UNDERSTANDING BENEFITS OF NETWORK FUNCTION VIRTUALIZATION TO TELECOM NETWORK OPERATORS

Sunil Patil*

Yatin Jog*

Harmanpreet Pall*

KanikaBatra*

Abstract

The research paper explores and analyses a comparatively nascent technological progression in the networking domain, commonly referred as Network Function Virtualisation. This technological transition leverages both IT and virtualization with intrinsic capability to transform in near future the existing traditional complex telecom network architecture into a cost effective and efficient solution, that will help the telecom network operators optimize their usage of network resources and meet the growing customer expectations in terms of effective end to end service delivery.

To conclusively arrive at the benefits accrued by Network Function Virtualisation an in detail secondary research analysis of various research papers and solutions of top market players in NFV domain was undertaken with specific emphasis on its drivers, timeline, market, ecosystem, benefits and possible challenges in the future. The findings of the research paper can be a stimulus for the NFV solution providers in formulating their marketing strategy and align their solutions to meet the requirements of the telecom network operators and service providers.

Keywords–NFV, Virtualization, Technological Transition, optimizing network resources

* Symbiosis Institute of Telecom Management, symbiosis International University, India

1.NFV Concept and Approach

1.1 Introduction

Network Functions Virtualization is conceptualized as the next wave in the technology world that leverages standard IT virtualisation technology to completely transform the existing traditional based network architecture of telecom operators. The idea was to enable consolidation of varieties of proprietary onto industry standard servers, switches and storage with high volume capacity. **[1]**

To meet the growing trend of software based networking technologies, in October 2012, an Industry Specification Group (ISG) within the European Telecommunications Standards Institute (ETSI) was formed that consisted of over twenty of the world's largest telecommunications service providers with the aim to define Network Functions Virtualization (NFV) and plan for its practical implementations in the real world.**[2]**

The theoretical concept of NFV is to simplify the network complexity of deploying hundreds of equipment but to decouplesuch network functions from dedicated hardware devices like routers, firewalls, load balancers etc.and allow network services to be hosted on virtual machines (VMs) under the control of a hypervisor i.e. a virtualization layer, on standard x86 servers.Network administrators will also find it easy to relocate the virtual machine or software based network functions to another physical server or provisions another virtual machine on the original server to take share part of the load during heavy bandwidth requirements by the users or in cases of unavoidable situations like failures.

This concept was brought into existence basically to meet various challenges like equipment and operational costs, power consumption, and time-to-market for new services and functionality that telecom network operators are still facing in their current architectures that comprise of dedicated telecom network equipment’s.

The telecom network operators will no longer have to be dependent on proprietary hardware from specific vendors and can deploy more devices virtually without any geographical or site constraints.

The market for NFV solution providers is massive and all the solutions in relation to technology are being developed at a very fast pace. Telecom Network Operators across the globe are collaborating with all these NFV solution providers in order to setup their own NFV based infrastructure as quickly as possible. The proposed advantages of NFV has raised the expectations of Telecom Network Operators as well as increased the competition in the NFV market to provide end to end solutions in various environments.

Some of the few major players in the NFV market as shown in figure 1 are Alcatel Lucent, Cisco, Redhat, Cyan, 6 Wind, Brocade and many more. All the NFV solutions provided by these vendors promise to help telecom network operators capitalize on the potential of NFV.

Figure 1 shows the NFV approach to classical architecture where instead of deploying separate individual hardware for each network function like firewall, router, server, load balancer etc., network operators will be able to integrate all the functions as software based applications on a standard x86 server with the help of a virtualization layer consisting of hypervisors and virtual machines**[3].**Each virtual machine will drive a separate operating system on which the various network functions will run as software applications.Hypervisor acts as a controller or manager of all the virtual machines running on a single machine.The different hypervisors that are being used in these systems are KVM, Exsi, Microsoft HyperV, Oracle VM server etc.

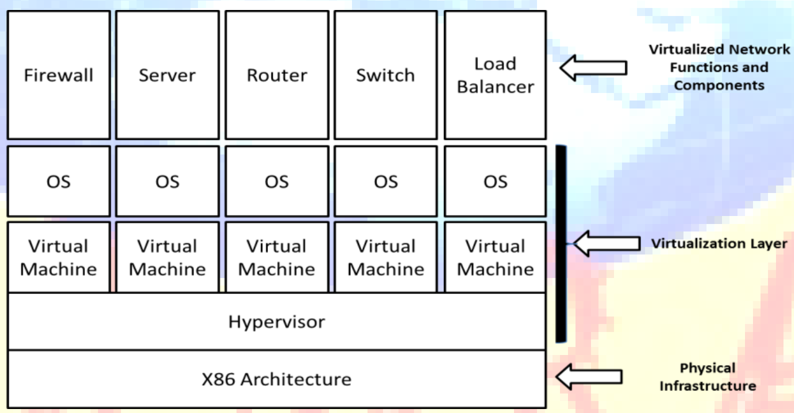

Figure 1: View of NFV

Figure 2 shows the complete idea of NFV i.e. completely changing the hardware based implementations into effective and efficient software based networks. Multiple devices like router , switch, firewall , server , load balancer etc. that are deployed individually occupying their own space in the infrastructure will all be consolidated over a single server having humongous capacity to bear the load of all the devices on a single machine .

