Study Paper on

Network Function Virtualization (NFV)

&

Its impact on

Future Telecom Networks

FN Division

Telecommunication engineering centre

New Delhi

Key points:

Network Functions Virtualisation, Software Defined Networking, IT virtualization technologies, ETSI, proprietary hardware appliances, Virtual Machines, Management and Orchestration, NFV Infrastructure, use cases, Cloud Computing.

Abbreviation:

ASICs : Application Specific Integrated Circuits
BRAS : Broadband Remote Access Server
COTS : Commercial Off-The-Shelf
CDN : Content Distribution Networks
CAPEX : Capital Expenses
CGN/LSN : Carrier-grade NAT/ Large Scale NAT
DPI : Deep packet inspection
EPC : Evolved Packet Core
ETSI ISG : European Telecommunication Standards Institute Industry Specification Group
GGSN : Gateway GPRS Support Node
MANO : Management and Orchestration
NFV : Network Function Virtualisation
NIC : Network interface controller
OPEX : Operating Expenses
OSS/BSS : Operation Support System/ Business Support Systems
PoC : Proof of Concept
STB : Set-Top Box
SGSN : Serving GPRS Support Node
SBC : session border controller
SDN : Software Defined Networking
VM : Virtual Machines
VPN : Virtual Private Network
VNF : Virtualized Network Function
WAN : Wide Area Network

Index

****

1. Introduction

The concept of Network Function Virtualisation (NFV) originated from the requirement of telecommunication service providers worldwide, to accelerate deployment of new network services and to support their revenue and future growth objectives. Present day telecommunication networks are over populated with a large and increasing variety of proprietary hardware appliances. Therefore, to launch a new network service, it often requires introduction of yet another variety of proprietary hardware requiring to find the space and power to accommodate these arrangements, which is becoming increasingly difficult. This is further compounded by the increasing costs of energy, capital investment, requirement of huge technical manpower etc. The variety of skills necessary to design, integrate and operate increasingly complex hardware-based appliances, poses real challenge to both developer and the network operator. Moreover, hardware-based appliances rapidly reach end of life and other cost oriented issues result in little or no revenue benefit. These constraints/limitations of hardware-based appliances (e.g. Routers, firewalls etc) led them to think beyond traditional network system and thereby, resulting into development of various IT virtualization technologies, their standards & incorporation of the same into their networks. To accelerate progress towards this common goal, service providers world-over came together to work it out with different standardisation bodies such as the European Telecommunications Standards Institute (ETSI). The ETSI Industry Specification Group for Network Functions Virtualization (ETSI ISG NFV) is the lead group responsible for the development of requirements, architecture and other concerned issues for virtualization of various functions within telecommunication networks.

Network Function Virtualization (NFV) is a new way to design, deploy, and manage networking services by decoupling the physical network equipments from the functions that run on them, which replaces hardware centric, dedicated network devices with software running on general-purpose CPUs or virtual machines, operating on standard servers. By decoupling Network Functions (NFs) from the physical devices on which they run, NFV has the potential to lead to significant reductions in Operating Expenses (OPEX) and Capital Expenses (CAPEX) and will facilitate the deployment of new services with increased agility and faster time-to-value. The concept of NFV is quite recent, though it is based on technologies that have proven their validity in IT sector, and is a result of careful experimenting and evaluation by players in the industry and academy in the recent years.

Network Function Virtualisation aims to transform the way, the network operators architect networks, by evolving standard IT virtualisation technology to consolidate many network equipment types onto industry standard high volume servers, switches and storage, which could be located in Data centres, Network Nodes and in the end user premises, as illustrated in Figure 1. These virtual appliances can be instantiated on demand without the installation of new equipment. For example, network operators may run an open-source software-based firewall in a Virtual Machine (VM). It involves the implementation of network functions in software that can run on a range of industry standard servers and can be moved to or instantiated in various locations in the network as required, without the need for installation of new equipment. In other words, Network Function Virtualisation promotes the implementation of network functions in software that can run on a range of standard IT hardware in data centres and can be managed (e.g. moved, or replicated) without the need of modifying the physical infrastructure.

