Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2017, 4(10):293-296**

Review Article

ISSN: 2394-2630
CODEN(USA): JSERBR

Network Functions Virtualization

Matthew N. O. Sadiku[1], Nana K. Ampah[2]*, Sarhan M. Musa[1]

[1]Roy G. Perry College of Engineering, Prairie View A&M University, Prairie View, TX 77446
[2]Lone Star College, Kingwood, TX 77339

Abstract Network functions virtualization (NFV) is the idea of replacing dedicated hardware devices such as routers and firewalls with software running on commodity servers. It is a network architecture philosophy that utilizes standard virtualization technologies to manage networking functions using software. It is to run network functions on virtual machines. This paper provides a brief introduction to network functions virtualization.

Keywords network functions virtualization, virtual network function, virtualization

Introduction

Virtualization has emerged as a way of decoupling the software networking processing and applications from their hardware and allow network services to be implemented as software. Network functions virtualization (NFV) (also known as virtual network function (VNF)) is a new way of designing, deploying, and managing networking services. It is a technology designed to replace dedicated hardware middle boxes with virtualized network functions (VNFs), offering equivalent functionalities while leveraging the flexibility, manageability, cost-efficiency, and programmability of virtualization. This will allow NFV to replace a wide range of network devices, from switches and routers to firewalls and intrusion detection systems (IDS).

NFV is a way of reducing cost and accelerate service deployment for network operators by decoupling functions like a firewall or encryption from dedicated hardware and moving them to virtual servers. Any that service can be delivered on a specific hardware should be able to be done on a virtual machine that performs various functions. The major goal of NFV is to decouple network functions from dedicated hardware devices such as gateways, routers, and firewalls. With NFV, the amount of proprietary hardware that is needed to launch and operate network services will decrease. Network administrators will not need to purchase dedicated hardware devices in order to build a service chain.

The concept of NFV originated from service providers who were looking to accelerate the deployment of new network services and were applying standard IT virtualization technologies to their networks. These providers came together and created a group which was part of the European Telecommunications Standards Institute (ETSI). NFV was first introduced in a white paper presented by this group in October 2012 in Darmstadt, Germany. ETSI defines the NFV architectural framework as shown in Figure 1 [1].

Software-defined networking (SDN) is a concept related to NFV, but they refer to different domains. SDN is essentially an approach to build data networking equipment and software that separates and abstracts elements of these systems. It represents the next generation of infrastructure automation that is completely programmable and application-aware. NFV is not dependent on SDN and is possible to implement a virtualized network function (VNF) as a standalone entity. However, there are inherent benefits in leveraging SDN concepts to implement and manage an NFV infrastructure [2]. The trend of integrating SDN with NFV (to form the so-called software-defined NFV) to achieve various network control and management goals has seen a noticeable growth [3].

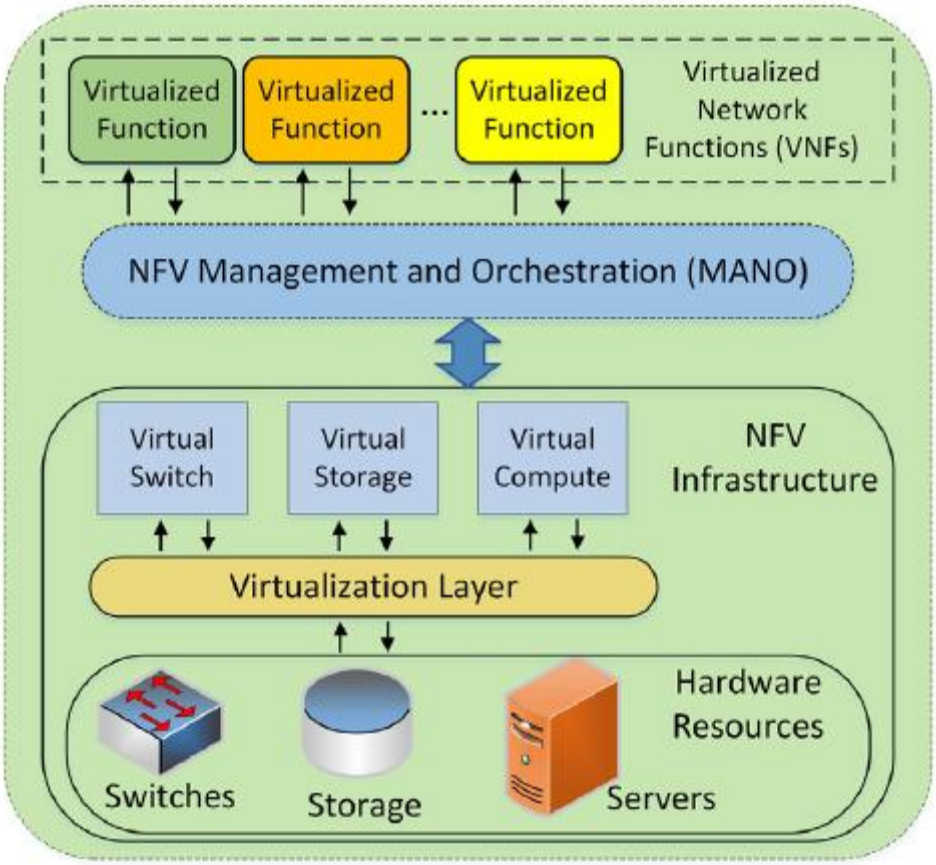

Figure 1: The NFV framework [1]

Recent efforts have been made to further leverage the cloud to enhance NFV. Thus, NFV is also regarded as an important technology that will enable the on-demand creation of cloud-based virtual mobile networks. NFV and cloud computing have emerged as key enablers to optimize resource utilization [4]. However, since there are privacy and security issues with using cloud computing, efforts have been made to allow for operating on encrypted data.

