AJEMA GLOBAL RESEARCH NETWORK

AMERICAN Journal of Engineering, Mechanics and Architecture
Volume 02, Issue 02, 2024 ISSN (E): 2993-2637

BACKGROUND, CONCEPT AND ARCHITECTURAL FEATURES OF NFV

***Kilichov Jasur Ruzikulovich*[1],**
***Xadjayev Muxammadzoir Safarmamatovich*[1],**
***Gayratov Zafarjon Kamoliddinovich*[1],**
***Almardonov Asliddin Faxriddin o'g'li*[2],**
***Najmiyev Mirjalol Makhmudjonovich*[2]**

[1] *The Samarkand branch of TUIT named after Muhammad al-Khwarizmi, teachers of department "Telecommunication engineering", Uzbekistan.*

[2]*The Samarkand branch of TUIT named after Muhammad al-Khwarizmi, students of faculty "Telecommunication Technologies and Professional Education", Uzbekistan.*

Abstract - The main tasks and security opportunities of network virtualization are considered. Functions (NFV), describes the design of the NFV architecture and some of the potential security issues and challenges of NFV. In addition, existing products and solutions in the field of NFV security were analyzed. and some promising lines of research in this area.

Keywords: *virtualization of network functions, software defined network, ISP, QoS, MANO, NFVI, COTS.*

Introduction. The evolution of network architecture. The capacity and bandwidth of communication and data networks have grown, and network capabilities have evolved over quite a long time. However, by 2019, it is increasingly noticeable that the increase in network bandwidth is not keeping up with the ever-faster growth in market demand for bandwidth and new services. According to Cisco Visual network Index, network traffic is growing exponentially at a CAGR of 26% until 2022, with no signs of slowing down further.

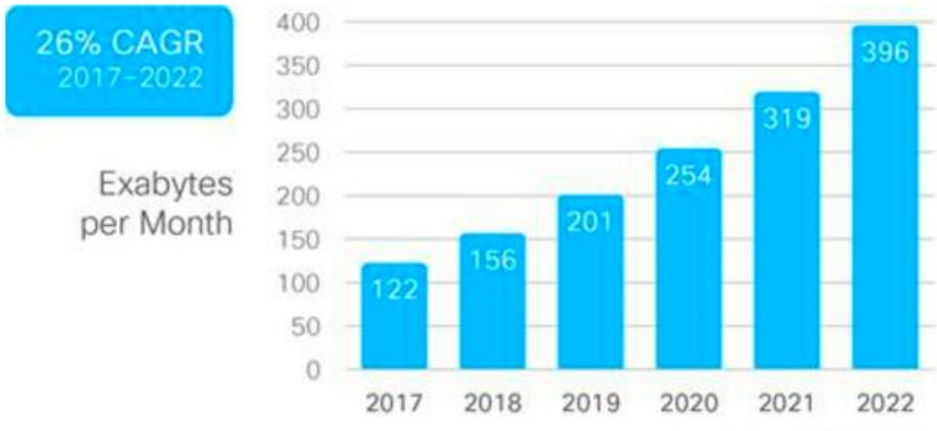

Figure 1. Network traffic growth 2017-2022 (source: Cisco)

Telecom operators and ISPs to expand their networks at an ever faster pace, while revenue from services is growing nowhere near as fast as bandwidth demand. Operators are trying to reduce the

cost of network development, as well as increase the speed of development and implementation of new features to increase revenue.

Traditional methods of network development are based on the "hardware" principle: "device - function". In most cases, in order to enter the next function, you need to install another device. However, these methods of developing networks and bringing new services to market using new physical devices face a number of limitations. Let's briefly consider these restrictions.

Flexibility limits. Proprietary vendor hardware design is that each network device has a fixed combination of hardware and software with slight variations. This greatly limits operators in the choice of functional combinations and equipment capabilities that can be deployed on the network. However, all the growing market demands for various services and services make the use of the resources of such vendor solutions inefficient.

Scalability Limitations. The scalability of physical network devices is limited in both hardware and software. Equipment requires power and space, which is often limited in densely built areas. On the other hand, the capabilities of existing physical devices often cannot keep pace with the growth in demand for modern networking features. Each device is designed with a certain limit of possibilities, and when it is reached, it is necessary to install a new device, which will remain underloaded for a long time.

Long time to market. The demands of the market are growing, but the growth in the number of functions and pieces of equipment is not always able to keep up with these requirements. Often the introduction of new functions requires an upgrade of existing equipment and the introduction of new equipment. This requires careful development of the migration process, validation and practical testing of the new solution. It requires evaluating new equipment, redesigning the network topology, and possibly attracting new equipment vendors that have the required devices and features in their portfolio. All this significantly increases the capital costs and cost of ownership of the network infrastructure, leads to business restrictions and loss of potential revenue if competitors are faster.

Administration restrictions. Monitoring systems use standard protocols such as SNMP (Simple network management Protocol), NetFlow, Syslog, etc. to collect information about the status of devices. However, for monitoring vendor-specific (proprietary) parameters, standard systems may not be enough. In this case, for each network domain built on the equipment of a certain vendor, a proprietary monitoring system is required. It also contributes to capital expenditures and cost of ownership by multiplying the "zoo" of such devices for the operator, requires staff training and the maintenance of specialists with certificates of the corresponding vendor in the state.

