DOI: 10.1561/9781638283591.ch2

Chapter 2

Network Function Virtualization (NFV)

NFV technology develops rapidly, significantly influencing the application of new networking concepts. It implies redesigning traditional, hierarchical, organized networks, implementing more flexible and scalable solutions, and a new concept of network infrastructure management. By operating in a virtual environment such as virtual machines (VMs) and containers, the NFV enables architecture scaling faster, easier, and without extra (specialized) hardware. For example, in the case of system failure on physical devices, the NFV can facilitate disaster recovery. We can relocate a virtual entity to another location in the network so regular functions can be resumed even more quickly. The absence of the need for additional hardware helps operators reduce operational expenses. The new pay-as-you-go business philosophy associated with applying the NFV concept and the cloud also helps clients reduce costs. That is why it can be said with great certainty that organizations are rapidly moving from using dedicated hardware with pre-implemented software to applying advanced software solutions on standard hardware. The significantly wider application of software technologies aims to ensure a substantially higher level of programmability in the network [9].

For the rapid acceptance of NFV technology, it is important to identify contemporary socio-economic trends and analyze the potential problems that follow the implementation of existing and future services in traditional computer networks. Therefore, it must be borne in mind that, besides the numerous advantages of the

NFV concept, certain risks slow down its wider application, primarily in operator networks. One risk refers to multiple standards and open-source initiatives (Open Platform for NFV, Open-Source MANO, Open Network Automation Platform, European Telecommunications Standards Institute – ETSI, and the Metro Ethernet Forum) that encourage NFV development. A clear architectural direction, which would provide acceptable conditions for all providers and operators, is necessary for the wider application of the NFV concept. Another risk is security in complex environments with the implemented NFV concept. Namely, it is essential to apply appropriate solutions to protect the physical layer, the virtualized layer, and the carrier application. This requirement additionally complicates the NFV setup.

Further, when moving from a physical to a virtual infrastructure, the degradation of network function performances may occur. Therefore, it is necessary to continuously monitor the performance of virtualized network functions and avoid potential traffic bottlenecks (e.g., a virtual switch can be a potential bottleneck between virtual machines and network services for different traffic). To correctly comprehend the changes, it is necessary to understand the importance of the transition from a hardware-based approach to a virtualized network approach based on the software [10].

Undeniably, the NFV concept, along with technologies such as software-defined networking (SDN), cloud and edge computing, and others, significantly affects telecom providers, technology vendors, and other players of the connected ecosystems. Widespread use of these technologies leads to further "softwarization" of network environments (5G and 6G networks), resulting in a new value chain for various industries, including public administrations. For example, many administrations implement citizen-centric, data-driven, and performance-focused governance, transforming their e-government system into a smart government [11]. This transformation implied the appliance of different virtualization techniques to solve problems from technical, financial, and privacy perspectives. Operators and providers have become aware of the need to build a more flexible, scalable, and resilient network infrastructure. The main feature of the new infrastructure must be a high degree of agility in responding to heterogeneous user requirements. In most cases, this refers to service requirements based on cloud technologies, new types of communication such as M2M (Machine-to-Machine), or the application of smart Internet of Things (IoT) environments [12]. In such circumstances, the role of NFV and other advanced software technologies is to "introduce" a significantly higher level of programmability into the computer network to create an appropriate basis for implementing and efficiently operating all services.

The rest of this section is organized as follows: Subsection 2.1 provides the characteristics of traditional, hierarchically organized networks and indicates shortcomings, whose solving is the motive for developing and applying the NFV concept.

Subsection 2.2 explains two main principles representing the NFV concept's basics. Further, we explain the ETSI NFV framework, application fields, and the role of VNF in modern computer environments in Subsection 2.3. Subsection 2.4. deals with the concept and the importance of the ETSI NFV framework application for modern ICT (Information and Communication Technology) trends and makes the general picture of the basic building blocks, with more detailed insight into the structure of each of them. Finally, Subsection 2.3.2 highlights the advantages of NFV deployment.

2.1 Computer Networks with the Traditional Architecture

Many computer networks still have the traditional, hierarchical network architecture model. A characteristic of this model (Fig. 2.1) is that numerous functionalities are defined on specially developed hardware, where specialized, proprietary software runs. When manufacturers design and build their equipment, they are guided by a generic set of requirements and offer functionality that combines specific hardware and software. Thus, hardware and software are integrated as a single entity and represent a certain manufacturer's property [9]. Such software remains the manufacturer's property (clients can use it under predefined conditions). Manufacturers want to protect their intellectual property. However, this approach restricts users'

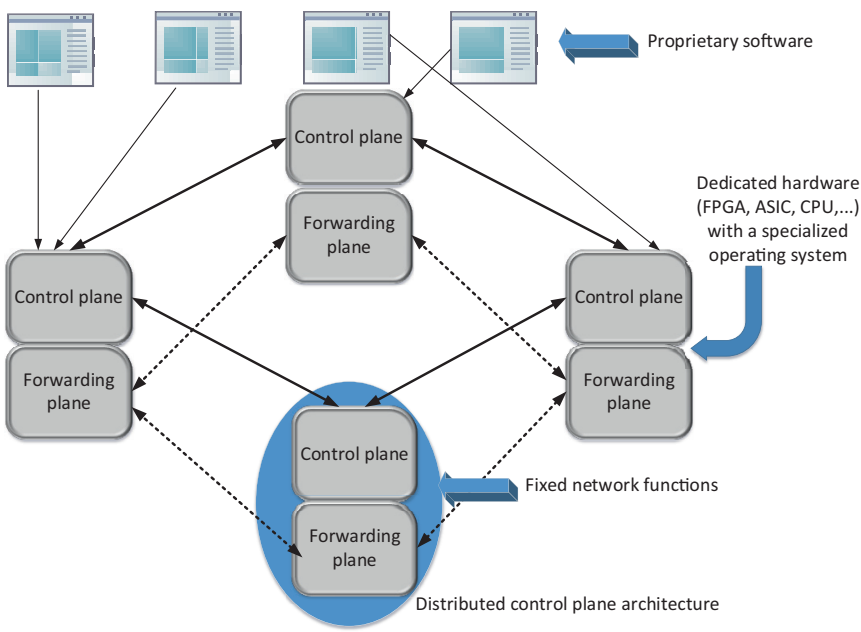

Figure 2.1. Characteristics of computer infrastructure in traditional networks.

rights to modify, distribute, or access its underlying source code, thereby diminishing flexibility and the possibility of rational use of available resources. Moreover, clients can become dependent on the manufacturer, which can produce negative effects from the financial and technical side (they must purchase equipment only from a certain manufacturer).

