi.org/NFV/NFV_White_Paper2.pdf

8 http://www.etsi.org/nfv

- **NFV Use Cases** document describes initial fields of application selected to span the scope of technical challenges being addressed by the NFV ISG.
- **NFV ISG Proof of Concept Framework** document describes a procedure for industry participants to influence the work of the NFV ISG and to encourage growth of the NFV ecosystem through multi-party implementations of Proof of Concept demonstrations (PoCs).

The fact that NFV is largely driven by service provides to respond to service provider challenges was reflected in the set of NFV use cases that were discussed in *Network Functions Virtualization: Network Operators Perspectives on Industry Progress.* For example, one use case that was discussed in that document focused on content delivery networks. According to *Network Functions Virtualization: Network Operators Perspectives on Industry Progress,* "CDN service providers commonly deploy content caches near the edge of a network to improve customers' quality of experience. Today, caches use dedicated hardware on a per-CDN provider, per-operator basis. As hardware resources are dimensioned for peak load, such resources remain under-utilized for most of their lifetime as peak load is a temporal phenomenon. By utilizing and deploying virtualized caches, the underlying hardware resources could be consolidated and shared among multiple providers' CDN caches and potentially other VNFs [Virtual Network Functions] in a more dynamic way thus improving resources usage."

As previously mentioned, in addition to creating a POC framework, the ETSI NFV ISG document encourages growth of the NFV ecosystem through multi-party implementations of Proof of Concept demonstrations (PoCs). The Appendix to this white paper contains a summary of nine POCs currently underway under the auspices of the ETSI NFV ISG.

ONF and ETSI

Until recently, the conventional wisdom in the IT industry in general, and on the part of the ONF and ETSI in particular, was that was that SDN and NFV were separate topics and didn't need to be formally coordinated. That conventional wisdom changed in March 2014 when the ONF and ETSI announced the signing of a Memorandum of Understanding (MOU).

As part of the announcing the MOU[9], the ONF and ETSI said that "Together the organizations will explore the application of SDN configuration and control protocols as the base for the network infrastructure supporting NFV, and conversely the possibilities that NFV opens for virtualizing the forwarding plane functions." Also as part of the announcement, the ONF released a document entitled the *OpenFlow-enabled SDN and NFV Solution Brief*[10]. The solution brief showcases how operators are combining NFV and SDN to achieve the common

[9] http://www.rethink-wireless.com/2014/03/19/etsi-nfv-group-closer-operator-sdn.htm
[10] https://www.opennetworking.org/images/stories/downloads/sdn-resources/solution-briefs/sb-sdn-nvf-solution.pdf

goals of both technologies to achieve greater agility of the networks. It discusses the network challenges that operators will need to overcome to implement NFV, and presents use cases that demonstrate how OpenFlow-enabled SDN can meet the need for automated, open, and programmable network connectivity to support NFV.

NFV Challenges

The document entitled *OpenFlow-enabled SDN and NFV Solution Brief* identified some of the NFV-related challenges that result form using today's static, expensive-to-manage networks. These challenges are listed below. Of the challenges listed below, the first two apply primarily just to NFV. The other three challenges apply both to implementing NFV in service provider networks and to implementing SDN in enterprise networks.

1. NFV global reach and cross-administration. Connectivity that spans multiple administration domains and geographies is essential.
2. Carrier-grade scalability and robustness.
3. Real-time and dynamic provisioning. The virtual network functions must be automatically deployed and managed in the NFV infrastructure.
4. Seamless control and provisioning of physical and virtual networking infrastructures.
5. Openness and interoperability. Like SDN, NFV envision an open environment where network elements and VNFs from multiple vendors interoperate and co-exist through open interfaces (i.e., OpenFlow) and APIs.

DevOps and the Role of Automation

As explained in the white paper entitled *An SDN Reality Check*, the phrase *DevOps* is a result of bringing to together two words: *Development* and *Operations*. That's appropriate because the point of adopting DevOps is to establish tight collaboration between a number of the phases of the application development lifecycle, including application development, testing, implementation and ongoing operations. According to a recent Information Week Report[11], sixty-eight percent of IT professionals are aware of DevOps and of those who are aware of it, twenty-one percent have currently embraced it. That report also stated that eighty two percent of the IT organizations that implemented DevOps saw at least some improvement in infrastructure stability and eighty three percent saw at least some improvement in the speed of application development.

[11] http://www.informationweek.com/strategic-cio/executive-insights-and-innovation/state-of-devops-big-gains-elusive/d/d-id/1113307

DevOps is relevant to NFV because current network change cycles are typically managed in a slow, manual process following a waterfall development process. Often-times, months pass between points when network changes are certified. However, waterfall methodology and related timelines will likely be insufficient for the pace of incremental changes that will occur with the deployment of NFV. For example, as described above, NFV requires real-time and dynamic provisioning as well as the seamless control and provisioning of physical and virtual networking infrastructures. In addition, as was also described above, both NFV and SDN are intended to work in a multi-vendor environment.

