Network Function Virtualization: A Survey

Shreyas Prabhakar
Computer Science Department
Clemson University
Clemson, United States of America
sprabha@clemson.edu

***Abstract* — Diverse proprietary network appliances increase both the capital expenses (CAPEX) and operational expenses (OPEX) of service providers, meanwhile causing problems of network ossification. To address these issues, Network function virtualization (NFV) was introduced. NFV is a new network architecture framework where network functions that traditionally used dedicated hardware (middleboxes or network appliances) are now implemented in software that runs through the virtual machines (VMs) on top of general purpose hardware such as high volume servers or cloud computing infrastructure. NFV emerges as an initiative from the industry (network operators, carriers, and manufacturers) in order to increase the deployment flexibility and integration of new network services with increased agility within operator's. NFV promotes virtualizing network functions such as transcoders, firewalls, and load balancers, among others, which were carried out by specialized hardware devices and migrating them to software based appliances. Integrated with Software Defined Networking (SDN), the software defined NFV architecture further offers agile traffic steering and joint optimization of network functions and resources. One of the major challenges for the deployment of NFV is the resource allocation of demanded network services in NFV-based network infrastructures. As with any new technology there are potential security challenges related to NFV. The NFV paradigm is still in infancy and there is a large spectrum of research opportunities to develop new architectures, systems and applications based on NFV, and to evaluate alternatives and trade-offs in developing technologies for its successful deployment. The resource allocation and security threats related to NFV are also some of the research challenges that needs to be addressed.**

Keywords—Network Function Virtualization; NFV; Network Functions; Security; Resource Allocation

I. INTRODUCTION

Service provision within the telecommunications industry has traditionally been based on network operators deploying physical proprietary devices and equipment for each function that is part of a given service. In addition, service components have strict chaining and/or ordering that must be reflected in the network topology and in the localization of service elements. These, coupled with requirements for high quality, stability and stringent protocol adherence, have led to long product cycles, very low service agility and heavy dependence on specialized hardware. However, the requirements by users for more diverse and new (short-lived) services with high data rates continue to increase. Therefore, Telecommunication Service Providers (TSPs) must correspondingly and continuously purchase, store and operate new physical equipment. This lead to high CAPEX and OPEX for TSPs. Therefore, TSPs have been forced to find ways of building more dynamic and service-aware networks with the objective of reducing product cycles, operating & capital expenses and improving service agility.

NFV has been proposed as a way to address these challenges by leveraging virtualization technology to offer a new way to design, deploy and manage networking services. The main idea of NFV is the decoupling of physical network equipment from the functions that run on them. This allows for the consolidation of many network equipment types onto high volume servers, switches and storage, which could be located in data centers, distributed network nodes and at end user premises. This way, a given service can be decomposed into a set of Virtual Network Functions (VNFs), which could then be implemented in software running on one or more industry standard physical servers. The VNFs may then be relocated and instantiated at different network without necessarily requiring the purchase and installation of new hardware.

NFV promises TSPs with more flexibility to further increase their network capabilities and services, and the ability to deploy or support new network services faster and cheaper to realize better service agility. To achieve these benefits, NFV paves the way to several differences in the way network service provisioning is realized in comparison to current practice. In summary, these differences are as follows:

1. Decoupling software from hardware.
2. Flexible network function deployment.
3. Dynamic scaling.

The European Telecommunications Standards Institute (ETSI) has proposed several use cases for NFV. The Figure 1 shows a typical (current) implementation of a Customer Premises Equipment (CPE) which is made up of functions like Dynamic Host Configuration Protocol (DHCP), Network Address Translation (NAT), routing, Universal Plug and Play (UPnP), Firewall, Modem, radio and switching. These functions may have precedence requirements. For example, if the functions are part of a service chain, it may be required