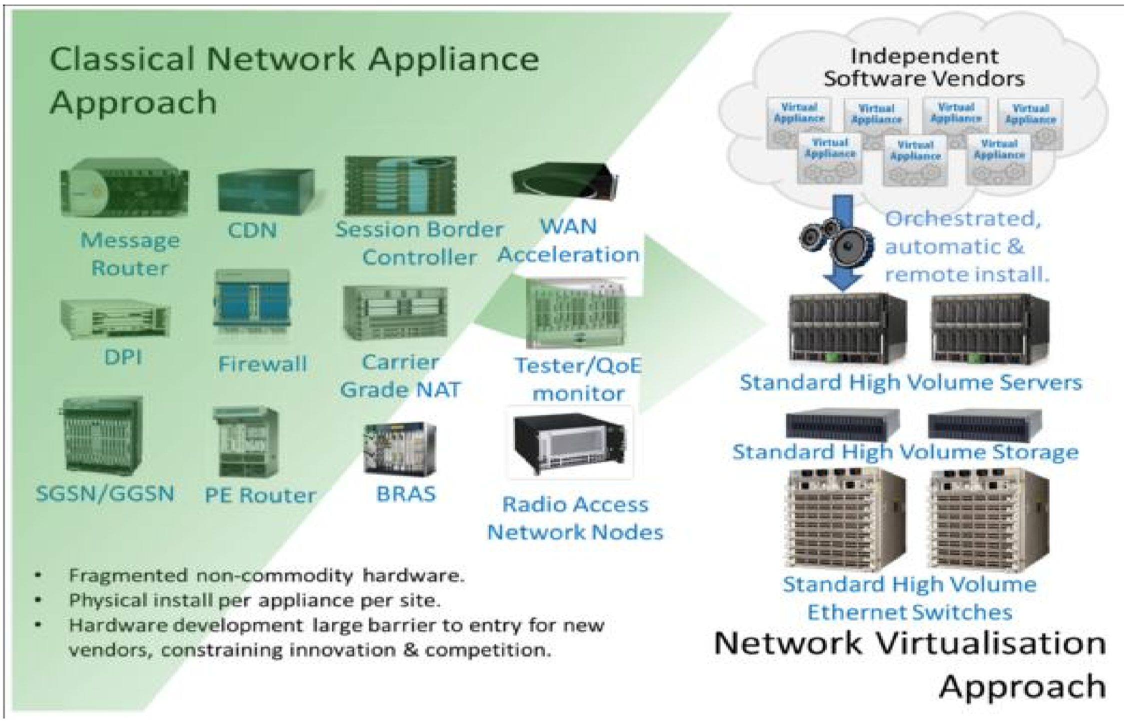

Figure 1: Vision for Network Functions Virtualisation

(Source: ETSI)

2. Network Function Virtualisation(NFV) and Software Defined Networks (SDN):

Relationship between NFV & SDN:

When discussing software-based networking, there is often confusion between NFV and SDN, leading to erroneous swapping of the two terms. In fact, NFV and SDN are two closely related, independent, yet **complementary** and mutually beneficial technologies. As shown in Figure 2, Network Functions Virtualisation is highly complementary to Software Defined Networking (SDN), but not dependent on it (or vice-versa). Network functions can be virtualized and deployed without SDN technologies, and non-virtualized functions can be controlled by SDN. The primary distinction between the two has to do with the domain to which they apply: While NFV replaces proprietary hardware network elements (NEs) with software running on standard servers, SDN deals with the replacement of standardized networking protocols with centralized control.

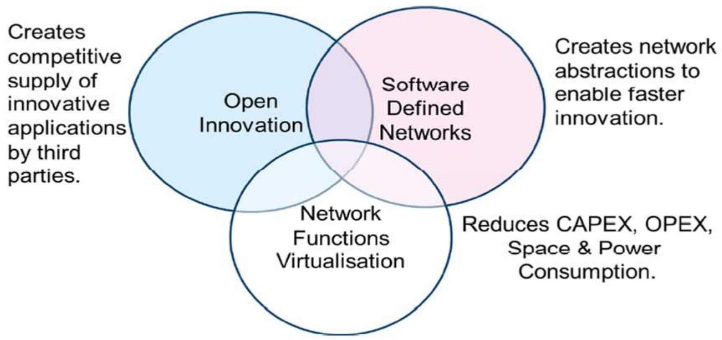

Figure 2: Network Functions Virtualisation Relationship with SDN (Source: ETSI)

While SDN function involves separation of control and data; centralisation of control and programmability of network whereas NFV deals with transfers of network functions from dedicated appliances to generic servers. Network Functions Virtualisation is able to support SDN by providing the infrastructure upon which the SDN software can be run. Furthermore, Network Functions Virtualisation aligns closely with the SDN objectives to use commodity servers and switches.

3. Benefits of Network Function Virtualisation

Network functions virtualization (NFV) is an emerging theme within the telecoms industry, and over the past few years, it has become a catalyst for major transformational changes in the network. Application of Network Functions Virtualisation brings many benefits to network operators, contributing to significant changes in the telecommunications industry.

Benefits include:-

- Reduced equipment **costs** and reduced power consumption through consolidating equipment. Cost efficiency is a main driver of NFV.
- NFV allows to abstract underlying hardware, and enables elasticity, scalability and automation. Improves the flexibility of network service provisioning and reduce the time to deploy new services.
- Increased speed of deployment by minimising the typical network operator cycle of innovation. Economies of scale required to cover investments in hardware-based functionalities are no longer applicable for software-based development, making feasible other modes of feature evolution. Network Functions Virtualisation will enable network operators to significantly reduce the maturation cycle.
- The possibility of running production, test and reference facilities on the same infrastructure provides much more efficient test and integration, reducing development costs and time to market.
- Services can be rapidly scaled up/down as required. In addition, speed of service deployment is improved by provisioning remotely in software without any site visits required to install new hardware.
- Enabling a wide variety of eco-systems and encouraging openness. It opens the virtual appliance market to pure software entrants, small players and academia, encouraging more innovation to bring new services and new revenue streams quickly at much lower risk.

- Reduced energy consumption by exploiting power management features in standard servers and storage, as well as workload consolidation and location optimisation. For example, relying on virtualisation techniques, it would be possible to concentrate the workload on a smaller number of servers during off-peak hours (e.g. overnight) so that all the other servers can be switched off or put into an energy saving mode.
- Improved operational efficiency by taking advantage of the higher uniformity of the physical network platform and its homogeneity to other support platforms.

4. Enablers for Network Function Virtualisation

The Network Functions Virtualisation (NFV) became achievable with several recent technology developments, such as given below.

4.1 Cloud Computing:

Network Functions Virtualisation leverages upon modern technologies such as those developed for cloud computing. At the core of these cloud technologies are virtualisation mechanisms: hardware virtualisation by means of hypervisors, as well as the usage of virtual Ethernet switches (e.g. vswitch) for connecting traffic between virtual machines and physical interfaces. For communication-oriented functions, high-performance packet processing is available through high-speed multi-core CPUs with high I/O bandwidth, the use of smart Ethernet NICs for load sharing and TCP Offloading, and routing packets directly to Virtual Machine memory, and poll-mode Ethernet drivers (rather than interrupt driven, for example Linux NAPI and Intel's DPDK).