Operating expenses. Vendor-specific equipment increases operating costs, since it requires the presence of appropriate specialists in the operator's staff. Requires the use of the so-called `managed services` (i.e. "professional services" provider). This leads to " vendor dependency ", that is, to being tied to a particular vendor's solutions. On the other hand, the use of equipment from many vendors on the network causes interoperability problems with dissimilar equipment and further increases operating costs.

Migration. Devices and networks must be periodically maintained and upgraded. This requires physical access to the network elements and a site visit by technicians to deploy new equipment, reconfigure physical links, and work on the site's engineering equipment. This creates a cost barrier to network migration and upgrade decisions, slowing down the offering of new services to users.

Smooth growth of network capacity. Requirements for network capacity growth (both for short and long periods) are difficult to predict. As a result, networks are often built with a large capacity margin to account for non-explosive growth in traffic needs. According to experts, more than 50% of the network capacity remains unclaimed most of the time. This leads to unproductive capital costs. On the contrary, when the resources of the network are exhausted, it takes a significant amount of time before the capacity of the network can be expanded. Thus, the development of the network occurs spasmodically, with alternating periods of insufficient and excess network capacity.

Interaction. It often happens that in order to speed up the introduction of equipment to the market, suppliers equip it with new features before the standardization process is fully completed. In many cases, this leads to incompatibility of heterogeneous equipment on the network, the need to test network solutions in the laboratories of operators and service providers before deploying these devices on the network. This is usually followed by a period of refinement by the equipment supplier and retesting. And even in this case, some of the incompatibilities cannot be identified, and this “pops up” already during the operation of the equipment on a “live” network.

The concept of virtualization of network functions. Virtualization is a technology that allows you to run multiple operating systems on a single physical server. The concept of server virtualization has long been used in data centers (data centers , data processing centers). At the same time, physical servers are replaced by their virtual "copies" running on top of hypervisors. This allows, among other things, to achieve a more efficient use of the physical resources of the data center.

NFV extends the concept of virtualization beyond servers to all types of network devices. NFV can be defined as a method and technology that makes it possible to replace physical network devices with certain functions with software entities that perform the same functions on public server hardware.

NFV is used as an umbrella term for an ecosystem that consists of virtual network devices, management tools, and infrastructure that integrates software entities with standard computer hardware.

