

## **General Perspective of Network Functions Virtualization**

Sérgio Pinto

Specialist Professor

*ISTEC - Instituto Superior de Tecnologias Avançadas*

### **Abstract:**

The Network Functions Virtualization (NFV) enables the emulation of Virtual Network Functions (VNFs) through SW configured over physical and sharable resources of generic HW, referred as COTS (Commercial off-the-shelf). Therefore, NFV replaces the traditional concept of network services implemented on dedicated HW and came to allow not only significant reductions in equipments acquisition (CAPEX) and operational costs (OPEX), but also to enable

a bigger agility and speed in the development and management of network services composed by VNFs.

**Keywords:** Network Functions Virtualization (NFV), Virtual Network Functions (VNF), Network Functions Virtualization Infrastructure (NFVI), Virtual Machine (VM), virtualization.

### **Introduction**

The Network Functions Virtualization (NFV) is a new way of design, deploy and manage network services by decoupling the physical network equipments from the functions that run on them. For this purpose, as it can be seen in Figure 1, network functions as firewalls, routers or NAT are SW emulated in VNFs configured on standard and generic physical HW resources (COTS), sharable by several VNFs. Therefore,

the NFV came to allow the replacement of the traditional concept of network functions deployed on dedicated HW and the splitting and abstraction of network functions from the physical infrastructure that supports them.