Cloud infrastructures provide methods to enhance resource availability and usage by means of orchestration and management mechanisms, applicable to the automatic instantiation of virtual appliances in the network, to the management of resources by assigning virtual appliances to the correct CPU core, memory and interfaces, to the re-initialisation of failed VMs, to snapshot VM states and the migration of VMs. Finally, the availability of open APIs for management and data plane control, like OpenFlow, OpenStack, OpenNaaS or OGF's NSI, provide an additional degree of integration of Network Functions Virtualisation and cloud computing.

4.2 Industry Standard High Volume Servers

The use of industry standard high volume servers is a key element in the economic case for Network Functions Virtualisation. An industry standard high volume server is a server built using standardised IT components (for example x86 architecture) and sold in the millions. A common feature of industry standard high volume servers is that there is competitive supply of the subcomponents which are interchangeable inside the server.

Network Appliances which depend on the development of bespoke Application Specific Integrated Circuits (ASICs) will become increasingly uncompetitive against general purpose processors as the cost of developing ASICs increases exponentially with decreasing feature size. Merchant silicon will remain applicable for commodity functions implemented at scale while ASICs will still be applicable for some types of very high throughput applications.

4.3Software Defined Networking (SDN)

Software defined networking (SDN) and NFV can be used independently, but SDN makes it much easier to implement and manage NFV. SDN manages network complexity via a network-wide software platform that enables centralized network coordination, control and programmability. SDN provides a programmable and customizable interface that controls and orchestrates the operation of a collection of devices at different levels of abstraction. With it, users can dynamically reconfigure the network to plumb in a function running on a server in the appropriate place in the network using just software mechanisms. Without it, NFV would require much more manual intervention to configure the network to appropriately plumb in software-instantiated functions.

5. Technical Requirement/Challenges for Network Function Virtualisation

As an emerging technology in network industry, NFV brings several challenges to network operators, such as the guarantee of network performance for virtual appliances, their dynamic installation and migration, and their efficient placements etc. These challenges to implement the Network Functions Virtualisation need to be addressed before implementing the same.

5.1 Interoperability and Compatibility: -

The key requirement/issue for NFV is to design standard interfaces between not only a range of virtual appliances but also between the virtualized implementations and the legacy equipment. One of the goals of NFV is to promote openness, therefore network carriers may need to integrate and operate servers, hypervisors and virtual appliances from different vendors in a multi-tenant NFV environment. Their seamless integration requires a unified interface to facilitate the interoperability among them. The developed NFV solutions need to be compatible with existing Operation and Business Support Systems (OSS/BSS) and Element and Network Management Systems (EMS/NMS), and work in a hybrid environment with both physical and virtual network functions. In the long run, network operators must be able to migrate smoothly from proprietary physical appliances to open standard based virtual ones, since they may not be able to keep updated all their existing services and equipment in proprietary physical network appliance based solutions.

5.2 Performance Trade-Off:-

Since the Network Functions Virtualisation approach is based on using industry standard hardware (i.e. avoiding any proprietary hardware such as acceleration engines) along with a virtualized networks & appliances, a probable decrease in performance may arise. The challenge is how to keep the performance degradation as small as possible by using appropriate hypervisors and modern software technologies, so that the adverse effects on latency and throughput are minimized. The available performance of the underlying platform needs to be clearly identified/ understood, so that virtual appliances know what they can get from the hardware. Using the right technology choice will allow virtualisation, not only of network control functions but also of data/user plane functions.

5.3 Migration from and co-existence of legacy while ensuring compatibility with existing platforms:-

Implementations of Network Functions Virtualisation (NFV) must co-exist with network operators' legacy network equipment and be compatible with their existing Element Management Systems, Network Management Systems, OSS and BSS, and potentially existing IT orchestration systems, if Network Functions Virtualisation orchestration and IT orchestration are to converge. The Network Functions Virtualisation architecture must support a migration path from today's proprietary physical network appliance based solutions to more open standards based virtual network appliance solutions. In other words, Network Functions Virtualisation must work in a hybrid network composed of classical physical network appliances and virtual network appliances. Virtual appliances must, therefore, use/support existing North Bound Interfaces (for management & control) and interwork with physical appliances implementing the same functions.

5.4 Management and Orchestration: -

Network Functions Virtualisation presents an opportunity, through the flexibility afforded by software network appliances operating in an open and standardised infrastructure, to rapidly align management and orchestration with North Bound Interfaces to well defined standards and abstract specifications. This will greatly reduce the cost and time to integrate new virtual appliances into a network operator's operating environment. Software Defined Networking (SDN) further extends this to streamlining the integration of packet and optical switches into the system e.g. A virtual appliance or Network Functions Virtualisation orchestration system may control the forwarding behaviours of physical switches using SDN.

5.5 Security & Resilience: -

When deploying virtualized network functions, operators need to ensure that the security features of their network will not be adversely affected. NFV may bring in new security concerns along with its benefits. Initial expectations are that Network Functions Virtualisation improves network resilience and availability by allowing network functions to be recreated on demand after a failure. A virtual appliance should be as secure as a physical appliance if the infrastructure, especially the hypervisor and its configuration, is secure. Network operators will be seeking tools to control and verify hypervisor configurations. They will also require security certified hypervisors and virtual appliances.

5.6 Reliability and Stability:-

Reliability is an important requirement for network operators when offering specific services (e.g., voice call and video on demand), no matter through physical or virtual network appliances. Carriers need to guarantee that service reliability and service level agreement are not adversely affected when evolving to

NFV. To meet the reliability requirement, NFV needs to build the resilience into software when moving to error-prone hardware platforms. All these operations create new points of failure that should be handled automatically.

