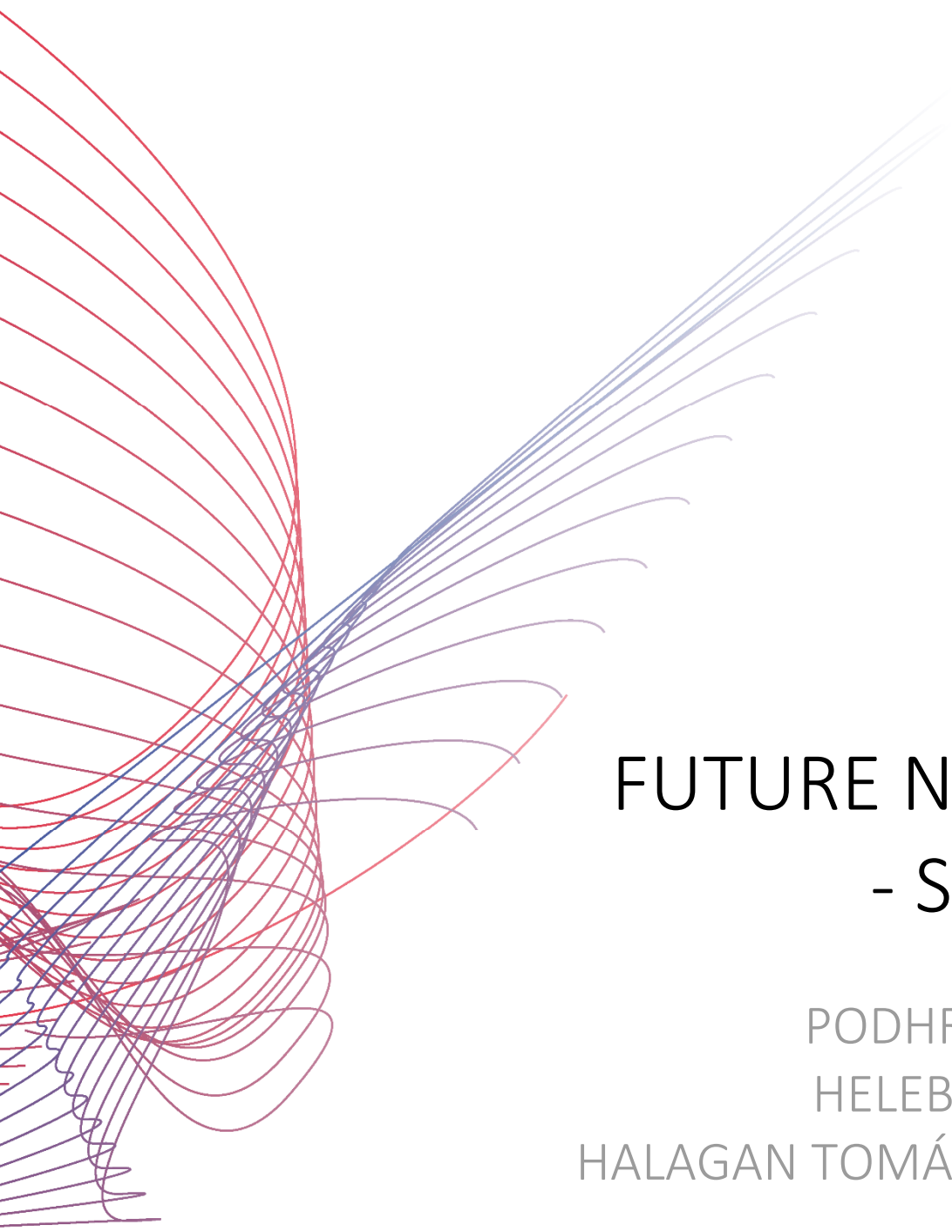
en
cs de
sk es

TECH pedia



FUTURE NETWORKS - SDN & NFV

PODHRADSKÝ PAVOL,
HELEBRANDT PAVOL,
HALAGAN TOMÁŠ, DROZD IVAN

Title: Future Networks - SDN & NFV

Author: Podhradský Pavol, Helebrandt Pavol, Halagan Tomáš, Drozd Ivan

Published by: Czech Technical University of Prague

Faculty of electrical engineering

Contact address: Technicka 2, Prague 6, Czech Republic

Phone Number: +420 224352084

Print: (only electronic form)

Number of pages: 38

Edition: 1st Edition, 2017

ISBN 978-80-01-06247-0

TechPedia
European Virtual Learning Platform for Electrical and Information Engineering

http://www.techpedia.eu

Erasmus+

This project has been funded with support from the European Commission.
This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Explanatory Notes

	Definition
	Interesting
	Note
	Example
	Summary
	Advantage
	Disadvantage

ANNOTATION

Current Internet is still based on Internet protocol that was defined over 40 years ago for certain set of services. During decades Internet acquired huge dimensions and it also didn't count with new applications like Web, video streaming, file sharing which significantly changed the nature of Internet traffic. The infrastructure of the Internet has been evolved by new technologies from fixed optical to wireless networks. New applications and services, technologies and amount and variability of end user devices call for flexible solutions. As the most challenging solutions seem to be interconnection of programmable - software defined networks and virtualization of network services. This modul mainly concentrates on these promising technologies for Future Internet but also gives overview of Next generation networks.

OBJECTIVES

Main objective of this course is to acquire basic knowledge about new trends in information and communication technologies mainly about evolution of current networks toward Future networks as well as Future Internet. Participants become familiar with basic characteristic of Next Generation Networks. However, the most inportant they will dispose with knowledge about state of the art technologies like Software Defined Networking and Network Functions Virtualization from point of view of basic architecture, principle and protocols. Moreover, a attention is also paid to actual limitations and requirements of Future Internet.

LITERATURE

[1] Mikoczy, E., Kotuliak, I., van Deventer, M. O.: Evolution of the converged NGN service platforms towards Future Networks. in Future Internet Journal, special issue Special Issue "Network vs. Application Based Solutions for NGN", 2011, ISSN 1999-5903.

[2] Mikoczy, E.: Next Generation of Multimedia Services in Context of Future Networks. In Proceedings of ETSI Future Network Technologies Workshop, Sophia Antipolis, France, 10–11 March 2010.

[3] Podhradský, P., Mikóczy, E., Lábaj, O., Londák, J., Trúchly, P., at al: NGN Architectures and NGN Protocols. LdV IntEleCT, Educational publication, 210 pages, Published by ČVUT Praha, ISBN: ISBN:978-80-01-04949-5, September 2011, CD version.

[4] Podhradský, P., Mikóczy, E., Dúha, J., Trúchly, P., at al: NGN – Selected topics, LdV IMProVET.Educational publication, 137 pages, Published by ČVUT Praha, ISBN: 978-80-01-05295-2, August 2013, CD versions (SK, EN, CZ).

[5] Nadeau, T. D., Gray, K.: SDN: Software Defined Networks. O'Reilly Media. 2013. ISBN: 978-1-449-34230-2.

[6] Helebrandt, P., Kotuliak, I.: Novel SDN multi-domain architecture. In IEEE 12th International Conference on Emerging eLearning Technologies and Applications (ICETA), pp.139-143, 2014.

[7] Open Networking Foundation: Software-Defined Networking: The New Norm for Networks. White Paper, 2012 https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf.

[8] McKeown, N.: OpenFlow and Software Defined Networks. online, Presentation. 2011 http://www.openflow.org/documents/OpenFlow_2011.pps.

[9] Open Networking Foundation. https://www.opennetworking.org.

[10] McKeown, N. et al.: OpenFlow: Enabling innovation in campus networks. In: ACM SIGCOMM Computer Communication Review, vol. 38, no. 2, pp.69-74, 2008.

[11] Open Networking Foundation: OpenFlow Switch Specification version 1.3.5. 2015 https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-switch-v1.3.5.pdf.

[12] Dong; L., Gopal, R., Halpern, J.: Forwarding and Control Element Separation (ForCES) Protocol Specification. IETF RFC 5810, 2010.

[13] Chiosi, M., Clarke, D., Willis, P., Reid, A., Feger, J., Bugenhagen, M., Khan, W., at al.: Network Functions Virtualisation: An Introduction, Benefits, Enablers, Challenges & Call for Action. SDN and OpenFlow World Congress, 2012. https://portal.etsi.org/nfv/nfv_white_paper.pdf.

[14] Chiosi, M., Wright, S., Clarke, D., Willis, P., at al.: Network Functions Virtualisation: Network Operator Perspectives on Industry Progress. SDN and OpenFlow World Congress, 2013. https://portal.etsi.org/nfv/nfv_white_paper2.pdf.