Figure 2: Classical Approach V/s NFV Approach

1.2 NFV Market

Market research predicts that the global service provider SDN/NFV market will reach $11 billion in 2018 from $ 500 million in 2023 **[3]** dividing the NFV Market revenue into three categories of new SDN/ NFV software products (20%) , products that companies will buy instead of buying the 'displaced' revenue (12% of SDN/NFV Market) and newly identified segments of existing markets: mostly the virtualized network functions (VNFs), and also ports on routers, switches, and optical gear (68% of SDN/NFV Market).

Cost optimisation of Capex and Opex, Service agility, deployment of new technologies, such as VoLTE and replacement of legacy systems and network and revenue from innovation will be the major drivers for the CSP to invest in the technology. Already existing and well established telecoms infrastructure and software are expected to have a significant impact in the next 10 years due to the modifications proposed by NFV technology, for which CSPs will first need to make ready their networks, systems, operations and organisation (people, process, culture) to ensure a successful NGN transformation.**[4]**

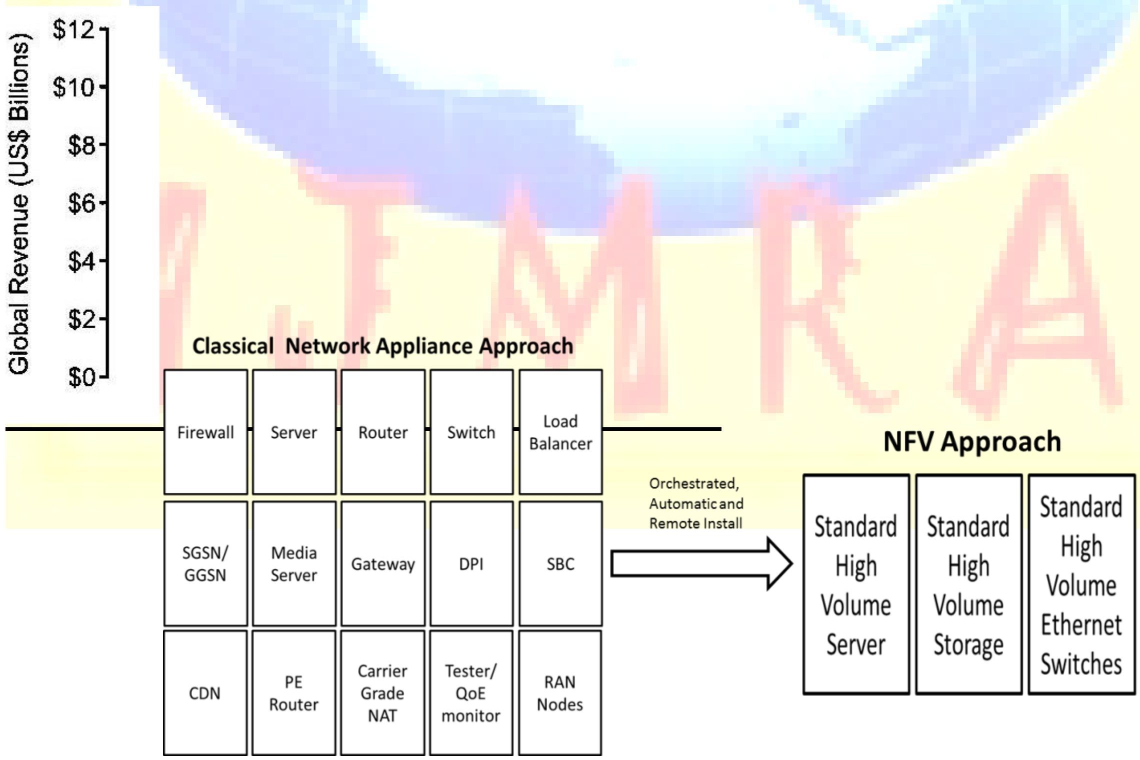

Figure 3 : Global NFV Revenue from Infonetics Research

1.3 NFV Timeline

According to experts, the last two years from 2013, have provided almost all the requirements to service providers for deployment of NFV in their networks. Two years of continuous trials and POC's (almost 33 according to ETSI), this year sets a perfect platform for few NFV use cases like v CPE to be deployed especially in the enterprise network. More than 100 NFV solutions in different segments are readily available for use by the service providers, fulfilling all the criteria of NFV implementation. OSS / BSS functions are yet to be virtualized; hence the present NFV solutions must integrate with the already existing OSS/BSS functions. The Service providers are taking one step at a time i.e. virtualizing only few network functions and not all. The widespread implementation of NFV in the service provider network will still take a few more years.