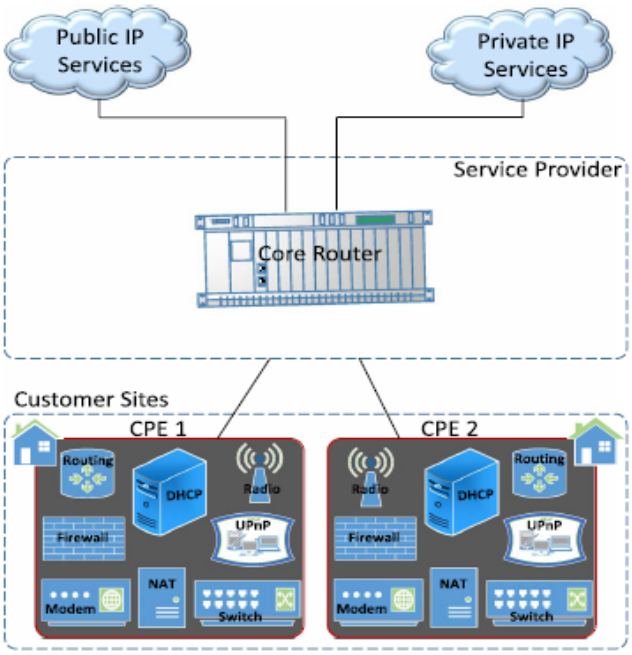

Fig1. Traditional CPE implementation

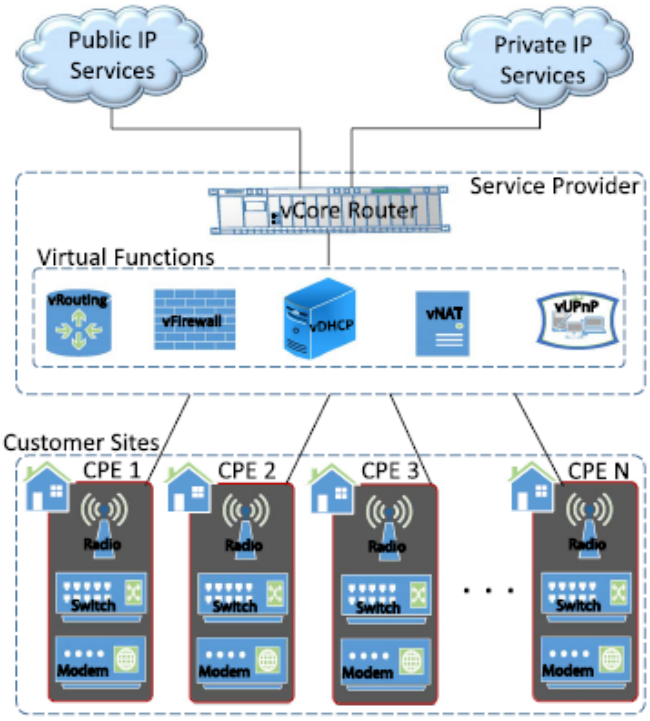

Fig2. Possible CPE implementation with NFV

to perform firewall functions before NAT. Currently, it is necessary to have these functions in a physical device located at the premises of each of the customers 1 and 2. With such an implementation, if there is a need to make changes to the CPE, say, by adding, removing or updating a function, it may require a complete change of devices. This becomes expensive for both the customers and the Internet Service Providers (ISPs). In Figure 2, we show a possible implementation based on NFV in which some of the functions of the CPE are transferred to a shared infrastructure at the ISP, which could also be a datacentre. This makes the changes described above easier since, for example, updating the DHCP for all customers would only involve changes at the ISP. In the same way, adding another function such as parental controls for all or a subset of customers can be done at once. In addition to saving on operational costs for the ISP, this potentially leads to cheaper CPEs if considered on a large scale.

II. Network Function Virtualization

A. *A Brief Overview of NFV*

The first white paper on NFV was published in October 2012 soon after the foundation of the NFV ISG. Nowadays, NFV ISG has developed to over 270 companies containing 38 service providers and greatly forwarded the development of NFV. The first NFV ISG output documents were released in October 2013 to provide guidance on the industry progress on NFV. A call for Proof of Concept (PoC) was launched to build an open ecosystem for NFV, and 38 PoC projects have been conducted by NFV ISG since then.

B. *NFV Architecture*

According to ETSI, the NFV Architectural framework includes multiple functional components, such as – 1. Network Function Virtualization Infrastructure (NFVI), Virtual Network Functions and NFV Management and Orchestration (NFV MANO). The NFV architecture is shown graphically in Figure 3.

- *NFV Infrastructure (NFVI)* – The NFVI is the combination of both hardware and software resources which make up the environment in which VNFs are deployed. The physical resources include commercial-off-the-shelf (COTS) computing hardware, storage and network (made up of nodes and links) that provide processing, storage and connectivity to VNFs. Virtual resources are abstractions of the computing, storage and network resources. The abstraction is achieved using a virtualization layer (based on a hypervisor), which decouples the virtual resources from the underlying physical resources. In a data centre environment, the computing and storage resources may be represented in terms of one or more Virtual Machines (VMs), while virtual networks are made up of virtual links and nodes. A virtual node is a software component with either hosting or routing functionality, for example an operating system encapsulated in a VM. A virtual link is a logical interconnection of two virtual nodes, appearing to them as a direct physical link with dynamically changing properties.
- *Virtual Network Functions and Services* – A NF is a functional block within a network infrastructure that