[15] ETSI GS NFV-INF 001 V1.1.1, Network Functions Virtualisation: Infrastructure Overview. Specification, 2015. http://www.etsi.org/deliver/etsi_gs/NFV-INF/001_099/001/01.01.01_60/gs_NFV-INF001v010101p.pdf.

[16] ETSI GS NFV-MAN 001 V1.1.1, Network Functions Virtualisation: Management and Orchestration. Specification, 2014. http://www.etsi.org/deliver/etsi_gs/NFV-MAN/001_099/001/01.01.01_60/gs_NFV-MAN001v010101p.pdf.

[17] ETSI GS NFV-SWA 001 V1.1.1, Network Functions Virtualisation: Virtual Network Functions Architecture. Specification, 2014. http://www.etsi.org/deliver/etsi_gs/NFV-SWA/001_099/001/01.01.01_60/gs_NFV-SWA001v010101p.pdf.

[18] SdxCentral:Network Functions Virtualization Report. 2015. https://www.sdxcentral.com/reports/network-functions-virtualization-report-2015/.

[19] Gruber C. G.: CAPEX and OPEX in Aggregation and Core Networks. In: Optical Fiber Communication, IEEE, 2009, pp. 1-3.

[20] Strategy Analytics: Global Internet Device Installed Base Forecast. August 2014. https://www4.strategyanalytics.com/default.aspx?mod=pressreleaseviewer&a0=5609.

[21] Wu, Y. et al.: CloudMoV: Cloud-Based Mobile Social TV. In: IEEE Transactions on Multimedia, vol.15, 2013, pp. 821-832.

[22] Roberts, J.: The clean-slate approach to future Internet design: a survey of research initiatives. annals of telecommunications - annales des télécommunications, Volume 64, Issue 5, 2009. pp 271-276.

[23] Banniza, T.R., Boettle, D., Klotsche, R., Schefczik, P., Soellner, M., Wuenstel, K.: A European Approach to a Clean Slate Design for the Future Internet. Bell Labs Technical Journal - Core and Wireless Networks, Volume 14 Issue 2, August 2009. pp. 5-22.

[24] McKeown, N. et al.: Openflow: Enabling innovation in campus networks. In: SIGCOMM Computer Communication Review, vol.38, no.2, 2008, pp. 69-74.

[25] Bashker, D., Cascio, W., Boudreau, J.: How to Apply HR Financial Strategies (Collection), Addison Wesley. Chapter 1, August 2013, ISBN 9780133743173. pp. 6-10.

[26] Barroso, L. A., Clidaras, J., Hölzle, U.: The Datacenter as a Computer: An Introduction to the Design of Warehouse-Scale Machines - Second Edition. Morgan & Claypool. Chapter 6., pp. 69-71, 2013, ISBN 9781627050104.

[27] Tits, Y.: Lack of standardization concerning interfaces between network equipments. In: Electricity Distribution (CIRED 2013), 22nd International Conference and Exhibition on, IET, 2013, pp. 1-4.

[28] McKeown, N., Girod, B.: Clean-Slate Design for the Internet A Research Program at Stanford University. White paper Version 2.0, 18 April 2006.

Index

1 Introduction

New topic in area of information and communication technologies is further evolution of **NGN** (*Next Generation Networks*) technologies towards Future Networks. There are several aspects that are influencing actual IMS based NGN architecture to enhance additional functionalities for next generation of multimedia services. Rapid development of internet services and content delivery services over heterogeneous networks are changing requirements from different aspects like additional functionalities, mobility, virtualization and sharing of resources, security, simplification of architecture and flexibility in control models with context awareness.

Recently ongoing discussions about changes of architectures of Internet (Future Internet) also in the area of telecommunications for *Future Networks* (**FN**) are running in research projects as well as standardization (ITU-T, ETSI).

2 NGN architecture evolution towards Future Network architectures

There have been identified 2 main streams of potential development:

1. Clean slate approach or revolution principle – Future Internet, where new architecture and protocols for Future Internet will be newly defined and designed (new network scenarios, models of new protocols and testing of revolutionary architecture modes), [1]. The revolutionary jump is expected as if the Internet had been designed from clean slate approach, by new technologies, not limited by present concepts.

2. Evolutionary concept where existing NGN architectures are enhanced by new requirements and functions leading to concept called Future Networks [1], [2]. NGN evolution can achieve expected capabilities of Future Networks using existing protocols and capabilities of NGN (enabled just with necessary enhancement of architecture and control mechanisms).

The second concept is more realistic approach towards Future networks from migration point of view where NGN networks and technologies are already available.

It is appropriate to look into the evolution and to outline of NGN future trends and the open issues to be solved as well. Migration scenarios of different types of networks platforms are based on the idea to integrate TDM and IP platforms into one converged NGN platform (from the point of network infrastructure, as well as services). New concepts and architectures of new generation of ICT based on converged ICT and NGN offer to operators new opportunities to implement and provide wide spectrum of multimedia services and applications.

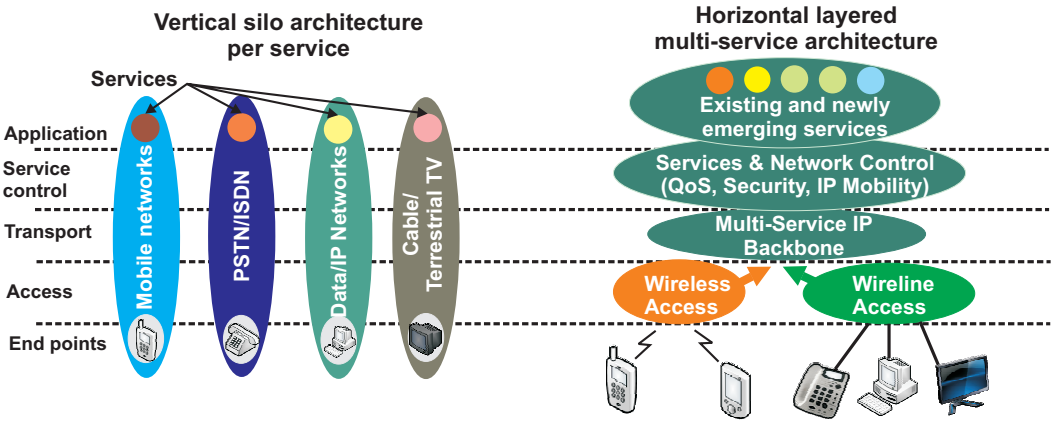


Fig. 1 - From vertical silos to horizontal NGN architecture [1]

Therefore operators can move from vertical silo architecture where each type of service has dedicated access, transport, control and application infrastructure per service, to horizontally oriented architecture more independent from provided services (Fig. 1).

2.1 NGN concepts and architectures

The main principles of the NGNs (Next Generation Networks) were formed when the idea of NGN itself emerged. The next two definitions from ETSI and ITU-T describe NGN in substance.

ETSI describes NGN as a concept for the defining and establishing of the networks, allowing a formal distribution of functionalities into separate layers and planes by using open interfaces. The NGN concept provides new conditions for creation, implementation and effective management of innovative services. ITU-T describes NGN as a network based on packet transfer, enabling to provide services, including telecommunication services, and is capable of using several broadband transmission technologies allowing guaranteeing QoS. The functions related to services are at the same time independent of the basic transmission technologies. NGN provides unlimited user access to different service providers. It supports general mobility providing the users with consistency and availability of services.

That is what definitions say, but probably eventually NGN advantages are of bigger importance. Worth mentioning are some requirements for NGN it should conform to:

- High-capacity packet transfer within the transmission infrastructure,
- Separation of managing functions from transmission features. Separation of service provisioning from the network,
- Support for a wide range of services and applications,
- Broadband capabilities, while complying with the requirements for **QoS** (*Quality of Services*),
- Various types of mobility (users, terminals, services),
- Various identification schemes and addressing,
- Converged services between fixed and mobile networks (as well as voice, data and video convergence),
- Conformance to the regulation requirements, such as emergency calls and security requirements,
- Cheaper and more effective technologies.

Within the NGN concepts the standardisation institutions are solving the following issues and problems:

- existing networks migration towards NGN,
- development in the field of access technologies,
- connection of other networks to IP networks,

- provision of services and development of new ones,
- interworking in the area of addressing,
- interworking of signalling systems,
- roaming and mobility.

There are many conceptual models and reference architectures for both the converged networks and VoIP architectures. Therefore, we have tried to find common features and to define a suitable conceptual model for NGN. An objective of the conceptual model is to determine functional layers (covering similar functionalities), their entities, reference points (interfaces) and information flows between them. Such a model then can be mapped more easily into the physical reference architecture (and it is independent of the physical entities, i.e. components of the architecture).