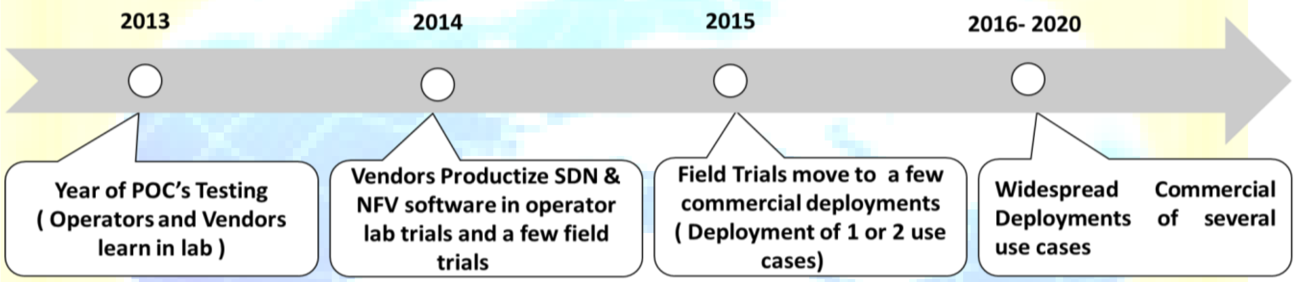

Figure 4: NFV Timeline

1.4 Standard Development Bodies and Committees

Many standard organizations have contributed towards development of NFV concept globally in the past few years. Some of them are

1.4.1 ETSI ISG

ISG is an Industry Specific group that was formed under the support of the European Telecommunications Standards Institute (ETSI) with the vision of NFV Implementation i.e. to convert today's hardware applications into fully virtualized appliance environment.

1.4.2 TM Forum

TM Forum is an industry group that is closely associated with the development of NFV. TM Forum announced its ZOOM project i.e. Zero-touch Orchestration, Operations and Management Project in 2014that defines a vision of the new virtualized operations environment, and a management architect based on the interaction between physical and virtual components. The main goal of ZOOM is to compliment the ongoing work of ETSI and other industry leaders

1.4.3 Internet Engineering Task Force

IETF has just started with its efforts to play a significant role in the evolution of standards for NFV. IETF play a vital role in creating standards that fit into the overall architectural frameworks defined by the ETSI NFV ISG. The IETF Service Function Chaining concept is an important capability of NFV networks. It provides efficient security architecture for NFV networks.

1.4.4Open Platform for NFV (OPNFV)

The Linux Foundation announced the establishment of the Open Platform for NFV Project (OPNFV)in September 2014. OPNFV will create a carrier-grade, combined, open source reference platform that will help in the advancement of NFV and also ensures consistency, performance and interoperability among multiple open source components.

1.4.5 3 GPP™

The 3GPP™ is the standards developing organization that defines the Network Architecture and specifications for the Network Functions (NFs) for mobile and converged networks. Hence it plays an important role in defining specifications for virtualized mobile environments like EPC and IMS.

2.Challenges /Problems Faced by Network operators in current architecture

Each new disruptive technology evolves with the aim of overcoming the shortcoming of the previous one. The limitations and faults in the traditionally deployed network architectures have forced the network operators to look for a more effective and efficient network implementation**[5].** The major factors that influenced the network operators to look forward to the shift are explained as follows:

2.1 Humungous capital investment on proprietary dedicated hardware

Thenetwork operators have to incur huge capital investment in deployment of variety of proprietary based dedicated hardware appliances for every new service that is to be rolled out, in order to match up with the current market trends, to keep up with the quality of service to serve several users and also manage the increased dependency on proprietary hardware vendors.

2.2 Continuous decline in revenues

Increasing disparity between costs and revenues is being faced by Network operators due to decrease in average revenue per user (ARPU) for voice and messaging services and also increasing competition from OTT players. Hence need for new innovative services with low costs incurred are required so that telecom operators can be back in the game and focus on increasing their revenues so that they may be able to balance out their huge investments like on spectrum and equipment.

2.3 Network Complexity

The Telecom operators are facing increased complexity problem due to large variety of proprietary hardware appliances that is deployed in their networks to deliver various services. For rolling out a single new service, operators have to place multiple dedicated appliances so that anend service is provided to the customer. Hence due to increase in the number of equipment also complicates the interconnectivity between the devices.

2.4 Limited Hardware Lifecycle

The operators have already invested huge amounts in deploying the current architecture but every equipment has a limited lifecycle.Reduced hardware lifecycles leads to purchase of new appliances in order to assure service continuity which adds on to the already bearing capital expenditure. Even if the operators try to prolong hardware's life period still they have to pay a lot to the vendors in terms of maintenance cost. The network operators are completely dependent on the vendors from whom they have purchased the equipment due to proprietary issues.

