**CHAPTER TWO**

**LITERATURE REVIEW**

**2.1 Introduction.**

This chapter is a comprehensive overview of scholarly articles, reports, and other documents that discuss Networking as they relate to the virtualization processes. It aims to provide an understanding of the current state of research and applications in the field of NFV, as well as to identify potential areas for further exploration. The review begins with an exploration of the available literature on the topic, evaluating the current state of NFV research and solutions, and discussing the key topics in this domain. It then examines the potential uses of NFV for IT improvement, discussing potential benefits and challenges associated with the use of NFV. Finally, the review presents an examination of the existing solutions and potential solutions for NFV.

**2.2 Generalities.**

To accelerate progress towards this common goal, service providers world-over came together to work it out with different standardization 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 equipment 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 Virtualization aims to transform the way, the network operators’ architect networks, by evolving standard IT virtualization technology to consolidate many networks equipment types onto industry standard high-volume servers, switches and storage, which could be located in Data centers, 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 Virtualization promotes the implementation of network functions in software that can run on a range of standard IT hardware in data centers and can be managed (e.g., moved, or replicated) without the need of modifying the physical infrastructure.

**Figure 2. 2: Vision for Network Functions Virtualization (Source: ETSI)**

* 1. **ETSI NFV Industry Specification Group**

Seven of the world’s leading telecoms network operators initiated ETSI Industry Specification Group (ISG) for NFV. These have been quickly joined by over 280 companies including network operators, telecoms equipment vendors, IT vendors and technology providers. ETSI has created the NFV ISG to define the requirements and architecture for the virtualization of network functions and to address their technical challenges.

These technical challenges include:

* Ensuring that virtualized network platforms will be simpler to operate than what exists today.
* Achieving high performance virtualized network functions which are portable among different hardware vendors, and different virtualization support systems.
* Achieving co-existence with legacy hardware-based network platforms whilst enabling an efficient migration path to fully virtualized network platforms.
* Management and orchestration of virtual network functions (particularly alongside legacy management systems) while ensuring security from attack and misconfiguration.
* Maintaining network stability and service levels without degradation during appliance load and relocation.
* Ensuring the appropriate level of resilience to hardware and software failures.
* Enabling the creation of virtual network appliances which will run, ideally without recompilation, on any hypervisor and hardware configuration, and integrate “on the fly” into the network operators’ existing management and orchestration systems.
* Analyzing requirements for future technical specifications and standards in relevant standardization organization and groups to be identified or created at ETSI and other ad hoc standards development organizations.
* Minimizing energy consumption

Since its creation in 2013, NFV ISG has published over 119 documents. The first release delivered end 2014 defined high level use cases and requirements, proposed a unified terminology for virtualization, defined an architectural framework, and described management and orchestration functions. Also included in this release were the infrastructures requirements for the compute, hypervisor and network domains. Other specifications covered best practices in security and resilience, performance and portability.

Release 2 outlines the necessary functional requirements in relation to a wide set of functional areas, such as management of virtualized resources, lifecycle management, network service fault/performance management, virtualized resource capacity management, etc.…

Release 3 development is ongoing. It will build on top of the work already delivered and plans to include 23 new Features.

NFV ISG has also defined a framework for coordinating and promoting public demonstrations of Proof of Concept (PoC) demonstrations illustrating key aspects of NFV. The objective is to encourage the development of an open ecosystem by integrating components from different players. The PoC concept has proven to be very popular and the number of individual PoC demonstrators listed on the ETSI website has continued to grow.