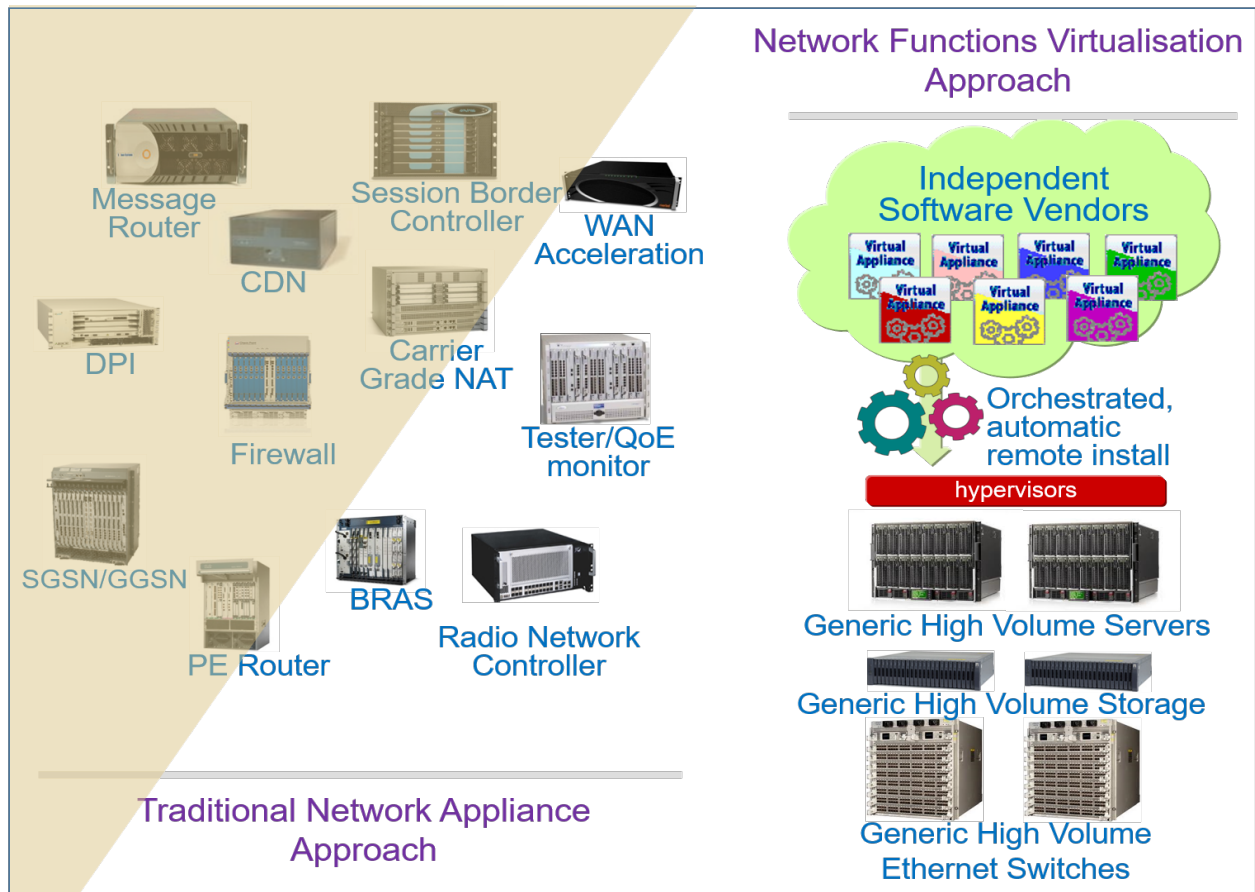


Figure 1: Traditional and NFV networks

Based on its features, the NFV came also to potentiate significant reductions in equipments acquisition (CAPEX) and networks operations (OPEX). These costs reductions are potentiated by the use of generic and sharable HW (COTS), which gives the possibility to reduce the usually significant times for new equipments acquisition, installation and integration tests, typical of the traditional scenario of network functions deployed on dedicated HW. Therefore, the NFV came also to allow a better operational efficiency (lower OPEX), not only by the increased physical resources uniformization: standards and non-proprietary (COTS), but also for the possibility of resources sharing and consequent total necessary equipments reduction and respective power consumption.

Finally, the NFV came also to allow an increased agility and faster network functions management by supporting its emulation and configuration, with possible instantiation and automatic capacity increase, without the need of new physical equipments (HW) acquisition. For instance, the network operators might run a SW to emulate on a VNF a firewall function in a Virtual Machine (VM) on a standard server (locally or remotely in Data Centres), which might be managed (for instance, configured, expanded, replicated) without the need of any relevant changes on its support physical infrastructure.

## NFV Architecture

The NFV architecture was defined by the ETSI ISG (Industry Specification Group) NFV group, being composed by the three main elements, identified in Figure 2:

- Virtual Network Functions (VNFs):  
The VNFs are software implementations of network functions that are deployed on virtual resources such as Virtual Machines (VM), that emulate a traditional network element, like a firewall, with all its functionalities. The VNFs might run as applications on one or several VMs, over the network HW support infrastructure, that might include routers, switches, servers, cloud computing systems and others. One network service is usually setup based on several VNFs, that might emulate different network functions.
- Network Functions Virtualization Infrastructure (NFVI):  
The NFVI consists of computing, storage and network interfaces on HW and virtual on SW (vCPU, vMem and vNIC). Between these two types of resources is located the virtualization layer that controls the VNFs (and respective VMs) access to the physical resources, via VM Monitors (hypervisors), that allows the splitting and abstraction of the physical resources allocated to the VNFs. It is the combination of both HW and SW resources which build up the environment in which VNFs are deployed, managed and executed.  
The NFVI can span across several locations e.g. places where NFVI PoPs are operated, but should be seen by the users as a common network infrastructure. Additionally, the network providing connectivity between these locations should also be regarded to be part of the NFVI.

- NFV Management and Orchestration functions (NFV MANO):

Provides the necessary tools to allow an automated management of the virtualized resources, namely, the VNFs life cycle via instantiation procedures (onboarding), automated dimensioning (scaling out/in) and VNFs removal. These procedures are made based on predefined descriptors, that contains each VNF requirements for virtual resources (vCPU, vMem, vNIC) and monitoring elements (KPIs, statistics, events).

Additionally, this element also allows the orchestration of NFVI resources allocated to the different VNFs under its control, including communication flows (VNF Forwarding Graph) in order to support the deployment of E2E network services.

In respect to the traditional scenario of network functions setup on dedicated HW, the NFV architecture came to allow the introduction of the following main features:

- Splitting of HW from SW:  
In order to allow the software to evolve independently from the hardware, and vice versa. Therefore, the SW tends to be a more valuable and differentiator element than the HW.
- Flexible deployment of network functions:  
The NFV aims to allow an automatically deployment of network functions in SW from a pool of HW resources, in different times and locations (locally or remotely on Data Centres)
- Dynamic network services provisioning:  
Taking advantage from the previous feature, NFV aims to allow network operators to dynamically and automated, on a grow-as-you-need basis, dimension the VNFs that compose a certain service.