2.5 Flexibility and agility issues

Lack of flexibility and agility in present network hardware architecture leads to the problem of service unavailability as network resources cannot move where & when needed which directly affects customer experience.

2.6 Hindrances in Time to market and Service Innovation

It is difficult to launch new services before completion of the lifecycle of existing services that is about one year and it often gets prolonged as yet another proprietary box is required to be integrated into existing systems. Hence this affects the operator's differentiation strategies to compete in the market as it has to limit itself in rolling out new services faster and in less time.

2.7Increased Power Consumption

Due to deployment of numerous and heavy network devices, it increases the need for cooling mechanism which adds on to the already high levels of power consumption. This only leads to increase in operational costs.

According to various research papers and white paper the major drivers of NFV are scalability in terms of either scaling up/down i.e. changing the scale of allocated resource, e.g. increase/decrease memory, CPU capacity orstorage size etc. or scaling out/ini.e.ability to scale by add/remove resource instances (e.g. VM) high costs in terms of investment on bulky equipment's and delayed service innovations. In a highly competitive NFV market, the solution providers are focussing on building their solutions which are free of the above problems.

3. NFV Framework and its Ecosystem

3.1. NFV Framework

The NFV framework four major constituents:

3.1.1NFV Infrastructure

NFVI provides the virtual resources (compute, storage and network) which are essential to support the implementation of the Virtualised Network Functions (VNFs). It includes Commercial-Off-The-Shelf (COTS) hardware, accelerator components, wherever it is required, and a software layer which virtualises the fundamental hardware.The companies involved in providing the NFV infrastructure are Redhat, CISCO, IBM, DELL,Intel.

3.1.2Virtualized Network Function

VNF is a software basedapplication of a network function which is capable of running over the NFVI. It consists of an Element Management System (EMS) which understands and manages an individual VNF. The VNF is the entity which is delivered as pure software free from hardware dependency.

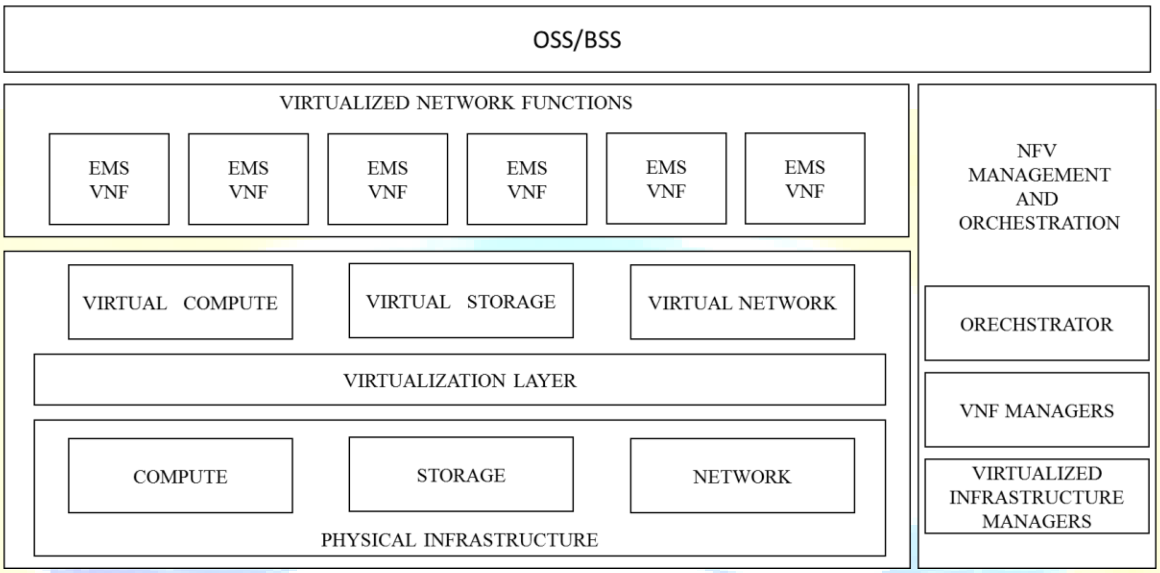

Figure 5: NFV Framework

3.1.3NFV Management and Orchestration

NFV MANO supports the infrastructure virtualization, and the lifecycle management of VNFs. It focuses on the virtualisation-specific management tasks necessary in the NFV framework and also interacts with the NFV's OSS/BSS landscape, which enables NFV to be assimilated into an already existing network-wide management landscape.

3.1.4OSS/ BSS

Operations support system and business support system are external to NFV framework that helps align the various information models and business processes in an efficient manner.

3.2 NFV Ecosystem

A successful NFV solution needs to merge hardware, software, communication and network services. Since each solution is customized, various stakeholders are required to come together to conceptualize, describe scope, develop, check and sustain a solution. Pushing NFV into new frontiers without a strong partner ecosystem is going to be adifficult task. Each of the below actors play a significant role in providing a complete end to end optimized NFV solution that will help built the networks in various fields of telecommunications.