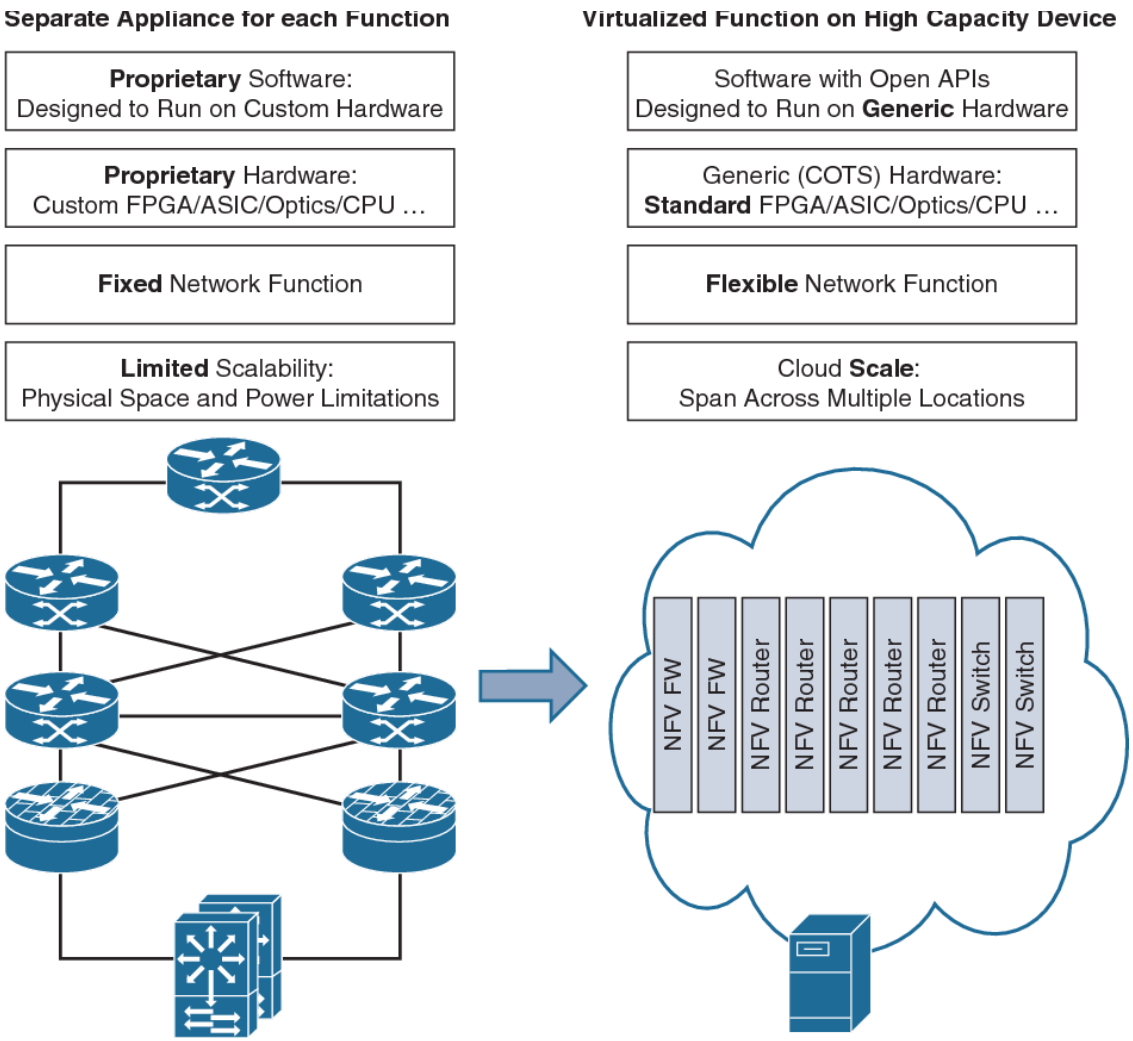

Figure 2. Migration from traditional to virtualized network infrastructure (source: Rajendra Chayapathi, Network Functions Virtualization (NFV) with a Touch of SDN. Copyright © 2017 Pearson Education, Inc.; TAdviser, 2019).

In fact, NFV separates the software from the hardware, and makes it possible to use any commercially available, standard COTS (Commercial Off the Shelf) to perform specialized network functions on it, which can be changed quickly and at any time.

Structure (Framework) of NFV. The term NFV was first introduced by the world's leading telecom operators at the SDN Congress open flow World Congress in 2012, the world's leading telecom operators. They analyzed the limitations of the traditional network development method above and formed a working group to develop the specifications of the NFV ISG (Industry Specification Group) under the leadership of the European Telecommunications Standards Institute ETSI (European Telecommunications Standards institute).

The ISG working group put forward three main criteria that should be implemented in the standards (recommendations) for NFV:

- Decoupling. Complete separation of hardware and software;
- Flexibility. Automated and scalable deployment of network functions;

- Dynamic operations (Dynamic operations). Control over the operational parameters of the network using precise (granular) control and monitoring of the network status.

Based on these criteria, a generalized NFV architecture was developed, shown in the figure below.

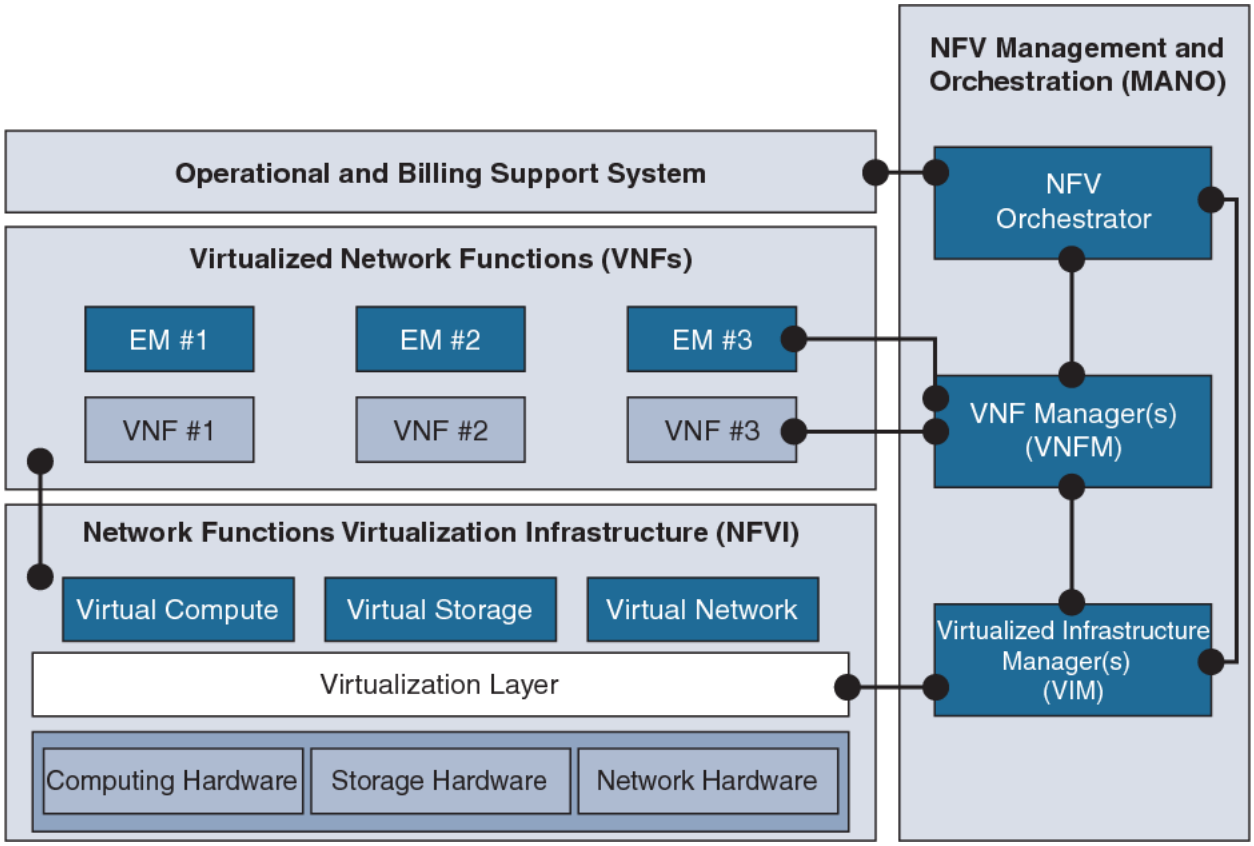

Figure 3. Generic NFV architecture (Source: ETSI, TAdviser).

