Advances in Mathematics: Scientific Journal **9** (2020), no.6, 4059–4066
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.9.6.87 Spec Issiue on ICAML-2020

A ROAD TO NETWORK FUNCTION VIRTUALIZATION AND APPLICATIONS

K. KAUR[1], K. KUMAR, AND V. MANGAT

ABSTRACT. Network Function Virtualization (NFV) is a new network architecture where network functions that previously implemented on physical hardware called middleboxes or hardware appliances are now running into software on top of general-purpose or Commercial-Off-the-Shelf (COTS) server. The trend towards an innovative architecture initiated from the telecommunication industry and operators (manufactures, network, and carriers) in order to gain maximum benefits from virtualization technology. It not only provides agility and flexibility in the network, but also significantly reduces capital and operational cost. In this paper, state-of-the-art history of NFV is provided. In general, the paper presents the road towards the NFV and then shed lights on usecases of NFV in different fields.

1. INTRODUCTION

In recent years, network operators are facing challenges to provide efficient network services according to users demand on their traditional network equipment. The capital and operational expenditure (CAPEX & OPEX) for network operators are rising day by day with the increasing rate and diverse nature of demands. The network operator used various types of middleboxes such as HTTP proxy, NAT, gateway, and Session Border Controller to meet the Service

[1]*corresponding author*

2010 *Mathematics Subject Classification.* 68M10, 94A05.
Key words and phrases. middlebox, virtual network functions, virtualization, hypervisors, network function virtualization .

Level Agreement (SLA). In this static environment, deployment and use of middleboxes is very inconvenience to meet the enormous user demands. The use of middleboxes in the network is suffer from number of shortcomings such as i) an expensive ii) difficult to add new services iii) difficulty in connection management iv) more power and space cost v) dedicated functionality, [1].

To address the problems of traditional middleboxes, NFV is a new virtualized networking paradigm developed by Telecommunication industry. It converts the hardware appliances into its software version using virtualization technology as shown in Figure 1. Now, the network functions (Firewall, IDS, IPS, WAN optimizer, HTTP proxy, etc.) are running on general-purpose server instead of dedicated hardware, [2]. The network function in its virtual form is called Virtual Network Function (VNF). The network function in virtual form offers number of advantages such as i) low cost ii) easy to migrate from one location to another iii) sharing resources among multiple VNFs iv) easy deployment of new functions v) less power and space consumption, [3,4].

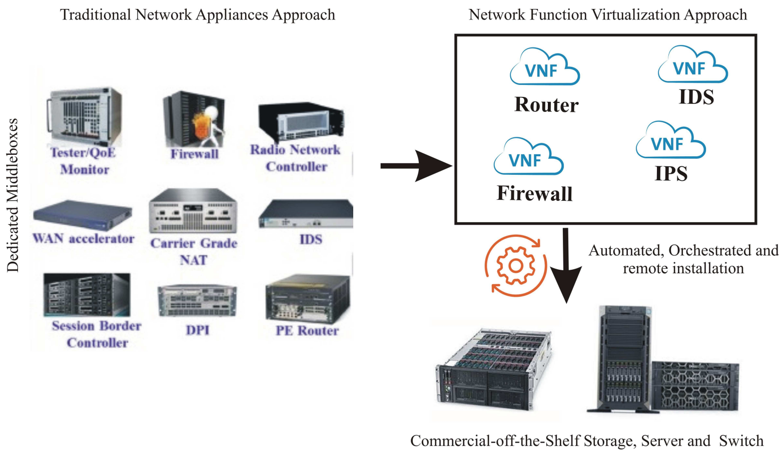

FIGURE 1. From physical hardware appliance to NFV based approach

The main contributions of this paper are to illustrate the detailed history of network function virtualization and shed lights on enormous use-cases in different fields. The structure of this paper organized in the following manner. The state-of-the-art history of network function virtualization technology describes in Section II. Section III provides various applications of NFV in different areas. The last section is used to conclude the paper.

2. History of Network Function Virtualization

This section discusses different technologies related to NFV and provide an overview of NFV with its advantages.

2.1. **Dedicated Server Model.** In this type of model, server consists of hardware resources, operating system, drivers and application.There is one to one relationship between application, operating system and hardware, and all the components are tightly coupled to each other. On a single hardware device, a single operating system such as Windows or Linux is installed and only single application such as Enterprise Resource Planning (ERP), Content Management System (CMS) etc. is installed (Figure 2(a)), [5]. To run second application, another server is used rather than installing it into same server. Furthermore, additional server is required for backup. This problem is known as server proliferation. Server proliferation leads to a number of problems for organizations such as increasing CAPEX and OPEX cost. There is only 10% to 15% utilization of server, more space is required, more power and cooling systems are required, [6].