The different ecosystem players are:

3.2.1 Infrastructure Providers

NFVI providers are vendors that provide the hardware and software resources i.e. high volume standard computing, storage and network equipment that provides processing, storage and connectivity to VNF's through the virtualization layer. NFVI providers include Merchant silicon/ Chip Vendors, NFV Hardware (Server) Vendors, NFV Storage Vendors and Hypervisor Vendor.

3.2.2 VNF's Providers

These are also called NFV application provider. A VNF provider is a vendor who provides software based virtualized instantiations of network functions like routers, load balancers, firewall etc., collectively referred to as a Network Service that are deployable on either single or multiple virtual machines in both virtualized and non-virtualized environments. Element Management System (EMS) manages a VNF by setting, monitoring and logging its fault, configuration, accounting, performance and security (FCAPS).

3.2.3 Management and Orchestration Providers

NFV MANO providers are vendors that provide a set of operational systems that support NFV Infrastructure. It includes Orchestrator, VNF Manager, Virtualized Infrastructure Managers and Cloud Management Platform vendors. NFV MANO is responsible for managing and maintaining data repositories, reference points and interfaces that are used to exchange information between all the components that make up the service.

3.2.4 OSS/ BSS Solution Provider

OSS/ BSS solution provider provide management systems that help providers deploy and manage various end to end telecommunication services such as ordering, billing, renewals, troubleshooting etc.

3.2.5 Cloud Management Platform Providers

These are also called Cloud Service Providers.Operators need to ensure that their networks deliver value to the users in different and unique ways. Network Functions Virtualization technology will enable common management and orchestration across network resources and cloud applications**[6].**

3.2.6 Testing, Measurement and Monitoring Solution Providers

They are vendors that provide innovative network testing, development and monitoring solutions for network service providers, cloud service providers, data centres, and Enterprise IT and network equipment vendors.

3.2.7 Standard Bodies and Committees

These are the organizations who are involved in formulating the NFV concept and developing it.

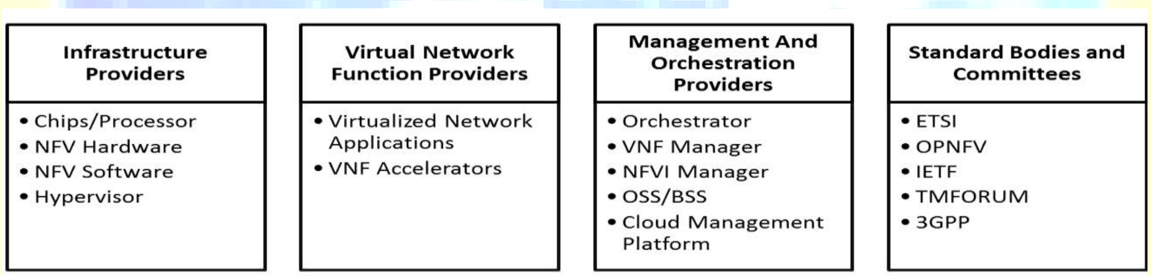

Figure 6: NFV Ecosystem

The major companies involved in the NFV ecosystem under each vertical head are**[7]:**

a) **NFV Infrastructure providers** - 6wind, Aricent, Cavium, Inc,ConteXstream, Intel Corporation,Metaswitch Networks,MRV, RAD, Red Hat, Dialogic Corporation

b) **NFV Management and Orchestration** providers - Alcatel Lucent, Amartus, Cisco System, Inc, Cyan, Inc, Hewlett- Packard Company, Juniper Networks, Overture Networks, Brocade, Luxoft

c) VNF Providers - 6wind, Allot Communications, Brocade,Cisco System, Inc¸Ericsson¸ Hewlett- Packard¸Juniper Networks, Metaswitch Networks, NEC/ Netcracker, Overture Networks, Procera Networks, QOSMOS, RAD, F5 Networks, Mavenir, Dialogic Corporation

d) VNF Component providers - Allot Communications, MRV, Procera Networks, QOSMOS

4. NFV Applications and Use Cases

4.1 NFV Applications

NFV applications are various areas in the network infrastructure of the Telecom/ Network service provider where the technology can be applied so as to avail the proposed benefits. The various important NFV Applications are:

4.1.1 Data protection, integration and security applications

These applications are important in a virtualized environment to promise complete segregation among users. Data Encryption of hidden content and link security is mandatory.Special considerations should be made to protect the data and configuration files.

4.1.2 Dynamic Bandwidth on Demand Applications

Buildthe capability to dynamically increase (or decrease) the amount of bandwidth as per the changes in the demand to enable optimized bandwidth provisioning for large number of Virtualized devices.

4.1.3 Network Security applications

These applications will enable protection of new interface showing the interconnectivity of NFV to end-to-end architectural components, guaranteesseparation of distinct VNF sets executing over NFVI and secure management of VNF sets from 3rd parties.

