White Paper based on the IEEE Workshop SDN4FNS (Trento 11th – 13th November, 2013)
29th January 2014
Editor and contact: antonio.manzalini@telecomitalia.it

Software-Defined Networks for Future Networks and Services

Main Technical Challenges and Business Implications

Antonio Manzalini, *Telecom Italia, Italy*
Roberto Saracco, EIT ICT Labs, Italy
Cagatay Buyukkoc, *AT&T Labs, USA*
Prosper Chemouil, *Orange, France*
Sławomir Kukliński, *Orange Polska, Poland*
Andreas Gladisch, *Deutsche Telekom, Germany*
Masaki Fukui, Wenyu Shen, *NTT, Japan*
Eliezer Dekel, *IBM, Israeal*
David Soldani, *Huawei, Germany*
Mehmet Ulema, *Manhattan College, USA*
Walter Cerroni, Franco Callegati, *University of Bologna, Italy*
Giovanni Schembra, Vincenzo Riccobene, *University of Catania, Italy*
Carmen Mas Machuca, *Technische Universität München, Germany*
Alex Galis, *University College London, U.K.*
Julius Mueller, *FhG FOKUS, Germany*

***Abstract* — In 2013, the IEEE Future Directions Committee (FDC) formed an SDN work group to explore the amount of interest in forming an IEEE Software-Defined Network (SDN) Community. To this end, a Workshop on "SDN for Future Networks and Services" (SDN4FNS'13) was organized in Trento, Italy (Nov. 11th-13th 2013). Following the results of the workshop, in this paper, we have further analyzed scenarios, prior-art, state of standardization, and further discussed the main technical challenges and socio-economic aspects of SDN and virtualization in future networks and services. A number of research and development directions have been identified in this white paper, along with a comprehensive analysis of the technical feasibility and business availability of those fundamental technologies. A radical industry transition towards the "economy of information through softwarization" is expected in the near future.**

Keywords—Software-Defined Networks, SDN, Network Functions Virtualization, NFV, Virtualization, Edge, Programmability, Cloud Computing.

I. INTRODUCTION

The ossification of Internet and Telecom networks is creating several difficulties for Service Providers (SP) and Network Operators (NO) to develop and deploy, flexibly, any innovative network functionalities, services and management policies, which are essential to benefit from the increasing dynamicity of the ICT markets. Launching new services, for example, is still time-consuming and requires expensive efforts: this is preventing any rapid roll-out of new businesses models and opportunities. A first requirement is thus making the innovation cycles of networks and services features faster and simpler. Moreover there is a need, for both SP and NO of reducing OPerational EXpenditures (OPEX) and CAPital EXpenditures (CAPEX): concerning the OPEX, for instance, automated operation processes (e.g. configuration of networks and services systems and equipment) could limit human intervention, reducing also wrong operations; on the other hand, concerning the CAPEX, a flexible and optimal provisioning of network functions and services could reduce systems and equipment costs and allows postponing investments.

Emerging paradigms such as Software-Defined Networks (SDN) [1] and virtualization, for instance Network Functions Virtualization (NFV) [2], if properly designed and deployed, could help in fulfilling the above mentioned requirements: as a matter of fact, a deeper integration of networks and IT (e.g. Cloud) domains, and the related Operations (now mainly carried out separately), could allow huge savings, and the acquisition of greater flexibility in services provisioning.

In particular, according to a widely accepted definition, SDN concerns the decoupling of the software-based control plane from the hardware-based data plane (e.g., packets forwarding) of networking and switching pieces of equipment; in principle, this would allow moving control logic (and states) to logically centralized controllers. NFV is one of the most innovative expressions of virtualization, and specifically it implies the virtualization of network functions and services that could run on general purpose hardware; this would allow dynamically placing and moving said functions in various locations of the networks and services infrastructures.

Importantly, it should be noted that different developments and deployment scenarios of SDN and NFV could be envisioned, depending on network segments (e.g., core or edge) and, consequently, on time horizon (e.g., medium-long term or short term). These deployment scenarios, in turn, could

require different amounts of investments (e.g., less investments in the edge), expected revenues and impacts on the Operations of NO and SP. Nevertheless, we are witnessing an overall trend of networks and services "softwarization" which is unstoppable as it is mainly due and driven by the continuous IT technology evolution and cost reductions.

In 2013, the IEEE Future Directions Committee (FDC) formed an SDN work group to investigate and determine the amount of interest in assembling an IEEE SDN community. In order to achieve this goal, a Workshop on Software-Defined Networks for Future Networks and Services (SDN4FNS'13) was held in Trento, Italy, on Nov 11-13th 2013 **Error! Reference source not found.**. Around 70 international experts from industry (e.g., NO, SP, Technology Providers, etc), SMEs and academia gathered together to present visions, pieces of results and to discuss and draw the key challenges about the potential adoption of SDN and virtualization. Three keynote speeches, thirty presentations and three panel discussions provided a comprehensive overview of current and future research and development work, socio-economic aspects and impacts.

In this white paper, leveraging the results of the workshop, the authors have further analyzed scenarios, prior-art, state of standardization, and reviewed the main technical challenges and socio-economic aspects of SDN and virtualization in future networks and services.

The rest of the paper is organized as follows. Section II reports some of the widely adopted terms and definitions of SDN and NFV, in order to align with the nomenclature; Section III summarizes the main outcomes of the IEEE Workshop SDN4FNS. Section IV describes some thought-provoking scenarios and use-cases. Section V provides an analysis of some of the more debated conceptual and functional models for SDN and related challenges. A brief status report on the main standardization activities is presented in Section VI. Conclusions and next steps are drawn in Section VII.

II. TERMS AND DEFINITIONS

According to the Open Networking Foundation (ONF)[1] **Error! Reference source not found.** a SDN is a network where the control (software-based) and data forwarding planes (hardware-based) are decoupled, so that, in principle, the network infrastructure could be abstracted from functions and business applications **Error! Reference source not found.**. The proposed concept and architecture for SDN is illustrated in Figure 1.

In a SDN, for example, the decisions concerning flows switching and engineering are taken by a so-called SDN controller which interacts with SDN switches via the OpenFlow protocol (as defined by ONF). The protocol procedures are mostly related to data flows, queues and ports, while applications and functions, running on top of the controller, (not defined by ONF) may be developed by other implementers.

Nevertheless, above SDN definition is still evolving in order to enrich said networks with functionality, for example, to provide support for mobility, to add control and programming capabilities of other abstractions and even of physical or virtual resources.

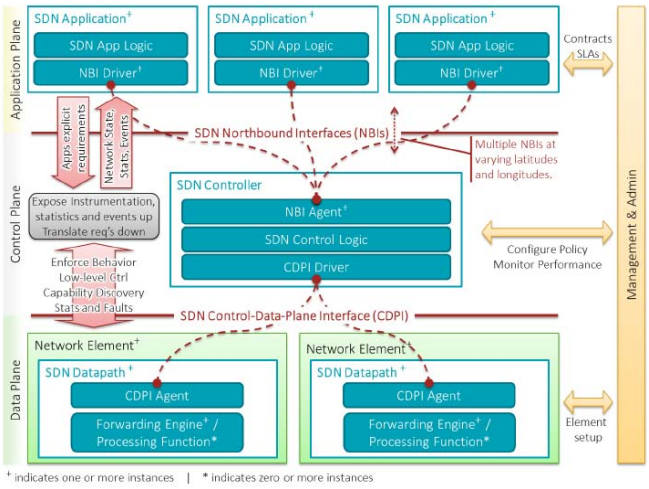

Figure 1 – SDN architectural model (Source: [4])

This evolution aims to cope with some specific problems and requirements such as scalability, performance, management, robustness or ability to adapt to multi-operator environment in which multiple SDN controllers or SDN domains have to co-exist. As high level functional definition may determine the elaboration of different systems and software architectures (with the related implementation for different networks' areas) there are, currently, several viewpoints in considering and assessing future deployments of SDN.

It has also to be noted that in the past other attempt have been made to decouple software from hardware and to achieve network programmability: an overview of such a concept was presented in **Error! Reference source not found. Error! Reference source not found.**. At present, several latest attempts, such as PCE **Error! Reference source not found.**, ForCES **Error! Reference source not found.**, or i2rs **Error! Reference source not found.** are also denoted as in line with SDN principles and an effort to consolidate them under the SDN umbrella can be perceived. Such integration would be justified by some similarities of these concepts, especially the programmability of some operations and the separation of control and data planes. However some concerns related to the overall complexity and cost of such integrated solution could arise. Moreover between these concepts some substantial differences also exist, as "distributed i2rs driven by real-time management" versus "centralized SDN with fundamental role of control plane", which make the integration of those troublesome.

It should be noted that SDN should not be confused with NFV, which is about the virtualization of some network

functions that could be executed on standard of the shelf hardware.

In principle, this approach could allow introducing in network operations, those features which are today normally carried out in Data Centers (DC), such as dynamic allocation, migration and cloning of virtual resources and functions (e.g. for server consolidation, load balancing, etc.).

In the IT context, virtualization is already well known and widely deployed in Data Centers for enabling the execution of multiple isolated instances of a software entity on top of a single physical server. IT Virtualization has several advantages, for example it increases resource utilization and improves state encapsulation.