In addition, ensuring service stability poses another challenge to NFV, especially when reconfiguring or relocating a large number of software-based virtual appliances from different vendors and running on different hypervisors. Network operators should be able to move VNF components from one hardware platform onto a different platform while still satisfying the service continuity requirement. They also need to specify the values of several key performance indicators to achieve service stability and continuity, including maximum non-intentional packet loss rate and call/session drop rate, maximum per-flow delay and latency variation, and maximum time to detect and recover from failures.

5.7 Simplicity: -

It needs to be ensured that virtualised network platforms will be simpler to operate than those that exist today. A significant and topical focus for network operators is therefore, on simplification of the plethora of complex network platforms and support systems which have evolved over decades of network technology evolution, while maintaining continuity to support important revenue generating services. It is important to avoid trading one set of operational headaches for a different but equally intractable set of operational headaches.

6. Design and Architectural Framework

The Network Function Virtualisation (NFV) architecture has been defined by the ETSI NFV ISG (document no. ETSI GS NFV 002 v1.1.1) and comprises three principal elements: the NFV Infrastructure (NFVI), Virtualised Network Functions (VNFs) and the NFV Management and Orchestration (MANO) functions.

- **The NFV Infrastructure** (**NFVI)** consists of physical networking, computing and storage resources that can be geographically distributed and exposed as a common networking/NFV infrastructure. It is the combination of both hardware and software resources which build up the environment in which VNFs are deployed, managed and executed. The NFVI can span across several locations i.e. places where NFVI-PoPs are operated. The network providing connectivity between these locations is regarded to be part of the NFVI.
- **Virtualised Network Functions (VNF**s) are software implementations or virtualisation of network functions (NFs) that are deployed on virtual resources such as VM. Virtualized network functions, or VNFs, are responsible for handling specific network functions that run in one or more virtual machines on top of the hardware networking infrastructure, which can include routers, switches, servers, cloud computing systems and more. Individual virtualized network functions can be chained or combined together in a building block-style fashion to deliver full-scale networking communication services.
- **NFV Management and Orchestration (NFV MANO)** functions provide the necessary tools for operating the virtualized infrastructure, managing the life cycle of the VNFs and orchestrating virtual

infrastructure and network functions to compose value-added end-to-end network services. NFV MANO focuses on all virtualisation specific management task necessary in the NFV framework.

Virtualization provides the opportunity for a flexible software design. Existing networking services are supported by diverse network functions that are connected in a static way. NFV enables additional dynamic schemes to create and manage network functions. Its key concept is the VNF forwarding graph which simplifies the service chain provisioning by quickly and inexpensively creating, modifying and removing Virtualised Network Functions service chains. On one hand, we can compose several VNFs together to reduce management complexity, for instance, by merging the serving gateway (SGW) and Packet Data Network Gateway (PGW) of a 4G core network into a single box. On the other hand, we can decompose a VNF into smaller functional blocks for reusability and faster response time. However, we note that the actual carrier-grade deployment of VNF instances should be transparent to end-to-end services.

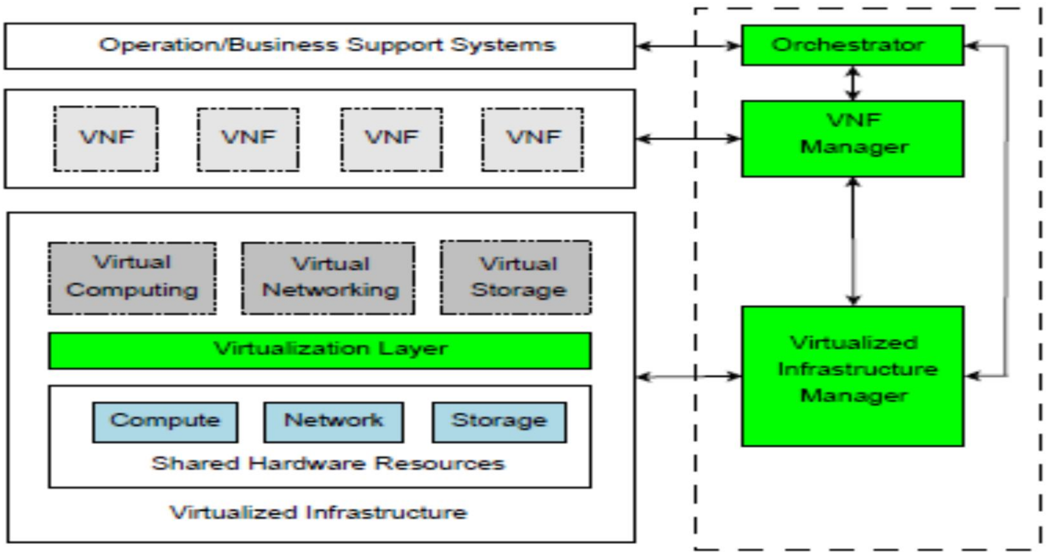

Fig: 3 NFV Architectural Framework

(**Source**: Network Functions Virtualization: Challenges and Opportunities for Innovations, AT&T Labs Research, Bedminster, USA)

Compared with the current practice, NFV introduces the following three major differences:

1) *Separation of software from hardware*: This separation enables the software to evolve independently from the hardware, and vice versa.

2) *Flexible deployment of network functions*: NFV can automatically deploy network-function software on a pool of hardware resources which may run different functions at different times in different data centres.

3) *Dynamic service provisioning*: Network operators can scale the NFV performance dynamically and on a grow-as- you-need basis with fine granularity control based on the current network conditions.

Network Function Virtualisation (NFV) Architectural framework (Figure 3) has four major functional blocks. 1) the orchestrator, 2) VNF manager, 3) virtualization layer and 4) virtualized infrastructure manager.

The orchestrator is responsible for the management and orchestration of software resources and the virtualized hardware infrastructure to realize networking services.

The VNF manager is in charge of the instantiation, scaling, termination and update events during the lifecycle of a VNF, and supports zero-touch automation.