The NFV architecture consists of three main subsystems:

- Virtualized NFV Network Functions (Virtualized network Function);
- NFVI Virtualization Infrastructure (NFV Infrastructure);
- Management and orchestration subsystem MANO (Management and orchestration);
- Other than NFVI, subsystems are software, not hardware.

NFVI includes both physical hardware (computing, storage, networks) and virtual "hardware": servers, storage systems , network devices. The virtualization layer (hypervisors and guest operating systems) makes it possible to deploy VM virtual machines (Virtual Machines) that perform any function assigned to them. For a VM, it does not really matter on which physical server it is deployed and running. Moreover, VMs can move (migrate) from one physical server to another without interrupting their work.

Strictly speaking, the NFV architecture also needs to include the Operations and Business Support Subsystem (OSS / BSS), which is part of the traditional carrier network system. However, the presence of this subsystem in the NFV architecture is temporary, since operators cannot immediately abandon existing OSS / BSS and immediately switch to MANO (this is only possible for new networks of operators starting their business from scratch and starting to build a network).

MANO must have full visibility (operational state, usage statistics, etc.) of all software entities deployed in the NFV system and manage them. Therefore, it is MANO that provides the most suitable interface for the OSS / BSS subsystem in terms of collecting operational data. In the future, as the network transforms, all OSS/BSS functions should move to MANO.

Interaction of NFV architecture elements. Generalized blocks of the NFV architecture, in fig. 3 consist, in turn, of functional modules of a lower level. For example, the administrative block MANO is a combination of three main functional modules: the VIM virtualization infrastructure manager (Virtualized Infrastructure Manager), VNFM Virtualized Network Function Manager (Virtualized network function Manager) and NFVO Orchestrator (NFV Orchestrator).

The architecture also defines reference points (reference points) between functional blocks and modules through which they interact with each other. It should be noted that reference points are not interfaces (software or hardware). These points are specifications of the information that should be transmitted through them, as well as where and how it should be processed.

In the figure below, the reference points are shown as bold circles with connecting lines. A more detailed description of them can be found in the description from ETSI , or here.

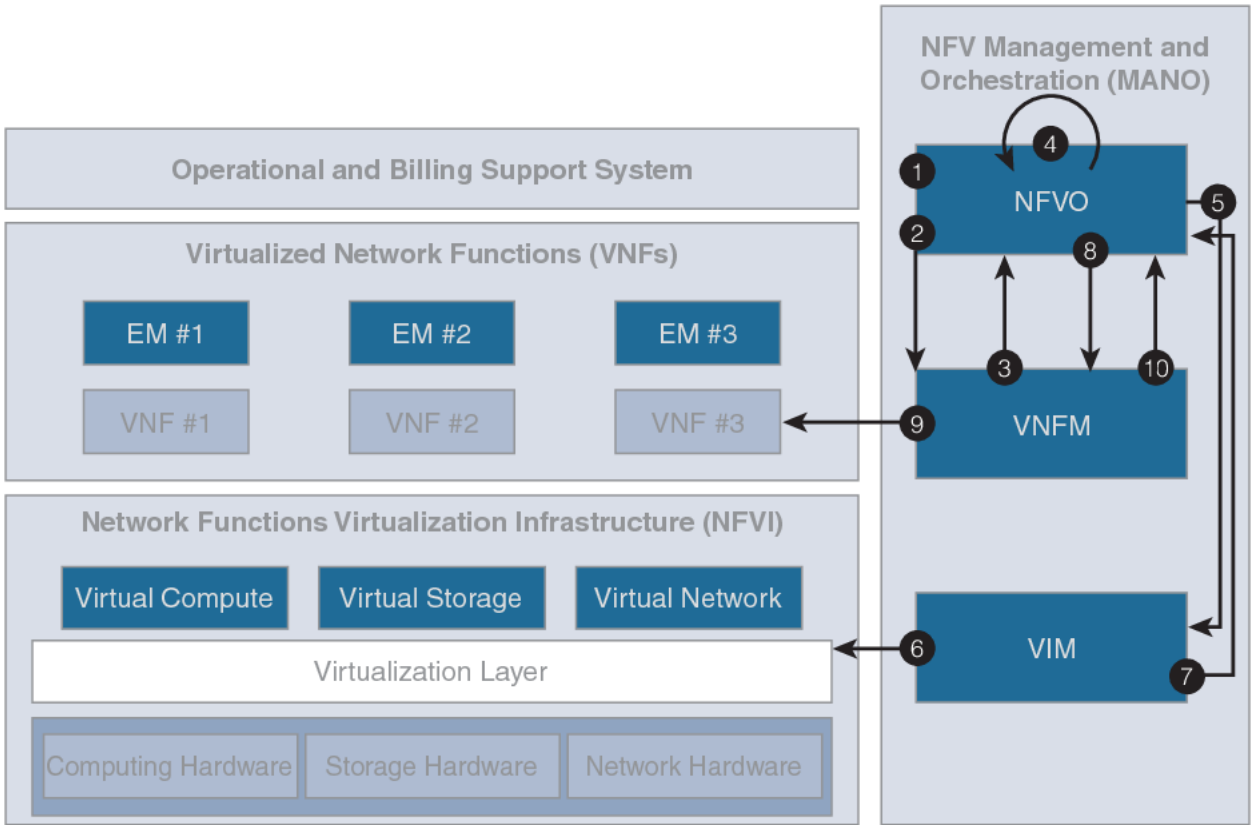

Figure 4. More detailed NFV architecture according to ETSI

Equipment resources in NFVI fall into three categories:

- Server hardware;
- Storage hardware;
- Network interface equipment.