Additionally, the described features should also allow not only the emulation of several VNFs in only one physical network element, but also a VNF decomposition into smaller functional blocks, in order to facilitate its reuse and adaptation to different network services requirements.

Therefore, the NFV architecture came also to allow a resilience and flexibility increase for the network services.

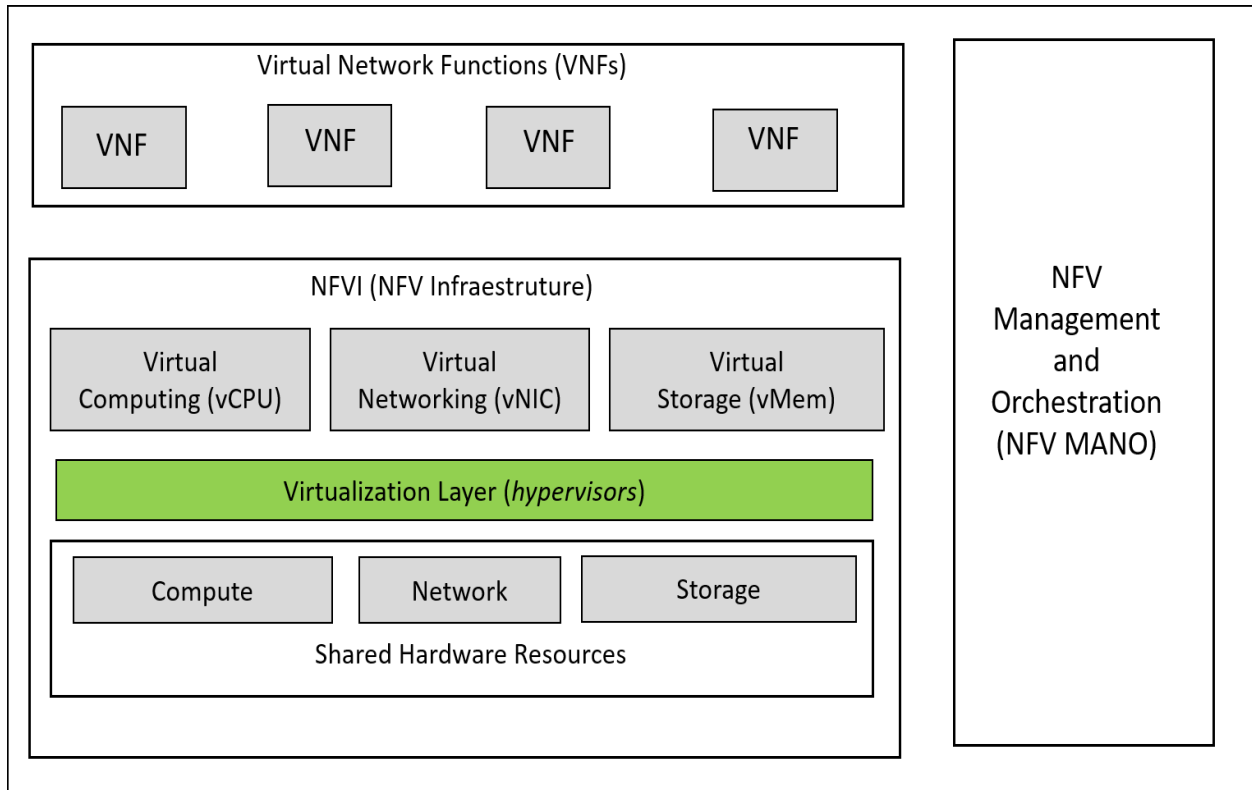


Figure 2: NFV simplified architecture

Finally, for this architecture success two enablers should be highlighted as NFVs triggers:

1) Availability of industry-standard servers (COTS):

This availability facilitates servers and their components acquisition with lower costs, potentiates a higher HW uniformity and life-cycle extension, by allowing SW updates that emulates VNFs on the same

HW. Finally, it should also reduce HW O&M costs.

2) Technologies developed for cloud computing:

Recent developments of cloud computing functionalities, such as various hypervisors, like VMWare, also make NFV more achievable in reality.