A number of service providers who are implementing SDN and NFV have commented on the impact that those approaches will have on their organization and the need to move away from a slow, manual process. One such provider is Deutsche Telekom. In a recent article[12], Deutsche Telekom was quoted as saying: "DT [Deutsche Telekom] needs to build a team that comprises IP, datacenter, programming, and operations specialists that can work in small, empowered, and agile teams, while both the carriers and vendors need to adjust for the migration from hardware-based to software-based business models." AT&T's intended use of SDN and NFV is detailed in a white paper entitled "AT&T Vision Alignment Challenge Technology Survey: AT&T Domain 2.0 Vision White Paper[13]". As stated in that white paper "There remains much to do before this vision [Domain 2.0] can be implemented, including pivots from networking craft to software engineering, and from carrier operations models to cloud "DevOps" models. We also see an important pivot to embrace agile development in preference to existing waterfall models."

Conclusion

As mentioned in the introduction, IT organizations of all types are on a journey to adopt a new IT operational model that is highly automated. The white paper entitled *An SDN Reality Check*, explained the impact that DevOps has on SDN. The impact on NFV will be similar. In particular, as part of the agile application development process that is associated with DevOps, new virtualized functions, like the broad spectrum of ones depicted in Figure 1, will be continually added or modified. Automating the development through testing phases of those virtualized functions will be extremely complex in part because of the exceptionally large number of possible permutations of functions and service chains and because the functionality has to be tested in conjunction with everything else in the environment, including both new and traditional network technologies as well as new and traditional network architectures. In addition, it isn't sufficient to validate the new functionality just within a single domain. The functions must be ensured both within and across all of the relevant domains; i.e., networking, compute, storage, security. No organization will be successful with NFV without implementing

[12] http://www.lightreading.com/ethernet-ip/routers/deutsche-telekom-a-software-defined-operator/d/d-id/706099
[13] http://www.att.com/Common/about_us/pdf/AT&T%20Domain%202.0%20Vision%20White%20Paper.pdf

a sophisticated and automated DevOps approach to ensure the ongoing deployment and modification of virtual functionality.

Appendix
Status of POCs

The following table highlights the status of NVF POCs as of February 2014[14]. These PoCs exemplify the transition of the NFV ISG from specification to implementation. Each PoC consists of multi-vendor teams including at least one operator, and multiple NFV technology providers, including hardware, software, and silicon vendors. The NFV ISG encourages interested parties to submit new PoC proposals based on the freely available PoC framework. Table I below summarizes the NFV PoCs accepted by the NFV ISG to date[15].

NFV ISG PoC	**NFV Use Case**	**Operators**	**Vendors**
CloudNFV Open NFV Framework	Use Case #5 Virtualization of the Mobile Core and IMS	Sprint Telefonica	6Wind Dell Enterprise Web Huawei Mellanox Overture Qosmos
Service Chaining for NW Function Selection in Carrier Networks	Use Case #2 Virtual Network Function as a Service (VNFaaS) Use Case #4 Virtual Network Forwarding Graphs	NTT	Cisco HP Juniper
Virtual Function State Migration and Interoperability	Use Case #1 NFV Infrastructure as a Service (NFVIaaS)	AT&T BT	Broadcom Tieto
Multi-vendor Distributed NFV	Use Case #2 VNFaaS Use Case #4	CenturyLink	Certes Cyan Fortinet RAD

[14] http://www.sdncentral.com/education/nfv-insiders-perspective-etsi-part-4-marc-cohn/2014/02/
[15] http://www.sdncentral.com/education/nfv-insiders-perspective-etsi-part-4-marc-cohn/2014/02/

	Virtual Network Forwarding Graphs		
E2E vEPC Orchestration in a multi-vendor open NFVI environment	Use Case #1 NFVIaaS Use Case #5 Virtualization of the Mobile Core and IMS	Sprint Telefonica	Connectem Cyan Dell Intel
Virtualised Mobile Network with Integrated DPI	Use Case #2 VNFaaS Use Case #5 Virtualization of the Mobile Core and IMS Use Case #6 Virtualisation of Mobile base station	Telefonica	HP Intel Qosmos Tieto Wind River
C-RAN virtualisation with dedicated hardware accelerator	Use Case #6 Virtualisation of Mobile base station	China Mobile	Alcatel-Lucent Intel Wind River
Automated Network Orchestration	Use Case #1 NFVIaaS	Deutsche Telekom	Ericsson x-ion
VNF Router Performance with DDoS Functionality	Use Case #2 VNFaaS	AT&T Telefonica	Brocade Intel