The computing equipment of servers includes a central processing unit CPU and memory, which can be distributed among computer nodes using clustering technologies.
Storage systems can be local NAS (Network Attached Storage), as well as connected using SAN technology (Storage area network).
The network hardware consists of a set of network interface cards and ports that can be used by VNFs.
None of these types of equipment are specifically designed to perform certain functions, but are public COTS hardware devices. All types of equipment (processors, memory, storage systems, network cards, etc.) are combined into a common pool. Separate devices from this pool are used as needed to create a VNF, and, after the end of the function, they are released again.
Functional blocks can extend between different computer nodes in a data center, and even between data centers themselves. That is, they are not usually concentrated in a single network node, location, or point of presence on a POP network (point of presence), but distributed.
This distribution is a very important quality of the NFV architecture, which provides many advantages.

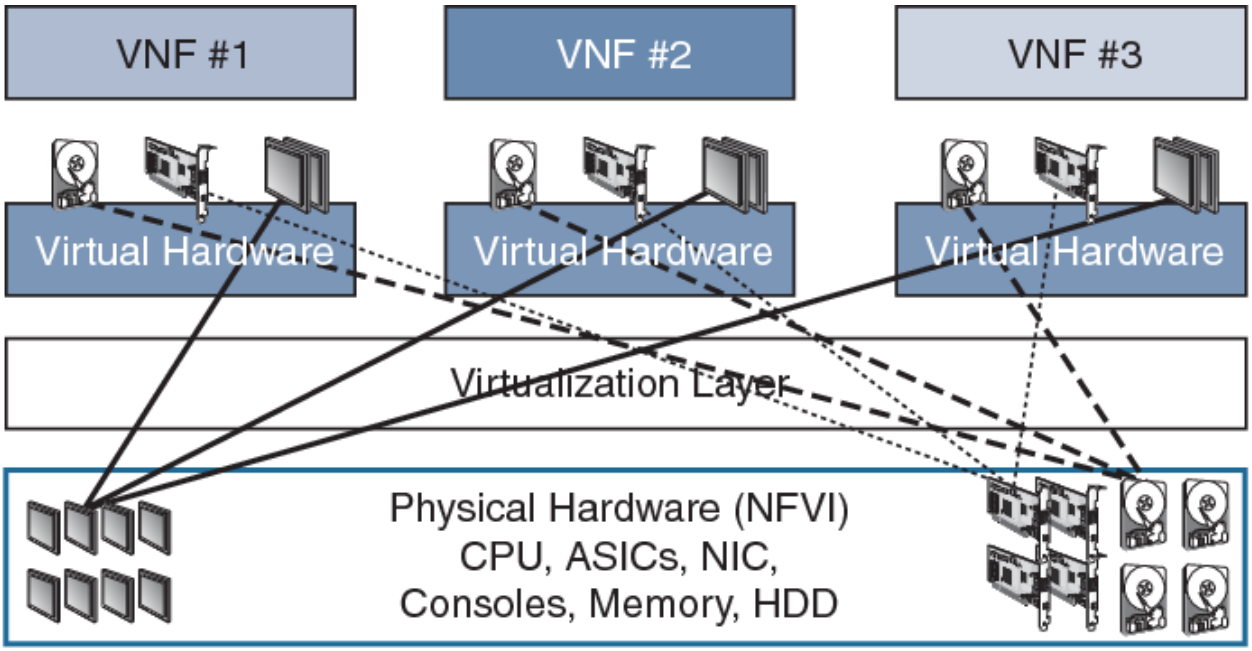

Figure 5. Principle of virtualization in NFVI.

The NFVI functional block provides hardware resources in the form of VM virtual machines (Virtual Machine) that run VNFs. Virtual machines are the virtual counterpart of physical hardware, which is provided to run VNF on them just as if it were physical hardware.
NFVI is managed by the VIM virtualization infrastructure manager (Virtualized Infrastructure Manager), which is part of MANO. It is responsible for managing the resources of the servers, storage and networking systems, and the software of the Virtualization Layer. VIM has complete information about the presence and employment of resources (inventory), as well as the attributes of their operation (for example, power supply, processor busy status, etc.), and in addition, means for monitoring operation parameters (for example, usage statistics).

The VNF manager, VNFM, is responsible for creating and managing the operation of virtual network functions. It, upon request from the NFV Orchestrator to form a virtual VNF function, requests the appropriate resources from the VIM and launches this VNF on them, or composes a complex function from other, more elementary VNFs. During its operation, if an expansion (scaling) of the power of the VNF is required, VNFM requests additional resources from the VIM, receives them and adds them to the running VNF (for example, adds CPU cores). This can be launching additional VMs, increasing the amount of memory or storage space, connecting new network interfaces. Since VIM is in charge of the "inventory" system, it can determine if COTS resources are available to satisfy the request, or if the system has reached the limit of their use. In the latter case, various measures can be taken, which are included in the functionality of ensuring the flexibility of the system.