It should be noted that NFV is closely related to other emerging technologies, like SDN (*Software Defined Network*). SDN is a networking technology that decouples the control plane from the underlying data plane and consolidates the control functions into a logically centralized controller. NFV and SDN are mutually beneficial, highly complementary to each other, and share the same purpose of

promoting innovation, creativity, openness and competitiveness. These two solutions can be combined to create greater value. For example, SDN can support NFV to enhance its performance, facilitate its operation and simplify the compatibility with legacy deployments.

### **Potencial NFV risks**

Some NFV features might originate possible risks for this technology success, mainly, for being applied to telecommunications services with QoS requirements usually more demanding than the required for traditional IT services. Below are described some of these features and the corresponding measures that should be taken to minimize the occurrence of the associated risks:

- Shared infrastructures:
  - Safe isolation between the different VNFs, mainly in the operators' cloud domain, in order to guarantee an efficient physical resources sharing.
  - Efficient resources allocation and reservation to avoid a VNFs QoS requirements non-compliance or even a possible complete failure of the VNFs supported services.
  
- HW resources isolation:
  - Proper HW resources monitoring in order to facilitate trouble-shooting tasks

and minimize possible problems impacts.

- Definition of O&M processes and responsibilities for the different elements that compose NFV architecture (Figure 2), in order to guarantee a fast response time in case of problems detection scenarios.
- 
- Delays originated by the virtualization layer:
    - The deployment of usual telecommunications features, with more demanding requirement for data processing (e.g. transcoding, encryption) or QoS (e.g. media traffic of real time services, interactive services) might require specific HW usage with better performance, more suitable to fulfill these features.

**Example of a possible NFV application: virtualization of home network**

The telecommunications operators usually offer services to their residential clients via dedicated equipments located in the clients' locations, named CPEs (Customer Premise Equipment). Usually, these CPEs include Set-Top-Boxes (STBs) for multimedia services support, and Residential Gateways (RGs) for internet access support.

As described in Figure 3, the emerging NFV technology came to potentiate a possible virtualization of residential services allowing the migration of some CPE features to VNFs (vSTB and vRG) in a NFV cloud. Therefore, either STBs, or some RGs features, such as: firewall, gateway VPN and NAT, used mainly by operators without own access networks, might be migrated to remote servers in Data Centres. This migration allows the operators to install in the clients' premises simpler and cheaper equipments. These equipments should have as main purpose to assure the clients' terminals connectivity to the operator services network

and for its simplicity also having lower maintenance cost.

This virtualized architecture aims to allow advantages for both operators and their residential clients. For the operators, for potentiating CPEs acquisition and operational costs reductions, mainly because they become simpler and therefore with reduced need for O&M procedures. For the clients, for allowing a better usage experience by increasing their personal contents storage capacity in the NFV cloud and for potentiate the access to the same contents from different terminals and access networks (e.g. wireless networks). For both, it should facilitate the launch and the adherence to new services in a smoother way, since it minimizes their dependence from CPEs features.