In real network environments, we meet numerous proprietary solutions, and the problem of establishing connections and communication between them (interoperability problem) is one of many problems we can encounter. Apart from the interoperability problem, the functioning of traditional computer networks is also significantly affected by the need to provide greater bandwidth. The emergence of new and more intelligent services (e.g., video, mobile, and IoT applications), as well as the exponential growth of the number of devices in the network, requires the engagement of significant resources and greater agility in the network. Telecom operators are challenged: How can they expand and scale network resources more effectively without increasing costs?

We must note that traditional networks have certain shortcomings which reduce operational efficiency, such as:

- Limited scalability due to the dependence on physical hardware devices.
- Low level of flexibility in coordinating between fixed-function network devices (require significant manual intervention).
- A single change can have a cascading effect because it can degrade the entire network's performance.
- A rigid, hierarchical architecture that is difficult to modify or adjust to varying user demands.

For example, to implement any hardware, providing a certain amount of electrical power and space for its accommodation is necessary, which can be a problem and an additional cost. Limitations also exist regarding software, as traditional network devices sometimes cannot keep up with changes in data networks (e.g., in terms of the number of routes to be created). In other words, traditional network devices are designed to function in a limited multidimensional space from the perspective of resources, so telecom operators have limited options for upgrading and expanding the network infrastructure.

Managing such a heterogeneous infrastructure is complex because there is no single management interface. For traffic measurement and computer resource load [13], monitoring tools are used with standardized monitoring protocols (e.g., Simple Network Management Protocol, NetFlow, and syslog). Often, more is needed, especially when monitoring parameters specific to certain manufacturers' equipment (e.g., the manufacturer uses a non-standard Management Information Base (MIB) or syslog messages). Work and business organization in

this environment represent a serious challenge for telecom providers. They must have highly trained staff capable of maintaining equipment from different manufacturers, which affects operating costs, i.e., increases them.

Traditional computer networks can only sometimes follow the changes in the ICT market and the constant growth of user numbers. The variety of service requests creates a need, initiates a network redesign, optimizes the system, and overcomes difficulties in choosing the appropriate equipment. The upgrade process is burdened with costs related to providing physical access to personnel who need to install new hardware, reconfigure the system, and perform service. Additional training or employment of newly trained personnel represents another cost and slows decision-making on acquiring and installing equipment from another manufacturer. This situation potentially leads to the "lock-in" of telecom providers with one manufacturer's equipment. Every change in network capacity that must be made to satisfy user requirements, even in a longer time interval, requires additional financial resources.

2.2 Fundamentals of NFV Concept

The rapid development of information technologies and the emergence of new forms of communication represent the main driving force behind the development of contemporary society. To enable continuous tracking of these trends, the academic and professional community must find adequate answers to numerous challenges. These challenges are mainly related to allowing the open and flexible implementation of new and increasingly demanding services, which can only be done in a flexible and scalable environment. Building such an environment is only possible through the continuous development and application of advanced software technologies, such as virtualization technology of the computer infrastructure and network as a whole [9].

Today, there is almost no computer network in which there is no virtual (logical) version of at least some devices, whether they are servers, operating systems (Oss), processors, data stores, switches, or routers. The virtualization technology itself has taken root, especially in data centers. Their physical infrastructure, consisting of many independent server systems, has already been largely replaced by virtual servers running on shared hardware. The NFV concept was built on the server virtualization technique, although it has a much larger scope today. It extends to network devices and enables the ecosystem to deploy and manage virtualized network entities. The implementation of the NFV concept in the network is based on two main principles:

- decoupling software from hardware, and

- building network functionalities independent of the network location (e.g., firewalls, load balancers, routers, customer equipment for connecting to the Internet, and even access devices can be implemented at any location with virtualized computing infrastructure).

The NFV concept is a technology that enables the construction of a specific ecosystem. That ecosystem comprises virtual network devices, management tools, and infrastructure that integrate these software solutions with computing hardware. In other words, this technology enables replacing physical devices that perform a network function with one or more software programs that serve the same function running on generic computer hardware (e.g., replacing a firewall with a virtual machine on a standard server). In this way, it is possible to build a suitable environment where network functions can be implemented on any generic hardware that offers basic data processing, storage, and transmission resources. The term COTS hardware is often used in practice and implies hardware that contains the required resources and can run any software (Fig. 2.2) [14].

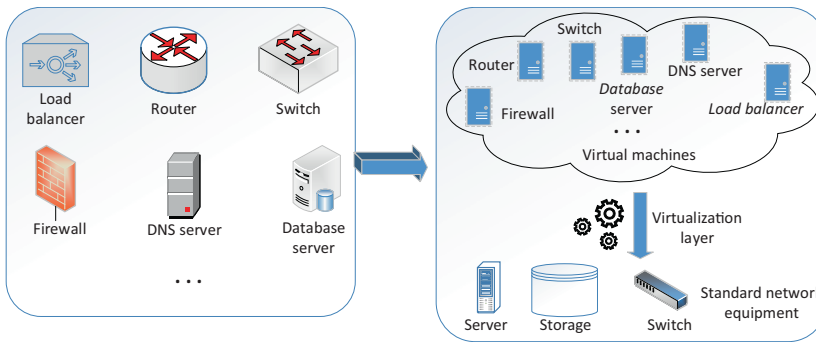

Figure 2.2. The transition from traditional to NFV networking concept.

In traditional computer networks, telecom operators fully control the hardware and software that performs a specific network function. However, the problem arises when user requirements change and when it is necessary to make quick changes in the network. The problem is most pronounced when it is needed to ensure the dynamic establishment of network functions and the rapid realization of the required services. That is why telecom operators, in such situations, opt for the application of NFV technology, with the important assumption that they have standard equipment with the necessary resources at the location [15]. Therefore, virtualizing the computer infrastructure and the network opens some new possibilities regarding configuration and network management. Through the application of open software interfaces, it is possible to create a flexible and scalable environment with the necessary level of agility to solve all user requests, realize certain innovations, and implement new network architectures optimally and efficiently.