These principles have not been fully extended to networks. Network virtualization already exists in virtual private networks (VPNs) which generally use the multi-protocol label switching (MPLS) technology, operating on the link level layer. Another form of virtualization is to segment the physical local area networks into virtual local area networks (VLANs). An overlay network is yet another form of network virtualization which is typically implemented in the application layer, though various implementations at lower layers of the network stack are also being used. Extension of IT virtualization principles to network equipment (such as routers and switches) could determine several advantages as well, i.e. optimizing the use of physical resources and allowing a deeper integration of IT and network resources.

NFV could bring the ability to co-locate multiple instances of network functions on the same hardware – each running in one (or more) different Virtual Machine (VM). This could provide NO and SP with the ability to dynamically instantiate, activate, and re-allocate resources and functions, and even program those according to needs and policies. SDN and NFV could be seen as mutually beneficial, but they are not dependent on each other: e.g., network functions can be virtualized and deployed without an SDN being required and vice-versa. An example of functional architecture from ETSI is depicted in Figure 2.

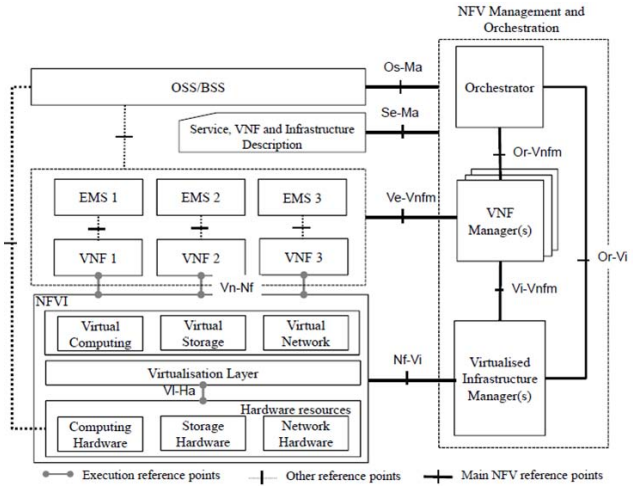

Figure 2 – Example of functional model for NFV (Source: ETSI).

III. SUMMARY OF THE SDN4FNS'13 WORKSHOP

This section intends to provide a brief overview of the most important topics covered by papers and discussions during the IEEE Workshop SDN4FNS. The Workshop was organized in three tracks: 1) Telecom and Internet SDN Scenarios, 2) Hardware and Software 3) Regulatory, Biz, Techno-Economic Sustainability. The main takeaways are briefly summarized in the following sub-sections.

A. Track 1: Telecom and Internet SDN Scenarios

There an emerging understanding that the disruptive potential of SDN and virtualization could provide a number of new opportunities to NOs, SPs, software developers and equipment vendors. However, all these new potential opportunities carry also a new set of challenges to cope with this transformation. State-of-the-art SDN and virtualization implementations have already shown many issues to be addressed, and a significant number of those are related to security aspects **Error! Reference source not found.**. In general, SDN could be seen as a paradigm helping in overcoming ossification of current layering and protocols stacks. For example, **Error! Reference source not found.** argued that, in the future, the TCP/IP layering itself may represent just one of the ways to deployment of a truly flexible software-defined networking environment.

Several interesting SDN applications scenarios have been presented and discussed, for both wired and wireless-radio and networks. For instance, SDN can be envisioned as a potential solution for efficient and scalable implementation of control functions in extremely dense and heterogeneous wireless networks **Error! Reference source not found.**. According to this vision, a novel network architecture, accounting for MAC control and Mobility Management, was proposed as part of the activities of the EU-funded FP7 CROWD project **Error! Reference source not found.**.

SDN and virtualization could also enable a flexible and more efficient implementation of the LTE Evolved Packet Core by splitting its main functions between a virtualized cloud environment and an SDN-based transport infrastructure **Error! Reference source not found.**. SDN could provide key functions such as load balancing over different wireless technologies and related flow admission control in heterogeneous 5G mobile networks **Error! Reference source not found.**.

Finally, the issues to enable switch mobility, while enforcing robustness against network attacks were addressed in **Error! Reference source not found.**, by introducing an enhanced transport layer, based on standard IP mobility techniques for OpenFlow controller-to-node communications.

One of the key challenges that could be faced with SDN is the optimization of (virtual) resource allocation and usage. Relevant case studies include: inter-data center communication for service brokerage over large scale

distributed and heterogeneous cloud environments **Error! Reference source not found.**; performance evaluation of virtual network functions migration across cloud-based edge networks **Error! Reference source not found.**; dynamic traffic engineering and adaptive network design to efficiently map logical/virtual topologies on physical network infrastructures **Error! Reference source not found.**, **Error! Reference source not found.**.

B. Track 2: Hardware and Software

Hardware performance advances and costs reductions are creating the mass market favorable conditions to a large adoption of the software-defined principles and virtualization.

Nevertheless this will create an high level of complexity in future networks and services platforms. As such, SDN and NFV will require to enhance current management systems with new capabilities, for example concerning the orchestration of virtualized functions and resources.

Moreover, in order to tame the growing complexity and the dynamism proper levels of software abstractions should be timely introduced, simplifying also the views of the architecture (e.g. slicing). Elasticity and flexibility could be achieved through systems and methods for VMs placement, move and traffic routing between VMs (i.e., solving double constrained optimization problems in almost real time).

In general, there are several efforts in this avenue, which appears to be very strategic.

Inter-domain SDN controller integration could be enforced by means of compatible east-west bound interfaces, based on either service-oriented architectures **Error! Reference source not found.** or inter-platform signaling for distributed flow processing **Error! Reference source not found.**.

Most of the ongoing discussions about SDN typically focus on control plane aspects. However, many unresolved issues arise when considering the programmability of the data plane, such as the relative importance of data plane vs. control plane services, the relevance of the underlying hardware platform, and the need for standardized northbound and southbound interfaces in the data plane **Error! Reference source not found.**.

Another very important aspect of SDN concerns service provisioning with guaranteed QoS: leveraging network programmability features provided by SDN, specific platforms addressing the QoS monitoring and enforcement issues were developed with managed [23] or autonomic **Error! Reference source not found.** approaches.

Then, considering the increasing deployment of OpenFlow-enabled equipment, a smart platform capable of detecting OpenFlow rules interactions and determining possible inconsistencies could be extremely useful as a sort of "debugger" for OpenFlow application development **Error! Reference source not found.**.

SDN can be considered as a powerful enabler for many emerging networking paradigms. It is indeed vital to deploy inter-cloud communication services over existing network infrastructures in a scalable and feasible way, as proposed within the European Future Internet initiative **Error! Reference source not found.**. It is also the key technology that can foster the implementation of multipath inter-data center communication architectures, building on emerging standard protocols **Error! Reference source not found.**. Finally, SDN may ease the deployment of Information-Centric Networking (ICN) in existing IP networks by effectively decoupling forwarding information from object names **Error! Reference source not found.**.

As mentioned, virtualization is one of the most important technologies intertwined the growing interest in SDN: the capability of virtualizing practically any network function and service and SDN principles are mutually beneficial. This is also the rationale behind the so-called "hyperconnected telecommunications environment", where most of the intelligence is moved to the network edges, eventually evolving into a fully interconnected Internet of Everything **Error! Reference source not found.**. It is of course intended that virtualizing networks at any scale would require some level of orchestration: technical challenges and potential architectural approaches to edge-to-edge virtualization, abstraction, control, and optimization of heterogeneous transport networks with packet- and circuit-switched technologies were discussed in **Error! Reference source not found.**.

Test-beds and proof-of-concepts of virtualized network functions can provide an insight into the major feasibility issues of network virtualization and a viability check of NFV performance. Good examples include: EmPOWER experimental test-bed for wireless network virtualization **Error! Reference source not found.**; an OpenFlow-based prototype of routing function virtualization **Error! Reference source not found.**; CONTENT project approach **Error! Reference source not found.** to infrastructure virtualization over heterogeneous wireless and optical networks. Last, but not least, the internal structure of a network node capable of function virtualization, which is also a critical aspect of SDN, may be implemented through a plug-in interface architecture as presented in **Error! Reference source not found.**.

C. Track 3: Regulatory, Biz, Techno-Economic Sustainability

Although SDN is still considered to be in its infancy, medium to long-term visions on how it will possibly evolve in the future can set the grounds for strategic research and investigations on the techno-economic sustainability.

Dynamic Network Service Chaining is, for example, one key research topic showing several challenges, considering the many aspects to be dealt with during the typical lifecycle of a network service **Error! Reference source not found.**. This is in alignment with the concept of "Forwarding Graph", which is used sometimes in preference to "Service Chain", in order to account for the fact that end-to-end forwarding within virtualized overlay service networks is not exclusively a one

dimensional chain: instead they may, and often will, have branches.

Form the techno-economic perspective, a wider and wider introduction of "software" in networks and services infrastructures [37] will accelerate the pace of innovation (as it is doing continuously in the IT domain) and will reduce operational costs (e.g., through optimizations exploiting big data and automation). This trend will move "competition" from hardware to software, lowering the threshold for several Players to enter into the ICT – Telco arena. It is likely that the so-called "softwarization" will to enter more and more in all socio-economic processes.