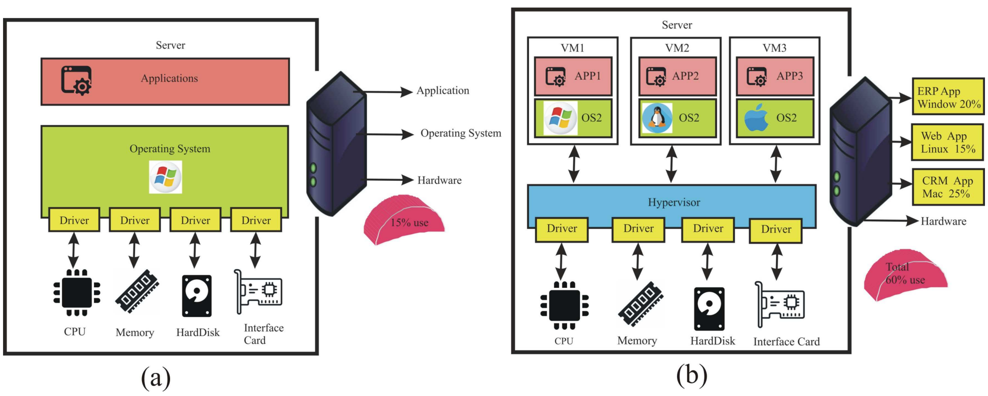

FIGURE 2. (a) Single OS, application running on single physical server (b) Multiple VMs running on hypervisor

2.2. **Virtualization as a solution to Server Proliferation.** Virtualization is a technology that is used to solve the problems of server proliferation. Virtualization means virtual version of something that can be hardware, network and functions. Using hardware virtualization, we can create multiple virtual instances consisting of different operating systems and applications on the same hardware as shown in Figure 2(b). This model offers increase in utilization of server, savings in cost, reduced power consumption and ease of maintenance. The main goal of virtualization is sharing the computer (compute, hardware, storage) among different users. There are basically three components that are needed to install a virtual machine (VM) on a computer: Host OS, Hypervisor (Type-I or Type-II) and guest OS, [7].

Type-I hypervisor is also called hardware level virtualization or Bare Metal virtualization. To install Type-I hypervisor (Citrix XEN, [8], VMware ESXI, [8], KVM, [9]), there is no need to install host OS. This is one of the biggest advantages that vulnerable layer of computer system has been removed. Type-I hypervisor directly interacts with the hardware to allocate the resources to VMs. Type-II hypervisor is also called host level virtualization [8]. Host operating system is needed to install Type-II hypervisor (VMware Workstation, [10], VirtualBox, [11]). These hypervisors are very easy to setup but they are not as secure as Type-I due to vulnerability of host OS. Type-II is also slow because it cannot directly interact with the hardware to allocate the resources to VMs.

2.3. **Network Virtualization (NV).** Network Virtualization, [12] is a type of virtualization that provides abstraction to network devices from the physical layer of the network. Network Virtualization allows network administrator to combine number of small physically separated networks into one virtual network or dividing a single large network into number of different logical groups. VLAN (virtual local area network) and VPN (Virtual private Network) are two technologies that comprise network virtualization.

2.4. **Network Function Virtualization (NFV).** In year 2012, ETSI developed Industry Specification Group for NFV, [13]. This technology is used to transform vendor-specific traditional network appliances into more flexible and agile software version contains same functionality as middlebox, [4]. The middlebox in virtual form is called virtual network function. There are number of virtual network functions such as video transcoder, load balancer, intrusion detection system (IDS), firewall, intrusion prevention system (IPS). Architectural framework of NFV allows us to convert hardware middlebox into same virtual function by means of VNFs. The main difference between NV and NFV is that NV is used to virtualize the network at layer 2 and 3 but NFV virtualizes the network at layer 4-7

3. Use Cases of NFV

There are a number of use cases of NFV that have been proposed by ETSI. In this section, we will discuss the most illustrative use cases. These are Virtual Customer Premises Equipment (v-CPE), virtual Evolved Packet Core (v-EPC), Virtual Gateway internet LAN (v-Gi-LAN).

3.1. Virtual Customer Premises Equipment (v-CPE).

Challenge: The deployment of new services in the network is very challenging when the infrastructure is inflexible. Moreover, it incurs CAPEX and OPEX costs to configure, and manage these CPEs at each location of the customer as shown in Figure 3(a). Moreover, if customer wants to change service or add more capacity, it is very cumbersome for service provider to configure and update the device.