2.3 ETSI NFV Framework

In traditional computer networks, where virtualization technology is not applied, the nodes usually contain network functions that represent a combination of software and hardware characteristics of a certain manufacturer. Virtualization technology is emerging as a natural solution to avoid being "lock-in" in specific hardware and software. Bearing in mind the main principles of NFV, it is easy to conclude that this technology represents a step forward in the realization of a more flexible and scalable computer infrastructure because it introduces the following novelties into the traditional network architecture [16]:

- The network element is no longer a set of integrated hardware and software entities because software is developed separately from hardware and vice versa.
- Flexible and scalable deployment of network functions – by separating software from hardware, a high level of flexibility is obtained regarding redistribution and sharing of infrastructure resources, enabling different network functions to be performed simultaneously on shared hardware.
- Dynamic performance of activities in the network – control of operational parameters of network functions takes place through granular control and monitoring of network conditions.

From a strategic point of view, the goal of NFV technology is to enable the implementation of network functions as software entities that run on a virtual infrastructure [17]. In doing so, virtual infrastructure is created on standard hardware (widely used and relatively inexpensive), using various virtualization software (so-called hypervisor tools). In Fig. 2.3, we show the program framework, which represents the basis for work on the standardization of NFV architecture. This programming framework was first presented by the ETSI Industry Specification

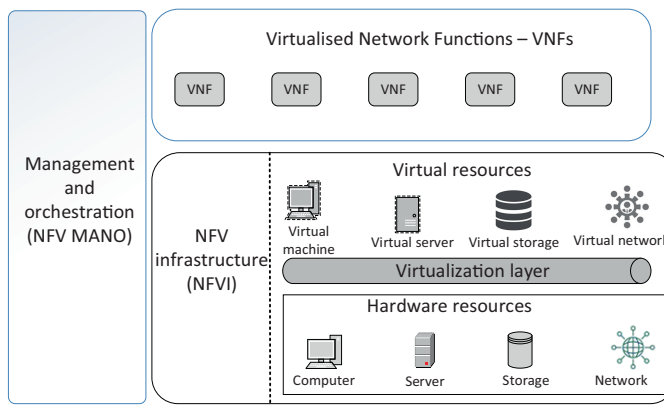

Figure 2.3. Structure of ETSI NFV framework.

Group (ISG) at the "SDN and OpenFlow World" congress, held in October 2012 in Germany [18].

The above mentioned program includes standards defining the management of virtualized network functions (VNF), relationships, mutual dependencies, data flow between VNFs, and allocating required resources. In this regard, the ETSI ISG divided roles within the program framework and categorized three functional blocks [19]:

- NFVI (Network Functions Virtualization Infrastructure) block – the basic building block of the entire architecture in which hardware for hosting virtual machines, software for virtualization, and virtualized resources are grouped.
- VNF block – the block with virtual machines with software-implemented network functions.
- MANO (Management and Network orchestration) block – the block for management and orchestration of network functions through constant interaction with NFVI and VNF blocks, ensures efficient management and orchestration of all resources in virtualized data centers (physical hardware, networking, and storage devices, resources of virtual machines, etc.), with the focus on the dynamic allocation of resources following the requirements of different services.

2.3.1 Application Fields

To better understand the NFV framework, we must consider that it is possible to apply NFV technology to various functions of packet processing in the control and packet forwarding planes, whether in fixed or mobile networks [20]. In practice, there are numerous solutions in which this technology is actively applied, such as:

- Software-implemented deep packet inspection (DPI) [21] – enables advanced analysis of packet content and traffic, simpler mechanisms for application, updating, testing, and scaling of resources following changing workloads, and multidimensional reporting.
- Functions – include Carrier Grade Network Address Translation (enables Internet access by allowing customers to share a single, public IP address) and Broadband Remote Access Server (a specialized server that enables easier convergence of multiple Internet traffic flows such as digital subscriber line (DSL), Ethernet, cable, and wireless).
- Virtualization of services in network environments [22].
- Virtualization of content delivery networks (CDN) enables easier expansion and scaling of content delivery services and allows reusing hardware to install other service delivery applications [23].

- Virtualization of mobile network core – enables more flexible network management and creates conditions allowing serving a larger amount of traffic with better use of resources (including energy saving, hardware consolidation, support for multi-tenancy access where one software instance with its infrastructure provides service to a larger number of users and faster configuration of new services) [24].
- Coordinated implementation of cloud technologies in organizations – enables on-demand services and network resources to the organization's needs (in general, different versions of a service coexist on shared hardware).

2.3.2 Virtual Network Functions

For an easier understanding of the process and the architecture defined by the ETSI NFV program framework, it is essential to correctly interpret the concept of virtual network functions (VNFs). This concept differs from the traditional concept, where network functions are usually implemented on specially designed hardware (the so-called integrated implementation of hardware and software entities). Instead, it implies a new method of implementation, where network functions shall be implemented as independent software entities on a standard and arguably cheaper computing infrastructure. Therefore, the basic idea on which we base the whole concept rests is the creation of prerequisites for software and hardware to be developed independently [25]. This approach is the only way to enable greater agility and innovation in providing various services in the network.

Industry efforts to articulate and standardize the context of virtual network functions initially took place within the ETSI NFV initiative and later in the open-source context, within projects such as Open Platform for NFV (OPNFV) [26], Open-Source MANO (OSM) [27], and Open Network Automation Platform (ONAP) [28]. Today, a widely accepted definition treats virtual network functions as software applications connected to the network and independent of hardware. That is the basis for the widespread use of microservice architectures, middleware platforms, and distributed applications.

By applying the VNF concept, telecom operators can improve their operations because they implement new services faster in their networks. The programmability that comes with this concept allows network functions to be upgraded and scaled dynamically and in a much more flexible way with a greater degree of granularity, which makes better use of available network resources and thereby reduces operational and capital costs. However, it is important to point out that the implementation level to which the advantages mentioned above will be realized depends primarily on the VNF model implemented in the network. Namely, the

basic requirements for designing virtual network functions include ensuring their modularity, portability (transferability to another virtualized resource), independence from hardware, multiple use, and scalability [29]. Implementing the VNF concept can be accelerated if there is already a certain set of hardware (physical) resources at the locations, which is very important from the speed and flexibility needed to, e.g., implement various cloud and network technologies.