Finally, the vision of a future network where most of the intelligence resides at the network edge was brought one step further. This is especially true, considering the vision that SDN and NFV solutions will be able to create a sort of distributed communication "fabric" around the users, covering all network equipment available at the edge (including any type of hyper connected devices, such us smartphones, robots, cars, drones, etc.), which can offer huge processing and storage capabilities to execute and consume practically any virtualized function and service **Error! Reference source not found.**.

D. Main Takeaways

Socio-economic drivers and technology progresses (with their down-spiraling costs) are steering the evolution of current networks towards a highly dynamic and flexible environment of virtual resources, interconnected by virtual links that are set up and torn down to serve multiple applications.

SDN and NFV are likely to represent a first step to this direction. In general, in the future, a growing number of industries and small medium enterprises will rely more and more on "digitalization" and "software". In this sense SDN and NFV could be seen as powerful enablers to create and develop new ecosystems capable of aggregating and driving investments, even outside the traditional Telco-ICT contexts. This requires embracing this crucial industrial transformation from a broader perspective.

This transformation is an unstoppable trend, because of the continuous technology evolution and cost reductions by lowering operating costs though simplified hardware, software, and management will definitely enable new economic paradigms. For example, SDN and NFV are claiming network cost reductions, due to the adoption (and consolidation) of standard hardware, capable of running virtualized network functions/applications. Nevertheless, we found wide consensus on the fact that this model will be successful only if SDN and NFV are really based on open source software solutions. (Closed software solutions, in fact, would move costs from hardware CAPEX to software OPEX, probably erasing the claimed advantages of SDN and NFV in terms of cost saving.)

The analysis is obviously more complex as it should take into account to which level the performance should be managed as well, and how all these virtual network functions should be efficiently orchestrated. Moreover, it was argued by several people that this r-evolution would happen at the edge, first, as it would require fewer investments, it would scale much more gracefully, and it would lead to immediate revenues. Evolution in Users' devices, terminals, Customer Premises Equipment (CPE) or aggregation edge nodes is much faster than in core or WAN equipment, especially due to the impact of SDN and NFV on traditional Operations Support Systems (OSS)/Business Support Systems (BSS).

Next sections will provide further analysis of scenarios, prior-art, state of standardization, and further discussions on technical challenges and socio-economic aspects.

IV. SCENARIOS AND HIGH LEVEL REQUIREMENTS

In this section, some scenarios (wired and radio, core and access/distributions, edge) are provided from the points of view of NOs and SPs, as well as from other players' angle, such as OTTs, Enterprise Networks Providers, Consumer Electronics Providers, etc.

A. Examples of core scenarios

Core networks scenarios typically consider SDN as a paradigm providing incremental improvements (in terms of flexibility, programmability, etc.) of current networking concepts; practically, it is recognized that the concept of the separation of hardware from (control) software is not really new, but the point is that the decoupling is made possible today thanks to the hardware technology advances.

In the context of these core scenarios, Dynamic Network Service Chaining is one of the most mentioned classes of use cases, where IT and networks resources are integrated: network services are provided by "chaining" the executions of several service components.

SDN is often assessed as an opportunity reducing CAPEX and OPEX costs. As previously mentioned, savings may derive from centralizing and, above all, automating processes and postponing investments through optimized usage of resources (provided that carriers' class performances are still achieved by the adoption of general purpose hardware).

On the other hand a deeper integration of networks and IT (e.g. Cloud) domains, and the related Operations requires also a deep "change of culture" in NOs and SPs, and maybe the development of new skills for mastering "software". This might require some time, also to define new models of business sustainability.

Seamless integration with legacy equipment and the related management systems might represent other critical issue, mainly demanded to the standardization of interfaces, which might be delayed. In summary, it remains to be seen whether SDN exploitation in core scenarios will be really followed, and what the time horizon will be.

B. *Examples of edge scenarios*

Edge scenarios concerns the exploitation of SDN principles for creating very dynamic virtual networks out of a variety of aggregation nodes, devices, elements located at the edge of current networks, up to around Users. Some of these elements usually are not considered yet as network nodes: for example, cars, robots, drones, any Users' devices, smart things with embedded communications, etc. In other words, this is about developing a "fabric" made of an enormous number of nodes and elements aggregated in an application driven way, as depicted in Figure 3.

In the past, the term "fabric" has been used to refer to a distributed computing system consisting of loosely-coupled storage, networking and processing capabilities interconnected by high-bandwidth links. It has also been used for describing flat, simple intra data center networks optimized for horizontal traffic flows, mainly based on a concept of "server-to-server connectivity". Based on these previous meanings, in this context, the term fabrics is extended to indicate the edges of the metro networks, becoming like as distributed Data Centers consisting of loosely coupled processing and storage resources interconnected by pervasive high speed wired and wireless links.

An example of use case is that of a SP that may want to provide end-to-end ICT services to users who are attached to edge networks, even if belonging to different infrastructure providers or NOs. This could be achieved by operating an overlay service platform capable of chaining, managing and orchestrating virtualized resources and functions made available by the different edge networks.

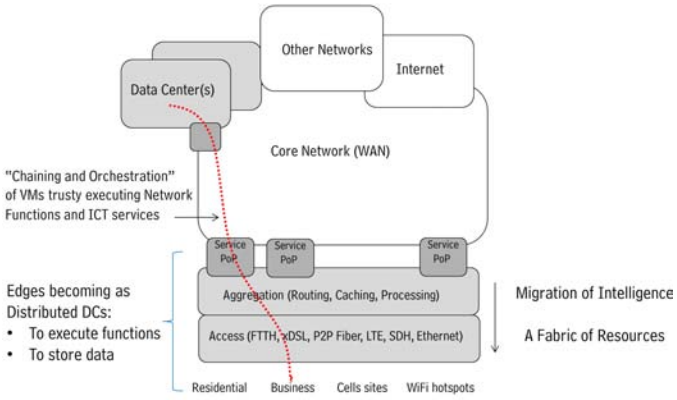

Figure 3 – Example of scenario where the "edge" is becoming a "fabric" of resources to execute networks functions and store data.

Another use case is that where Data and ICT services (seen as apps executed via chains of VMs) will follow the users when they are moving from one network attachment point to another one, even across different edge networks.

Management and orchestration capabilities should allow this "follow-me" service whereby personal data and ICT services will be moved seamlessly with little or no impact on the Quality of Experience (QoE) of users. Moreover, data and services associated to users can be even federated to build distributed virtual data center at the edge (ideal for example for universities, enterprises, etc) at costs which are a small and a fraction of traditional clouds.

C. *Other Expectations and Requirements*

In general, NOs and SPs expectations related to the SDN/NFV frameworks are much broader than the currently addressed Telco's requirements. One far-reaching circumstance is that the carriers have made huge deployment investments in legacy networks. Hence, many of the novel SDN capabilities need to enable the transformation of the current nodes to the new infrastructure vision the research community is creating.

This is a fundamental requirement: developing a radical simplification on how carrier networks are designed, built, deployed, operated and managed. End users should have the desired QoE, new services should be easily introduced, and resources should be optimally used for meeting all performance requirements of the new complex applications. The networks will transform into a new "market" where all actors' (users, applications, networks) requirements are appropriately addressed with the new supported and deployed capabilities.

This transformation is a big task, and the existing paradigm is not quite ready in achieving this objective, but the capabilities at hand should allow the research community to work in this research direction.

In the IEEE SDN4FNS Workshop, several contributions were given towards this goal. Yet, some other key areas would need to be addressed in the upcoming period by the research community, including, but not limited to:

(a) Development of an end-to-end SDN framework for Collaboration (Coordination, Cooperation, Communication Orchestration) taking into account the current and new actors (prosumers/functions/applications), in order to agree and achieve global goals (i.e., utility maximization, resource optimization QoE, Policy, Security…).There is an ongoing work with this broad aim, but new capabilities are definitely needed. As an example, Identity, Security, Mobility and QoS Management are key high level objectives; providing these in a modular way, across the network/s and all layers need corresponding abstractions from all, as well as new concepts and architectures of Access and Non Access Strata. In the security context, perimeter defenses do not usually work, instead of firewalls at the perimeter, using internal modular firewalls to define enclaves within the network, and using secure protocols [e.g., Secure Sockets Layer (SSL) or Transport Layer Security (TLS)] and service validation at their inputs to prevent attacks might be a better approach. Similarly, E2E QoS and mobility objectives should be apportioned and relegated to the corresponding domains and layers to provide the necessary carrier grade performance.

(b) Development of an SDN/NFV framework for Service Providers. The existing paradigm would need to be extended beyond data centers and enterprise networks. This would require longer geographic reach and diversity. All different access, core, and link technologies (e.g., RAN, cellular, Wi-Fi, optical, etc.) should be brought into the framework as well, to create an end-to-end infrastructure, where these domains could be offered as a Service. It also requires fundamental rethinking on how the current network may evolve (typically, delivery of new network-based services takes weeks and in some cases months) and how new services may be provisioned using a much more dynamic business process, characterized by the configuration and management of all virtual resources to provide even network services, as previously introduced. Dynamic network provisioning and configuration needs to be coordinated and orchestrated, in order to efficiently direct the assignment, creation and configuration of virtual resources, and, especially, to satisfy customer requests and manage customer experience per SLA. Network Orchestration will play a key role in implementing these requirements at various levels and will be responsible for coordinating the delivery of the resources and attributes of a customer request into an operational service that embodies the runtime requirements of that request. Network Services Orchestration is expected to provide highly reliable and scalable capabilities to enable these expectations. SDN would require a new set of capabilities that would work with the existing networks. Legacy networks should gracefully evolve to the future network through an evolution. Key control and management functions should interoperate with existing frameworks. This is a key requirement for SP that cannot afford a clean slate approach.