The virtualization layer abstracts the physical resources and anchors the VNFs to the virtualized infrastructure. It ensures that the VNF lifecycle is independent of the underlying hardware platforms by offering standardized interfaces. This type of functionality is typically provided in the forms of VMs and their hypervisors.

The virtualized infrastructure manager is used to virtualize and manage the configurable compute, network and storage resources and control their interaction with VNFs. It allocates VMs onto hypervisors and manages their network connectivity. It also analyzes the root cause of performance issues and collects information about infrastructure fault and for capacity planning and optimization.

From the study of the above architecture two major enablers of NFV are 1) industry-standard servers and 2) technologies developed for cloud computing. A common feature of industry-standard servers is that their high volume makes it easy to find interchangeable components inside them with competitive price, compared with network appliances based on bespoke Application Specific Integrated Circuits (ASICs). Using these general purpose servers can also reduce the number of different hardware architectures in operators' networks and prolong the lifecycle of hardware when technologies evolve (e.g., running different software versions on the same platform). Recent developments of cloud computing, such as various hypervisors, OpenStack and Open vSwitch, also make NFV achievable in reality. For example, the cloud management and orchestration schemes enable the automatic instantiation and migration of VMs running specific network services.

NFV is closely related to other emerging technologies, such as SDN. 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 feature 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. However, it is worth noting that the virtualization for deployment of network functions does not rely on SDN technologies, and vice versa.

7. Standard Related Activities of NFV

European Telecommunications Standards Institute (ETSI) has created an Industry Specification Group (ISG) for NFV to achieve the common architecture required to support virtualized network functions through a consistent approach. This ISG was initiated by several leading telecommunication carriers, including AT&T, BT, China Mobile, Deutsche Telekom, Orange, Telefonica and Verizon. Is now having 280 Member Companies (115 ETSI Members, 165 participant organisations). It has quickly attracted broad industry support and has participants ranging from network operators to equipment vendors and IT vendors. The

ETSI NFV ISG currently has four working groups: 1) Infrastructure Architecture, 2) Management and Orchestration, 3) Software Architecture and 4) Reliability & Availability; and two expert groups: 1) Security and 2) Performance & Portability. It has also developed a Proof of Concept (PoC) Framework to coordinate multi-vendor PoCs and build the confidence that NFV is a viable technology. This group (ISG) seeks to define the requirements that network operators may adopt and tailor for their commercial deployment. The approach that the ETSI NFV ISG is taking is that the virtualisation of network functionality is applicable to any data plane packet processing and control plane function in both fixed and mobile networks.

The key goals of the ETSI's NFV-ISG are to:

a. Reduce network equipments costs and power consumption by consolidating networking appliances.
b. Improve time to market of new services.
c. Enable the availability of multiple applications on a single network appliance
d. Enable the multi-version and multi-tenancy capabilities.
e. Encourage a more dynamic ecosystem through the development and use of software-only solutions.

These goals/benefits can be derived from the use of commercial, off-the-shelf (COTS) hardware that can be purposed and repurposed for multiple telecom-related services that currently use proprietary hardware. NFV is taking the software defined networking (SDN) concept of the virtualization movement and adapting it to benefit the telecommunications application infrastructure.

Much of the current phase of NFV development focuses on mobile networks. This is only natural as the majority of those networks are in transition, with massive deployment of new infrastructure for LTE/LTE-Advanced.

8. Fields of Application and Use Cases

Network Functions Virtualisation is applicable to any data plane packet processing and control plane function in mobile and fixed networks.

Potential examples that can be listed include:-

Network Element	Function
Switching elements	Broadband Network Gateways (BNG), Carrier Grade Network Address Translation (CG-NAT), Routers
Mobile network nodes	Home Location Register/Home Subscriber Server (HLR/HSS), Gateway, MME, , GPRS Support Node, (SGSN,GGSN)/PDN-GW, Radio Network Controller (RNC), various node B functions, eNode B
Customer premise equipment	Home Routers, Set Top Boxes
Tunnelling gateway elements	IPSec/SSL Virtual Private Network Gateways
Traffic analysis	Deep Packet Inspection (DPI), Quality of Experience (QoE) measurement
Assurance	Service Assurance, Service Level Agreement (SLA) monitoring, testing and diagnostics

Signalling	Session Border Controller (SBCs), IP Multimedia Subsystem Components (IMS)
Control Plane / Access Functions	AAA Server, policy control and charging platform
Application optimization	Content delivery network (CDN), cache server, load balance, accelerators
Security	Firewalls, virus scanners, intrusion detection system, spam protection

Table *1: Potential Functions to be virtualised*

Some use cases of NFV, including the virtualization of cellular base station, mobile core network and home network etc are discussed below.

8.1 Virtualization of Cellular Base Station

Mobile network traffic especially data traffic is significantly increasing with day by day increase in cellular mobile applications. As the emerging cellular network system is choice of telecommunication industry, LTE specifications are motivated by demand for higher data rates, Quality of service, low complexity, continued cost reduction of radio access and packet core.

The large numbers of RAN (Radio Access Network) nodes such as eNodeB are usually based on proprietary platforms and are suffering from long life-cycle in development, deployment and operation.
Virtualization of mobile base station came from IT virtualization technology to realize at least a part of RAN nodes onto standard IT servers, storages and switches which is expected to provide advantages of lower footprint and energy consumption coming from dynamic resource allocation and traffic load balancing, easier management and operation, and faster time-to-market.