We can implement a network service using only one virtual network function (as an independent entity) or by combining several virtual network functions. If different virtual network functions are combined, it must be emphasized that there is communication between them. However, they must know they are not physically connected or work on standard hardware. In Fig. 2.4, we explain the implementation of virtual network functions for security (firewall functionality), encryption, and load balancing.

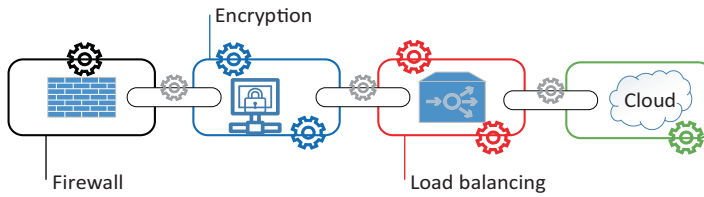

Figure 2.4. An implementation of network services by combining virtual network functions.

To run virtual network functions from Figure 2.4, one can use only one general-purpose hardware device with generic hardware resources (processor, storage, memory, and network interfaces) or multiple devices (so-called integrated hardware solution) that provide the necessary hardware resources to run them [1]. Both solutions have been used in data centers for a long time, whether concerning hypervisor-based virtualization [30] or container-based virtualization [31].

Therefore, virtualized infrastructure (NFVI) is a virtual computing environment. This environment is created when certain subsets of resources are extracted from standard hardware (a common set of resources) and following the technical requirements of the VNF software application. When creating virtual environments, it is imperative to consider the software vendor's recommendations, which refer to the minimum requirements regarding resources to be provided. The virtualization layer plays a key role in this process, which uses physical hardware to create a virtual environment with the resources needed to implement a VNF software application. It is important to point out that any VNF needs to be aware of another with which it may even share physical hardware. In virtualized network architectures (networks with applied NFV programming framework), a functional system must oversee the management, automation, coordination, and interconnection of layers and available blocks.

2.4 Layered Design of the NFV Architecture

To properly understand the concept and the importance of the ETSI NFV framework application for modern ICT trends, apart from the general picture of the basic building blocks, it is necessary to have a more detailed insight into the structure of each of them. This point of view implies the need to define elements within these blocks with different roles and responsibilities to realize certain processes [1]. In this sense, in Fig. 2.5, a detailed view of the ETSI NFV framework is given, where functional blocks are grouped into three layers:

- The infrastructure layer (consists of hardware and software components that build the environment for VNFs)
- The layer of virtual network functions (a place where the virtual network functions operate)
- The application layer (consists of many applications/functions, such as network management, fault management, configuration management, service management, etc.).

Each layer deals with a certain aspect of NFV implementation.

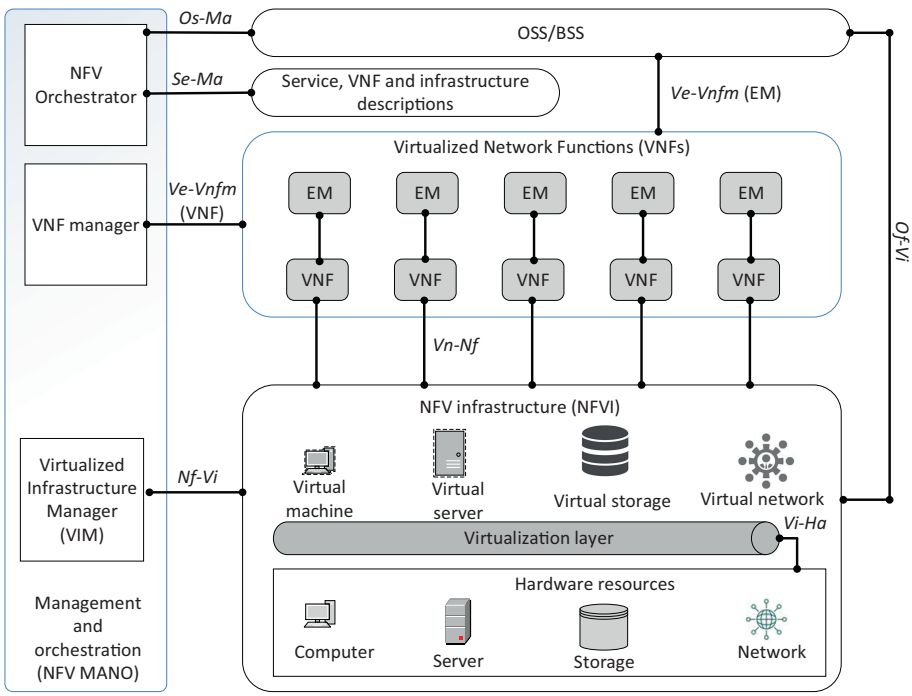

Figure 2.5. Detailed structure of the ETSI NFV framework [1].

2.4.1 Infrastructure Layer

For the functioning of VNFs, virtual resources must be available in the NFV infrastructure layer (NFVI), which can emulate the virtual environment by the software installed on the physical hardware. The building blocks of this layer are physical (hardware) resources, a virtualization layer, and virtual resources, as shown in Fig. 2.6.

In the ETSI NFV program framework, hardware resources are divided into computers (client computers, servers, processors, and memories that can be combined into clusters), data storage resources organized using Storage Area Network (SAN) [32] or Network-Attached Storage (NAS) technologies for data storage [33]) and network resources consisting of sets of network cards. Developing specialized hardware resources for implementing virtual network functions is unnecessary because we can apply virtualization technology to physical hardware available on-site (COTS hardware) and build the requested environment. Therefore, virtual environments (virtual resources) are created by virtualizing the available hardware, which can be connected even when located on different physical hardware and even in different locations. To enable this connection and provide the NFV infrastructure needed to implement virtual network functions, network devices (switches, routers, and so on) are used. These devices are installed physically and are not part of the resources allocated to a virtual network function.

The part of the NFV infrastructure that is responsible for creating a suitable virtual environment (virtual machine with computer, network, and storage resources) in which the VNF software application will be executed is the virtualization layer (hypervisor), i.e., through direct interaction with the physical hardware. Its role is twofold: (i) it must decouple the software application from the hardware, and (ii) allow the VNF software applications to function independently.