Looking at Flexible Service Control, the virtualization technologies for telecommunication infrastructures enable more opportunities in terms of flexibility, scalability and efficiency for on demand driven dynamic network dimensioning and traffic engineering. For instance, the flexible control of radio (Cloud-RAN/evolved-NodeBs) and core network (Evolved Packet Core, IP Multimedia Subsystem, Service Delivery Platform) resources enables novel lifecycle management and control possibilities.

The main advantages for virtualization, with respect to today's telecommunications architectures are:

(a) Data path optimization for signaling and user data plane. The influence of SDN and NFV on the control and data plane within Telco architectures allows a precise and particular optimization in overloaded parts of the network. Energy consumption and carbon footprint are playing an important role in the ICT in general and telecommunication in particular, since clouds, data center, network elements and base stations are responsible for a large amount of the total energy consumption. Therefore, the influence of virtualization on Telco networks, as a method for enabling optimized network design and traffic engineering instead of over-provisioning the Telco network, arise. High performance, flexible, elastic and demand-driven solutions are addressed in European research projects (MCN **Error! Reference source not found.**, iJOIN [64]**Error! Reference source not found.**, etc).

(b) Network aware service enablement / QoS on demand. Flexible QoS control is one of the key denominators in emerging future telco environments. Features such as user demanded QoS, QoS level per subscriber base, and differentiation between multiple Mobile Virtual Network Operator (MVNO) on top a physical network infrastructure all require flexible QoS control to ensure connectivity for dedicated service types. These service types might be emergency calls, public safety services or critical infrastructures such as smart metering.

V. Conceptual and Technical Challenges

This Section describes a list of the most important technical challenges for the development and deployment of SDN.

A. Management and Orchestration

The fundamental feature of SDN is the decoupling of the network control plane from the network forwarding (data) plane. Such separation is well-known in telecommunication networks. However, network architectures always include an additional plane, namely the management plane. Such plane and their functions are defined and standardized by the TeleManagement Forum and ITU-T. The functions include fault management, configuration management, accounting management, performance management and security management.

The role of management (including fault, configuration, accounting, performance and security areas) is especially critical in large, production networks. Typically, in such networks, the operators interact with the network via the management system. After network deployment, the most typical network operator's actions are usually related to network reconfiguration, as a result of network enlargement or topology changes. It is commonly agreed that in order to cope with future demands and the ever-growing number of managed devices, the network management should be automated.

Hence the network availability is expected to be improved and OPEX related to the network management significantly reduced. This type of management lies on performing selected management operations in "real-time", which is often referred to as autonomic.

The management of SDN can reuse some well-known network management concepts and it should incorporate the latest trends in network and service management as well. So far it is not the case. In facts, the management issues of SDN have been as of today ignored. This situation can be explained by the experimental status of deployed networks.

In the current SDN approaches, the usage of existing IP network management systems combined with OpenFlow is often assumed. The analysis of the OpenFlow protocol leads to the conclusion that it lacks primitives that are able to cope with network management operations. In order to support

management functions, ONF has defined the OF-Config protocol. This protocol is used for configuration of links between the OpenFlow switches and the controller. In the short term, the SDN management operations could be supported by the existing network management protocols (SNMP [63], NETCONF [62]).

The openness of OpenFlow enables the implementation of some network management functions, but the lack of standardization of a management interface makes impossible to use third-party management solutions in a way as they are used in legacy management systems.

SDN-based networks have some specific properties. Their owner or operator has not only the ability to manage them but also the possibility of defining their functionality.

There are several management issues that appear to be specific to SDN only. Most of them are related to the critical role of the controller, which has to perform most of its operations in a real-time manner. It means that the performance of the controller has to be monitored, and the controller processes should be categorized and handled according to their real-time requirements. In case of controller failure, a hot swap operation is necessary. Controller programmability requires special care. In order to fully use such capability, the network operator should be able to remotely add new controller functions and to update the existing ones. Such functionality means on-the-fly re-programmability of the controller. The management operations should be able to start, stop and monitor each software module. Moreover abnormal behavior of such modules has to be monitored and cure taken. Last but not least, the security of the controller platforms is critical and has to be handled accordingly. This includes also the authentication of newly added switches. It has to be combined with the security of the management platform.

It is important to determine a border line between the SDN network operations (implemented in the controller) and SDN-based applications implemented in application servers. Such a separation can help in the definition of the management system role. In order to cope with scalability and complexity, separate platforms for the control and the management of SDN networks are highly recommended. A proper information exchange between these platforms is necessary, and it could be provided by programmable interfaces.

It is an open issue whether the management will be fully centralized, or implemented by distributed functionalities. There is however no doubt that the added complexity should not significantly increase the cost of the SDN nodes and that the distribution of functionalities should still give a centralized view of the network.

1) Adaptive and Autonomic Methods and Systems

This research challenge deals with the critical nature of developing the methods, enablers and systems for autonomic management functions applied not only to the physical resources, but also virtual resources located inside the physical / virtual network.

In this avenue, even if the requirement of unification of all autonomic functions might be highly desirable, it will be almost impossible to achieve it, as the number of functions is expected to be large. New approaches probably should be developed, allowing separated autonomic managers to coordinate and resolve conflicts in their activities autonomously with minimal disruption.

One example is that where management and control functions would be distributed and located or hosted in or close to the managed network and service elements, enabling control of CAPEX and significant operational costs reduction for physical (i.e. OPEX) and virtual (i.e. VPEX) systems. These may include adaptive re-allocation of virtual resources according to changing network conditions or service demands. Additionally, this challenge deals with the critical nature of developing autonomous actions that provide network stability and optimizations in absence of higher-level control.

2) Optimised allocation and orchestration of resources

It has been mentioned several times that one major challenge will be the capability of dynamically instantiating, orchestrating and migrating multiple VMs across the networks and services infrastructures. Orchestration, in this context, means also lifecycle management of physical and virtual resources.

Specific optimization techniques are required for both the placement of the VMs into the physical networks and the traffic routing between VMs (e.g., this means solving double constrained optimization problem in “almost” real time).

In the case of wireless infrastructures, other characteristics and capabilities have to be considered, e.g. limited bandwidth, processing capabilities, storage, energy (battery), type of interfaces supported of the mobile nodes and mobility, conflicting requirements. As the mapping of virtual to physical resources should be transparent to higher control layers, mechanisms have to be developed that allow the seamless hand-off between different wireless devices. Additionally, algorithms will be identified that optimize the coverage of wireless radio connections to provide access to enough physical resources while avoiding unnecessary energy consumption.

In the case of wireline networks, optimized allocation will involve a wide variety of resources available from the underlying wireline network, including communication, execution and storage capabilities. The mapping will take into account the top-level service/operational requirements such as the demanded QoS requirement and resilience capability to be embedded into the resulting virtual network. By addressing this challenge virtual networks will be customized with optimally allocated capabilities such as virtual nodes (with computing and storage capabilities), virtual links and paths for specific networked services.

As an example, the Cross Layer Optimization paradigm as outlined in [65] maps top-level service/operational QoS requirements against underlying network capabilities and thus enhances network management and traffic engineering

sustainable. Individual characteristics of user profiles, service descriptions and network topologies have to be optimized given a connectivity with certain requirement on the transport system in order to guarantee QoS. Algorithms and concepts for realizing a network-awareness for services through Cross Layer Optimization are required in the scope of SDN and NFV for dynamic service chaining and optimal network function placement.

3) Energy Management

Finally, looking at the management aspects of energy consumption, we may relate this challenge to the critical nature of developing mechanisms for energy-aware networking, including the optimization of energy consumption within the limits of a single domain and/or multiple domains. Such energy-aware capabilities would include the optimal dynamic distribution of VMs across the set of networks and servers and providing stabilization of the local networks in response to variable electricity demand-response requirements.

4) Security and Safety

Security in terms of privacy, integrity has to be guaranteed in a virtual environment **Error! Reference source not found.** in at least a similar or a higher level than in today's networks to foster the acceptance. Even more security challenges arise in a virtualized environment due to shared hardware, processor, memory, system bus and control interface. Virtualization enables new charging models, which require precise monitoring, policy control and charging from the virtualized system. Existing Operation and Management system need to be adapted or renewed for facing the challenges of virtualized environments. The safety of SDN systems requires redundancy and reliability of the controller, the real and virtual resources and other ad-hoc engineering solutions **Error! Reference source not found.**. The flow paradigm offers interesting opportunities for security processing: one example is traffic steering for automated malware quarantine. Another area to be explored is how SDN could also bring to network security the ability for security policies to follow logically specific network applications or VM.

B. Interoperability and federation

SDN solutions count already on numerous Open Source and commercial OF software and hardware switches and controller. Already the large heterogeneity of OF Switches, OF Controller and OF versions challenges interoperability. Evolution of OF protocol and the use of other protocols than OF will require to make sure that interoperability is guaranteed.

In general interoperability between the different NOs and different domains with the same NO is extremely important. This challenge would include:

- interfaces that will allow a servicing /networking virtual function to federate. Using this interface, the networking function should be able to cooperate in order to provide inter-domain communication;
- authentication for other NOs, and the different NOs to confirm with each other the identity of the different users of a particular service;
- mechanisms for communication and programmability of service modules deployed by different operators for the same service;
- mechanisms for end-to-end service management, monitoring, and accounting.