4.1.4 VNF Testing and Monitoring applications

These applications provide a platform for continuous monitoring of infrastructure requirements of a VNF and collect performance related information regarding usage of compute, storage, networking resources.

4.1.5 Traffic Engineering Applications

These applications will enable complete traffic management and control mechanisms including flexible traffic selection criteria and traffic analytics.

4.2 NFV Use Cases

ETSI ISG consolidated all the above application areas into 9 general environments also known as NFV use cases**[8].** Various Global telecom service providers have begun to implement NFV use cases in various countries on a trial basis. The use cases are as follows:

4.2.1 VNFaaS– Virtual Network Function as a service adopts the cloud computing notion of software as a service in which VNF functionality is made available to the enterprise as a service.

4.2.2 VNF FG – Virtual Network Function – Forwarding graphs also known as Service Function Chaining (IEEE) defines how the packet traverses through the sequence of VNFs.

4.2.3 Virtualization of Mobile Core Network &IMS- In this environment all the network functions involved such as HSS, MME, PGW, PCRF, GGSN, SGSN, MRF, APP Servers etc. can be targeted for virtualization.

4.2.4 Virtualization of Content Delivery Networks – The components of content delivery networks can be virtualized so as to meet the increasing requirements for quality of video delivered via IP networks.

4.2.5 NFV Infrastructure as a Service - This use case provides an approach to map two combined cloud computing service models of Infrastructure as a Service and Network as a Service as elements of NFVI , hence providing an environment in which VNF's can execute.

4.2.6 Virtualization of Fixed Access Network– The virtualization of fixed access network will able to change the trend of DSL and ADSL 2+ to higher standards of VDSL and above to provide very high data rates.

4.2.7 Virtualization of Home Environment– In this use case all the network functions involved as part of residential gateways and home setup box can be targeted for virtualization.

4.2.8 Virtualization of Mobile Base Station - This use case focuses on leveraging the benefits of IT virtualization technology to realize at least a part of RAN nodes on Standard IT servers, Storage and switches.

4.2.9 NFV Platform as a Service – In this use case service provider will be able to make available a suite of infrastructure and applications as a platform on which enterprise can deploy their network applications.

5.Proposed Benefits of Network Function Virtualization to Telecom Network Operators

Network functions virtualization (NFV) promises the service providers to moderate the burden by granting the flexibility to move from multiple dedicated equipment and integrate onto equivalent generic industry standard devices by using standard IT virtualization as it will make the network more agile and efficient**[9].**

5.1 NFV paves the Way to Improved Cost Efficiencies

Nowadays telecom providers and network operators are looking for cost effective alternative to virtualize workloads on industry standard servers. NFV provides a cost-effective solution to the capital cost of hardware with the intelligence delivered via virtual hypervisors. It reduces equipment costs and power consumption by merging various network equipment onto standard COTS servers. For Example: A hardware router in a small branch size company costs about $18,935 whereas a software router with the same services costs about $ 14,435. Hence, companies ranging from small to large size can save their CAPEX cost by utilizing the benefits of NFV in their architecture**[10].**

NFV provides with the facility of running production, test and reference on the same infrastructure that provides much more efficient test which leads to reduced development costs. This eliminates the need for application specific hardware and provides cost effective solutions to reduce the development costs.

5.2 NFV improves Time to Market velocity

NFV enables rolling out of new services by reducing the typical network operator cycle. Cost required for hardware would no longer be applicable for software-based development. Software development for a virtualized application is less constrained than in a typical embedded system. This not only reduces the time needed to develop apps, but also to add new features as there are more development tools, fewer memory constraints, faster CPUs and a wider pool of engineers capable of programming in a standard environment.

Moreover it does not rely on specific hardware. With virtual applications, there is no need to wait for equipment orders to arrive and hardware to be installed. New services can be launched on the existing server infrastructure. NFV try out services with lower risk and hence reduces the time-to-market for deploying newadvanced services to customers.

5.3NFV provides Continuous Service Availability

There will be no geographic or site limitations for introduction of new service. Rapid scaling up / down of service can be done as per requirement. Remote provisioning in software improves service without any need to install new hardware. NFV thus delivers continuous availability with geographic redundancy for virtualized and cloud environments.

5.4Open Ecosystem

It enables a wide variety of eco-systems and encourages more openness and innovation by exposing the virtual market to pure software entrantsin order to bring new services and revenue streams quickly at much lower risk **[5].** Open source projects solve major technical implementation challenges of NFV by integrating, testing and validating Network Function Virtualization solutions thus resulting into increased industry-wide interoperability, reliability and efficiency that can shorten time to market. For Example: Red Hat is active in all of the projects which make up the OPNFV platform. They help to define the future open source NFV platform, includingOpen Stackas the Infrastructure-as-a-Service layer, Open Daylightand Open vSwitchfor virtual network etc.**[11]**

5.5Automatized traffic in real time

NFV technologies are critical in the service provider context to enable real-time, software-controlled configuration of the underlying networking infrastructure in a fully automated manner. But there is no need of manual configurations as topology changes. NFV helps to optimize network configuration in real time onto the actual traffic/mobility patterns and service demand.