Figure 2.6 shows that the structure of this layer, in addition to the previously mentioned NFV infrastructure, also consists of a virtualized infrastructure manager

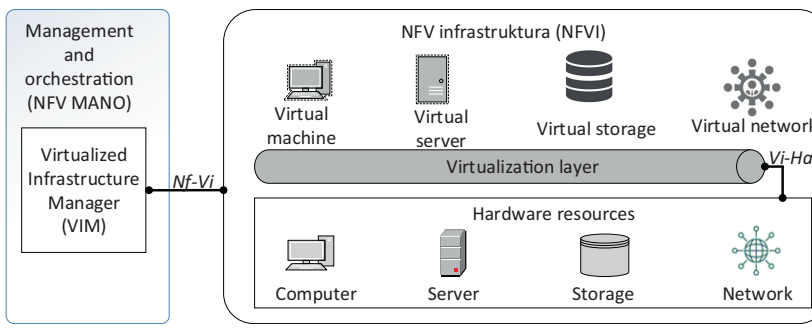

Figure 2.6. Infrastructure layer in the ETSI NFV framework [1].

(VIM) responsible for managing its resources [1]. The management process implies that this manager, having full information about hardware resources and their operational attributes (power supply and status), directly implements management functions over the virtualized infrastructure. In other words, the virtual infrastructure manager also manages the virtualization layer, thus controlling the hardware resources. It is important to note that one virtual infrastructure manager can control multiple devices, and even multiple virtual infrastructure managers can simultaneously control various hardware devices from one or more locations. The VIM can allocate resources under traffic engineering rules to support defining operational rules, define hub-to-facility mapping, and provide information for provisioning virtual infrastructure orchestration (VIO).

2.4.2 Virtual Network Function Layer

The layer of virtual network functions (VNF) layer is a part of the programming framework, which is responsible for their implementation. The structure of this layer is shown in Fig. 2.7. This layer is composed of two basic building elements: a Block of virtual network functions (VNF block) and a control block (VNF Manager – VNFM) [1].

In general, the idea of virtualization of network functions (regardless of which network function it is – router, firewall, load balancer, nodes in mobile networks, and other devices) emphasizes software development:

- which can be implemented on any hardware with the necessary resources and
- with identical characteristics and external interfaces, as in traditional computer networks.

Certain specificities must be considered when realizing network services via NFV infrastructure. In a real environment, we can implement network services by using only one VNF software or by combining several VNF software applications

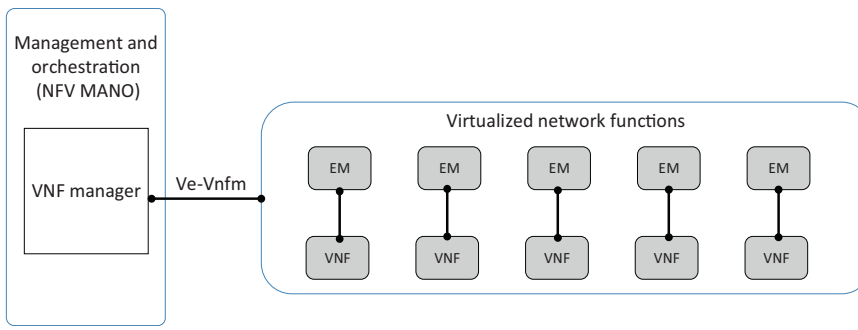

Figure 2.7. Virtual network function layer in ETSI NFV framework [1].

(between VNFs, a particular dependency can exist). If there is a dependency between VNF software applications, then such network services are implemented per a specific procedure. That procedure implies that the data must be processed according to some predefined sequence to ensure connectivity between VNF instances (software applications). This kind of implementation is called service chaining and is executed following the graph for forwarding VNF instances (VNF Forwarding Graph – VNF-FG). If there is a dependency between VNF software applications, then such network services are implemented per a specific procedure. That procedure implies the data must be processed according to a predefined sequence to ensure connectivity between VNF instances (software applications). This kind of implementation is called service chaining and is executed following the VNF-FG instances.

Implementing network services using the NFV concept can be nicely explained using the example of vEPC (virtual Evolved Packet Core) implementation in 4G, 5G, and 6G [34] mobile networks. It is a standard framework for processing and routing voice and other packets through the IP backbone, the key virtual components of which are:

- Mobility Management Entity (MME) – responsible for authentication and monitoring of users on the network, as well as session state management.
- Serving Gateway (SG) entity – enables the routing of packets through the network.
- Packet Data Network Gateway (PDN GW) entity – manages the quality of the provided service and enables deep packet analysis.
- Policy and Charging Rules Function (PCRF) entity – helps implement the charging policy and enables disclosure of services-related data.

Some VNF instances, such as the MME and SG, operate in parallel to enable some vEPC functionality but perform their functions independently. The MME entity manages the mobile devices, authenticates the user, and selects the appropriate SGV, while the SGV forwards the user's packets independently of the MME function. However, implementing the VNF instance for the PDN GW implies data processing after implementing the VNF instance for the SG, indicating a dependency. Figure 2.8 shows the interconnection of the mentioned VNF instances, carried out under a certain procedure or sequence, and represents the so-called VNF-FG.

To properly understand the activities in the core of the mobile network, we should focus on two types of traffic: control and user traffic. Therefore, it is necessary to introduce the Network Forwarding Path (NFP) concept to identify the

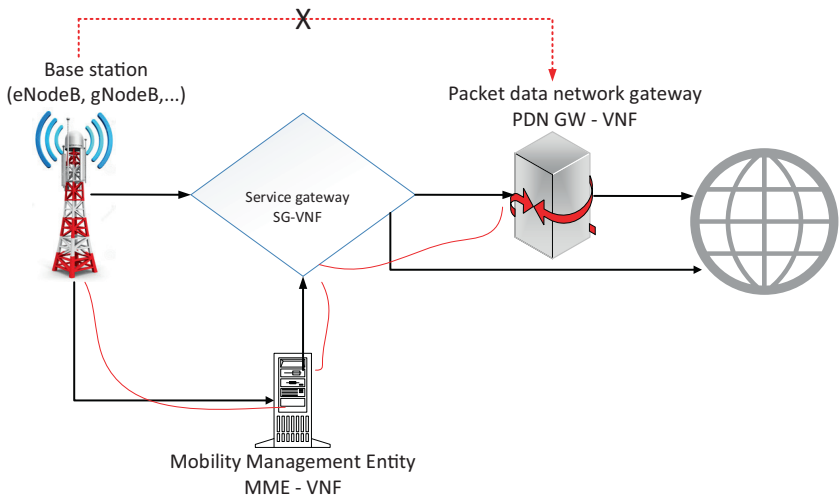

Figure 2.8. A vEPC implementation in mobile networks using the NFV concept.

actual traffic flows on virtual links. Figure 2.8 clearly shows that the control traffic has two paths, and the user traffic has only one. Therefore, the network service is implemented by combining the activities of the component functional blocks, including individual VNF instances and the VNF graph for packet forwarding. Forwarding Graph [1].