In major mobile operators' networks, multiple RAN nodes from multiple vendors are usually operated with different mobile network system e.g. 3G, LTE and WiMAX, in the same area. These multiple platforms can be consolidated into a physical base station (BS) based on IT virtualization technologies. RAN node utilization is usually lower than its MAX capacity because the system is designed to cover the peak load, however the average load is far lower, and each proprietary RAN node resource cannot be shared with other nodes. BS virtualization can achieve sharing of resources among multiple logical RAN nodes from different systems, dynamic allocation of resources as well as reduction in power consumption. Centralized(C-RAN) technology with virtualization can leverage more efficient resource utilization among different physical BSs (fig 4). C-RAN is a centralized, cloud computing based new radio access network architecture that can support 2G, 3G, 4G system and future wireless communication standards. Its name comes from the four 'C's in the main characters of C-RAN system, which are "Clean, Centralized processing, Collaborative radio, and real-time Cloud Radio Access Network.

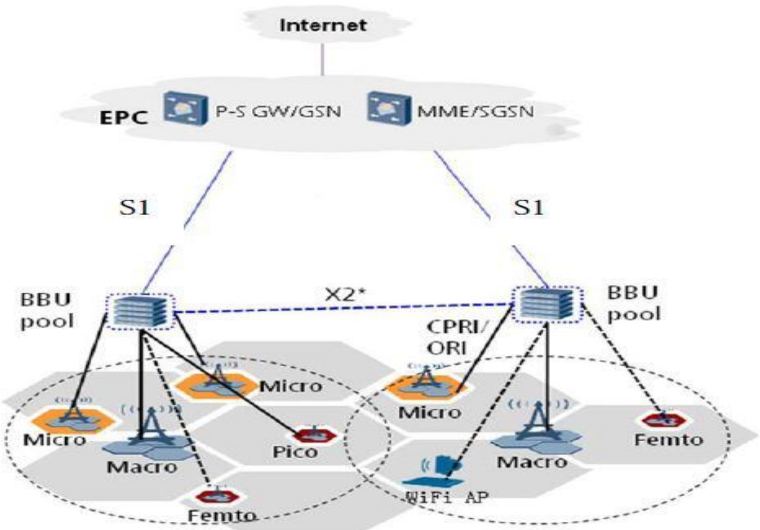

Fig 4: The Cloud RAN architecture (Source: ETSI)

BS is a generic term to designate 2G BS, 3G NodeB and 4G eNodeB. In LTE, BS is in charge of the Physical layer (PHY), Media Access Control (MAC), RLC (Radio Link Control), Radio Resource Control (RRC) and Packet Data Convergence Protocol (PDCP) functions. BS virtualization requires baseband radio processing using IT virtualization technologies, such as high-performance general purpose processors and real-time processing virtualization to provide the required signal processing capacity. Moreover, BS virtualization for C-RAN requires building the processing resource, i.e. Base Band Unit (BBU) pool for aggregating the resources onto centralized virtualized environment such as a Data Center (DC) or cloud infrastructure.

8.2 Virtualization of Mobile Core Network

Today's mobile core networks are populated with a large variety of expensive proprietary hardware appliances as well as hard state signalling protocols. When a specific function is not available, cellular operators have to replace an existing equipment even if it is still sufficient for most purposes, which reveals the difficulty to scale up and scale down the offered services rapidly, as required.

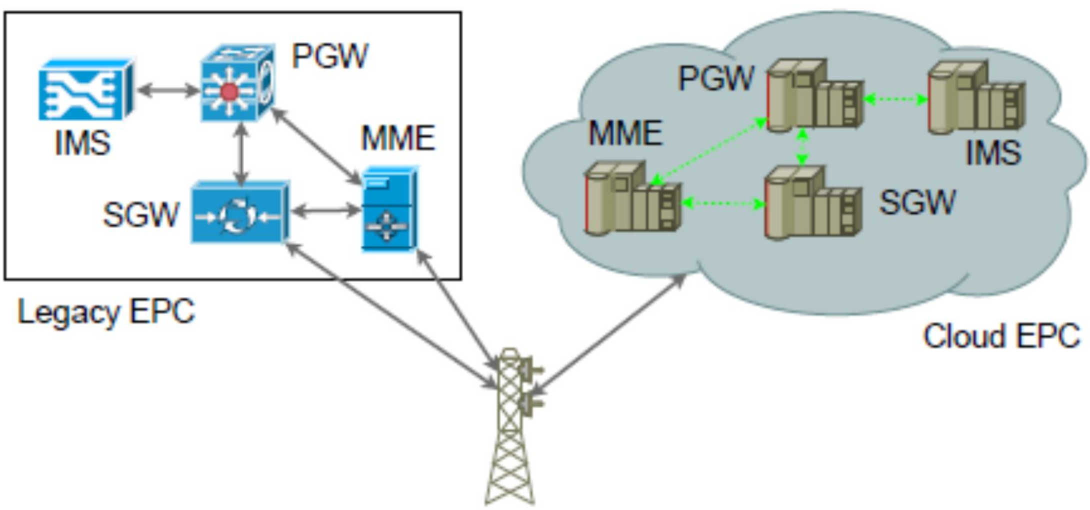

Fig 5: Virtualisation of EPC

(**Source**: Network Functions Virtualization: Challenges and Opportunities for Innovations, AT&T Labs Research, Bedminster, USA)