Solution: To solve this issue, we can take advantage of NFV infrastructure and can deploy the network services in the cloud as v-CPE. The v-CPE is also called cloud CPE. In cloud model, pool of resources such as compute, storage is sharable among multiple virtual network functions. Using v-CPE, service provider can make the network agile, automated, cloud centred and delivery of services can be on demand as shown in Figure 3(b). Instances of virtual network function can be increased or decreased according to customer demand. All network functions can be deployed as a service such as DNS as a service (DNSaaS), Firewall as a service (FWaaS), etc., [2].

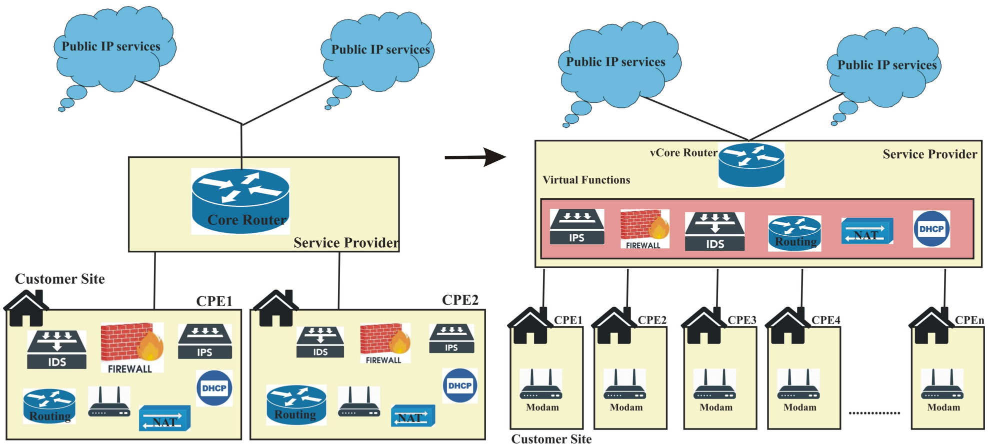

FIGURE 3. (a) Traditional CPE Model (b) CPE Model with the help of NFV

3.2. **Virtual Evolved Packet Core (v-EPC). Challenge:** Due to advancement in technology, mobile users and video traffic is increasing day by day in current networks as we move from 2G to 4G/LTE. To provide the services to mobile user with QoS, there is a need to architect the Evolved Packet Core (EPC) so that it can handle traffic and also ensure the QoS. All functions are based on proprietary hardware in EPC so management is very difficult because minor change in device requires a full replacement of that equipment. Moreover, these hardware devices are difficult to handle in a situation when replacement of devices is necessary, but compatibility issues occur.

Solution: v-EPC is an architecture that is used to virtualize the network functions that are required in the LTE (long term evolution) mobile network, [14]. Software version of EPC allows us to dynamically scale, update the network according to the requirements of mobile user, and to do so in an efficient manner.

3.3. **Virtual Gateway internet LAN (vGi-LAN). Challenge:** The area between packet gateway and internet is called Gi-LAN where service providers deploy their IP functions. Existing Gi-LAN architecture has number of problems such as hardware-based devices, non-flexible framework, requires long time for new services, and inefficient manual configuration. Moreover, communication service provider (CSP) uses devices from different vendors, so compatibility issues also occurs. CSPs use static service chaining that is pre-configured to forward the traffic from different subscribers as shown in Figure 4(a). CSP defines different service chain for different subscriber pool with the help of access point name (APN).

Solution: For better utilization of network resources, service function chaining should be dynamic with the help of SDN and NFV technology in the Gi-LAN network, [15]. SDN dynamically decides the service function path according to the traffic flow. Commercial-off-the-shelf server is used to deploy these network functions as a software version and then steer the traffic across different service function chains according to the input traffic as shown in Figure 4(b).