The VNF instance manager (VNFM) is responsible for configuring and managing VNF instances and their resources. Its role is to communicate with the VIM, and before starting the instantiation of a new virtual network function or modifying the resources assigned to one of the existing VNF instances, to check whether additional hardware is available. Essentially, this manager manages the configuration of VNF instances, i.e., parameters that directly depend on their performance, security, errors, and resource distribution (Fault, Configuration, Accounting, Performance, and Security – FCAPS).

The element manager (EM) is responsible for the implementation of management functions, which can be applied to one or more VNF instances [1]. This entity ensures reliable communication, i.e., interaction by proxy model, with the VNF instance manager (VNFM) and the VNF instances themselves. For this purpose, it uses proprietary methods to communicate with VNF instances. In contrast, it uses open standards for communication with the VNF instance manager, as shown in Fig. 2.9 (the VNF instance manager can have a centralized or distributed architecture).

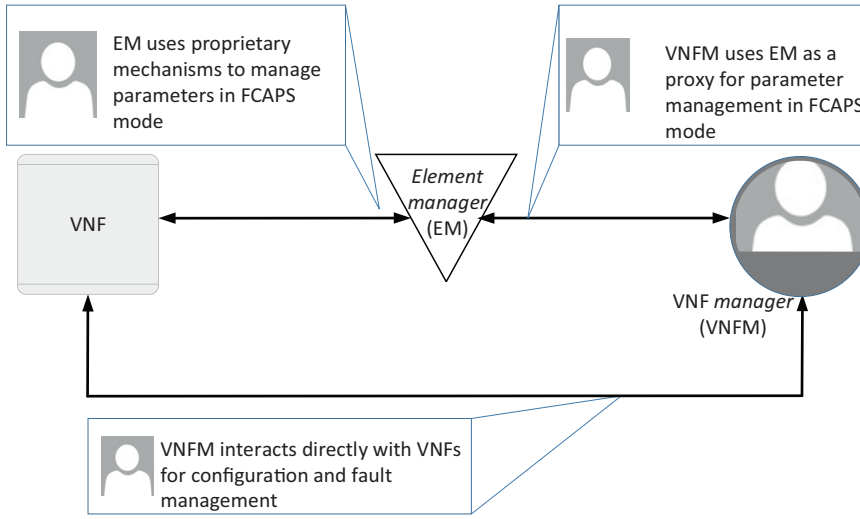

Figure 2.9. Management of VNF instances by the VNF manager.

2.4.3 Operational and Business Support Layer

This layer consists of two functional components, as shown in Fig. 2.10 [35]. The first component is the Operation Support Subsystem (OSS), which manages the network, errors, configuration, and service operations. The long component is the mobile operator's Business Support System (BSS) from user management, services, and user requests. In the NFV architecture, the mobile operator's BSS/OSS systems most often integrate with NFV management and orchestration through standard interfaces.

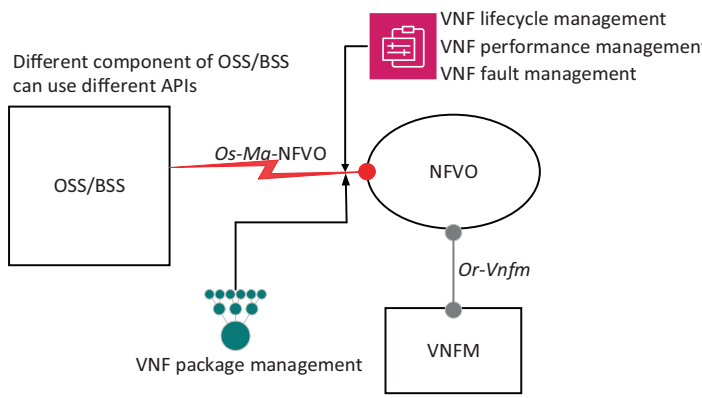

Figure 2.10. OSS/BSS support layer.

After moving to a virtual infrastructure, many operators do not make changes regarding the tools used for management and do not implement new OSS/BSS

applications. They prefer to rely on systems that are built within organizations. This approach limits the ability to take full advantage of the NFV programming framework, as it is not designed to communicate with functional management blocks such as VNFM and VIM. Therefore, one of the solutions can be the gradual evolution of existing tools and systems to create conditions for connection with functional blocks for management and to take advantage of the advantages of the NFV program framework, such as elasticity, agility, and flexibility.

2.4.4 NFV Management and Orchestration

By virtualizing network functions, we introduce a much higher level of programmability into computer networks, which entails applying a new method of managing the network infrastructure and orchestrating resources and services. Unlike traditional networks, where network functions are tied to specific hardware, in modern computer networks, we use virtualization technology to decouple the software implementation of network functions from computer storage and network resources. In this way, building new virtual entities (VNF instances) and establishing connections within the NFV infrastructure (NFVI) is possible. In most cases, network services are provided by interconnecting these virtual entities. On the other hand, in practice, there are also examples of a certain network service being implemented by connecting virtual entities with network functions implemented traditionally, i.e., using dedicated hardware.

Therefore, network services can be fully or partially realized by connecting virtualized and non-virtualized resources. Virtualized resources are generally associated with virtual machines, which can be viewed as containers that run programs and execute applications on software computing resources (rather than a physical computer). Such an environment is created on physical hardware. It functions as a virtual computer system with its central processing unit (CPU), memory, network interfaces, and data storage (with storage organized on block or file access).

For the implementation of virtual network functions, the orchestration of virtual resources on virtual machines is of particular importance, which implies allocating the virtual resources necessary to release those that are no longer needed. Orchestration is a complex task, especially considering different requirements and constraints (e.g., some VNF instances require low latency, while others require high-bandwidth links to communication participants). It should be noted here that allocating the necessary resources has a dynamic character, especially considering that the needs of VNF instances for resources change and that it is required to respond to them almost in real time. In other words, the NFV concept relies on the service orchestration process as on a service definition model using VNF instances and applying different topologies of their connection.