5.6Multi-tenancy capability

NFV allows network operators to provide services and connectivity for numerous users, applications or other network operators, all co-existing on the same hardware with suitableprotected administrative domains.

Network Functions Virtualisation supports the coexistence of several types of network service by providing an effective production environment which can be used by diverse applications, users and tenants, hence enabling multi tenancy capabilities**[12].**

5.7Improved Energy efficiency, planning and provisioning

NFV exploits power management features in standard storage devices. The virtualisation aspect of network function assumes some separation of communication, storage or computing resources which implies changes in energy consumption. NFV framework also optimizes energy consumption on demand and manages power states as needed.

NFV platform enables flexible planning and provisioning capabilities for network providers. Network Functions Virtualization (NFV) improves flexibility and speeds provisioning by shifting legacy network functions from hardware appliances to software.

6. Challenges for NFV Implementation

NFV not only promises major business benefits for telecom operators, but also presents significant technical challenges for its implementation. High performance and distributed network bandwidth is required in order to virtualize various networking functions on a single standard device like server**[13].**A traditional environment doesn't deliver the required network performance. Various businesses will be able to deploy new services quickly and gain a competitive edge as NFV proposes to make networks more flexible, scalable, secure, and cost–effective but the various challenges involved after implementation of NFV in the existing architecture are predicted as follows:

6.1 Portability/Interoperability

The key issue for NFV is to design standard interfaces between not only a range of virtual appliances but also virtualized implementations and legacy equipment. As one of the goals of NFV is to promote openness, 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**[4].**

Portability/Interoperability is thus the ability to load virtual appliances standardised surroundings, provided by different vendors for different operator and also allow the operator to optimize the location and required resources of the virtual appliances without constrictions.

With interoperability, elements are not integrated to each other to form applications; rather, loosely coupled objects are connected by references to an information model. This approach enables applications to be assembled based on abstract contracts, which are logical models of a service with metadata references.

Hence a unified interface needs to be defined which clearly detaches the software from the underlying hardware, as represented by virtual machines and their hypervisors.

6.2Performance Trade-Off

Virtualization-aware appliances are the bridge between the networks of today and the software-based model of the future. They provide real-time insight that enables event- driven automation of policy decisions and real-time reaction to those events, thereby allowing the full promise of NFV to unfold**[14].**

It is better to use appropriate hypervisors and modern software technologies to keep the performance degradation as low as possible. Virtual appliances should be clearly aware about the capabilities of the underlying hardware.

6.3 Co-existence,relocation and compatibility of legacy system with existing platforms

NFV must be compatible and coexist with legacy network appliances and their existing EMS, NMS, OSS and BSS and Orchestration systems to enable efficient and profitable convergence of technologies and that can automate the configuration, deployment and scaling processes, thus providing a gradual migration path toward a fully elastic service, leveraging existing infrastructures**[14]**.

Hence, NFV should be able to effectively work in an amalgamation of both classical and virtual networks.

6.4 Consistent Management and Orchestration

Integration of new virtual appliances into an existing operating environment will become easy due to the flexibility provided by Software based implementations which rapidly align management and orchestration in an open standardised infrastructure.

It enables orchestration of the end-to-end NFV lifecycle, beginning with the deployment and management of the infrastructure resources and SDNs through monitoring and remediation. Users can define their own custom policies for handling complex processes and .procedures, such as continuous delivery and/or rolling upgrades, for increased agility and faster time.

Example: Alcatel-Lucent CloudBand is the first-to-market carrier grade NFV management and orchestration (MANO) platform purpose-built for service providers. It offers high availability service deployment and assurance capabilities**[15].**

6.5 Automation and Integration

Service providers must automate security processes and implement as part of the management system that oversees the cloud environment in all data centres and compute nodes. A centralized management system for command and control can ensure systematic and consistent implementation of security. Effective scaling is only possible if the functions can be automated.

Also, operators need to pay attention to operational process integration with NFV resource management solutions that handle required complexity and functions at the lowest level.Key challenge for NFV is to seamlessly integrate multiple virtual appliances onto existing industry standard high volume servers and hypervisors. Hence "mix & match" of servers, hypervisors and virtual appliances from different vendors should be taken care of without incurring significant integration costs.

6.6 Security & Resiliency

During deployment of virtualized network, operators have to make sure that the security features of their network are not affected. NFV uses virtualisation technology to provide networking services, so it is important to assure that the security of this new combination is not affected.**[16]**

NFV enables faster arrangement of critical security upgrades and allows customers to securely migrate from computing to cloud by delivering a robust and easy to operate virtual network. Several cloud service providers have deployed "zero knowledge" security in which only their customers have the keys to decrypt the stored data. **[17]**

Network Functions Virtualisation allows network functions to be rebuilt on demand after a failure which improves network resilience and availability. The level of security for a physical appliance in the infrastructure should be same for virtual appliance as well; especially the hypervisor.