4. CONCLUSION

This paper introduced the background detail of Network Function Virtualization including different evolution stages. Moreover, we also discussed applications in different areas to highlights the advantages of this field. In the

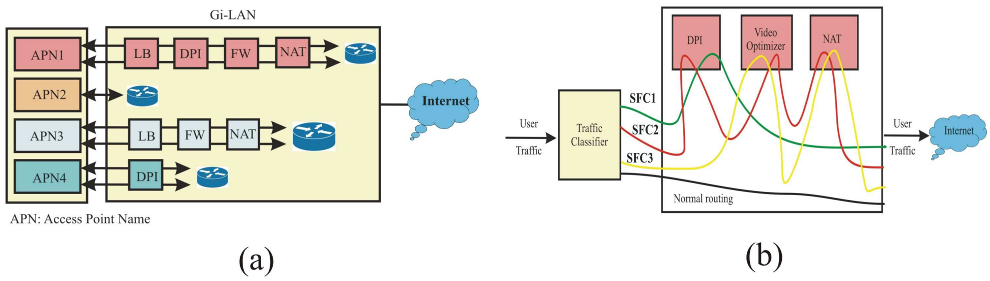

FIGURE 4. (a) Static service chaining in Gi-LAN (b) Dynamic service chaining

last, we concluded that NFV is based on virtualization technology that is widely adopted by Internet Service provider, Application Service Provider, Carrier Service Provider to offers services to users with minimum cost.

REFERENCES

[1] B. HAN, V. GOPALAKR : *Network Function Virtualization: Challenges and Opportunities for Innovations*, IEEE Commun. Mag., **53**(2) (2015), 90–97.

[2] R. MIJUMBI, J. SERRAT, J. L. GORRICHO, N. BOUTEN, F. DE TURCK, R. BOUTABA : *Network function virtualization: State-of-the-art and research challenges.*, IEEE Commun. Surv. Tutorials, **18**(1) (2016), 236–262.

[3] P. WILLETTS: *Network Functions Virtualization - Everything Old Is New Again*, Br. Journal. Rev. **18**(2) (2007), 53–58.

[4] J. SHERRY, S. HASAN, C. SCOTT, A. KRISHNAMURTHY, S. RATNASAMY, V. SEKAR: *Making middleboxes someone else's problem: Network Processing as a Cloud Service*, ACM SIGCOMM Comput. Commun. Rev., **42**(4) (2012), 13–24.

[5] J. DOHERTY: *SDN and NFV simplified: a visual guide to understanding software defined networks and network function virtualization*, Ist edn. Addison-Wesley Professional, 2016.

[6] A. A. ATEYA, A. MUTHANNA, I. GUDKOVA, A. ABUARQOUB, A. VYBORNOVA, A. KOUCHERYAVY: *Development of intelligent core network for tactile internet and future smart systems*, J. Sens. Actuator Networks, **7**(1) (2018), 1–20.

[7] R. MORABITO, J. KJÄLLMAN, M. KOMU: *Hypervisors vs. lightweight virtualization: A performance comparison.*, IEEE International Conference on Cloud Engineering, IC2E, (2015), 386–393.

[8] H. FAYYAD-KAZAN, L. PERNEEL, M. TIMMERMAN: *Benchmarking the Performance of Microsoft Hyper-V server, VMware ESXi and Xen Hypervisors.*, J. Emerg. Trends Comput. Inf. Sci., **4**(12) (2013), 922–933.

[9] J. P. WALTERS, A. J. YOUNGE, D. I. KANG, K. T. YAO, M. KANG, S. P. CRAGO, G. C. FOX: *GPU passthrough performance: A comparison of KVM, Xen, VMWare ESXi, and LXC for*

CUDA and openCL applications., IEEE 7th International Conference on Cloud Computing, (2014), 636–643.

[10] VMware Workstation, https://my.vmware.com/. Last accessed 24 April 2020

[11] Oracle VirtualBox, https://www.virtualbox.org/. Last accessed 24 April 2020

[12] N. M. M. K. CHOWDHURY, R. BOUTABA : *A survey of network virtualization*, Comput. Networks, **54**(5) (2010), 862–876.

[13] European Telecomunication Standard Institute, https://www.etsi.org/technologies/nfv. Last accessed 24 April 2020

[14] Virtual Evolved Packet Core (v-EPC), https://www.nec.com/en/global/solutions/tcs/vepc /index.html. Last accessed 24 April 2020

[15] Y. TURK, E. ZEYDAN: *An Implementation of Network Service Chaining for SDN-enabled Mobile Packet Data Networks*, IEEE International Symposium on Networks, Computers and Communications (ISNCC), (2019), 1–6.

DEPARTMENT OF INFORMATION TECHNOLOGY
UIET, PANJAB UNIVERSITY
CHANDIGARH
Email address: bhullar1991@gmail.com

DEPARTMENT OF INFORMATION TECHNOLOGY
UIET, PANJAB UNIVERSITY
CHANDIGARH
Email address: k.salujauiet@gmail.com

DEPARTMENT OF INFORMATION TECHNOLOGY
UIET, PANJAB UNIVERSITY
CHANDIGARH
Email address: vmangat@pu.ac.in