In most analyzed cases the NGN conceptual model layers are from the point of view of functionalities divided into independent parts as follows (Fig. 2): access (some reference architectures do not include it directly into the NGN model or replace it by the adaptation one), transport (transmission, switching), control (call/sessions control) and application (services).

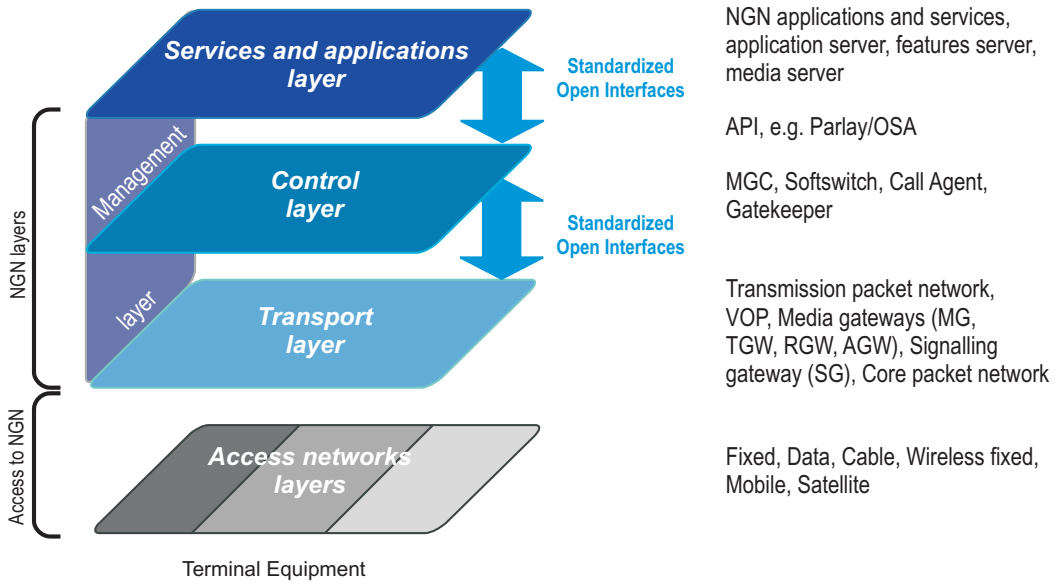


Fig. 2 - NGN conceptual model and its functional layers

2.2 Conceptual model layers

The **access layer** provides the infrastructure, for example an access network between the end user and the transport network.

The **transport layer** ensures the transport between the individual nodes (points) of the network.

The **control layer** includes the control of services and network elements. This layer is responsible for set-up/establishing, control and canceling of the multimedia session.

The **service layer** offers the basic service functions, which can be used to create more complex and sophisticated services and applications.

In the NGN it is required that the network control is not determined only by the terminal equipment applications, but that the network intelligence may carry out control over the network at all levels of the reference model. The network management reference model implies the following **tasks for the network intelligence** it has to ensure:

- Resource management (capacity, ports, and physical elements) and QoS in access to the network and in the transport network, as necessary.
- Various media processing, encoding, data transfer (information flows).
- Management of calls and connection. Management and interworking of all elements of the reference architecture.
- Service control.

The NGN concept and architectures are in more details described in [3], [4].

There are several concepts and evolution trends leading to new network architectures which are able to provide the wide spectrum/portfolio of new multimedia services/multimedia content.

New network architectures based on “Software Defined Networking” and “Network Functions Virtualization” are introduced and described in chapter 3 and 4, respectively and "Future Internet" concept in chapter 5 of this "Learning Module".

3 Software Defined Networking (SDN)

3.1 Introduction to SDN

SDN (*Software Defined Networking*) is a new approach to ICT network architecture with aim to programmatically control the whole network.

This enables solving of many problems in traditional approaches to networking while also enabling new features as well. In general the idea of SDN is to increase the flexibility, manageability and extensibility of ICT networks, with secondary goal of decreasing equipment costs. This can be achieved by taking advantage of fast development and deployment cycle of relatively cheap software applications in contrast to expensive specialized networking hardware.

The main motivation for SDN in the beginning came from the need for a better solution for innovation in network research and development. At that time, there were only two available methods to test new features - software simulation or hardware testbeds.

The simulation offers great flexibility and repeatability.

However, simulations are usually not run in real time - in parallel with the code production, and it is not easy to connect simulated network to real network and test coexistence of the new features in a more realistic environment. On the other hand, testbeds implemented with custom hardware are difficult to program, can be difficult to modify once set up and are very expensive.

This can lead to compromises in their adoption - either using a shared testbed used by more research projects that limits time available for experiments and repeatability. Or alternatively, creating own testbed using traditional network devices available from equipment providers. These are mostly supplied as a black box with minimal customization, limiting testbed capabilities for new and more exotic experiments required for more revolutionary than evolutionary innovations.

In late 90's and early 2000's, the computing power of general purpose computers was significantly increased compared to specialized networking hardware. This coupled with advances in virtualization and a few other technologies led to their utilization in execution for software implemented control of simple network nodes used for fast packet switching. Controlling software could be modified as easily as simulation, while cheap hardware with limited higher level features used for packet switching provided packet handling rates comparable to custom hardware testbeds. It was one of the central pillars of SDN, which lies in separation of control and forwarding plane that is described in the following section in more details [5].

3.2 Separation of Network Control and Data Forwarding Plane

Before we describe the concept of SDN, it is necessary to define what the Control plane and Data Forwarding plane are.

In most of routers (or any networking equipment for that matter) there is specialized hardware for fast switching of data between interfaces - Data Forwarding plane. The forwarding is managed by rules created by processor running operating system, routing algorithms, address translation, and other higher functions - this is the Control plane.

In traditional networking, both control plane and data forwarding plane are implemented in every network node. This enables every device to be totally autonomous and make all high level decisions, such as packet routing independently.

This stems from origin of the Internet – ARPANET, initially designed by and for the military with high resilience and survivability as primary concern. Flexibility, straightforward modification or adoption of new features was a secondary goal at best.

The fundamental principle of SDN is separation of control and data forwarding plane in network as depicted in Fig. 3. By the implementing of the separated control plane by the software for general purpose computer from forwarding plane on network equipment, it is possible to centralize routing and switching decisions as well as configuration of all network devices.

The centralized control plane implemented in software executed on general purpose processors can bring many advantages to networking - especially speeding up innovation, new network features development and deployment.

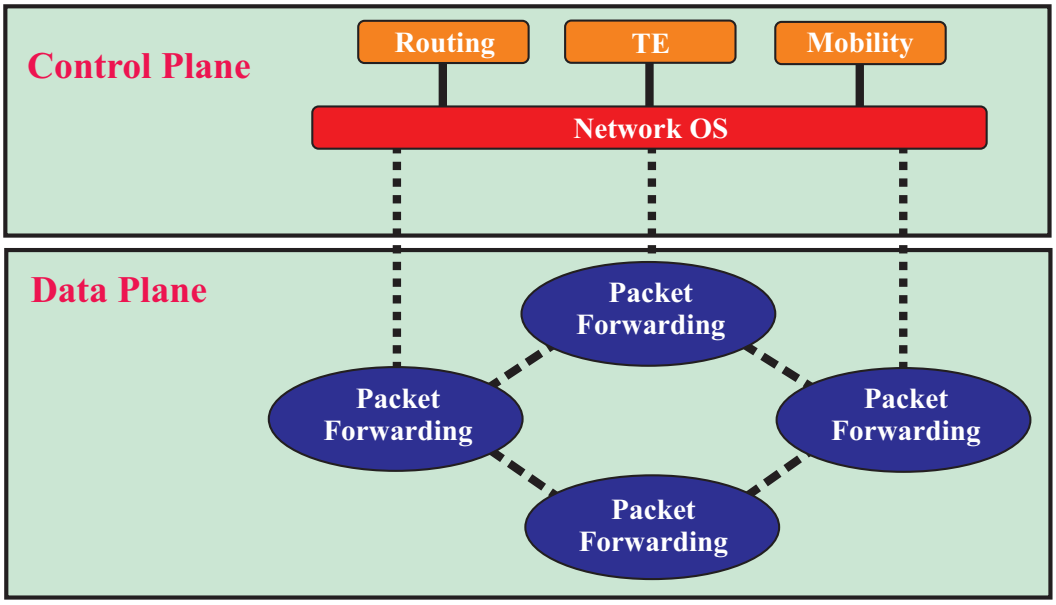


Fig. 3 - Basic SDN architecture

3.3 Centralized Control and Network Programmability

In modern network equipment the control plane gathers information about the status of connections to neighbors and network as a whole that is supplied to routing algorithms. The distributed algorithms provide automatic solution to routing network traffic, but one their shortcomings is possible problem with convergence. Since every device gathers information about the network and makes routing decisions by itself, delay in information propagation about network changes can lead to problems in network operation.