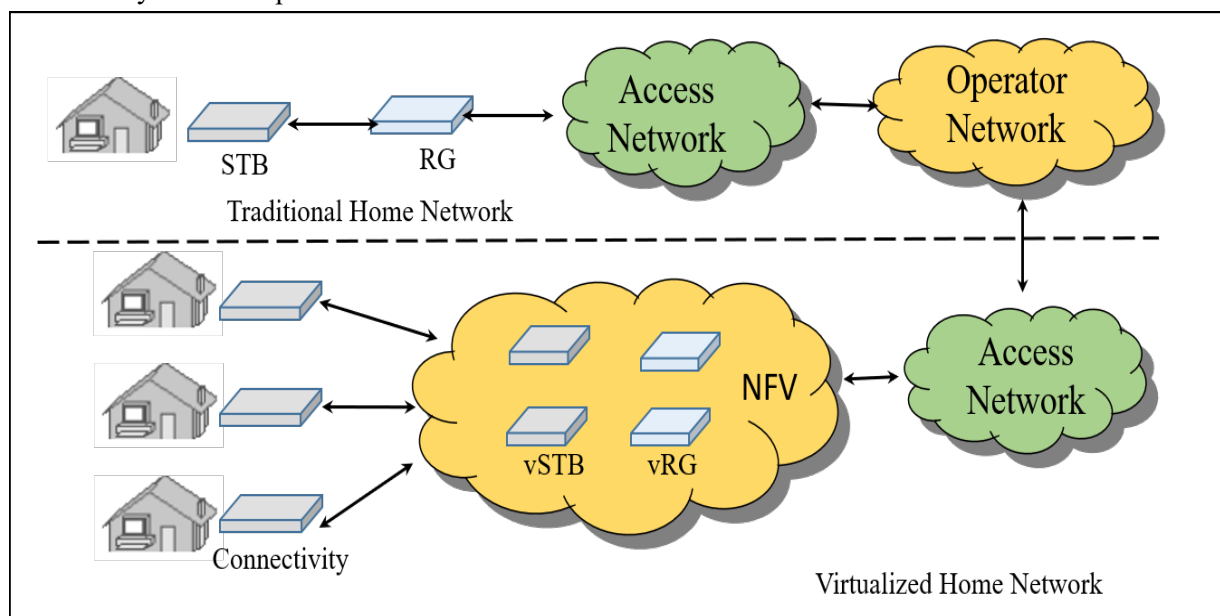


Figure 3: Virtualization of home network

## Conclusion

The NFV is an emerging technology in the telecommunications industry that came to allow a great transformation in its network architectures with the consequent potential benefits, which contribute to allow the operators to become more competitive, especially, in respect to the OTT competitors. From these benefits, described throughout this paper, we can highlight the following: faster development of new services and faster time to market answer, total costs of implementation reduction (CAPEX), better operational efficiency (lower

OPEX), higher network management simplicity and higher network services resilience.

It should be noted that most of the network operators did not yet started the virtualization process on their networks and those who have already started are yet in a preliminary phase, using only manual instantiation procedures.

However, it is estimated that in the mid-term the first VNFs with automated orchestrations will be available, ideally, for scenarios of network services supported E2E by VNFs.

## Glossário

CAPEX *CAPital EXpenditure*

CPE *Customer Premise Equipment*

COTS *Commercial Off-The-Shelf*

E2E *End To End*

ETSI *European Telecommunications Standards Institute*

GR *Gateway Residencial*

HW *Hardware*

ISG *Industry Specification Group*

MANO *Management and Orchestration functions*

NAT *Network Address Translation*

NFV *Network Functions Virtualization*

NFVI *Network Functions Virtualization Infrastructure*

OPEX *OPerational EXpenditure*

OTT *Over The Top*

QoS *Quality Of Service*

KPI *Key Performance Index*

SDN *Software Defined Network*

STB *Set-Top Box*

SW *Software*

TI *Tecnologias de Informação*

TTM *Time To Market*

VNF *Virtual Network Function*

VM *Virtual Machine*

vCPU *Virtual Central Processor Unit*

vMem *Virtual Memory*

vNIC *Virtual Network Interface Card*

## Referências

Heming Wen, Prabhat Kumar, Tho Le-Ngoc, “Network Virtualization: Overview”, Springer, 2013

U C Meena, R. Saji Kumar, Chandra Shekhar, “Study Paper on Network Function Virtualisation: Architecture and core network applications”, IT Division, Telecom Engineering Center, Department of Telecommunications, New Delhi

ETSI, “Network Function Virtualisation; use cases by ETSI”; ETSI GS NFV 001 v.1.1.1 (2013-10)

ETSI, “Network Function Virtualisation; Architectural framework by ETSI”; ETSI GS NFV 002 v.1.1.1 (2013-10)

ETSI, “Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV”; GS NFV 003 V1.4.1 (2018-08)

IEEE, R. Mijumbi, J. Serrat, JL Gorricho, N. Bouten, F. De Turck, R. Boutaba “Network Function Virtualization: State-of-the-art and Research Challenges”, 2015

IEEE, B. Han, V. Gopalakrishnan, L. Ji, and S. Lee “Network Function Virtualization: Challenges and Opportunities for Innovations”, 2015

IEEE, YONG LI1, MIN CHEN “Software-Defined Network Function Virtualization: A Survey”

FCA, A. Ferreira, “Introdução ao Cloud Computing”, 2015

4G America, “Bringing Network Function Virtualization to LTE”