6.7 Network Stability and Simplicity

To ensure service stability is another challenge for NFV, especially while relocating a large number of software-based virtual appliances from different vendors and running onto 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.

During relocation and reconfiguration events, potential instability might occur in the networks which may jeopardize the performance. Hence mechanisms capable of ensuring network stability must be built to add on to the benefits of NFV.

Moreover, NFV ensures that virtualized platforms will enable simpler operations than already existing complex network platforms and support systems while ensuring continuous support to new revenue generating services. Hence this becomes a primary concern for network operators to see if NFV fulfils its promises or not.

7. Conclusion

NFV thus enables the separation of network functions from dedicated hardware using a private carrier cloud infrastructure. It allows service providers greater freedom in distributing service functionality throughout a network coverage area, and network functions can be shared across common hardware. NFV will bring not only cost efficiencies but will also improve time-to-market for rolling out of new services and bring innovation to the telecommunication industry infrastructure and applications. It will be achieved through disaggregation of the traditional technology involved in telecommunications applications. To run a distributed NFV infrastructure efficiently, a number of challenges concerning networking, hardware, power consumption etc. need to be addressed so that the operators have the flexibility to relocate network functions from dedicated appliances to industry-standard, high-volume servers, switches and storage. Hence the Service providers are taking one step at a time i.e. virtualizing only few network functions and not all. The widespread implementation of NFV in the service provider network will still take a few more years.

References

[1] Alan Weissberger,' China's Subsidized Broadband Investments Boosts Growth in Global CPE Market (IHS & China State Council)', COSMOC communities , IEEE Communications Society [Blog] http://community.comsoc.org/blogs/posts

[2] http://www.ciscoway.com/

[3] SDN and NFV Strategies: Global Service Provider Survey Carrier SDN and NFV Hardware and Software Report, Infonetics Research , March 27, 2014

[4] Network Functions Virtualization (NFV) Market: Business Case, Market Analysis and Forecasts 2015 – 2020, February 2015, Research and Markets

[5] 'Network Functions Virtualisation (NFV) : Network Operator Perspectives on Industry Progress', European Telecommunications Standards Institute (ETSI) NFV Industry Specification group ,Issue 1, October 15-17, 2013 [Online] https://portal.etsi.org/nfv/nfv_white_paper2.pdf

[6] 'Why a Cloud Management Platform (CMP)?' , Scalr, 2015 [Online] http://www.scalr.com/whyacmp

[7] Network Functions Virtualization Report: Market Report , SDxCentral, 2015 Edition

[8] 'Network Functions Virtualization : Use Cases', European Telecommunications Standards Institute (ETSI) NFV Industry Specification group , 2013

[9] http://www.networkcomputing.com/networking/5-nfv-benefits-and-the-trends-driving-them/a/d-id/1269263

[10] 'Network Functions Virtualization : An Introduction, Benefits, Enablers, Challenges & Call for Action', European Telecommunications Standards Institute (ETSI) NFV Industry Specification group ,Issue 1, October 22-24, 2012.[Online] https://portal.etsi.org/nfv/nfv_white_paper.pdf

[11] Dave Neary, 'Upstream First: Turning OpenStack into an NFV platform', 2015 [Online] http://community.redhat.com/blog/2015/03/upstream-first-turning-openstack-into-an-nfv-platform/

[12] Virtualized EPC: Delivering on the promise of NFV and SDN, Alcatel Lucent, 2014

[13] Glen Ragoonanan and Anil Rao, 'SDN and NFV at a crossroads: vendors innovating and positioning for the future of CSPs' network virtualisation' , September 2013, Analysys Mason

[14] Bo Han, Vijay Gopalakrishnan, LushengJi and Seungjoon Lee, 'Network Functions Virtualization: Challenges and Opportunities for Innovations' AT&T Labs Research Bedminster, NJ 07921, USA http://web2-clone.research.att.com/export/sites/att_labs/techdocs/TD_101400.pdf

[15] Cloud-based Authoritative Domain and Caching Name Service (DNS)' , Alcatel Lucenthttps://www.alcatel-lucent.com/solutions/cloudband

[16] 'Network Functions Virtualisation (NFV) : Network Operator Perspectives on Industry Progress European Telecommunications Standards Institute (ETSI) NFV Industry Specification group ,Issue 1, October 14-17, 2014 https://portal.etsi.org/Portals/0/TBpages/NFV/Docs/NFV_White_Paper3.pdf

[17] Sarah Murry, Connected Blog, Rajiv Ramaswami in Silicon India: "NFV Can Make Networks Agile, Cost-Effective, Scalable and Secure", Broadcom, 1 September 2014 ,http://www.broadcom.com/blog/network-infrastructure/rajiv-ramaswami-in-silicon-india-nfv-can-make-networks-agile-cost-effective-scalable-and-secure/