Eliminating control plane from every network node and using centralized control plane not only allows for a complete view of the network without difficulties with convergence inherent to distributed routing algorithms, but they also decrease cost. Additionally, without need for distributed traffic routing, new algorithms can be used, modified and developed. Furthermore, configuring the central control plane makes network management simpler, removing need for configuring every node separately. This reduces chance for misconfiguration and expedites troubleshooting too. The added benefit of software implementation of centralized control plane is ease of modification and development of new features.

However, opponents of SDN and centralized control plane especially point to limits of its usability in large scale networks such as the Internet. Their criticism focuses on controller being the single point of failures for the whole network and insufficient scaling.

Solution of these problems is using logically centralized, but physically distributed control plane – where a number of controllers manage the part of the network and communicate together to reduce the control plane latency, provide high availability and single logical management point for the network administration. New architecture for the inter-domain connection with associated communication protocol for SDN controllers is proposed in [6].

3.4 Comparison to distributed control plane of traditional networks

Traditional network equipment incorporates the control plane, network applications and other higher level capabilities in device firmware. This means all network nodes make routing decisions locally - effectively using a fully distributed control plane, as displayed in Fig. 4. This can be contrasted to the centralized control plane in SDN architecture shown in Fig. 3.

Integration of many functions provides greater functionality of the every node and makes them more independent, almost eliminating single point of failure.

But it is achieved at the expense of the increased complexity. That correlates to more expensive equipment; higher power consumption and can lead to delays in the traffic handling caused by the need to process it by various applications. Furthermore, the configuration or modification of the network requires manual configuration of many devices and often the use of complex management tools. Network management is additionally complicated by implementation and configuration disparities between different vendors causing interoperability issues.

As it is stated in [7], all that complexity leads to static networks what is in contrast with the need for a dynamic environment with greater user mobility and server virtualization. Inconsistencies in network-wide policies and limited network scalability are further effects of traditional network intricacies in large networks.

Centralized control plane in SDN allows network administrator to shape traffic without the need to manually configure many devices, thus providing easier network management and greater flexibility.

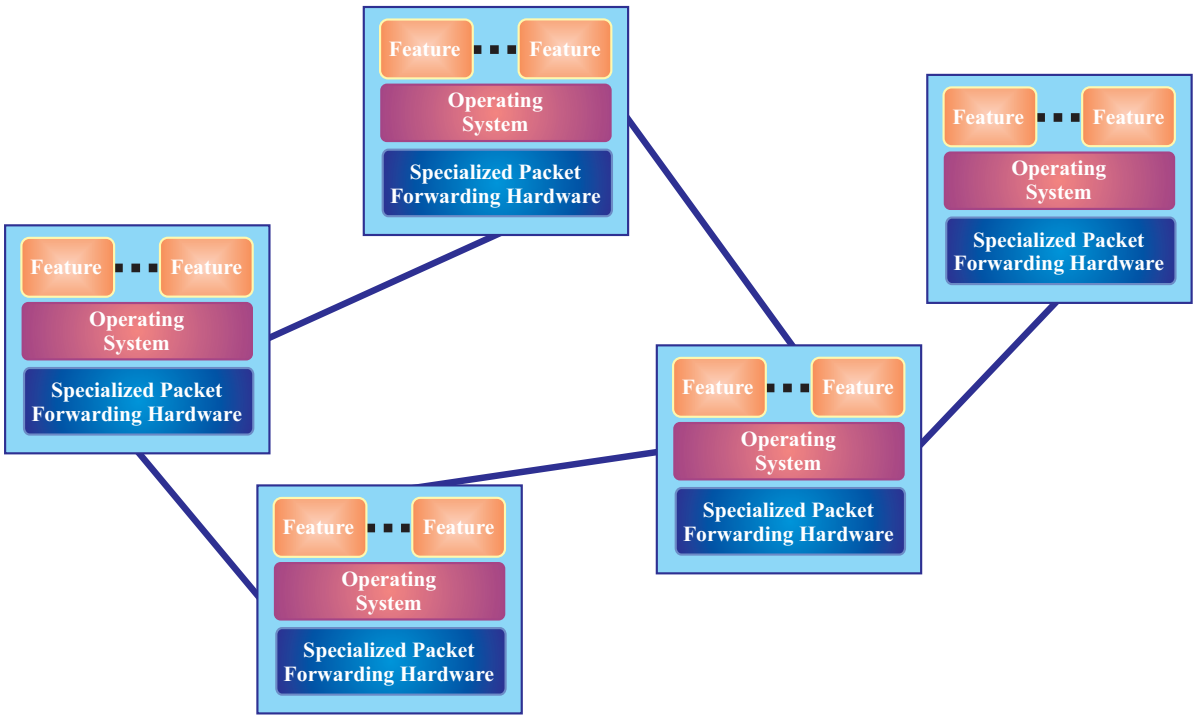


Fig. 4 - Traditional packet network architecture [8]

While MPLS is superficially similar to SDN with fast switching of traffic flows established by the control plane, it does so in a different manner. There is no centralized control plane, which is in every MPLS router with every LER able to create a path and distribute it using Label Distribution Protocol (LDP).

3.5 SDN Protocols

The separation of the control and data forwarding plane – one of the central pillars of SDN together with centralization of control plane means that there is a need for communication protocol. In this section we introduce some of them, starting with the most popular – OpenFlow.

OpenFlow

OpenFlow is an open standard originally developed at universities and currently maintained by *Open Network Foundation* (**ONF**) [9] – a non-profit consortium with mission to commercialize and promote OpenFlow based SDN. ONF succeeded spectacularly, with OpenFlow being the most popular protocol used for communication between control plane and data forwarding plane – becoming the de facto standard. However, this ONF campaign led to many misunderstanding that OpenFlow equals SDN.

Despite existing software based switching solutions allowing research into new methods and networking protocols, most do not provide the sufficient computational performance and/or port densities for large scale experiments.

The simplest of examples are many open software based implementations of routing or switching protocols running on general purpose computers with several network interfaces. These techniques can be categorized into the first group that is lacking performance wise, when compared to dedicated networking equipment. On the other end of the spectrum there are hardware based networking research solutions like the NetFPGA utilizing specialized FPGA card for line-rate processing of the traffic.

NetFPGA is used mainly in the academia and rapid prototyping because it is limited to only 4 ports per card.

As mentioned in [10] these are limiting factors for academic networking researchers, with OpenFlow being a compromise between low-performance generality and freedom of research solutions and closed and not very modifiable high-performance of network equipment from commercial vendors.

The OpenFlow protocol defines communication interface between control plane and forwarding plane devices and so it must be implemented by both sides. Since OpenFlow provides extremely granular control on per-flow basis, it enables the network to react to topology, application or user changes in real-time.

ONF white paper [9] notes that the classical network routing solutions today do not support the control on this level of the granularity.

