Network Virtualization: Paving the Way to Carrier Clouds

(invited)

Slavisa Aleksic
Institute of Telecommunications
Vienna University of Technology
Vienna, Austria
slavisa.aleksic@tuwien.ac.at

Igor Miladinovic
Alcatel-Lucent
Vienna, Austria
igor.miladinovic@alcatel-lucent.com

***Abstract*—Network function virtualization (NFV) and multi-layer software-defined networking (SDN) will enable an automated control, management and orchestration of network resources across several network layers and areas. They may also open new possibilities for communication service providers (CSP) to expand their business and offer cloud services with carrier-level service-level agreements (SLA). In this paper, we briefly review technological, legal and business aspects of NFV and carrier clouds.**

Keywords—Network Function Virtualization (NFV); Carrier Clouds; Software-Defined Networking(SDN); Multi-Layer SDN; Business Aspects

I. INTRODUCTION

Network function virtualization (NFV) is a current trend in the telecommunications industry that transforms traditional software and hardware components, i.e., functions from physical to virtual in order to enable cloud-like virtualization and orchestration of network resources. NFV goes hand in hand with the software defined networking (SDN), which is a paradigm that provides for separation between the control and the data (switching or forwarding) planes. Both approaches promise cost reduction and a rapid service delivery, i.e. an improved service agility and a revenue growth for network operators. Recently, ETSI Industry Specification Group for Network Functions Virtualization created several documents defining the architectural framework and requirements for NFV and addressing use cases for various network functions. Many component and system vendors already offer solutions that integrate SDN at different levels of implementation and various network layers. Network operators already show an increased interest in integrating SDN and NFV in their networks. Use cases include the virtualization of mobile networks (base stations, mobile core – EPC, IMS), content delivery networks (CDNs), wired access networks as well as home/enterprise networks. The virtualization of network resources opens new ways for network operators, i.e., communication service providers (CSPs) to extend their business by integrating small and medium-scale data centers into their network infrastructure, thereby building carrier clouds and offering conventional and new cloud services with carrier-grade service level agreement (SLA).

In this paper, we briefly review recent developments in NFV and SDN and indicate the main benefits and challenges of network virtualization and carrier clouds from the technological, performance and legal aspects.

II. CARRIER CLOUDS

In the carrier cloud, the cloud infrastructure is owned and cloud services are provided by a communication service provider (CSP). The main benefit is that CSPs have control over both network and data centers, which can lead to better performance by means of low latencies and high throughput on links between consumers and data centers as well as on intra-data-center links. Moreover, a CSP can easily realize geo-distributed cloud infrastructure by placing small and medium-scale data centers close to consumers. Thus, carrier clouds are able to offer high-quality services to cloud consumers and, even more important, to guarantees the carrier-grade service level agreement (SLA). Because both network and cloud infrastructures are owned and managed by the same entity, the status of the network can be considered in conjunction with that of cloud resources, leading to an application awareness across the entire network (i.e., fixed, mobile, access and core). Similar to other cloud implementation options, carrier clouds support private, public and hybrid services.

III. NETWORK FUNCTION VIRTUALIZATION

Virtualization of network functions is one of the primary aims and enabling steps towards carrier clouds. Actually, network virtualization is not an essentially new method; network designers and operators have already used it for many years. The only difference to conventional approaches and the challenge in creating carrier clouds is the need for separating network control functions from hardware and for automated control of virtualized resources.

Different mechanisms and architectures can be applied to achieve virtualization of network functions. In the following, we will briefly review the most prominent ones such as overlay networks, virtual local area networks (VLAN), virtual private networks (VPN) and software defined networks (SDN).

A. Overlay Networks

Overlay networks are virtual networks that create a virtual topology on the top of the physical topology through adding an additional layer of indirection/virtualization and changing the properties of one or more areas of the underlying network. A prominent example is the Internet, which is essentially an overlay network that is built on local area networks (LANs) by adding an Internet Protocol (IP) header to all packets that are exchanged between LANs.

The main benefit of overlay networks is that there is no need to deploy new equipment or modify existing software/protocols. The reasons for deciding to implement or not an overlay network are usually: (i) providing quality of service (QoS) guarantees, (ii) reducing memory and bandwidth consumption as well as (iii) achieving a high level of security, e.g. in case of service denial attacks, and scalability.

B. Virtual Local Area Network (VLAN)

VLAN is essentially a layer 2 technique, in which Ethernet frames belonging to the same VLAN bear a common VLAN identifier (ID) as specified in IEEE 802.1q. VLAN-enabled switches use both the destination MAC address and VLAN ID to forward frames while multiple VLANs can share a single link between switches.

C. Virtual Private Network (VPN)

In a VPN, communicating parties are connected through tunnels over public communication networks (e.g. the Internet). Each VPN consists of one or more customer edge (CE) devices, which are connected to one or more provider edge (PE) routers. Usually, VPNs are provisioned and managed by a VPN service provider. VPNs can be realized at different layers, namely at layer 3, layer 2 or even layer 1.