NFV Components

According to ETSI, the NFV Architecture has three key elements: Network Function Virtualization Infrastructure (NFVI), VNFs and MANO [5]:

- NFVI: Network functions virtualization infrastructure (NFVI), which can span several locations, is the totality of all hardware and software components that build the environment where VNFs are deployed. It provides the virtualization layer and the physical compute, storage, and networking components that host the VNFs.
- VNFs: Virtual Network Functions (VNFs) are software-based applications that provide one or more network services. The running of VNFs needs the instantiation of VNF Instances (VNFIs) that in general are software modules executed on virtual machines. A single VNF may be composed of multiple internal components, and hence it could be deployed over multiple virtual machines.
- Management and orchestration (MANO): This provides the overarching management and orchestration of the VNFs in the NFV architecture.

Benefits and Challenges

The potential benefits of NFV are expected to be significant. Perhaps the major advantage of using NFV is to reduce middle boxes (firewalls, network address translator, intrusion detection system, etc.) deployed in the traditional networks. This reduces cost and allows flexibility. NFV is expected to reduce capital expenditures

(CAPEX) and operational expenditures (OPEX), and accelerate time-to-market. Other benefits are speed, agility, and cost reduction. NFV utilize resources more effectively and achieve reduction of system complexity. It supports innovation by enabling services to be delivered via software on any standard server hardware.

In spite of the numerous benefits of NFV, there also exist some technical challenges triggered by the adoption of NFV. The virtualization challenges include [6]: 1) where to instantiate VNFIs; ii) how many resources to allocate to each VNFI; iii) how to route SFC requests to the appropriate VNFIs in the right sequence; and iv) when and how to migrate VNFIs in response to changes to SFC request intensity and location.

Existing CPU, memory, and network interface architectures cause network service performance to be sensitive to their placement within an NFV platform. Emerging NFV standards must confront the challenge of exposing certain platform architectural parameters to enable services to be orchestrated in an effective manner [7].

NFV faces security challenges (*e.g.*, multi-tenancy and live migration) which make it vulnerable to some cybersecurity attacks. Since software-based virtual functions can be controlled by an external entity, the whole network could be potentially compromised [1]. Other technical challenges in terms of instantiation, creation, programming, operation and management, and security of an overall network virtualization environment are yet to be investigated.

Conclusıon

NFV has emerged as a key technology for future wired and wireless networks. With NFV we are transforming the global communications network. Although the NFV paradigm is still in its infancy, it has attracted significant attention from both industry and academia as an important shift in telecommunication service provisioning. It promises to bring significant flexibility and cost savings to networking services.

NFV is different from software-defined networking (SDN) but is complementary to it. With the new open architecture that embraces the principles of SDN and NFV, service providers are able to maximize capital efficiencies. NFV is widely described as the biggest game changer in the telecommunication industry. Many service providers everywhere are embracing NFV and have announced support for NFV. A comprehensive introduction on NFV is provided in [8].

References

[1]. Firoozjaei, M. D., et al. (2017). Security challenges with network functions virtualization. *Future Generation Computer Systems*, 67:315–324.

[2]. "Network function virtualization," *Wikipedia*, the free encyclopedia https://en.wikipedia.org/wiki/Network_function_virtualization

[3]. Li, Y., & Chen, M. (2015). Software-defined network function virtualization: A survey. *IEEE Access*, 3:2542-2553.

[4]. Bilal, A., Vajda, A., & Tarik, T. (2016). Impact of network function virtualization: A study based on real-life mobile network data. *Proceedings of International* Wireless *Communications and Mobile Computing Conference* (IWCMC), 541-546.

[5]. Mijumbi, R., et al. (2016). Network function virtualization: State-of-the-art and research challenges. *IEEE Communications Surveys & Tutorials*, 18(1): 236-262, First Quarter.

[6]. Eramo, V., et al. (2017). An approach for service function chain routing and virtual function network instance migration in network function virtualization architectures. *IEEE/ACM Transactions on Networking*, 25(4):2008-2025.

[7]. Nemeth, B., et al. (2015). The limits of architectural abstraction in network function virtualization. *Proceedings of IFIP/IEEE International Symposium on Integrated Network Management*, 633-639.

[8]. Gray, K., & Nadeau, T. D. (2016). *Network Function Virtualization*, Morgan Kaufmann, Cambridge, MA.

Authors

Matthew N.O. Sadiku is a professor in the Department of Electrical and Computer Engineering at Prairie View A&M University, Prairie View, Texas. He is the author of several books and papers. His areas of research interests include computational electromagnetics and computer networks. He is a fellow of IEEE.

Nana K. Ampah is an adjunct faculty at Lone Star College, Kingwood, Texas. His research interests include enterprise network security, power optimization, smart grid and renewable energy. He is a member of IEEE.

Sarhan M. Musa is a professor in the Department of Engineering Technology at Prairie View A&M University, Texas. He has been the director of Prairie View Networking Academy, Texas, since 2004. He is an LTD Spring and Boeing Welliver Fellow.