NFV Management and Orchestration (MANO) systems were primarily developed to manage virtual network functions in 5G/6G networks in an agile and flexible manner. In this sense, the ETSI ISG has adopted appropriate instructions, which describe the requirements and standards that the software and hardware of the NFV MANO system should satisfy from the realization of virtual network functions [18]. However, mobile operators offer different solutions. They should choose the best solution: the MANO system that suits their needs. For mobile operators to make a quality choice, it is necessary to define the MANO system's key performance indicators (KPI), based on which the performance analysis and comparison could be performed.

Defining key performance indicators, which would be used to quantify the performance of the NFV MANO system, is a big challenge, especially when considering the dynamics and flexibility of services provided by VNF instances [36]. In addition to performing traditional infrastructure management, providing life cycle management of VNF instances and network services is necessary. All key performance indicators of the MANO system can be classified as functional and operational. Functional performance indicators define the so-called non-runtime features of the MANO system, such as:

- Number of committed resources (resource footprint).
- List of different VIM platforms (virtual infrastructure manager solutions) that the MANO system can manage.
- The number of virtual infrastructure managers that one MANO system can effectively manage.
- The maximum number of VNF instances that the MANO system can monitor and manage within the NFV infrastructure.
- Support for DevOps (procedures and tools that increase delivery applications and services compared to the traditional software development process), management of VNF images, and integrated monitoring.

Operational performance indicators define the so-called run-time operations, and their quantification is done through the measurement of delay and efficiency determination of the control procedure/task. One of these indicators is the time required to launch the virtualized network function image (so-called onboarding process delay), i.e., a virtual machine with all its resources. This image is a package which contains the following:

- VNF descriptor file (VNFD) – a file with information about the configuration, network requirements to be met, resources to be provided, routing and security policies, available IP ranges, and interfaces.

- Network Service Descriptor (NSD) – a template that describes the network service requirements in terms of function, operation, security, characteristics of virtual links, quality of service, quality of experience, and reliability. It includes VNF-FG (identifies the types of VNF instances, the sequence of their chaining, and the characteristics of the virtual links connecting them).

The next important indicator is the time required to start one VNF instance inside a virtual machine, and the network service becomes operational [37]. That is a critical parameter when it comes to complex network services (composed of multiple VNF instances), where the role of the MANO system is precisely to provide the necessary resources for instantiating VNFs and connecting them via appropriate virtual links and then configuring each VNF -a following the information contained in NSD templates and VNFD files.

A further important indicator is the delay in orchestrating various management procedures. Namely, with each management action, the delay can be quantified by measuring the time interval from the moment when the action was started to the moment when the action initiated by that action was completed. The use value of this indicator largely depends on the monitoring system that continuously monitors the state of VNF instances during their life cycle.

Also, an important indicator is the quality-of-decision, which represents a metric that can be used to quantify the performance of the MANO system in terms of managing the life cycle of VNF instances (VNF Life Cycle Management), their scaling, and migrations. In other words, this indicator indicates the effectiveness of management decisions from the point of view of committed resources (e.g., whether long-term and short-term resource requirements for a specific VNF instance are provided in the selected computing node or how the instantiation action affects other VNF instances in the same computing node).

2.4.5 NFV Referent Points

By virtualizing network functions, a much higher level of programmability is introduced into computer networks. One of the basic requirements implemented within the ETSI program framework is providing open and consistent communication between its functional blocks. Reference points are defined to identify and effectively monitor this communication precisely. They represent a specific working environment for VNFs by applying the NFV concept and building the NFV infrastructure (without defining a special control protocol, a hardware-independent life cycle, performance, and portability requirement of VNFs are guaranteed). In this sense, the ETSI NFV framework defines the following reference points:

- *Os-Ma* is a reference point between the OSS/BSS system and the MANO control block, which defines the communication between OSS/BSS and NFVO as follows:
  - Activates network service and VNF instances lifecycle management by generating and sending adequate requests.
  - Exchanges information about the status of functional blocks defined by the NFV framework.
  - Creates different policies and forwards management instructions, which is necessary for NFVO operations.
  - Exchanges data obtained using analytical methods.
  - Forwards record that refers to the use of NFV resources and calculate billing accordingly.
  - Exchanges information about the capacity of the NFV infrastructure and its availability.
- *Ve-Vnfm* is a reference point that defines the communication between the manager of virtual network functions on the one hand and EMs and VNF instances on the other through:
  - Requirements for managing the lifecycle of VNF instances.
  - Exchange of configuration information
  - Exchange of information necessary for managing the life cycle of network services.
- *Nf-Vi* represents a reference point where virtual infrastructure managers exchange information with functional blocks of NFV infrastructure (e.g., information on configuration and state of hardware resources, availability of virtual resources, and their allocation according to current requirements).
- *Or-Vnfm* is the point of reference through which the NFV orchestrator communicates with the virtual function manager related to the instantiation of VNF software applications (e.g., authorization, validation, reservation and allocation of virtual resources by the VNF instance manager, forwarding the appropriate information to enable the VNF instances to adequately configured within VNF-FG) and forwarding collected information about the state of VNF instances that is necessary for managing their life cycle.
- *Or-Vi* is a reference point through which the NFV orchestrator directly communicates with the virtual infrastructure manager and forwards potential requests for reservation and resource allocation based on previously exchanged information about the configuration and state of virtualized hardware resources.
- *Vi-Vnfm* is the reference point through which communication occurs between the VNF instance manager and the virtual infrastructure manager (e.g., they send requests to the VNF instance manager to allocate resources

based on information about the configuration and state of the virtualized hardware resources).

- *Vn-Nf* is a reference point through which performance information is transmitted to the infrastructure block, indicating the need to migrate VNF instances to another.
- *Wi-Ha* is the reference point through which the virtualization of hardware resources takes place.