C. Networked and Computing Services Operations

Service Operation deals with keeping the service infrastructures (and the services it provides) up and running smoothly. It includes, for example, monitoring the services execution environments to spot problems, provisioning of services, ensuring programmability, etc.

1) Performant and Safe Network Execution Environments

This challenge refers to the network hosting virtual environments and virtual machines to overcome the problem of having several execution environments implemented in various technologies, and providing different abstractions, interfaces, and so on. This challenge could be faced by developing a unified network execution virtual environment and by having groups of virtual machines which are managed (creation, change/update, deployment, migration, orchestration, deletion) as one. The advantage of having an explicit notion of a virtual environment is to provide generic means to manage access and resource control on the node-level. While execution environments support the installation, instantiation, and configuration of services code in various ways, the virtual environment puts a uniform management layer on top. This allows external clients to interact with services through the interface of the virtual environment in a generic way, and the interactions will be mapped to specific interfaces of the execution environments. Several execution environments can be attached to a virtual environment, just the same way as other resources. This leads to another aspect of virtual environments: the partitioning of resources. The network provider can set up virtual environments on selected network nodes, and assign them to a particular service provider, in order to offer a virtual network. Access to the virtual environments will be made available to the respective service provider so that it can manage its own virtual network. The resource partitioning implemented among virtual environments will prevent interference with other service providers and, additionally, allow an accounting per service provider.

2) Programmability in Future Networks and Services

This challenge refers to solutions for the fast, flexible, and dynamic deployment of new network services though programmable enablers and primitives for all planes of SDN environments (e.g. application, operation, management, control and forwarding planes). This is also aimed to provide easy introduction of new network services by realizing the dynamic programmability of the network and its devices such as routers, switches, and applications servers. Dynamic programming refers to *executable code* that is injected into the network

element in order to create the new functionality at run time. The basic idea is to enable third parties (operators, service providers and other authorized users) to inject application-specific services (in the form of code) into the network. Applications may utilize this network support in terms of optimized network resources and, as such, becoming network aware. Hence, network programming provides unprecedented flexibility in telecommunications. However, viable architectures for programmable networks must be carefully engineered to achieve suitable trade-offs between flexibility, performance, security, and manageability.

The exploitation of such flexibility for the benefit of both the operator and the end user would require guarantees against jeopardizing the integrity and stability of the network based on solutions for

- Rapid deployment of new services;
- Customization of existing service features; optimization of network resources;
- Scalability and cost reduction in network and service management;
- Independence of network equipment manufacturer;
- Information network and service integration;
- Guarantees for Quality of Service;
- Diversification of services and business opportunities in particular for virtual environments and clouds.

D. Architectural and Functional Models

The current developments in SDNs and NFVs are highlighting new and critical research topics related to what and how create the conditions to effectively and continuously update and change the networking functions (e.g., softwarization of future networks and services without reinventing every time the network architectures or network layering).

This means the use of software to program individual network devices, network systems and services dynamically and therefore control, manage and operate programmatically the behaviour of the network as a whole. Key software features of the future networks and services are already identified **Error! Reference source not found.**, [44] and include: service diversity, functional flexibility, programmability, ease of new services introduction, virtualisation of resources, energy consumption, service universalization, network management, mobility, optimisation, identification, reliability and security would need to be realised as part of the future network services and continuously updated.

The future networks and services need to move from being merely defined by software to be programmable by software and must be capable of supporting a multitude of providers of services that exploit an environment in which services are dynamically deployed and quickly adapted to heterogeneous physical wire, wireless and smart object infrastructure(s), according to evolving and sometimes conflicting customer requirements.

Programmability is a key property that SDN framework enables, but it does not make it "easier", as the proper abstractions and a set of layering have not been completely defined yet.

1) Architectural Models

Different abstractions, layering, conceptual models and architectural approaches have been proposed in the research literature. Some of them are discussed in the following.

Programmability of network elements (switches, routers, and so forth) was introduced about a decade ago, this set the basis for rapid deployment and customization of new services, as illustrated in Figure 4..

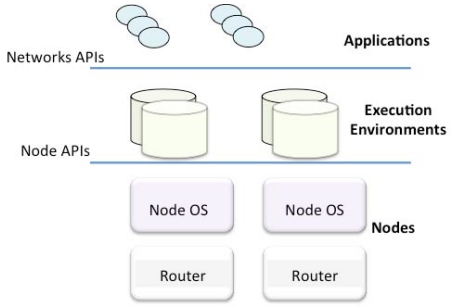

Figure 4 – Example of model of a programmable router network

Advances in programmable and virtual networks have been driven by the adoption of Open-Flow, which has led to refined high level architectural model, as in Figure 1.

We are now witnessing a growing interest moving from the centralized control and "monolithic" approaches, where systems are vertically integrated, towards a component-based approach, where systems are made of multiple components from different manufacturers, interacting with each other through open interfaces to form new services **Error! Reference source not found.**.

As depicted in Figure , the expected results would make it possible to achieve a level playing field, where different stakeholders, such as infrastructure and services providers, would compete with each other, while users may select and customize services according to their needs **Error! Reference source not found.**,**Error! Reference source not found.Error! Reference source not found.**.

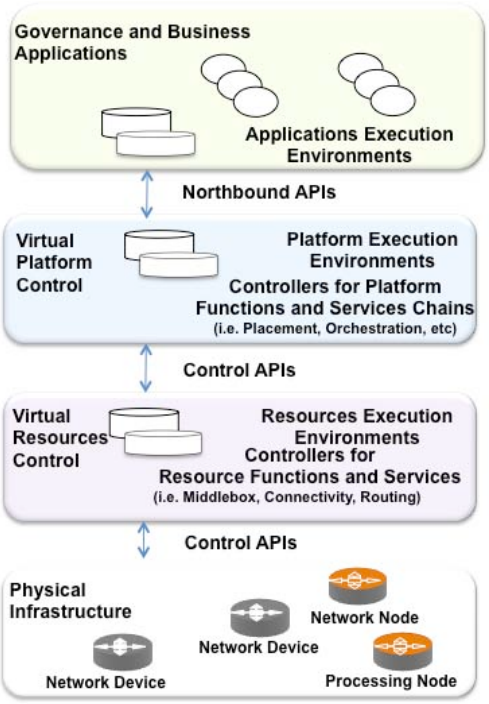

Figure 5 – Example of model of a unified environment integrating connectivity, computational power and storage

A fundamental characteristic of the architectural model of Figure 5 is the evolution towards a unified environment integrating connectivity, computational power and storage. This is requiring proper enhancement of current control and management planes and the introduction of orchestration capabilities.

Before that, there is a need of defining a meaningful functional model capable of abstracting and representing all network functions and capabilities which will appear in SDN and NFV (which means including processing and storage).

Realizations and instantiations (with proper adaptations) of the above model to Cloud **Error! Reference source not found.** and in RAN **Error! Reference source not found.** and cellular-wireline **Error! Reference source not found.** domains (figure 6).

One of the main problems with the earlier models is that the richness and diversity of applications and technologies prevents a simple model to be representative for all approaches (just a simple northbound API might not be enough).

A recursive approach is needed, where a new set of abstractions are developed, depending on the area or domain and the set of layers as necessary.

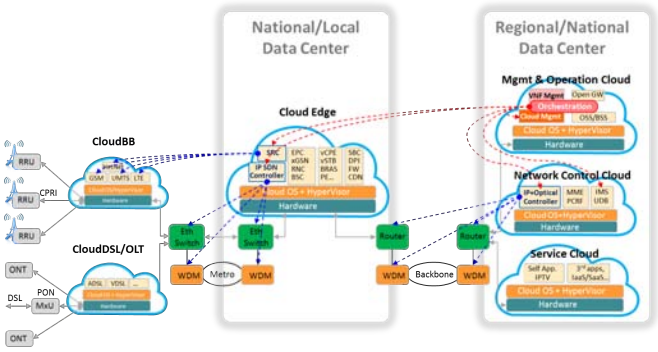

Figure 6 – Example of instantiations of SDN in Cloud, RAN and Cellular/Wireline domains (SDN4FNS Workshop)

In addition as a result of users shifting to mobile environments and devices, the need to create denser networks and more efficient usage of wireless resources are vital. (i.e., usage is rapidly growing on the demand side, on the resources side). Generalizing a set of abstractions to mobile networks and applying the SDN framework, would presumable bring additional benefits in management, converged resources control and agile deployment areas of increasingly dense networks.

In these scenarios, there is a need for efficient resource control and management across various wireless protocols, ability to tie and coordinate these capabilities with other core network functions, creating a common and programmable data plane, and creation of a wireless network operating system.

This will be only possible by rethinking the 3GPP architectures, starting from the definition of the logical network domains; session, mobility and identity management concepts and architectures, as well as Access and Non-Access Stratum protocols. For instance, it remains to be seen how mobility will be ultimately handled in SDN without tunnels, and whether the protocols implementing the bearer service (3GPP layer) will converge with the protocols in the transport network layer, which have been evolving separately.