VNFM manages VNFs through EM (Element Management, see fig. 4). These devices are needed in order to ensure that the VNF also interacts with the physical network functions of the PNF (Physical network Functions) of ordinary physical devices of the operator's network, which are inherited from the traditional network. For the sake of simplicity, the PNFs are not shown in the figures.

The scope of responsibility of EM is similar to the traditional EMS element management and administration system (Element management System). In the traditional, physical network of the operator, it is intermediate between the network management system NMS (Network management System) and physical network elements that perform network functions. EM interacts with VNF using specialized protocols left over from the traditional network, and with VNFM using open protocols defined by ETSI.

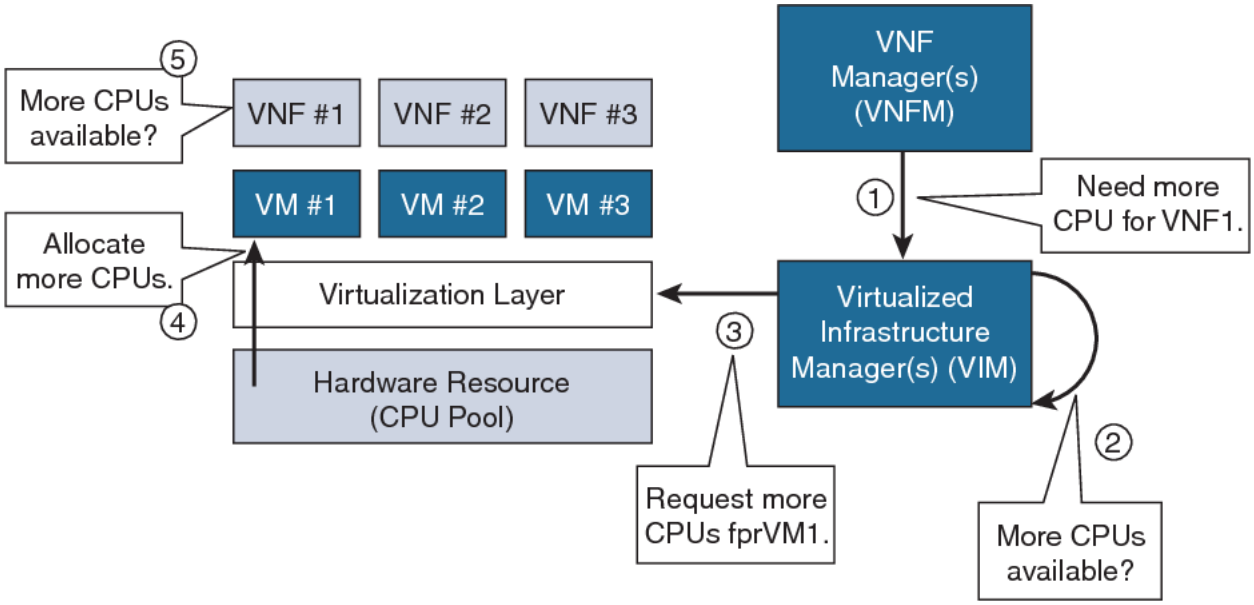

Figure 6. An example of allocation of additional CPU resources for VNF1.

In a network evolving to NFV, which contains both parts - traditional and virtualized, EMs are also needed for the universal execution of FCAPS functions (Fault, Configuration, Performance,

Accounting, Security), that is, for fault management (fault), configuration (configuration), measurement of work parameters (performance), accounting (accounting) and security (security). In a fully virtualized network, FCAPS functions will be entirely under the responsibility of VNFM. When moving from physical to virtual network elements, carriers are generally reluctant to change or transform the network management tools they are used to and that work well with traditional OSS/BSS systems . The ETSI structure takes this into account and does not require operators who embark on the path of NFV transformation to change the entire existing network management system at once. That is, existing governance systems can continue to operate even when the physical network elements are replaced by VNFs. However, existing OSS/BSS systems have their drawbacks, which do not allow them to take full advantage of all the advantages of NFV, and also they cannot communicate directly with NFV control units - VNFM and VIM. Of course, existing systems can somehow be adapted to take advantage of the advantages of NFV, such as responsiveness and elasticity. But this is not an optimal approach, because such systems are usually designed according to the principle of "proprietary", which does not allow management of open platforms.

To solve this problem, the MANO structure has another functional block called the NFV Orchestrator, NFVO. It allows legacy OSS/BSS to manage operations in NFVI and VNF via VNFM and VIM (See Figure 4).

The role of NFVO is not as obvious as VIM and VFNM, and, at first glance, it just looks like a buffer between them and traditional OSS/BSS. However, the NFVO orchestrator plays a very important role in the ETSI NFV framework. It manages the end-to-end deployment of services across the network, builds a global picture of service virtualization, and shares this information with VIM and VNFM for service deployment. In particular, shown in Fig. 6 "Request for processor performance enhancement from VNF1" comes from NFVO.

NFVO also works with VIM and has a complete picture of the availability of the resources it manages. There can be many VNFMs and VIMs in one NFV system, but it is the NFVO that coordinates their work.

The above described is only a simplified picture of the operation of the NFV system, since the format of the article does not allow us to consider all aspects in more detail.

Benefits of NFV. In the beginning, the limitations of traditional methods of developing communication networks were briefly described. Let's take a look at how NFV network function virtualization solves most of these limitations, as well as adding additional benefits. Much of what was not possible in the traditional carrier network, and therefore such possibilities were not even considered, becomes possible in NFV.