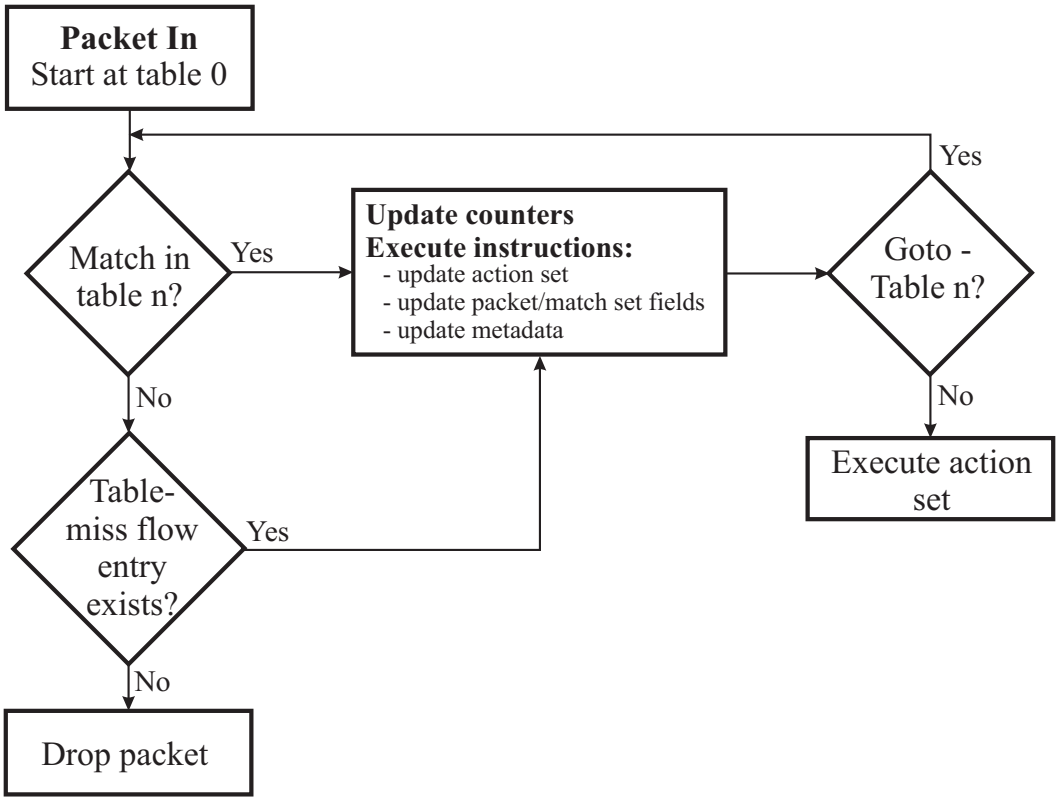


Fig. 5 - Flowchart detailing packet handling in OpenFlow logical switch [11]

When a packet is received by OpenFlow enabled switch, it is handled in OpenFlow pipeline composed of one or more Flow Tables, each containing entries with rules and actions to be performed on the packet belonging to flow. If the match for the packet is not found in any Flow Table and the rule to send unknown packets to Controller is set-up, it is sent to the controller. Controller processes the packet and either drops the packet or establishes a new flow, by creating a new entry in Flow Table. The handling mechanism of a received packet inside the OpenFlow switch is charted in Fig. 5.

ForCES

Forwarding and Control Element Separation (**ForCES**) protocol [12] defines an architectural framework and associated protocols to standardize information exchange between the control plane and the forwarding plane in a ForCES Network Element.

ForCES addresses mainly the open API/protocol that provides a clear separation between control and forwarding plane.

The major strength of ForCES lies in its Forwarding Element Model that enables description of new forwarding plane functionality without changing the protocol between control and forwarding planes.

ForCES development aimed to split network device into distinct control and forwarding planes. The motivation behind this arose from the desire to build forwarding plane of network elements from flexible hardware components independently from control plane. This results in ForCES creating a new architecture for network devices, while OpenFlow aims to create new network architecture.

NETCONF

NETCONF is a network management protocol that provides mechanisms to remotely install, manipulate, and delete the configuration of network devices.

NETCONF protocol itself is divided into four layers with a set of base protocol operations using **RPC** (*Remote Procedure Call*) methods with XML-encoded message parameters.

One of the goals of NETCONF is to provide a programmatic interface to the device that closely follows the functionality of the device's native interface.

Although it was initially developed as a successor to SNMP and some of the CLI protocols for configuration of network elements, NETCONF capabilities can be used to create a form of a hybrid SDN. Moreover, NETCONF support is a requirement for network devices to be compatible with OF-CONFIG part of OpenFlow specification.

PCE-P

Path Computational Element (**PCE**) is an entity that computes paths on behalf of the nodes in the network that can find optimal paths for MPLS and GMPLS P2P and P2MP traffic engineered *label switched paths* (**LSPs**).

PCE then communicates this path to network nodes using PCE Communication Protocol. Thus, PCE can also be perceived as extending MPLS and GMPLS TE capabilities narrowing the gap between SDN and standard MPLS/GMPLS.

Although PCE in itself was not primarily developed as an SDN enabling technology, it can provide logically centralized management model for existing technologies with a few additional enhancement.

Interface to the Routing System

Interface to the Routing System (**I2RS**) is one of the more ambitious approaches to SDN that is still in early stages, being developed by IETF. The I2RS is a bidirectional programmatic interface for communication between routing system and applications - allowing network monitoring, reservation of resources and modification of the routing configuration. While I2RS is concerned with communication to and from the routing system, it is not intended to provide direct

interfaces to forwarding plane, making use of existing mechanisms to distribute selected routes into forwarding plane.

Cisco ONE

Even though Cisco is a part of the Open Networking Foundation and is actively participating in the OpenFlow development, it is not the only SDN project it is working on. One of their proprietary alternatives is *Open Network Environment* (Cisco **ONE**), which is providing programmatic interface to directly control Cisco equipment. The key component of Cisco ONE is *ONE Platform Kit* (**onePK**) – developer kit including several platform APIs, enabling easy development of network applications using direct access to networking equipment through network abstraction layer.

Nuage

In April of 2013 Alcatel-Lucent launched spin-out company Nuage Networks tasked with creating a SDN solution built on its earlier Application Fluent Network but with freedom to utilize alternative fresh technologies. The product of this endeavor is Nuage Virtualized Service Platform, a software solution that focuses on the problem of the network virtualization in data centers and *Cloud Service Providers* (**CSPs**). Because Nuage VSP is implemented in software and uses VXLAN as the encapsulation across hypervisors, it is not dependent on a specific type or brand of TOR switches to function.

4 Network Functions Virtualization (NFV)

An integral part of Telco (Telecommunication) operators are proprietary hardware devices. Telco (Telecommunication operators) does not avoid buying new hardware with the same functionality and services, as these devices are required for the provision of new services. It presents many complications associated with both the increasing costs and with the time demands of this deployment, such as **TTM** (*time to market*) and **TTD** (*time to deploy*). These complications are becoming nowadays for Telco operators limiting factors to providing quality of services.

Fig. 6 illustrates new approach in network architecture based on *Network Functions Virtualization* (**NFV**).

This approach provides to network/telco operators the opportunity to consolidate many network equipment types onto industry standard high volume servers, switches and storage, which could be located in Datacenters, Network Nodes and in the end user premises.

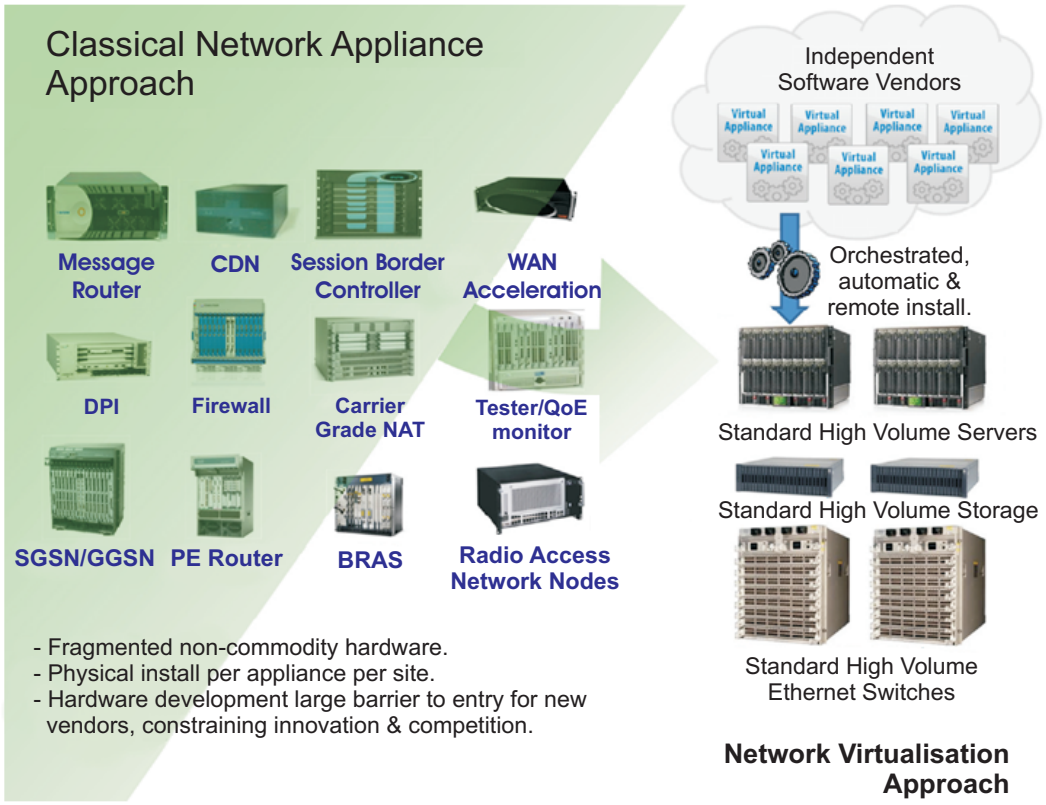


Fig. 6 - Vision of Network Functions Virtualization [13]

Benefits for network/telco operators:

- Reducing **CAPEX** (*capital expenditure*) and **OPEX** (*operational expenses,* such as Repair and maintenance) by reducing the cost of equipment and reduce energy consumption,
- Shorter time to market for deploying new network services
- Better return on investment of new services,
- Greater flexibility scalability or developing services
- Opportunities to testing and deployment of new innovative services with lower risk.