**Figure 2.3 ETSI release evolution summary**

## 2.4 Considerations while planning & designing NFV’s

Planning and designing NFV deployments in Telco cloud environments requires careful consideration of various factors to ensure a successful implementation. Here are some key aspects that service providers need to keep in mind:

* **Hardware Requirements**: Service providers need to carefully assess the hardware requirements for their NFV deployments. This includes selecting appropriate server hardware that meets the performance, scalability, and reliability requirements of the virtualized network functions (VNFs) being deployed. Factors such as CPU, memory, storage, and networking capabilities need to be considered, along with redundancy and fault tolerance requirements. Proper sizing and provisioning of hardware resources are essential to ensure optimal performance and resource utilization in the Telco cloud environment.
* **Network Architecture**: The network architecture plays a crucial role in the success of NFV deployments. Service providers need to carefully plan and design the network architecture to ensure efficient traffic flow, high availability, and optimal performance of VNFs. This may involve considerations such as network segmentation, routing, switching, load balancing, and quality of service (QoS) policies. Proper integration of VNFs into the existing network infrastructure or designing a new network architecture that aligns with NFV principles is crucial to ensure smooth operations and reliable service delivery.
* **Operational Processes**: NFV deployments require well-defined operational processes to ensure smooth operations and efficient management of VNFs. This includes processes for VNF onboarding, provisioning, scaling, upgrades, monitoring, troubleshooting, and decommissioning. Service providers need to establish standardized operational processes and workflows to streamline the management of VNFs in the Telco cloud environment. Automation and orchestration tools can also be utilized to simplify operational processes and ensure consistency in managing VNFs across the entire lifecycle.
* **Testing and Validation**: Proper testing and validation of VNFs and their integration into the Telco cloud environment is essential to ensure their stability, reliability, and performance. Service providers need to establish rigorous testing and validation procedures to verify the functionality and performance of VNFs before deployment. This may involve testing VNFs in isolation, as well as in integrated environments with other VNFs and the overall Telco cloud infrastructure. Comprehensive testing and validation help identify and resolve potential issues early in the deployment process, minimizing downtime and service disruptions.
* **Scalability and Flexibility:** NFV deployments should be designed with scalability and flexibility in mind. Service providers need to plan for the ability to scale VNFs up or down based on changing demands, as well as the flexibility to deploy new VNFs or decommission existing ones as required. This may involve considerations such as dynamic resource allocation, automated scaling, and elasticity in the Telco cloud environment. Ensuring scalability and flexibility in the NFV deployment allows service providers to meet evolving business and operational requirements in a cost-effective manner.

**2.5 NFV ARCHITECTURE:**

The Network Function Virtualization (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), Virtualized 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 NFVIPoPs are operated. The network providing connectivity between these locations is regarded to be part of the NFVI.
* **Virtualized Network Functions (VNF**s) are software implementations or virtualization 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 virtualization specific management task necessary in the NFV framework.

**2.5 HIGH LEVEL NFV**



**Figure 2.5: high level NFV**

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 Virtualized 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.

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 centers.
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 Virtualization (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.

**2.6 Network Services**

An end-to-end network service can be described by an NF Forwarding Graph of interconnected Network Functions (NFs) and end points These network functions can be implemented in a single operator network or interwork between different operator networks. Some architectural options reported in GS NFV-IFA 009. The underlying network function behavior contributes to the behavior of the higher-level service.

The end points and the network functions of the network service are represented as nodes. These nodes correspond to devices, applications, and/or physical server applications. An NF Forwarding Graph can have network function nodes connected by logical links: Example: **chain of network functions**. NFV area of activity within the operator-owned resources Customer-owned devices are out of the scope. But virtualization and network-hosting of customer functions is possible and is in the scope of NFV Network service behavior: combination of the behavior of its functional blocks (individual NFs, NF Sets, NF Forwarding Graphs, and/or the infrastructure network).



**2.7 NFV Principles**

VNFs are the building blocks used to create end-to-end network services. Three key NFV principles are involved in creating practical network services:

* **Service chaining**

VNFs are modular and each VNF provides limited functionality on its own. For a given traffic flow within a given application, the service provider steers the flow through multiple VNFs to achieve the desired network functionality

* **Management and orchestration (MANO)**

Deploying and managing the lifecycle of VNF instances. Examples: VNF instance creation, VNF service chaining, monitoring, relocation, shutdown, and billing. MANO also manages the NFV infrastructure elements

* **Distributed architecture**

A VNF may be made up of one or more VNF components (VNFC)

* Each VNFC implements a subset of the VNF’s functionality
* Each VNFC may be deployed in one or multiple instances. These instances may be deployed on separate, distributed hosts to provide scalability and redundancy.