Freedom of choice of equipment. Because NFV uses conventional, commercially available COTS computer hardware, operators can choose the most cost-effective and supported hardware from multiple vendors, and thus best build their networks in terms of both cost and functionality.

We can say that the whole variety of traditional network equipment supplied by vendors in NFV comes down to only three of its types: server, storage system, network devices. However, the number of suppliers of such standard equipment is much greater than that of specialized telecom equipment. All functionality is provided by software functions that work on this limited range of equipment.

The process of modifying traditional equipment on a telecom operator's network is usually very long and costly. With NFV, operators can implement new features with a few clicks from the admin control panel, rather than having to deploy new devices on the network with highly trained technical staff.

For example, if it is necessary to expand the capacity of the Internet gateway, instead of installing new boards in the blade server basket, configuration, modifying tables, etc., the operator can simply assign new virtual machines from the existing resource pool, on which the corresponding VNFs will be launched.

Speed and efficiency. Unlike physical hardware, VNF network functions can be created and deleted on the fly, mostly automated, without the need for technical personnel.

This property is called " agile " (agile - flexible, operational, agile, efficient), a term that has taken root in the technical literature in English transcription, since it cannot be translated into Russian in one word.

Scalability and elasticity. The introduction of new services and applications that require significant network bandwidth in today's environment often force operators to work under constant stress in order to meet the ever-increasing needs of subscribers and users for new services so that they work normally on existing resources. Traditional resources often represent a "bottleneck" (bottleneck), when all other network resources allow you to provide a new service without problems, but the physical network elements of one or two resources are insufficient, and expanding them is long and expensive.

This problem is solved in NFV, which allows you to get the necessary resources very quickly by deploying new VNFs on VMs from the existing resource pool.

Since these VNFs are not limited by the parameters of the specialized physical hardware, they can provide "elasticity" properties, that is, they can be expanded when they are needed and collapsed when they are not needed.

It also avoids the common situation in a traditional network where some network elements are overloaded while others are underloaded. The rapid deployment of VNF allows you to evenly distribute the currently available load.

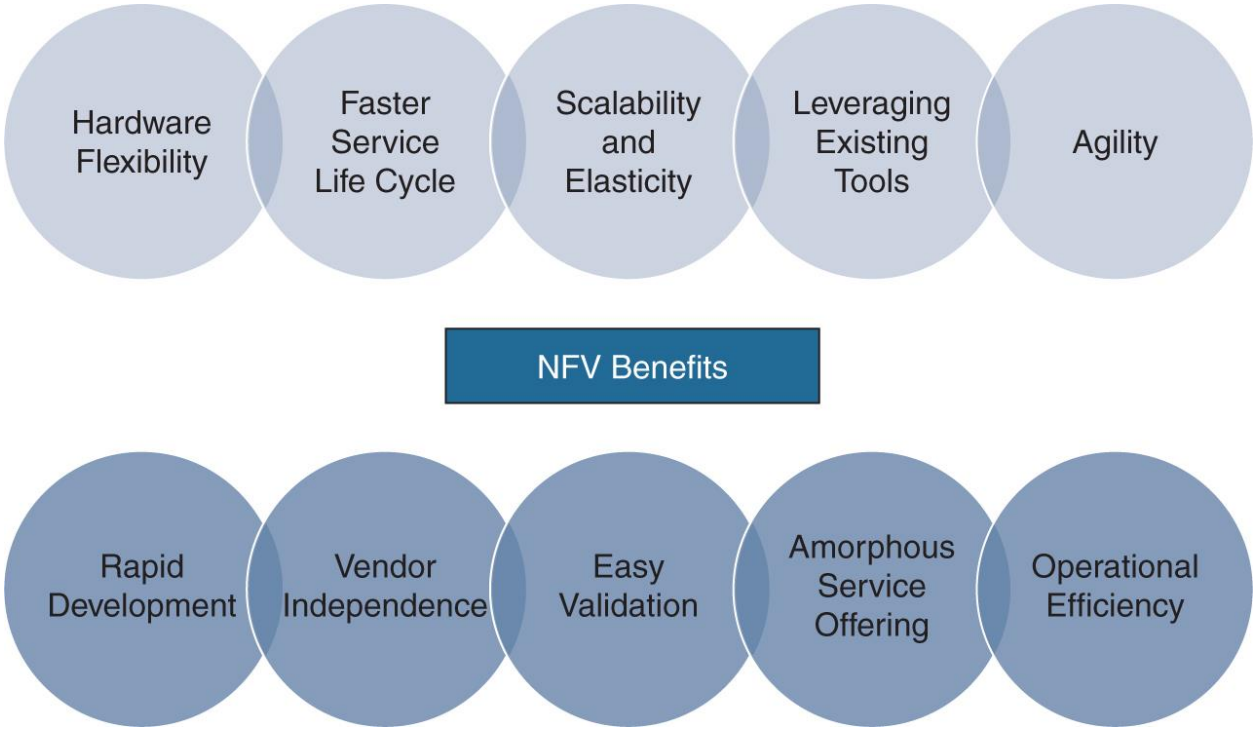

Figure 7. NFV elasticity.

Use of standard IT tools. Since NFV uses the same infrastructure as standard data centers, it can use all the deployment and management techniques that have been developed in them. This makes it possible to use existing IT methods and tools for telecommunication networks.