In October 2012 the white paper that presented the first draft of NFV was published [13]. ETSI set out the various requirements which are placed on the technology and described the benefits that come with NFV technology and this technology should bring. *Network Functions Virtualization Industry Specification Group* (**NFV ISG**) has been created to cover all tasks related to new emerged technology. This Group was created by the *European Telecommunications Standards Institute* (**ETSI**). From October 2012 the NFV ISG Group was gradually increased and about 235 conducted companies attended several meetings in Asia, Europe and North America. Outputs of the first meeting of the group NFV ISG were in the form of documents, and were issued in October 2013. The documents cover all the architecture NFV with all components and interfaces between them written down. From 2013 through 2015 this group ran the second phase and newer documents are available directly on the website NFV ISG.

4.1 What has enabled NFV?

If it is possible to build networks in a manner that represents technology NFV, the question logically arises why the network, from the very beginning of its establishment, is using proprietary hardware. The answer is that the industry-standard servers with the operating system and software have only recently acquired high performance to be able to effectively compete with proprietary devices, particularly in terms of prices, electricity consumption and reliability.

We can specify “Recently” time as the last four to five years. During this period, we have witnessed a dramatic improvement in network throughput and packet processing throughput of x86 processors as well as rapidly increasing the number of processor cores available on a single physical device industrial server.

4.2 Requirements for NFV

List of essential requirements which should meet NFV [13]:

- Portability - solving abilities loading and launching of moving software functions via various standard data centres.
- Performance - performance targets software features.
- Management and orchestration - mechanisms that must exist because orchestration and lifecycle management software functions, resources, infrastructure and various operations for making them.
- Flexibility - ability to provide solutions easier way scalability of hardware resources.
- Security - the fixed dimensions that must be analysed, since the virtualization environment can be subjected to external attacks.
- Continuity of services - functions that are necessary for the continued provision of services in accordance with the specification of services *Service Level Agreement* (**SLA**).
- Operations - automation of operational functions (e.g. Adaptation of network capacity, downloadable software update, repair of detected malfunctions, etc.).
- Energy efficiency - help to minimize the energy consumption of large virtualized networks.
- Migration and Coexistence with existing platforms - support the transition from today's networks where non-virtualized network coexists with virtualized without interruption of services or other unpleasant effects on the user.

The ability of remote deployment and operation of virtualized network functions on NFV infrastructure provided by different service providers enables efficient service to customers worldwide.

4.3 NFV architecture

Architecture of NFV technology was designed in the second edition of white paper [14] (Fig. 7) and consists of the following components:

- **NFVI** (*virtualized network functions infrastructure*) - provides virtual resources needed to support the implementation of virtualized networking functions - commercial COTS hardware components for acceleration, layer of software that virtualizes and abstracts the underlying hardware.
- **VNF** (*virtualized network feature*) - software implementation of network functions that is able to run by NFVI and may be accompanied by EMS - Element Management System, which manages the VNF. VNF is an entity corresponding to today's network node, which is expected to be delivered as a pure software independent of the hardware.
- NFV **MANO** (*management and orchestration*) - covers orchestration and lifecycle management of physical and / or software tools that support the virtualization and infrastructure lifecycle management VNFs. NFV MANO focuses on virtualization management tasks, which is necessary for NFV framework. It also collaborates with external NFV OSS / BSS and enables integration NFV to existing networks.

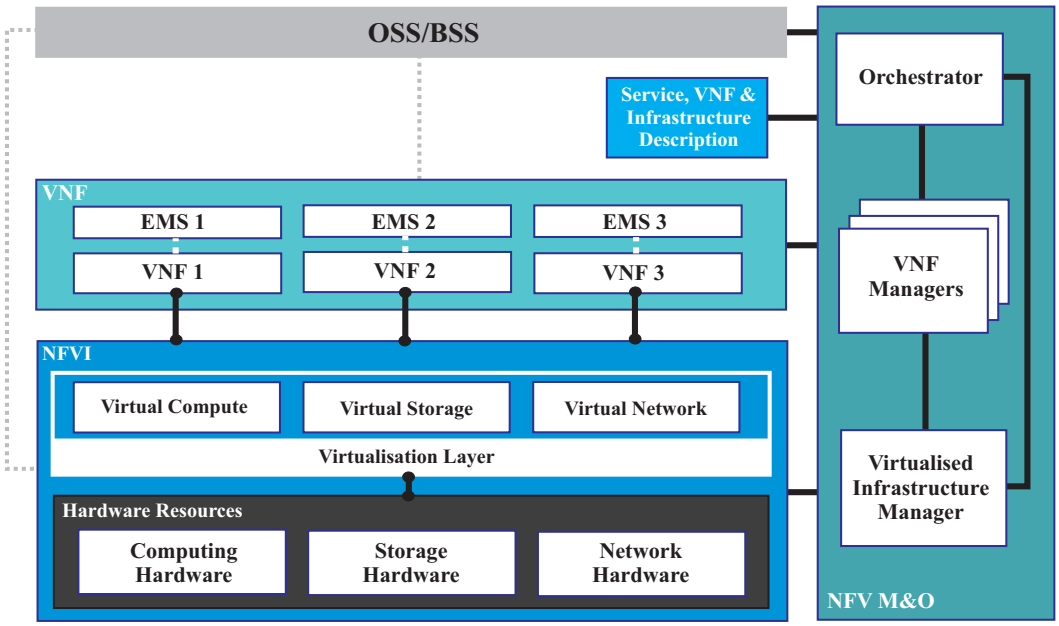


Fig. 7 - Architecture of NFV [14]

The entire system is powered by a set of metadata describing NFV services VNFs and infrastructure requirements to NFV MANO to manage accordingly. These descriptions together with services, VNFs and infrastructure can be provided by other industry players.

4.4 Infrastructure NFV - NFVI

Infrastructure NFV is divided into three domains [15]:

- Computer domain - the domain of computer role is to provide computing and storage resources and when used in conjunction with the hypervisor. It provides an interface to a domain network infrastructure, but does not connect to the network itself.

- Hypervisor domain - the domain role is to mediate computational resources domain software running on virtual machines. Hypervisors have been developed for the needs of cloud solutions, and attach importance to the allocation of the available hardware simply can achieve a high level of portability of virtual machines. The hypervisor can emulate (imitate) each type of hardware platform and even in some cases, completely emulate the instruction set so that the virtual machine considers that runs on a completely different processor architectures than the real one.

- Domain network infrastructure - its role:

    - create a channel of communication between multiple **VNFC** (*virtualized network functions components*) distributed VNF (virtualized network functions)

    - create a channel of communication between multiple VNF

    - create a communication channel between VNF and MANO

    - create a channel of communication between components NFVI and their orchestration and management

    - provide a means of remote control VNFC

    - provide a means of linking with the existing network operator

4.5 Management and Orchestration NFV (MANO)

Management and orchestration includes three components [16]:

- NFV Orchestrator - is responsible for orchestration (management) NFVI source to multiple **VIM** (*Virtualized Infrastructure Manager*), perform functions orchestration of resources, lifecycle management of network services (e.g. Management policies instances, scaling, performance measurement, event correlation), filling function orchestration for network services, global resource management, validation and approval of applications NFVI sources.

- VNF Manager - responsible for managing the lifecycle of instances of the VNF (he may be assigned to the management of one VNF instance, and can also manage multiple instances of the same or another type), overall coordination and adaptation of configurations and incident reporting between NFVI and E/NMS

- Virtualized Infrastructure Manager (VIM) - is responsible for the control and management NFVI calculation, memory and network resources within the infrastructure sub-domains of a single operator, the collection and transmission performance measurements and events.

4.6 Software architecture - Virtualized Network Functions (VNF)

Virtualized network feature is a network feature capable of operating on NFV infrastructure (NFVI) and is managed by *NFV orchestrator* (**NFVO**) and VNF manager. Internal VNF architecture is illustrated on Fig. 8.