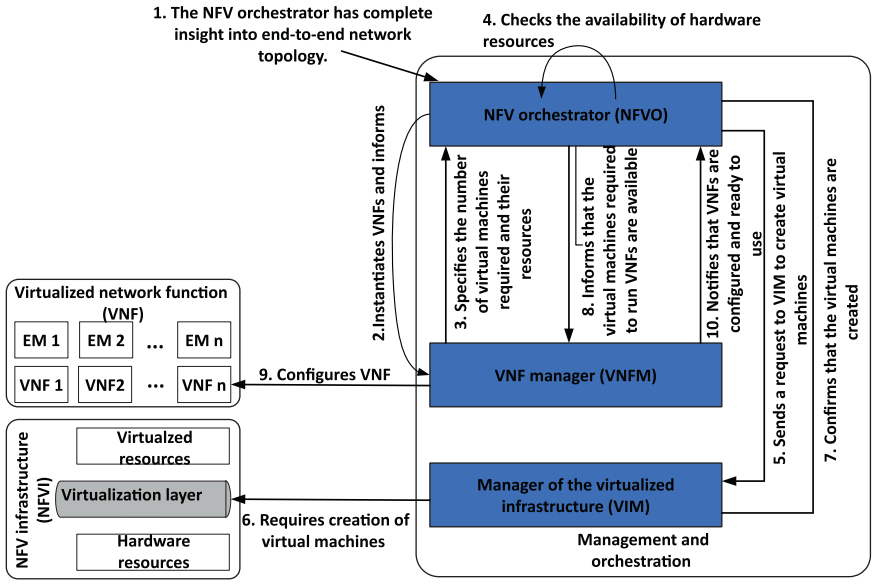

Figure 2.11. End-to-end (E2E) communication flow in the ETSI NFV framework.

Figure 2.11 shows a generic scheme that describes end-to-end (E2E) communication in a general way, which takes place between different functional blocks defined by the ETSI NFV program framework, intending to implement some network service.

2.5 Advantages of Applying the NFV Concept

The NFV concept application aims to eliminate numerous problems that hamper the application of new and increasingly demanding services in computer networks. The virtualization of network functions changes the network's design, infrastructure configuration, individual network units, and the way of managing the network, fundamentally affecting the introduction of a new work model in the network environment. Figure 2.12 shows the main advantages of implementing this technology.

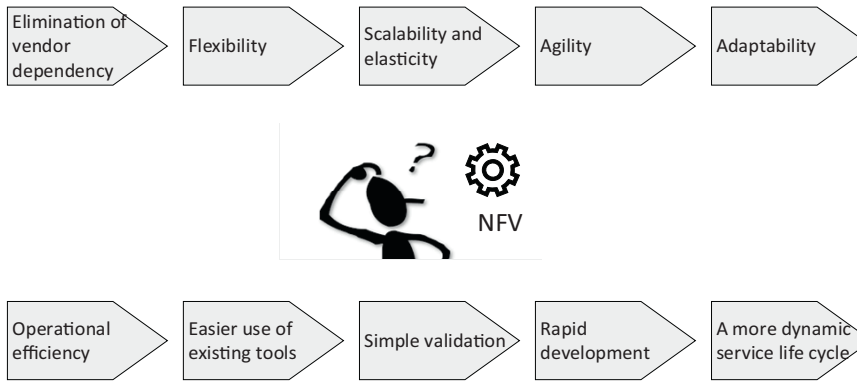

Figure 2.12. Benefits of applying the NFV concept in modern computer networks.

Those advantages primarily refer to the following:

- Elimination of vendor dependency (no vendor lock-in) – allows the creation of the conditions to replace the existing equipment or expand the infrastructure faster and at a lower cost (it is possible to choose equipment based on the availability of functions, software licensing prices, and support models after implementation).
- Flexibility – free hardware choice (the NFV concept enables the use of COTS hardware), the possibility of building a network environment that best suits service requirements, and running VNFs across different servers or moving them around as needed.
- Scalability and elasticity – introducing into the network a higher level of programmability, which will enable the creation of a network environment in a flexible and scalable manner and resource allocation and release dynamically (when there is a need for it, and it is the so-called fast elasticity, which is primarily characteristic for the cloud environment).
- Agility – enables fast deployment and creation of new network services, reducing time-to-market and improving competitiveness.
- Adaptability – enables adaptation to changing customer requests and other conditions (NFV components possess flexible and customizable character).
- Operational efficiency – fast implementation of network services and functions on request and, as needed, allows the application of a virtual network function or services in different places in the network without changes or with minimal changes in the configuration. Also, hosting VNF instances on standard hardware reduces operational costs because there is no longer a need to host them on special, purpose-built hardware.
- Easier use of existing tools – provide easy implementation of the existing tools from traditional computer networks, which even more easily can be used in modern computer networks (on the same physical infrastructure)

- Simple validation – simpler implementation of a test environment enables the check of new solutions and validation of various service capabilities when necessary.
- Rapid development – The open-source components of NFV prioritize code development and represent the base for quickly delivering proof of concepts (PoC) for use case implementation specified by the standards (the simplification led to the development and deployment of sustainable solutions easily).
- A more dynamic service life cycle – implies ease and fast usage of VNFs, maintenance over their lifetime, and deployment when needed (the NFV facilitates such an approach and provides benefits from VNFs by performing adequate tasks).

2.6 Conclusion

NFV allows for the separation of network services from dedicated hardware, meaning that network operations provide new services dynamically and without installing new hardware. This way, we can deploy network functions more easily and quickly than in traditional networks. Besides that, virtualized functions run on generic hardware, which is less expensive. The application of the NFV concept includes additional reasons, such as pay-as-you-go models that allow us to pay only for what we use, fewer appliances that lead to lower operational costs, and faster and easier scalability, which do not require the procurement of additional hardware. The application of the NFV concept has certain risks that we must consider. These risks refer to security in NFV-based networks. Virtualizing network components increases their vulnerability to new attacks compared to the physical devices. Traditional tools for traffic monitoring need to be more efficient to identify malicious traffic between virtual machines within a network infrastructure. The complex layered architecture can cause numerous issues. For this reason, we must implement more comprehensive security policies.

At each layer of the NFV infrastructure, we have solutions representing an example of applying different virtualization techniques. This application aims to enable the rapid development of network services with elastic scale and automation. In the next section, we will provide many more details, which can give a closer look at each virtualization technique, the subject matter, goals, and their ranges. Accurately understanding virtualization technology's essence, benefits, and limitations is crucial to properly comprehending the NFV concept and the principles of modern computing environments.