These problems can potentially be addressed by Cloud EPC (Evolved Packet Core, EPC is the core network for LTE) by virtualization of the mobile core network to meet changing market requirements. The virtualization targets of EPC include Mobility Management Entity (MME), Home Subscriber Server (HSS), Serving Gateway (SGW), Packet Data Network Gateway (PGW) and Policy and Charging Rules Function (PCRF). To better support Voice over LTE (VoLTE), cellular operators can also virtualise the components of an IP Multimedia System (IMS), including various Call Session Control Functions (CSCFs) such as Proxy-CSCF, Serving-CSCF and Interrogating-CSCF, and Breakout and Media Gateway Control Functions. Virtualization of EPC for 4G LTE networks and its coexistence with the legacy EPC is illustrated in Figure 5. The coexistence is made possible through technologies such as MME pooling. It should be noted that it is possible to virtualize only part of the mobile core network, such as SGW and PGW, and use physical appliance for other components. By virtualising the aforementioned network functions, Cloud EPC allows us to move towards a more intelligent, resilient and scalable core architecture which enables flexible distribution of hardware resources to eliminate performance bottlenecks and rapid launch of innovative services to generate new revenue sources (e.g., machine-to-machine communications). The virtualization of EPC frees distributed network resources from their geographic limitations to ensure service reliability and stability in the event of local resource failure and reduce the Total Cost of Ownership (TCO). It also makes the flexible deployment of SGW and PGW possible, for example, co-locating them with an eNodeB and thus eliminating the long-distance tunnels. With Cloud EPC, cellular carriers can not only expand their current horizontal market business, but also capitalize on previously untouched vertical markets.

8.3 Virtualization of Home Network

Network service providers offer home services through dedicated Customer Premise Equipment (CPE) supported by network-located backend systems. Typical CPE devices include Residential Gateways (RGs) for Internet access and Set-Top Boxes (STBs) for multimedia services.

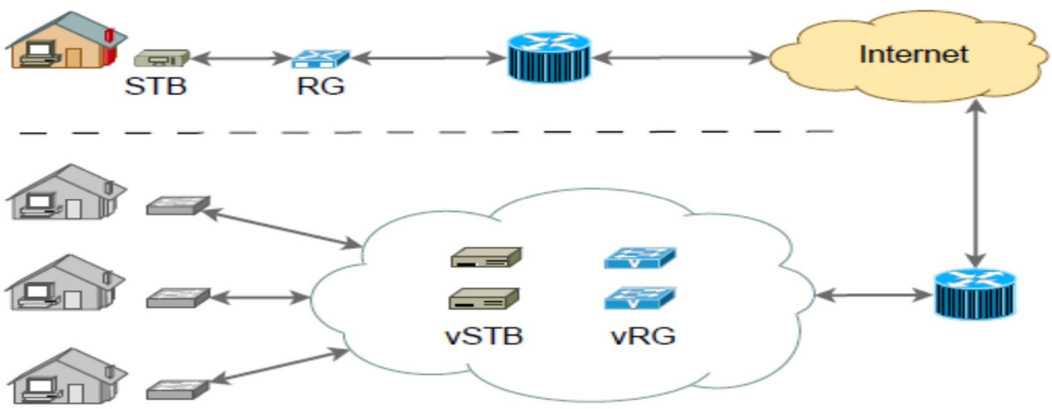

Fig 6: Virtualisation of home network

(**Source**: Network Functions Virtualization: Challenges and Opportunities for Innovations, AT&T Labs Research, Bedminster, USA)

The emerging NFV technology facilitates the virtualization of home network, services, functionality migration from home devices to the NFV cloud as shown in the fig 6 which shows Architecture of virtualized home networks. The virtualization targets are STBs and a range of components of RGs, such as firewall, Dynamic Host Configuration Protocol (DHCP) server, Virtual Private Network (VPN) gateway and Network address translation (NAT) router. By moving them to data centres, network and service operators need to provide only low cost devices to customers for physical connectivity with low maintenance requirements, demonstrated by the three gray boxes at the left hand bottom corner of Figure 6. This virtualized architecture presents numerous advantages to network operators and end users.

First, it reduces the operating expense by avoiding the constant maintenance and updating of the CPE devices and alleviating the call centre and product return burdens. Second, it improves the quality of experience by offering near unlimited storage capacity and enabling access to all services and shared content from different locations and multiple devices, such as smart phones and tablets. Third, it allows dynamic service quality management and controlled sharing among user application streams which helps content providers programmatically provision capacity to end users via open APIs. Finally, it introduces new services more smoothly and less cumbersome by minimizing the dependency on the CPE functions.

8.4 Virtualisation of CDNs (vCDN)

Content Delivery Networks (CDN), specially video content have gained a popular role among application service providers (ASPs) and telecommunication network. A CDN is an overlay network that gives more control of asset delivery by strategically placing servers closer to the end-user, reducing response time and network congestion. Many strategies have been proposed to deal with aspects inherent to the CDN distribution model. Virtualisation of CDN (vCDN) involves moving Content Distribution Networks (CDNs) from physical servers to a virtualized environment covering all components of CDN, where first impact addressed on cache node for achieving acceptable performance (e.g. throughput, latency etc.), allows for new constructs that simplify the CDN architecture.

9. Status of NFV Adoption:

Network Function Virtualisation is going through its initial phase. With changing competitive environment, the telecommunication networks also facing technological changes to be occurred in it. Based on survey done by M/s Webtorials, while only a modest number of organisations have implemented NFV in a production network, a large percentage of Telecom/IT organisation are currently in varying stages of analysing NFV. Within a few years, the majority of organisations are likely to have made a significant deployment of NFV.

10. Impact of NFV on future telecom networks:

Being the fastest growing sector, the telecommunication industry is facing increased competition as new players are entering with emerging technologies. There is, thus, a need for existing players to invest in and adopt new technologies such as Software Defined Networking/Network Function Virtualization, cloud, analytics, etc. which can enable them to help telecom operators increase service agility and efficiencies. Communication Service Providers and Vendors are investing a lot of resources going in that direction and for good reasons. It is clear that many opportunities will be created during the development and market implementation of such emerging technologies.

Network Function Virtualisation offers a great business potential, in terms of cost savings and additional revenue sources for operators, new opportunities for solution providers and, most importantly, in opening new business models and innovation opportunities. NFV will create business model challenges, specifically how the leading network equipment providers charge for their products. Currently, the majority of the $100 billion-plus market for telecom equipment is sold as integrated systems with applications running on proprietary high-availability middleware and optimized hardware platforms. Migrating to an applications software model will be highly disruptive to existing revenue streams and profit margins.