**2.8 Implications of NFV**

The NFV architectural framework addresses the following:

* The functionality that is required to be realized by the NFVI (NVFI).
* The functionality that is required due to decoupling network functions into software and hardware (NFV).
* The functionality that is required for NFV-specific management and orchestration (MANO).

|  |  |
| --- | --- |
| **Term** | **Definition** |
| **Compute domain** | Domain within the NFVI that includes servers and storage |
| **Infrastructure network domain** | Domain within the NFVI that includes all networking that interconnects compute/storage infrastructure |
| **Network Function (NF)** | Functional block within a network infrastructure that has well-defined external interfaces and well-defined functional behavior. Typically, a network node or physical appliance |
| **Network Functions Virtualization (NFV)** | Principle of separating network functions from the hardware they run on by using virtual hardware abstraction |
| **Network Functions Virtualization Infrastructure (NFVI):** | The totality of all hardware and software components that build up the environment in which VNFs are deployed. The NFV-Infrastructure can span across several locations. The network providing connectivity between these locations is regarded to be part of the NFVI |
| **NFVI-Node** | Physical device[s] deployed and managed as a single entity, providing the NFVI Functions required to support the execution environment for VNFs |
| **NFVI-PoP** | N-PoPwhere a Network Function is or could be deployed as Virtual Network Function (VNF) |
| **Network forwarding path** | Ordered list of connection points forming a chain of NFs, along with policies associated to the list |
| **Network Point of Presence (N-PoP)** | Location where a Network Function is implemented as either a Physical Network Function (PNF) or a Virtual Network Function (VNF) |
| **Network service** | Composition of Network Functions and defined by its functional and behavioral specification |
| **Physical Network Function (PNF)** | An implementation of a NF via a tightly coupled software and hardware system. This is typically a proprietary system |
| **Virtual Machine (VM)** | A virtualized computation environment that behaves very much like a physical computer/server |
| **Virtual network** | A topological component used to affect routing of specific characteristic information. The virtual network is bounded by its set of permissible network interfaces. In the NFV architecture, a virtual network routes information among the network interfaces of VM instances and physical network interfaces, providing the necessary connectivity |
| **Virtualized Network Function (VNF)** | An implementation of an NF that can be deployed on a NFVI |
| **VNF Forwarding Graph (VNF FG)** | Graph of logical links connecting VNF nodes for the purpose of describing traffic flow between these network functions |
| **VNF Set** | Collection of VNFs with unspecified connectivity between them |

**2.9 NFV Terminology**

**2.10 NFV REFERENCE ARCHITECTURE**



**Figure 2.10: NFV REFERENCE ARCHITECTURE**

* **NFV infrastructure (NFVI)**

HW and SW resources that create the environment in which VNFs are deployed. NFVI virtualizes physical computing, storage, and networking and places them into resource pools.

* **VNF/EM**

Collection of VNFs implemented in SW to run on virtual computing, storage, and networking resources, and Collection of element management systems (EMS) that manage the VNFs

* **NFV management and orchestration (NFV-MANO)**

Framework for the management and orchestration of all resources in the NFV environment (computing, networking, storage, and VM resources)

* **OSS/BSS**

Operational and business support systems implemented by the VNF service provider.

The NFV Management and Orchestration (MANO) includes the following functional blocks:

* **NFV orchestrator (NFVO)**

Responsible for installing and configuring new network services (NS) and virtual network function (VNF) packages, NS lifecycle management, global resource management, and validation and authorization of NFVI resource requests

* **VNF manager (VNFM**)

Oversees lifecycle management (e.g., instantiation, update, query, scaling, termination) of VNF instances.

* **Virtualized infrastructure manager (VIM)**

Controls and manages the interaction of a VNF with computing, storage, and network resources under its authority, in addition to their virtualization.