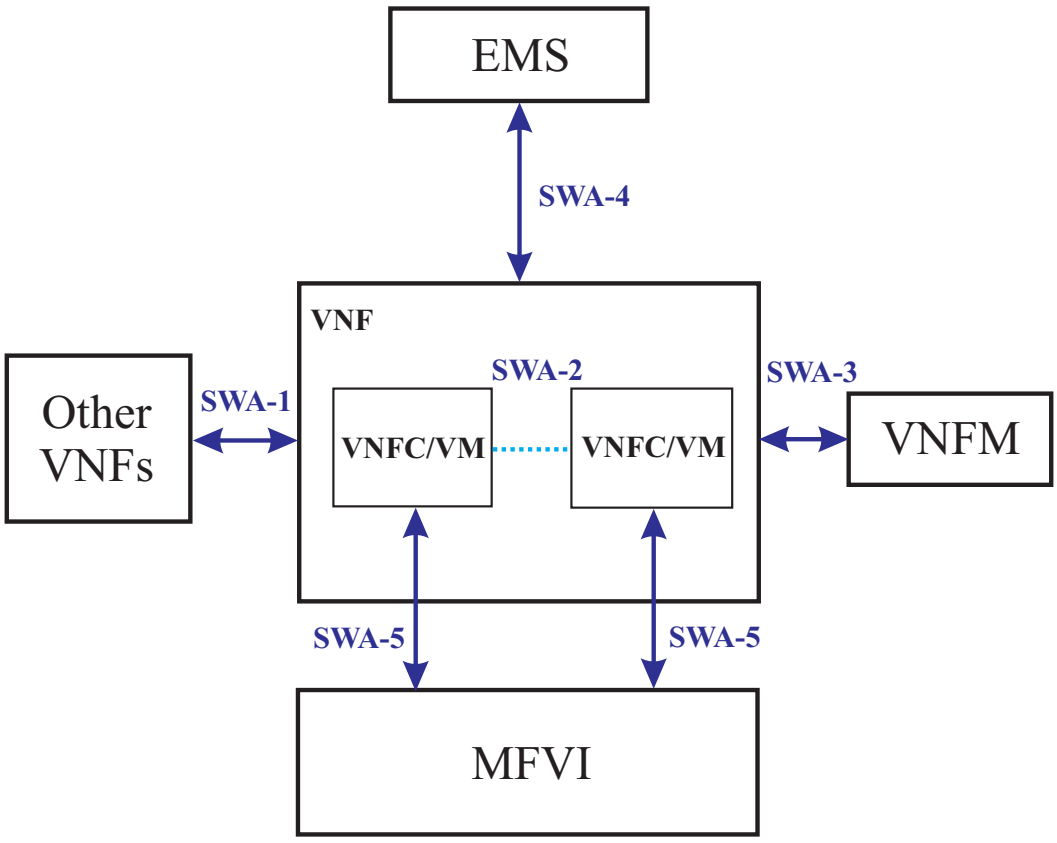


Fig. 8 - Architecture of NFV [17]

This architecture ensures quality connections using the interface:

- Interface SWA-1 - with this interface several VNF communicate with each other, they may use this interface to play together and perform tasks across a network.
- Interface SWA-2 - using this interface components within VNF are connected, each component plays a role for running virtualized network functions.
- SWA-3 Interface - This interface connects with VNF Manager.
- Interface SWA-4 - Using this interface it is connected to the VNF (EMS).
- Interface SWA-5 - NFVI connects with each VNFC.

4.7 Use cases for NFV

NFV on the one hand offers many advantages, simplification, innovative approaches to networking functions and on the other hand, opens up an endless amount of use cases, which are more or less useful in the real network traffic.

Nevertheless, currently we can say that NFV is not a separate fully workable solution, even the ETSI organization develops continuous efforts to create a strong unified NFV standard. NFV is idea to profit from virtualization, what approach will be taken for the provision of network functionalities and how to manage and orchestrate it all.

Web portal SDxCentral annually publishes a comprehensive report called Network Functions Virtualization Report [18], which includes the main idea of NFV, its evolution, and overview of Vendors delivering NFV solution as well as most beneficial use cases listed below.

Virtualized Network Functions

Nowadays, well-functioning cloud already offers many opportunities how to easily, flexibly and quickly distribute or develop applications, infrastructure or platforms. Virtualized Network Functions are being adapted to fully respect the already existing method in the world of cloud. For Cloud Service providers is most attractive the provision of virtual routing, virtual private network (VPN), layer 4-7 acceleration and security services to help them connect, scale and protect their cloud-based applications.

Virtualized/Cloud Radio Access Network

This use case is particularly important for Mobile Service Providers who are looking for ways to simplify and accelerate the creation of new *radio access networks* (**RANs**), while controlling the costs. A number of functionalities that run on proprietary hardware located in a base station may be moved onto virtual machine or set of virtual machines that could operate locally on COTS servers, on an aggregation point or in the cloud.

Virtualized Mobile Core

Mobile operators are often faced with tasks of upgrading their networks, services and also to extend their services to rural areas which are hard to reach. Use case lies in taking the functions from proprietary hardware in mobile core and putting them on COTS servers in a cloud environment. Mobile operators are mainly looking for the following services to have virtualized: IMS, EPC, MME, S-GW, P-GW, HSS and PCRF.

Virtualized Edge

Service providers are also trying to find an easy solution how to simplify their edge, which incorporates *Customer Premises Equipment* (**CPE**) and *Customer Edge* (**CE**), to sell more services to both consumer and business customers. NFV can be a possible solution to grow their revenues. For enabling the NFV in service provider's world, it is necessary to have virtualized edge components - vCPE and vCE.

5 Future of Internet

Today's times could be characterized as times of *Information and Communication Technologies* (**ICT**). Internet as we know it today is a clear success. However, some aspects of the current Internet fall short of both current expectations for a reliable communication infrastructure and future demands that we would like to be able to put on such a network.

By 2015 the global public Internet network will connect approximately 6 billion people, more than 4 billion people will use the network services via mobile devices and more than 2 billion people will use wired broadband connection to the Internet.

These assumptions can be found in the paper of Claus G. Gruber [19] as well as the assumption that network traffic will have the growth rate from 40% to 200% compared with today's network traffic in the coming years. It is therefore relevant to assess in what state are today's computer networks and other elements that are an integral part thereof. High internet penetration encourages and accelerated also use of mobile devices such as laptops, mobile phones, tablets. In the Fig. 9 we can see the forecast of devices connected to the global public internet [20].

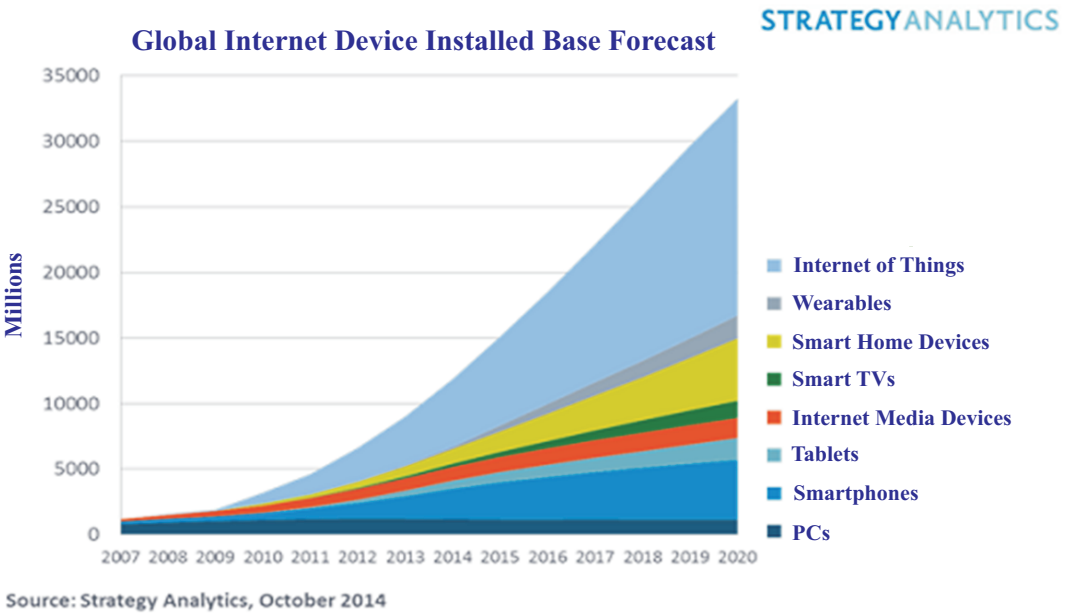


Fig. 9 - Global Internet device installed forecast

The requirements of mobile networks are often more demanding than the requirements of users in the wired network, in particular as regards the availability of any-time, anywhere [21]. Therefore, today's networks must be adaptive and agile providing not only high availability of services, but also their quality.