NFV offers significant potential to change the way that service providers architecture future networks, including increased flexibility and lower costs. Driving widespread adoption of NFV over the next few years will require significant cooperation and partnership by the leading service providers and their IT/equipment suppliers.

To provide network functionality, a virtual function can be instantiated on-demand wherever it is needed in the network, rather than only at those points where the dedicated device is located. This decoupling of function and location means new possibilities for:

- Independent NFV providers to offer network functions as a service to network service providers, following technology and charging patterns similar to those currently in use in cloud infrastructures;
- Network Service providers to share infrastructure and services on demand to optimize their resource usage or cost structure, and to cope with traffic peaks by offloading some traffic to partner resources;
- Network operators to provide long tail services that are practically impossible to address with current infrastructures, covering new market niches, expanding their service and charging options, and enabling a new breed of application services that rely on them; and
- Over the Top (OTT) provider to compete in quality-of-experience offers with established providers at reasonable costs by means of agreements with network service providers for specialized services.

Network Functions Virtualization (NFV) has the potential to advance significant change in the way telecom networks are built and operated. Led by major communications service providers, NFV provides a standards-based approach to virtualizing a range of telecom applications, thus enabling them to run on industry standard servers.

Advances in Telecom/IT technology, including more powerful processors (e.g., Intel x86 and Cavium), faster switching fabrics (e.g., 40GB), and advances in network software (e.g., SDN) have brought a wealth of network functions in the scope of commercial off-the-shelf (COTS) equipment. NFV proponents hope to virtualize a wide range of network elements, including:

- Mobile core networks
- Deep packet inspection (DPI)
- Session boarder controllers (SBC)
- Security appliances (firewalls, IDS/IPS, SSL VPNs)
- Server load balancers
- WAN acceleration

On the technology front, there remain several challenges to widespread NFV adoption, including:

- Delivering standards-based, highly scalable COTS servers and high-availability middleware that meet the performance, reliability and availability requirements of the service providers.
- Implementing NFV elements which interoperate not only with each other, but also with network elements in the installed (legacy) networks. This includes links to existing telecom OSS/BSS systems.
- Automation of the management and orchestration features of NFV applications.
- Ensuring that security of the network is not compromised by the introduction of NFV technologies.

11. Conclusion

The introduction of Network Function Virtualisation is a core structural change in the telecommunication infrastructure marketplace. NFV will bring cost efficiencies, time-to-market improvements, new business models & services and increased innovation to the telecommunication industry infrastructure and applications. This paper, presented an overview of the emerging network functions virtualization technology, illustrated its architectural framework, summarized several use cases, benefits of Network Function Virtualisation as well as the challenges involved in its wide spread adoption. NFV evolution is real and it is happening now; therefore, the telecom industry needs to consider leveraging this opportunity to start down the migration path to NFV and start reaping the benefits.

Apart from the opportunities, the telecommunication industry may have to take into consideration several technical challenges that might hinder its progress. Network operators, vendors, Telecommunication academicians need to be aware of these challenges and explore new approaches to overcome them. Each player in the industry may need to position/ reposition itself in the new 'Network Function Virtualisation' market. As an emerging technology, NFV may bring several challenges to network operators, such as the guarantee of network performance for virtual appliances, their dynamic instantiation and migration, and their efficient placement. Therefore, the challenge for network operators may be how to migrate their operations and skill base to software based networking environment while carefully re-targeting investment to maximise reuse of existing system and processes. It may take some investment of time, resources, education and operational transformation, but it may be the most efficient strategy going forward to keep pace with the rapid growth of the Telecommunication networks of tomorrow.

12.Recommendations

Network Functions Virtualisation is likely to deliver many benefits for network operators and their partners and customers while offering the opportunity to create new types of eco-systems which may encourage and support rapid innovation with reduced cost and reduced risk. To reap these benefits, the technical challenges, as described above, need to be addressed by the industry. To arrive at possible solutions to these technical challenges, the IT and Telecom Network industries may have to combine their complementary expertise and resources in a joint collaborative effort to reach broad agreement on standardised approaches and common architectures which may address these technical challenges, and provide tested and interoperable solutions for delivery of end to end virtualised services with economies of scale. NFV need to be part of the broader transformation effort and may require service providers to make significant changes and progressive efforts. To make NFV fully operational, there is a need of coordination of three interlinked but separate development paths: virtualisation, orchestration, and automation. NFV is considered to be a disruptive technology. Specially, it is expected to change the way current networks are being built, operated & managed. The multi-vendor management and orchestration objective of NFV need to be streamlined towards smooth migration.

13. References:

1. http://www.etsi.org/
2. ETSI. Network Functions Virtualisation; Use Cases, from http://www.etsi.org/technologies-clusters/technologies/nfv
3. Network Function Virtualisation; Architectural framework by ETSI; ETSI GSNFV 002 v.1.1.1 (2013-10)
4. Network Function Virtualisation; use cases by ETSI; ETSI GS NFV 001 v.1.1.1 (2013-10)
5. Network Functions Virtualization: Challenges and Opportunities for Innovations by AT&T Labs Research Bedminster, NJ 07921, USA
6. https://f5.com/resources/white-papers/network-functions-virtualization-everything-old-is-new-again
7. Bringing Network Function Virtualization to LTE by 4G America

8. http://portal.etsi.org/NFV/NFV_White_Paper.pdf
9. http://www.radio-electronics.com/info/telecommunications_networks/nfv-network-functions-virtualization/basics-tutorial
10. http://www.sonus.net/sites/default/files/2016_guide_to_sdn_and_nfv_-_part_4_-_sonus.pdf