as well defined external interfaces and well-defined functional behaviour. Examples of NFs are elements in a home network, e.g. Residential Gateway (RGW); and conventional network functions, e.g. DHCP servers, firewalls, etc. Therefore, a VNF is an implementation of an NF that is deployed on virtual resources such as a VM. A single VNF may be composed of multiple internal components, and hence it could be deployed over multiple VMs, in which case each VM hosts a single component of the VNF [5]. A service is an offering provided by a TSP that is composed of one or more NFs. In the case of NFV, the NFs that make up the service are virtualized and deployed on virtual resources such as a VM. However, in the perspective of the users, the services—whether based on functions running dedicated equipment or on VMs—should have the same performance. The number, type and ordering of VNFs that make it up are determined by the service's functional and behavioural specification. Therefore, the behaviour of the service is dependent on that of the constituent VNFs.

- *NFV Management and Orchestration (NFV MANO)* – According to the ETSI's MANO framework, NFV MANO provides the functionality required for the provisioning of VNFs, and the related operations, such as the configuration of the VNFs and the infrastructure these functions run on. It includes the orchestration and lifecycle management of physical and/or software resources that support the infrastructure virtualization, and the lifecycle management of VNFs. It also includes databases that are used to store the information and data models which define both deployment as well as lifecycle properties of functions, services, and resources. NFV MANO focuses on all virtualization-specific management tasks necessary in the NFV framework. In addition, the framework defines interfaces that can be used for communications between the different components of the NFV MANO, as well as coordination with traditional network management systems such as Operations Support System (OSS) and Business Support Systems (BSS) so as to allow for management of both VNFs as well as functions running on legacy equipment.

The implementation of NFV faces a few major challenges. For example, how to manage and orchestrate all virtual resources and how to integrate the virtual resources so they are compatible with existing platforms. The implementation requirements are addressed by the NFV virtualization requirements document. To guarantee the service availability and maintain resiliency in NFV, automated recovery from failures should be enabled. Some related open source projects have made contributions to the growth of NFV, for example, OpenDaylight and OpenStack. Open Platform for NFV (OPNFV) aims at developing open source projects to overcome the implementation challenges.

There has been a rapidly increasing interest in NFV. Current NFV trending research topics include secure, reliable, energy efficient NFV architectures, and performance optimization for NFV. There are many use cases for NFV, such as virtualization of mobile core network and IMS, virtualization of home and enterprise networks, virtualization of content delivery networks, and fixed access NFV. Cloud computing and industry standard high volume servers contribute to the realization of NFV.

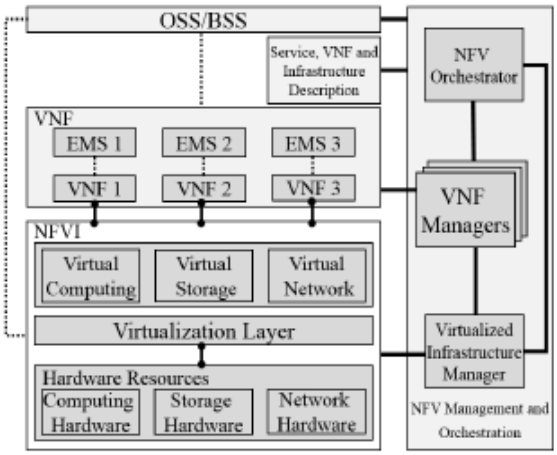

Fig 3. Architecture Framework of NFV.

The infrastructure layer consists of switching devices such as routers and switches, and other network hardware resources in the data plane. The main functionality of this layer is data forwarding based on the instructions provided by the control layer. This layer is also responsible for collecting network status, storing them temporarily and forwarding them to the controller. This status may include network traffic statistics, network usage and network topology.

III. Challenges In NFV

Even with all the anticipated benefits, and despite the immense speed at which it is being accepted by both academia and industry, NFV is still in early stages. There still remain important aspects that should be investigated and standard practices which should be established. This section discusses crucial research directions that will be invaluable as NFV matures.

A. Security Challenges

NFVI suffers from both internal and external security threats. Internal threats result from inappropriate operations of people and it can be avoided by following strict operational procedures. External threats exist because of design or implementation vulnerabilities. To solve this problem, the NFVI devices should have a security certification process to eliminate possible threats. The security of the NFVI should be ensured by the NFV framework. In addition, NFVI should adopt standard security mechanisms for authentication, authorization, encryption and validation.

Defining standard interfaces for various security functions is a big challenge when implementing security services in a virtualized network platform. Monitoring and managing the NFVI and VNFs for security reason is a challenge since they

are much more complex and dynamic in the virtualized environment. Security issues also exist in the management of VNFs, such as managing and maintaining consistent configurations of VNFs, and seamlessly transferring the state information from one VNF to another.