In summary, as previously pointed out, SP's networks require a much more complex set of controls and layered abstractions, which can be iteratively realized. A lot of details are still in need of development but a key piece, a coordination/collaboration proxy, that needs to receive policy directives from "above", i.e., from nonfunctional requirements (i.e., business, technology and quality) and translates them into the domain of applicability is a key function that is missing to achieve a global goal.

An overarching architectural model should include shared virtualised resources, and all the corresponding abstractions, including those in wired, wireless and resource-constrained mobile devices and smart objects. Such an model would need to be engineered to facilitate the integration and delivery of a variety of ICT services, computing and network Clouds and to enhance integration of the key enabling technologies: programmability, networks, network virtualization and network function virtualisation and self-management.

2) Functional Modeling

Starting from the OSI Layering **Error! Reference source not found.** integration of the software infrastructures and traditional communication / telecommunication technologies has been always a challenge for network and service operators, as far as service deployment and management are concerned **Error! Reference source not found.Error! Reference source not found.**. This is due mainly the fact that OSI layers were designed to address IP packet delivery paradigm of early Internet days.

Interestingly, to overcome this problem, ITU-T developed a functional formalism capable of modelling transport networks in a technology independent way. ITU-T Recommendation G.805 describes the modeling of connection oriented (point to point) transport networks; then G.809 has been developed to model connectionless network and, eventually, G.800 reports a model for unified connection oriented/connection less architecture.

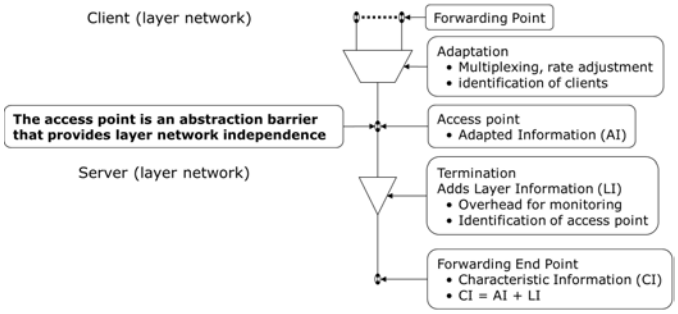

Figure 7 – G.805 components for functional modeling

The main characteristics of this functional modeling has been the capability of describing recursively any transport networks in terms of information transfer capability, in a technology-independent manner, and by using a small set of components. Moreover the model is capable of relating the equipment/logical resource/management views.

This approach has been very effective for the design and the management of networks. It is argued that a similar approach, obviously with proper enhancements, should be adopted for the functional modeling of SDN.

The key point will be definition of a small set of functional components capable of modeling recursively a SDN in all its aspects (i.e., including also processing and storage features).

VI. Standardization and Open Source Activities

A. Standardization Bodies and other Fora

The theoretical concept of SDN has been realized by multiple standardization organizations (ONF, IETF/IRTF, ETSI, ITU-T, IEEE, etc.) into practical solutions (ONF's OpenFlow, CISCO's OpenPK, IBM's DOVE, NEC's Programmable Flow and more).

Several working and discussion groups of the Open Networking Foundation (ONF) are covering various SDN related topics. These are currently Active Working Groups, Architecture and Framework, Configuration and Management, Forwarding Abstraction, Market Education, Migration Discussion Group, Northbound Interface, Optical Transport, Testing and Interoperability, Discussion Groups, Wireless & Mobile. The OpenFlow protocol in version 1.4.0 and OpenFlow Config protocol version 1.1.0 have been standardized by ONF. Both have the largest market share and influence at this point in time, since most vendors and manufacturers support at least OpenFlow as part of their portfolio.

IRTF Software Driven Networks focuses within SDNRG on areas of interest covering the classification of SDN models, relationship to work ongoing in the IETF and other SDOs, SDN model scalability and applicability, multi-layer programmability and feedback control systems, system complexity network description as well as security [55].

The IETF working group Forwarding and Control Element Separation (ForCES) defines an architectural framework and associated protocols to standardize information exchange between the control- and data plane in a ForCES Network Element (ForCES NE). ForCES defines Network Elements (NE), Control Element (CE) and Forwarding Element (FE). In comparison to the SDN concept, which strictly separates forwarding from control in different functional elements, ForCES allows each NE to consist of multiple NE's and FE's. A NE is therefore more complex and is controlled through a CE Manager and FE Manager -each managing the referring Control or Forwarding Element(s) [56].

ITU-T Study Group 13 ITU (Future networks including cloud computing, mobile and NGN) is standardizing FNs with the objectives of service, data, environmental and socio-economic awareness as part of the topic Software-defined Networking (SDN) [57]. Standardization efforts include support network virtualization, energy saving features for FNs, and an identification framework. Future plans are to develop different facets of the smart ubiquitous network, requirements of network virtualization for FNs, framework of telecom SDN and requirements of formal specification and verification methods for SDN.

The standardization activities of the Object Management Group (OMG) aim to set a vendor-neutral global standard for SDN through the investigation of opportunities to foster the development of open SDN specifications.

B. Open Source Software Initiatives

A great number of Open Source communities are working on SDN, NFV, and Network Virtualization projects. As a matter of fact, the number of open-source projects is rapidly growing. SDNCentral aims to capture a list of the main Open Source SDN projects [58].

OpenDaylight is an example of forum created through the combination of open community developers and open source

code and project governance that guarantees an open, community decision making process on business and technical issues. The main goal is to help accelerate the development of technology available to users and enable widespread adoption of Software-Defined Networking [59].

Currently we are already witnessing a growing number of Industries (big but also SME) which are starting adopting Open Source (e.g. OpenStack, Avana, etc) - properly customized - for real production environments. It is a sort of bottom-up move that could change the rules of the game, as it is lowering the thresholds to new Players (even with little investments) to enter the market. Arguably this will happen first at the edge, thus creating a fertile environment for creating and developing new ecosystems. Also this will create new roles and new ways of cooperating and competing. "Competition" will move more and more at the software level, so there is also a great value in testing, assessing and certifying Open Source component, systems or platforms for security, trust, performances and interoperability.

C. *Need for Certification*

It seems that there are very limited certification related activities on SDN. The Cisco Certified Network Professional (CCNP) Service Provider certification program, which is aimed at developing the skills and knowledge of IT professionals to deploy and manage next-generation networks; however, this is not specifically tailored for SDN, There is also Indiana University's InCNTRE Lab, which is a sort of certification lab for Open Flow.

Certification can be provided in the following three areas:

- Professional Certification (SDN-P): This may consist in the establishment of Body of SDN knowledge (BoSK); creation of BoSK Learning Tools that should include the curriculum, books, newsletters, classes, as well as the support. In addition, development of BoSK Examination Tools including SDN-P Certification Exam and Renewal is needed.
- Components Certification (SDN-C): This will require that components requirements, application areas, and benchmarks need to be developed by solicitations and interactions with the industry. Revisions need to be managed. Also, evaluation tools for SDN Certification test-bed, SDN-C Benchmark tests, and SDN-C Certification need to be established. The process for certification renewals needs to be established as well.
- Internal SDN-test bed development: Certification procedures should be developed based on the initial test bed evaluations. Implementation of a test bed via Internet 2.0 and local data centers/supercomputer centers is necessary to utilize state-of-the-art resources. Education activities will be included in the SDN-test-bed for education/curriculum activities. Third party requirements which require SDN test-bed specs and heavy Industry relations need to be established. Finally, an evaluation board for test-bed certification need to formed.

VII. CONCLUSIONS

Socio-economic drivers, IT technology progresses, hardware down-spiraling costs and availability of open source software are steering the evolution of future networks and services infrastructures. It is likely that a wider and wider adoption of "software" in said infrastructures will accelerate the pace of innovation of processes (as it is doing continuously in the IT domains) and will reduce operational costs (e.g., through optimizations exploiting big data) for NOs and SPs.

Emerging paradigms as SDN and NFV represent a first concrete step to this direction, catalyzing the idea of decoupling software defined control plane from hardware driven data plane and the virtualization of network functions on general purpose hardware. This will influence significantly the future developments of 5G technologies and architectures.

As a matter of fact, we are witnessing a growing number of other industries moving to the same direction. In this sense, SDN and NFV could be seen as powerful enablers for new ecosystems capable of aggregating and driving investments beyond the traditional Telco-ICT contexts. It is argued that this transformation is unstoppable, because of the continuous hardware technology evolution and cost reductions, which will enable new economic paradigms. In facts, this will move the competition from hardware to software, creating the favorable conditions for a sustainable "economy of information".

This will require different business rules, and different kinds of jobs, workers and skills than the economy of the 20th century, mostly based on industrial factories, manufacturing and manual work. Economic and cultural values in the economy of information are, and will be, placed on information, knowledge, creativity and intelligence to cope with the fast-changing socio-economic environment. To this end, the development of new skills, mindsets and education are required to face this transformation.

In synthesis, a number of research and development avenues are envisaged:

Core-Edge split. SDN deployment strategies for Core and Edge networks should be distinguished in terms of technical approaches, business models and time horizons [60]. Details and control frameworks for end-to-end networks with core/edge functional split require fundamental rethinking in the fabric designs. This implies impactful aspects such as addressing the virtualization of L4-L7 middle-boxes and the RAN evolution. NOs and SP's spend 60-80% of CAPEX on RAN technologies that are not keeping up with the changing application requirements. In SDN, it remains to be seen whether we need the classical core network functionalities at all, as most of the intelligence will be placed in terminals for handling mobility and at the Edge (data centers) for hosting any type of service, from basic connectivity to Internet and applications.