**2.11 NFVI**

The NFVI is the combination of both HW and SW components which build up the environment in which VNFs are deployed, managed and executed Can span across several locations Where NFVI-PoPsare operated. The network providing connectivity between these locations is considered part of the NFVI From VNF perspective, the virtualization layer and the HW resources are a single entity providing the desired virtualized resources

**2.11.1 NFVI: HW resources**

Physical resources include computing HW, storage and network (nodes and links). Computing HW assumed to be commercial-of-the-shelf (COTS). Storage resources can be shared network attached storage (NAS) or storage that resides on the server itself

* **Network resources**. 2 types of networks
  + - 1. **NFVI-PoPnetwork**
* Interconnecting the computing and storage resources contained in an NFVI-PoP
* Also includes specific switching and routing devices to allow external connectivity
  + - 1. **Transport network**

Interconnecting NFVI-PoPs, NFVI-PoPsto other networks owned by the same or different network operator, and NFVI-PoPsto other network appliances or terminals not contained within the NFVI-PoPs.

**2.11.2 NFVI: Virtualization layer and Virtualized resources**

Virtual resources are abstractions of the computing, storage and network resources. Abstraction achieved using the Virtualization layer, Decouples the VNF software from the underlying hardware, thus ensuring a hardware independent lifecycle for the VNFs Hypervisors and VMs for computing and storage resources. The virtualization layer is responsible of:

* Abstracting and logically partitioning physical resources
* Enabling the software that implements the VNF to use the underlying virtualized infrastructure
* Providing virtualized resources to the VNF, so that the latter can be executed

A VNF is envisioned to be deployed in one or several VMs. ETSI GS NFV-EVE 004 discusses other virtualization technologies. Not restricted to any specific virtualization layer solution E.g., In some cases, VMs may have direct access to hardware resources (e.g., network interface cards) for better performance. Hypervisors is one of the present typical solutions for the deployment of VNFs, but not the only possible one VNF operation should be independent of its deployment scenario. Network HW is abstracted by the virtualization layer to realize virtualized network paths that provide connectivity between VMs of a VNF and/or between different VNFs. Several techniques can be used, e.g., virtual networks and network overlays, such as VLAN, VxLAN, NVGRE, etc. Also considered approaches that centralize the control plane of the transport network and separating it from the forwarding plane, such as SDN.

**2.11.3 Virtualization Layering and NFVI Support**

The primary tools to realize the virtualization layer are the hypervisors. The NFV architectural framework should accommodate a diverse range of hypervisors. The primary means of VNF deployment is instantiating it in one or more VMs. The virtualization layer should provide open and standard interfaces, Independence of HW resources and portability, Performance and cost efficiency are also important.

* 1. **NFV MANO**
* **The MANO:** Provides the functionality required for the provisioning of the VNFs, and related operations the configuration of the VNFs, and the configuration of the infrastructure the VNFs run on. Includes orchestration and lifetime management of physical and/or software resources supporting the infrastructure virtualization and the lifecycle management of VNFs. Includes databases used to store information and data models defining deployment and lifecycle properties of functions, services and resources. Defines interfaces used for communications between components of the MANO, as well as coordination with traditional network management, such as OSS/BSS.
  1. **VNF States and Transitions**

A number of generic internal states represent the status of the VNF. Before a VNF can start its lifecycle, it has to be on-boarded. On-boarding: process of registering the VNF with the NFVO and uploading the VNF data (VNFD, SW images, etc.). On-boarding is the responsibility of NFVO

**Figure 2.13: VNF States and Transitions**

|  |  |
| --- | --- |
| **State** | **Description** |
| **Null** | **A VNF Instance does not exist and is about to be created** |
| **Instantiated Not Configured** | **VNF Instance does exist but is not configured for service** |
| **Instantiated Configured -Inactive** | **A VNF Instance is configured for service** |
| **Instantiated Configured -Active** | **A VNF Instance that participates in service** |
| **Terminated** | **A VNF Instance has ceased to exist** |

**2.14 Fields of Application and Use Cases**

Network Functions Virtualization is applicable to any data plane packet processing and control plane function in mobile and fixed networks. Potential examples that can be listed include: -

* **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

**2.15 Partial Conclusion**