5.1 Limitations of Internet

Current Internet is mainly based on the IP protocol. It was created over 40 years ago by group of scientists for interconnection of their local networks. Mainly for file transferring, e-mail communication etc.

Today's Internet has considerably exceeded the original assumptions. From less than few hundreds interconnected computers to several hundred millions of them now. The Internet also didn't count with new applications like Web, video streaming, file sharing which significantly changed the nature of Internet traffic. The infrastructure of the Internet has been evolved by technological process to optical, wireless etc. [22].

In the Fig. 10 you can see the evolution of the Internet from the past, through the present. The IP is at the center of the layered model with applications on the top and technologies below.

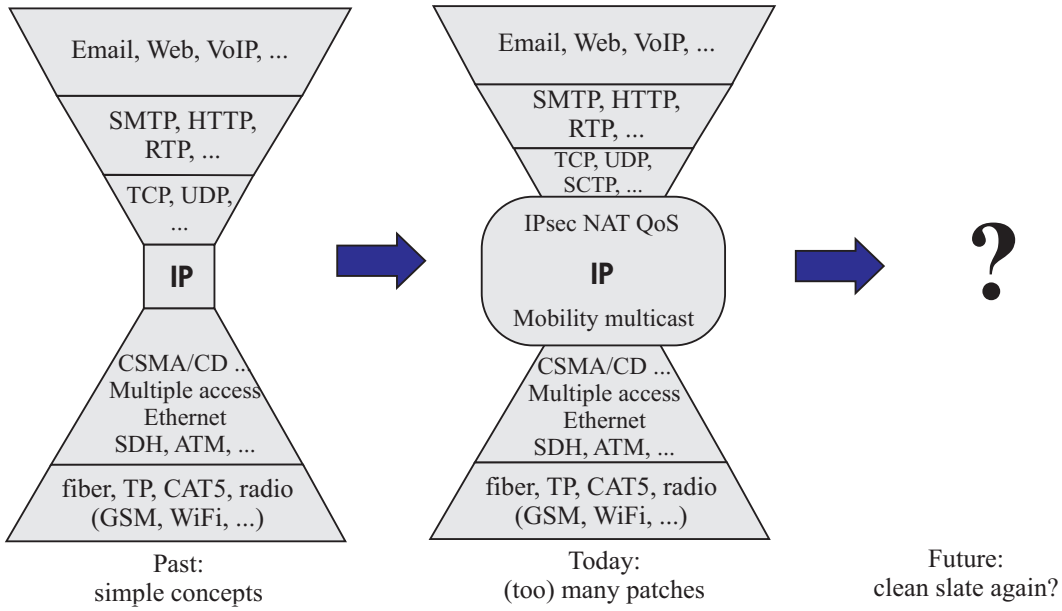


Fig. 10 - Evolution of the Internet [23]

At present, there is almost no possibility of a practical way to experiment with new network protocols, device settings, to the extent that this experiment can gain credibility for wide deployment in the networks of *Internet Service Providers* (**ISP**) and *Network Service Providers* (**NSP**).

The authors in [24] confirm that enormous amount already installed network devices using the same network infrastructure with the same network protocol, being used for decades, form a huge barrier to entry for innovative solutions, research and development in computer networks. The result of this pathway approach is also the fact that a number of new research community's ideas are untested, unproven. Attributes of today's computer networks is so-called "ossified".

It is important to note that just Internet project was being constructed for the purpose of research. Architects, that have built the infrastructure of the Internet, did not realize the possibility of the arrival of huge networks that currently we have. Security, mobility, flexibility, resilience of networks has never been solved, because in times of formalizing of the Internet, the computers were not mobile and researchers wanted to spread new ideas across the freely open environment. Vision of the perfect internet environment has begun to fade with increasing number of users in the network. The amount of basic concepts from the time of their formation has changed. With the rapid development of technologies in the field of informatics and information technologies, the public Internet can not meet and satisfy emerging demands. It is obvious that today's networks need a new proposal, which would be better adapted to new trends.

Operation of computer networks requires a number of resources related to the cost. The costs can be divided into investment costs and operational - operating costs which are called as capital expenses (CAPEX) and operating expenses (OPEX) [25]. CAPEX refers to investments that must be made in advance and written off after a certain period of time. An example would be the construction of the data centre (DC) or the purchase price of the server, network equipment and other critical network components. Operating expenses OPEX associated with recurrent monthly costs of actual equipment operation, such as energy costs, repairs, maintenance, salaries of administrative staff.

5.2 Characteristics of new Internet

Characteristics of new Internet are:

- Robust and available – Future networks should be robust, fault-tolerant and available.
- Security – One of the biggest issue of today's Internet is security, especially end-host security. That is the reason why the future network design must be built with security in mind from the start. The network should provide tools to quarantine fast-spreading infections, mitigate Denial of Service attacks, and provide better source authentication [22].
- Support mobile end-hosts – As we mentioned in text above the number of end-users of the Internet will rapidly increase and the number of mobile users will form major part of them. The future Internet is meant to facilitate mobility of users, terminals, and networks and even of applications, when a communication is moved from one device to another, for example [22].
- Economically viable and profitable – The future networks should be profitable for those who provide network services.
- Evolvable – the architecture of the future internet should pre-suppose that it will change and evolve over time.
- Predictable - The user should know what to expect from the network, and it should provide predictable and repeatable service.
- Support anonymity where prudent, and accountability where necessary.

5.3 Redesign of Internet Technologies

As already mentioned, a number of connected devices to the Internet tends to constant and unstoppable growth, year after year disproportionately multiplied.

To obtain a stable, safe, flexible and agile network, we can no longer remain in the standards of the sixties and seventies, while it is forced to move forward and open doors to new technologies. As the most challenging seems to be interconnection of programmable - software defined networks and virtualization of network services. Such newly created architecture promises not only a connection the indisputable advantages of both technologies, but also the emergence of new improvements.

The breakthrough idea is certainly architecture for the automated provisioning of network services in virtualized form. Software defined networks can create the perfect automated network environment that automatically configures the network in the enterprise as well as the customer's environment. Moreover, the applications on top of the SDN Controller will be able to dynamically generate and evaluate network quality and if necessary change the network path so that the parameters of the network are retained, but also to intervene in case of failure of a particular network line.

In the context of automation, we can also reflect on specific templates, or policies for specific virtualized services, but also pointed tailored policies for the specific client. Through software driven approach we are able to maintain the desired configuration across a number of network services which are even consistent - this will avoid inconsistency which may arise from human factor.

The biggest challenge is the centralization and transfer of own services, so called “travel with my network services”. That services are no longer in a physical form of large, heavy and hard to portable devices, each client is able to travel with their services, configured network worldwide without the need to transfer something physically.

Thanks to flexibility of these future networks it is much better to monitor and adjust product on offer - a service as well as offering new enhancements, which has not yet been possible for a dedicated purpose-built appliances.

All these ideas are worded tempting, but deployment of the architecture interconnecting SDN and NFV technologies require replacement of existing outdated infrastructure, which is not so simple. As the possible transition can be integration and testing architecture SDN and NFV in the existing environment and the subsequent replacement of outdated technologies.

Software defined networking is a new approach which should enable us to manage, change and control the network dynamically through well defined interfaces. The centralized control embeds all the intelligence and maintains a network-wide view

of the data path elements and links that connect them. This centralized up-to-date view makes the controller suitable to perform network management functions while allowing easy modifications to the networking functions through the centralized control plane. SDN makes it possible to manage the entire network through an intelligent orchestration and provisioning system that enables on-demand resource allocation.

Basic assumptions of the new network architecture [22]:

- Flow recognition – first point researchers in [22] believe to be important is the flow recognition.
- Network addressing – addressing should be more intuitive, referring to the services and people and not to the interfaces.
- Routing protocols – routing protocols should be more reliable and stable.
- Exploiting structure.
- Dynamic circuit switching.
- Backbone desing – backbones should be more predicable, failure resistant and stable.
- Models of the end-to-end principle.
- Cross-layer design – There is no doubt that layered model has lots of advantages but it has also lots of inefficiencies.
- Network virtualization – network infrastructure should evolve over time.

In this section, some basic ideas about Future Internet were presented.

Currently, there are many projects running concurrently and working to create a clean slate Internet concept. This research is still in its infancy so it is hard to talk about it and introduce the exact network architecture, trends etc. Many researchers are working on it and every research group talks about it from its point of view. But one thing is clear. Because the current Internet based on the IP is here over 40 years, we are already facing its limitations. Clean slate Internet concept will be very important and its deployment is only a matter of time.