Functional modeling and architecture. A proper functional architecture would accelerate the development and the standardization of SDN. (In facts, there is an urgent need to

standardize interfaces.) The main characteristics of the functional architecture should make it possible to model recursively all SDN features, in a technology-independent manner, using a small set of components. The model should be capable of relating the equipment/logical resource/management-control views. It might be advisable to follow the effective philosophy of the ITU-T G-805 functional modeling, with proper enhancements to take into account the nature of a SDN (i.e., processing, storing and transferring information).

Management and Orchestration. Complexity and dynamism of SDN will require enhancing current management systems (OSS/BSS) to cope with of a sheer number of real and virtual ICT resources. The border between IT and network resources will blur, requiring the integration of the operations of the two domains. Another major requirement will be the automation of business management processes (e.g., introducing autonomic and learning features exploiting networks and services big data) and adopting decentralized approaches (at the current centralized model will not scale properly). Moreover, the SDN management needs to be complemented with new capabilities such as programmability and orchestration of the life-cycles of virtual network functions and services. Security is one of the key areas of management which should be deeply investigated in SDN.

Distributed computing. SDN and virtualization will offer the opportunity to enhance and adopt in the network infrastructures means and methods today widely used in Data Center. At the same time Data Center concepts need to be evolved reliably and efficiently, especially looking at the integration with networks. Achieving scale by using collections of distributed components (e.g., out of the shelf) and devices will enable reliability and create a more competitive Technology Providers ecosystems. Major issues on consistency and reliable distribution for various network tasks remains to be tackled. Distributed sets of data representing states of network resources and functions demand for carriers' class solutions in compliance with the limits imposed by the CAP (Consistency, Availability, Partition tolerance) theorem.

Taming heterogeneity, geographic distribution and scale. NOs' and SPs' networks will become far more distributed and capillary, geographically and technologically. The way of putting all this diversity under a common end-to-end framework remains a major challenge, especially to cope with the rigid performance requirements in terms of QoS and QoE, for instance. SDN could be a powerful enabler to meet the above requirements but proper levels of abstractions and recursive control and management planes needs to be achieved

Pursuing Open Source Software. There will be a great value in testing, assessing and certifying Open Source component, systems or platforms for security, trust, performances and interoperability.

Peering and Software Defined Internet Exchange. Current inter-domain routing protocol, BGP, is lacking in simplicity of management, security and flexibility in defining relationships. SDN could allow the evolvability of BGPs independently of from the underlying nodes hardware. SDN programmability could mitigate the main problems in inter-domain routing: security and accountability; pricing and contracts; and traffic management [61].

Edge Self-Organization. In the future, the edge of the network will see a sheer number of nodes and devices (i.e. aggregation nodes, terminals, machines, sensors, actuator...): each of these elements with sufficient processing, storage and communication capacities will become like a network node, capable of sharing its capabilities. Them these nodes will be able to aggregate to create local self-organized networks, which, selecting appropriate gateways, will connect to the big network. Nodes decisions will be made based on local conditions, adopting autonomic and self-organization capabilities [38], [66].

Socio-economic impacts. In general, SDN and virtualization appear to be expressions of a softwarization trend in Industry. In ICT, this is lowering the thresholds for new Players to enter the market. This will also create new business roles and new ways of cooperating and competing. Competition, in fact, will move to the software level, whilst the hardware will no longer be a differentiator. New business models and value chains and networks should be defined. As an example, in the long term, one could even imagine scenarios with a galaxy of ecosystems, where "trusted" network services and functions could be provided by different Developers, exchanged and traded like in stocks exchange.

GLOSSARY AND DEFINITIONS

AAA	Authentication-Authorization-Accounting
ADN	Application-Defined Networking is an enterprise data network that uses virtual network and security components to provide a dedicated logical network for each application, with customized security and network policies to meet the requirements of that specific application.
AP	Application Plane – It is plane where applications and services reside and execute.
API	Application Programming Interface (a set of routines, protocols, and tools for building software applications)
ASIC	Application Specific Integrated Circuit
BNG	Broadband Network Gateway
BRAS	Broadband Remote Access Server
BSS	Business Support System
CDN	Content Delivery Network
CP	Control Plane - Control Plane – It is responsible for taking and executing decisions on how packets should be forwarded. It focuses mostly on the forwarding plane and less on the operational plane. It could use operational and management planes information for fine-tuning and modification of the forwarding

	plane actions.
CPU	Central Processing Unit
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
DPI	Deep Packet Inspection
FP	Forwarding Plane – It is responsible for controlling actions on packets in the data-path, including dropping, changing and forwarding packets. It contains forwarding resources such as classifiers and actions.
HV	Hypervisor
I/O	Input/Output
LAN	Local Area Network
LB	Load Balancer
MP	Management Plane is responsible for monitoring, configuring, optimizing, maintaining state of systems, equipment, devices and the overall networks. It maintains and executes the processes that modify the operation of the control plane and it configures the forwarding and control planes.
M2M	Machine-to-Machine communications
MVNO	Mobile Virtual Network Operator
NFV	Network Functions Virtualization
NGN	Next Generation Network
NIC	Network Interface Controller
NMS	Network Management System
NO	Network Operator
OAM	Operations Administration & Maintenance
OGF	Open Grid Forum
ONF	Open Networking Foundation
OpenFlow	Specifications developed by the Open Networking Foundation
OpenNaaS	Specifications developed by the OpenNaaS community
OpenStack	Specifications developed by the OpenStack Foundation
OSS	Operations Support System
OTT	Over The Top
PCE	Path Computation Element
PoP	Point of Presence
RAN	Radio Access Network
QoE	Quality of Experience
SLA	Service Level Agreement
SP	Service Provider
SDN	Software Defined Network
VN	A virtual network (VN) is a network that consists of virtual resources (e.g. processing) and virtual network links. The two most common forms of network virtualization are protocol-based virtual networks, (such as VLANs, VPNs, and VPLSs) and virtual networks that are based on virtual devices (such as the networks connecting virtual machines inside a hypervisor).
VM	Virtual Machine
VPN	Virtual Private Network
vswitch	Any Ethernet switch implemented in software alongside or inside a hypervisor. There are proprietary and open implementations of vswitch.
WAN	Wide-Area Network
Xen	Open Source Hypervisor

REFERENCES

[1] White paper on "Software-Defined Networking: The New Norm for Networks" https://www.opennetworking.org/;

[2] White paper on "Network Functions Virtualisation" http://portal.etsi.org/NFV/NFV_White_Paper.pdf;

[3] SDN4FNS website: http://sites.ieee.org/sdn4fns;

[4] ONF, "SDN Architecture Overview" Version 1.0, December 12, 2013 https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/SDN-architecture-overview-1.0.pdf ;

[5] N. Feamster, J. Rexford, and E. Zegura, "The road to SDN: An intellectual history of programmable networks," ACM Queue, December 30, 2013 http://www.cs.princeton.edu/courses/archive/fall13/cos597E/papers/sdnhistory.pdf;

[6] A. Galis, S. Denazis, C. Brou,C. Klein (ed) –"Programmable Networks for IP Service Deployment" ISBN 1-58053-745-6, pp450, June 2004, Artech House Books, http://www.artechhouse.com/International/Books/Programmable-Networks-for-IP-Service-Deployment-1017.aspx;

[7] Path Computation Element (PCE) - IETF RFCs 4655 and RFC 5;

[8] IETF FORCES Forwarding and Control Element Separation; http://datatracker.ietf.org/wg/forces/ ;

[9] IETF i2rs - Interface to the Routing System https://datatracker.ietf.org/wg/i2rs/;

[10] S. Scott-Hayward et al., "SDN Security: A Survey", Proc. of IEEE SDN4FNS'13, Trento, Italy, Nov. 2013;

[11] Y. Bar Geva et al., "Tearing down the Protocol Wall with SDN", Proc. of IEEE SDN4FNS'13, Trento, Italy, Nov. 2013;

[12] H. Ali-Ahmad et al., "An SDN-based Network Architecture for Extremely Dense Wireless Networks", Proc. of IEEE SDN4FNS'13, Trento, Italy, Nov. 2013;

[13] FP7 CROWD project - http://www.ict-crowd.eu;

[14] A. Basta et al., "A Virtual SDN-enabled LTE EPC Architecture: a case study for S-/P-Gateways functions", Proc. of IEEE SDN4FNS'13, Trento, Italy, Nov. 2013;

[15] S. Namal et al., "SDN as an enabler for inter-technology load balancing and admission control", Proc. of IEEE SDN4FNS'13, Trento, Italy, Nov. 2013;

[16] S. Namal et al., "Enabling Secure Mobility with OpenFlow", Proc. of IEEE SDN4FNS'13, Trento, Italy, Nov. 2013;

[17] M. Mechtri et al., "SDN for Inter Cloud Networking", Proc. of IEEE SDN4FNS'13, Trento, Italy, Nov. 2013;

[18] F. Callegati and W. Cerroni, "Live Migration of Virtualized Edge Networks: Analytical Modeling and Performance Evaluation", Proc. of IEEE SDN4FNS'13, Trento, Italy, Nov. 2013;

[19] R. Trivisonno et al., "Virtual Links Mapping in Future SDN-enabled Networks", Proc. of IEEE SDN4FNS'13, Trento, Italy, Nov. 2013;