Fast deployment and getting rid of vendor dependency. Because NFV provides the means to quickly deploy standard solutions without the overhead associated with " single-vendor " solutions, operators can get rid of so-called "single-vendor" solutions. " vendor dependency ", i.e., excessive attachment to specialized solutions of a small number of vendors on the network.

New solutions can be deployed to the network quickly, without the need to wait for new features to be developed by traditional vendors, which often takes a long time.

In addition, it allows you to quickly deploy new solutions on test domains, test them, and if the tests are successful, also quickly deploy them to a live network. In case of failure, their cost is minimal, since such tests are only associated with installing and running software, and not with acquiring and running new expensive equipment.

Simplification of maintenance and technical operation. Maintenance and support of operations on the NFV helps to reduce possible periods of unavailability of services. For example, a failure of a virtual machine running a network function will immediately launch a backup virtual machine that will perform VNF from exactly the same place where the active VM failed.

This also makes it possible to achieve software upgrades during the ISSU (In-Service-Software-Upgrade) operation in 24/7 mode. All this significantly reduces and even completely eliminates the losses associated with network failures.

Reducing capital and operating costs. Since COTS equipment is inexpensive compared to specialized solutions of traditional telecom vendors, and NFV allows to achieve more optimal

equipment utilization, operators' capital costs for building and developing networks can be significantly reduced.

Reducing operating costs in NFV can be achieved by automating operations, increasing the ratio of the number of pieces of equipment per technician, as well as eliminating the need for specially trained personnel to maintain one or another proprietary solution of traditional vendors.

Conclusion. NFV reduces hardware costs and improves operational efficiency, but contains security issues that need to be addressed if NFV is rapidly deployed. For example, user authentication, user privilege control, and network configuration can be predefined before using the security features.

References:

1. NFV: An Introduction, Benefits, Enablers, Challenges & Call for Action. NFV white paper. URL: http://portal.etsi.org/NFV/NFV_White_Paper.pdf

2. OpenNF: Enabling Innovation in Network Function Control / A. Gember-Jacobson, R. Viswanathan, C.
Prakash, R. Grandl [et al.] // SIGCOMM ’14. Aug. 2014. P. 163–174.

3. Toward a Telco Cloud Environment for Service Functions / J. Soares, C. Goncalves, B. Parreira [et al.] // IEEE Communications Magazine. Feb. 2015. Vol. 53, No. 2. P. 98–106.

4. OpenSCaaS: An Open Service Chain as a Service Platform Toward the Integration of SDN and NFV / W. Ding, W. Qi, J. Wang, B. Chen // IEEE Network. May/Jun. 2015. Vol. 29, No. 3. P. 30–35.

5. Virtualized Security at the Network Edge: A UserCentric Approach / D. Montero, M. Yannuzzi, A. Shaw [et al.] // IEEE Communications Magazine. April 2015. Vol. 53, No. 4. P. 176–186.

6. ETSI Group Specification: Network Functions Virtualization (NFV) NFV Security Problem Statement. URL: http://www.etsi.org

7. ETSI Group Specification: Network Functions Virtualization (NFV) Virtualization Requirements, October 2013. URL: http://www.etsi.org/deliver/etsi_gs/NFV/001_099/002/01.01.01_60/gs_NFV002v010101p.pdf

8. ETSI Group Specification: Network Functions Virtualization (NFV) Resiliency Requirements, January 2015. URL: http://www.etsi.org/deliver/etsi_gs/NFVREL/001_099/001/01.01.01_60/gs_NFVREL001v010101p.pdf

9. ETSI Group Specification: Network Functions Virtualization (NFV) Use Cases, October 2013. URL: http://www.etsi.org/deliver/etsi_gs/NFV/001_099/001/01.01.01_60/gs_NFV001v010101p.pdf

10. Elastic Network Functions: Opportunities and Challenges / R. Szabo, M. Kind, F.-J. Westphal [et al.] // IEEE Network. May/Jun. 2015. Vol. 29, No. 3. P. 15–21.

11. A novel approach for integrating security policy enforcement with dynamic network virtualization / C. Basile, A. Lioy, C. Pitscheider, F. Valenza, M. Vallini // NetSoft. April 2015. P. 1–5.

12. Cisco and/or its affiliates, Cisco Evolved Services Platform At-a-Glance, Oct. 2014. URL: https://www.cisco.com/c/dam/global/hr_hr/assets/ciscoconnect/2014/pdfs/2014_04_see_epn_mpls_4x3.pdf

13. VMware, Datasheet: VMware vCloud NFV, Sep. 2015. URL: https://www.vmware.com/content/dam/digitalmarketing/v mware/en/pdf/solutions/vmware-vcloud-nfv-datasheet.pdf
14. VMware, Datasheet: VMware vCloud NFV, Sep. 2015. URL: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/solutions/vmware-vcloud-nfv-datasheet.pdf
15. Alcatel-Lucent White Paper, «Providing Security in NFV: Challenges and Opportunities», May 2014. URL: http://www.tmcnet.com/tmc/whitepapers/documents/whitepapers/2014/10172-providing-security-nfv.pdf
16. Dovgal V.A., Dovgal D.V Analysis of perspective methods of behavioral biometry for users authentication // The Bulletin of the Adyghe State University. Ser. Natural-Mathematical and Technical Sciences. 2017. Iss. 3 (206). P. 139–142. URL:http://vestnik.adygnet.ru