B. Challenges in Resource Allocation

Resource allocation in NFV requires efficient algorithms to determine on which HVSs VNFs are placed, and be able to migrate functions from one server to another for such objectives as load balancing, reduction of CAPEX and OPEX, energy saving, recovery from failures, etc.

In the NFV architecture framework the component that performs the resource allocation is the orchestrator. The orchestrator evaluates all the conditions to perform the assignment of VNFs chains on the physical resources, leaning on the VNF managers and the virtualized infrastructure managers. The resource allocation in NFV is carried out in three stages: 1) VNFs Chain composition (VNFs-CC), also known in the literature as Service Function Chaining 2) VNF Forwarding Graph Embedding (VNF-FGE)2 and 3) VNFs Scheduling (VNFs-SCH).

C. Research Challenges

- *Management and Orchestration* – The current approaches are focused on NFV management without considering management challenges of SDN. Traditional Management approaches must be improved to accommodate each of them. In these cases, we not only need to create dynamic traffic flows, but the switching points also change dynamically. Finally, while the ETSI-proposed NFV MANO framework considers the management and orchestration requirements of both virtualized and non-virtualized functions via interfaces to traditional network management functions OSS/BSS, the relationship between them is yet to be fully defined.

- *Energy Efficiency* - NFV will put InPs under even more pressure to manage energy consumption not to only to cut down energy expenses, but also to meet regulatory and environmental standards. Topics about energy efficient hardware which could allow reductions in CPU speeds and partially turning off some hardware components, more energy-aware function placement, scheduling and chaining algorithms, will be important. All these should be carefully considered to ensure that there is a balance in the trade-off between energy efficiency and function performance or service level agreements.

Since we are in the early stages of NFV, there are still a lot of challenges that needs to be fixed, hence there is a lot of scope for research related to NFV, other than the ones mentioned above, like the NFV Performance, NFV Implementation, modelling of resources, functions and services. There is also lot of work to be done related to working in conjunction with Cloud Computing and Software Defined Networking (SDN).

IV. CONCLUSION

Due to user demands for real-time, on-demand, online, inexpensive, short-lived services, TSPs have been forced to look for new ways of delivering these services in ways that are agile, and with OPEX and CAPEX savings. NFV has emerged as a possible approach to make network equipment more open, and hence allow TSPs to become more flexible, faster at service innovations and reduce operation & maintenance costs. It is clear that NFV, together with the closely related and complementary fields of SDN and cloud computing may be big parts of future telecommunication service provision.

In this paper, we introduced NFV in Section 1. In section 2, we described its architecture as defined by ETSI and briefly explained the major functional blocks of NFV architecture. We talked about the challenges related to NFV in Section 3. We talked about the challenges relate to security in NFV in Section 3.A., Challenges in Resource Allocation in section 3.B., and then some of the research challenges pertaining to NFV in section 3.C., like the challenges in Management and Orchestration and Energy Efficiency.

V. REFERENCES

[1] R. Mijumbi, J. Serrat, J. L. Gorricho, N. Bouten, and F. De Turck, “Network Function Virtualization: State-of-the-Art and Research Challenges,” IEEE Communications Surveys and Tutorials, vol. 18, pp. 236-262, 2016.

[2] W. Yang, and C. Fung, “A Survey on Security in Netwrok Functions Virtualization,” IEEE NetSoft Conference and Workshops, pp.15-19, 2016.

[3] J. G. Herrera, and J. F. Botero, “Resource Allocation in NFV: A Comprehensive Survey,” IEEE Transactions on Network and Service Management, vol. 13, pp. 518-532, 2016.

[4] Y. Li, and M. Chen, “Software-Defined Network Function Virtualization: A Survey,” IEEE Access Journal, vol. 3, pp. 2542-2553, 2015.

[5] N. M. M. K. Chowdhury and R. Boutaba, “Network virtualization: State of the art and research challenges,” IEEE Communications Magazine, vol. 47, no. 7, pp. 20-26, 2009.

[6] R. Guerzoni et al., “Network functions virtualisation: An introduction, benefits, enablers, challenges & call for action,” Proceedings in SDN OpenFlow World Congress, pp. 1-16, 2012.

[7] C. Price and S. Rivera, “Opnfv: An open platform to accelerate NFV,” White Paper, 2012.

[8] B. Han, V. Gopalakrishnan, L. Ji, and S. Lee, “Network function virtualization: Challenges and opportunities for innovations,” IEEE Commun. Mag., vol. 53, no. 2, pp. 90–97, 2015.