[20] J. Mueller et al., "Scalable On-Demand Network Management Module for Software Defined Telecommunication Networks", Proc. of IEEE SDN4FNS'13, Trento, Italy, Nov. 2013;

[21] J. Zhu et al., "Software Service Defined Network: Centralized Network Information Service", Proc. of IEEE SDN4FNS'13, Trento, Italy, Nov. 2013;

[22] F. Salvestrini et al., "Towards a distributed SDN control: Inter-platform signalling among flow processing platforms", Proc. of IEEE SDN4FNS'13, Trento, Italy, Nov. 2013;

[23] I. Bueno-Rodríguez, "OpenNaaS based SDN framework for dynamic QoS control", Proc. of IEEE SDN4FNS'13, Trento, Italy, Nov. 2013;

[24] M. F. Bari, "PolicyCop: An Autonomic QoS Policy Enforcement Framework for Software Defined Networks", Proc. of IEEE SDN4FNS'13, Trento, Italy, Nov. 2013;

[25] R. Bifulco and F. Schneider, "OpenFlow rules interactions: definition and detection", Proc. of IEEE SDN4FNS'13, Trento, Italy, Nov. 2013;

[26] E. Escalona et al., "Using SDN for cloud services provisioning: the XIFI use-case", Proc. of IEEE SDN4FNS'13, Trento, Italy, Nov. 2013;

[27] M. Coudron et al., "Boosting Cloud Communications Through A Crosslayer Multipath Protocol Architecture", Proc. of IEEE SDN4FNS'13, Trento, Italy, Nov. 2013;

[28] M. Vahlenkamp et al., "Enabling Information Centric Networking in IP Networks Using SDN", Proc. of IEEE SDN4FNS'13, Trento, Italy, Nov. 2013;

[29] E. Patouni et al., "Network Virtualisation Trends: virtually anything is possible by connecting the unconnected", Proc. of IEEE SDN4FNS'13, Trento, Italy, Nov. 2013;

[30] D. Siracusa et al., "Edge-to-Edge Virtualization and Orchestration in Heterogeneous Transport Networks", Proc. of IEEE SDN4FNS'13, Trento, Italy, Nov. 2013;

[31] R. Riggio et al., "EmPOWER: A Testbed for Network Function Virtualization Research and Experimentation", Proc. of IEEE SDN4FNS'13, Trento, Italy, Nov. 2013;

[32] J. Batalle et al., "On the implementation of NFV over an OpenFlow infrastructure: Routing Function Virtualization", Proc. of IEEE SDN4FNS'13, Trento, Italy, Nov. 2013;

[33] CONTENT FP7 project http://content-fp7.eu;

[34] K. Katsalis et al., "CONTENT Project: Considerations towards a Cloud-based Internetworking Paradigm", Proc. of IEEE SDN4FNS'13, Trento, Italy, Nov. 2013;

[35] Y. Kanada, "A Node Plug-in Architecture for Evolving Network Virtualization", Proc. of IEEE SDN4FNS'13, Trento, Italy, Nov. 2013;

[36] W. John et al., "Research Directions in Network Service Chaining", Proc. of IEEE SDN4FNS'13, Trento, Italy, Nov. 2013;

[37] A. Galis et al., "Softwarization of Future Networks and Services – Next Generation SDNs", Proc. of IEEE SDN4FNS'13, Trento, Italy, Nov. 2013;

[38] A. Manzalini and R. Saracco, "Software Networks at the Edge: a shift of paradigm", Proc. of IEEE SDN4FNS'13, Trento, Italy, Nov. 2013;

[39] FP7 IP MobileCloud Networks: Mcn consortium, project number: 318109. http://mobile-cloud-networking.eu;

[40] Interworking and JOINt Design of an Open Access and Backhaul Network Architecture for Small Cells based on Cloud Networks: iJOIN. https://www.ict-ijoin.eu/;

[41] D. Kreutz, F.M.V. Ramos, P. Verissimo, "Towards secure and dependable software-defined networks"- the second ACM SIGCOMM workshop on Hot topics in software defined networking, August 2013, http://conferences.sigcomm.org/sigcomm/2013/;

[42] S. Shin et al. "FRESCO: Modular Composable Secu- rity Services for Software-Defined Networks". In: In- ternet Society NDSS 2013;

[43] Y.3001 ITU-T recommendation – "Future networks: Objectives and design goals" – 2011 http://www.itu.int/rec/T-REC-Y.3001-201105-I;

[44] D. Matsubara, T. Egawa, N. Nishinaga, M.-Ki, Shin, V. P. Kafle, A. Galis, -"Toward Future Networks: A Viewpoint from ITU-T" - IEEE Communications Magazine, March 2013, Vol. 51, No. 3, pp: 112 – 118;

[45] E. Haleplidis, S. Denazis, K. Pentikousis, J. Hadi Salim, D. Meyer, O. Koufopavlou, SDN Layers and Architecture Terminology draft-haleplidis-sdnrg-layer-terminology-03, December 5, 2013, http://tools.ietf.org/html/draft-haleplidis-sdnrg-layer-terminology-03;

[46] J. Rubio-Loyola, A. Galis, A. Astorga, J. Serrat, L. Lefevre, A. Fischer, A. Paler, H. de Meer, "Scalable Service Deployment on Software Defined Networks"–IEEE Communications Magazine/ Network and Service Management Series, ISSN: 0163-6804; December 2011 http://dl.comsoc.org/ci1/;

[47] OpenStack - Open source software for building private and public clouds- http://www.openstack.org;

[48] ETSI 'Software-aware and Management-aware SDN" - 3rd ETSI Future Networks Workshop 9-11 April 2013 - http://docbox.etsi.org/Workshop/2013/201304_FNTWORKSHOP/eproceedings_FNT_2013.pdf;

[49] M. Banikazemi, D. Olshefski, A. Shaikh, J.Tracey, and G. Wang, "Meridian: An SDN Platform for Cloud Network Services", IEEE Communications Magazine • February 2013;

[50] L. Erran Li, Z. Morley Mao J. Rexford, CellSDN: Software-Defined Cellular Networks, Open Network Summit (Research Track). Santa Clara, CA, USA (April 2013);

[51] A. Gudipati_, D. Perry_, L. Erran Li, S.Katti, SoftRAN: Software Defined Radio Access Network, HotSDN 2013;

[52] Open Systems Interconnection (OSI) model (1994)- www.ecma-international.org/activities/Communications/TG11/s020269e.pdf;

[53] D. Matsubara, T. Egawa, N. Nishinaga, M.-Ki, Shin, V. P. Kafle, A. Galis, - "Open the Way to Future Networks – a viewpoint framework from ITU-T" – invited paper "The Future Internet- Future Internet Assembly 2013: Validated Results and New Horizons" Lecture Notes in Computer Science 7858, Springer, pp370, May 2013, ISBN 978-3-642-38081-5; http://www.springerlink.com/content/978-3-642-38081-5/;

[54] A. Galis, J. Rubio-Loyola, S. Clayman, L. Mamatas, S. Kukliński, J. Serrat, T. Zahariadis, "Software Enabled Future Internet" - 5th International Conference on Mobile Networks and Management (MONAMI 2013), 23-25 Sept 2013, Cork, Republic of Ireland, http://mon-ami.org/2013/show/home;

[55] http://irtf.org/sdnrg;

[56] D. Kreutz, F.M.V. Ramos, P. Verissimo, "Towards secure and dependable software-defined networks"- the second ACM SIGCOMM workshop on Hot topics in software defined networking, August 2013, http://conferences.sigcomm.org/sigcomm/2013/;

[57] S. Shin et al. "FRESCO: Modular Composable Secu- rity Services for Software-Defined Networks". In: In- ternet Society NDSS 2013;

[58] Open Source SDN projects http://www.sdncentral.com/comprehensive-list-of-open-source-sdn-projects/;

[59] Open Daylight Foundation - http://www.opendaylight.org;

[60] A.Manzalini, R. Minerva, F. Callegati, W. Cerroni (2013). Clouds of Virtual Machines at the Edge, IEEE Com. Mag. "Future Carriers Networks", July 2013;

[61] Scott Whyte. Project CARDIGAN: An SDN-Controlled Exchange Fabric. http://www.nanog.org/meetings/nanog57/ presentations/Wednesday/wed.lightning3.whyte.sdn.controlled.exchange.fabric.pdf, 2012;

[62] IETF NETCONF Configuration protocol http://tools.ietf.org/html/rfc4741;

[63] IETF SNMP - Simple Network Management Protocol http://tools.ietf.org/html/rfc5343:

[64] iJOIN FP7 Project http://www.ict-ijoin.eu.

[65] J. Mueller, T. Magedanz, 'Towards a Generic Application Aware Network Resource Control Function for Next-Generation-Networks and Beyond', International Symposium on Communications and Information Technologies (ISCIT), DOI:10.1109/ISCIT.2012.6381026, ISBN:978-1-

4673-1156-4, Page(s): 877 - 882, Gold Coast, Australia, October 2–5, 2012, www.iscit2012.org;

[66] A. Manzalini, P.H. Deussen, S. Nechifor et alii "Self-optimized Cognitive Network of Networks", in Oxford Journals "The Computer Journal"; 2010, Volume 54, Issue 2, pp 189-196.