- *Layer 3 VPN*: uses a layer 3 (or layer 2.5) protocol such as IP or MPLS in the VPN backbone. Here, we differentiate between the CE-based VPN and PE-based VPN. In a CE-based VPN, tunnels are created, managed and closed by CE devices without the knowledge of the service provider network. Tunneling requires various protocols such as a carrier protocol (e.g. TCP/IP), an encapsulating protocol and a passenger protocol. The encapsulating protocol (e.g. GRE, PPTP, IPSec) is used to wrap the original data, while the passenger protocol is nothing but the original data format in customer networks. Differently, in a PE-based VPN, PE devices route and forward customer traffic based on customer network addressing. The customer traffic is usually forwarded over VPN tunnels that are based on label-switched paths (MPLS), IPSec tunnels or GRE tunnels. Here, CE devices are not involved in establishing tunnels and do not know that they are participating in a VPN.
- *Layer 2 VPN*: provides an end-to-end layer 2 connection between distributed sites by transporting layer 2 frames (typically Ethernet but also ATM and Frame Relay)
- *Layer 1 VPN*: rapid advances in next generation optical networks such as the definition and implementation of optical transport network (OTN), generalized multi-protocol label switching (GMPLS), automatically switched optical network (ASON), hybrid optical switching (HOS) and elastic optical networks (EON) enable connection provisioning directly in the optical domain.

D. Software-Defined Networking (SDN)

SDN is a complementary technology to network virtualization. It provides: (i) unbundling network control software from network hardware, i.e., separating the control and the forwarding planes, and (ii) standardized programming interface for application developers. In this approach, network control functions and intelligence are provided by a component called SDN controller rather by network elements, which simplifies operations and makes multi-vendor and multi-domain networks easier to manage. The SDN controller makes decision on how a connection or a flow needs to be set up and configures the network accordingly. The necessary actions are communicated to the forwarding plane using a network control protocol (e.g. OpenFlow).

IV. Performance, Security and Privacy Aspects

As the usage intensity of cloud services grows, providing high performance to cloud consumers becomes more challenging because of a number of reasons:

1. The traditional data center network design is not scalable enough to meet the ever increasing requirements on storage capacity and processing power.
2. Many advanced cloud services demand high-bandwidth and low-latency. However, these requirements are difficult to meet, especially for traditional cloud service providers because they cannot monitor and control the performance of the network, so it is almost impossible for them to offer and meet strong SLAs due to non-deterministic latencies and data losses.
3. The rapid growth of cloud data centers and increased usage intensity lead to a rapid increase in total energy consumption of the cloud infrastructure.
4. There are legal and regulatory issues that restrict the flexibility in implementing and optimizing cloud infrastructures.
5. Many customers are concerned about the security of their data.

In the following, we will briefly address the above mentioned issues.

A. Scalability and Network Virtualization

In a traditional data center network, the boundary between layer 2 (L2) and layer 3 (L3) is placed on the wide area network (WAN) router. L2 VLAN is not scalable enough and can hardly meet high tenant scale requirements. Due to the

fact that L2 forwarding is per-VLAN, an efficient load balancing strategy cannot be applied.

These scalability limitations can be addressed either by optimizing the L2 forwarding scheme or by using an optimized L3 routing instead [1]. An example of optimized L2 forwarding is the Ethernet Virtual Private Network (E-VPN), which provides L2 multi-point bridging with control and data planes similar to L3 VPN. The result is a better scalability and load balancing. L3 routing can be optimized by moving the L3 gateway deeper into the data center in order to reduce the L2 domain and thus achieve a better ARP scale.

B. Increasing Bandwidth Demand

The continuous growth of Internet traffic has led to rapidly increasing capacity provided by network infrastructure. Observations have shown that the main contributor to the traffic increase in the Internet is the traffic from residential customers [2]. This is mostly because of introduction of new bandwidth-hungry applications for residential users, but also due to the fast growth of the number of broadband subscribers [3]. Due to the concurrent growth of Internet traffic and the number of subscribers, both the number of network elements and their capacity are also expected to increase in the future. Recent introduction and wide penetration of smartphones and tablets confirm this trend. Furthermore, according to the vision of the "Internet of Things" it is expected that in the foreseeable future, a huge number of smart autonomous devices will communicate via the Internet, which is referred to as Machine-to-Machine (M2M) communication. It is projected that 50 Billion smart autonomous devices will be connected to the Internet in 2020 [2]. Thus, the requirements on both the communication network and data centers are contentiously increasing.

In the past, user traffic was increasing by about 100 % per year. Within the last few years, this growth has slowed somewhat, so that the traffic volume in global communication networks is currently increasing by approximately 40 - 50 % per year [4]. In order to keep track with this increasing demand for bandwidth, the capacity of underlying network components has to increase too.

Driven by the rapid development and wide use of cloud computing applications, the amount of cloud-related network traffic both between and inside data centers has been drastically increasing during the last years. It has been reported that the amount of data center traffic has already reached 1.8 zettabytes per year. It will nearly quadruple to about 6.6 zettabytes per year until 2016 [5]. This corresponds to a compound annual growth rate (CAGR) of 31% from 2011 to 2016. As a result, the number of servers in data centers and their capacity are growing very fast in order to meet the increasing traffic demand. While only a few years ago 1 Gb/s network cards were typically used, the majority of currently deployed servers inside data centers provide 10 Gb/s ports and, in the near future, 40 Gb/s and 100 Gb/s ports are expected to be used [6].

C. Latency

Some latency-sensitive applications such as telephony, online gaming and video conferencing have strong requirements on the maximum roundtrip delay. The expected response time of a cloud depends on several parameters such as the distance between the client and the serving data center, the status of the network, the capacity of the interconnecting links, the architecture and the load of the data center as well as the application characteristics and the time needed to process the request by the server. It has been shown by recent measurements that the response time of current public clouds increases linearly with the distance from clients and usually lies between 100 and 500 ms [7], which can cause severe difficulties in providing acceptable quality of experience.

In a distributed cloud, such as in a carrier cloud where small and medium-scale data centers are placed closer to end users and the network between the users and data centers is managed by the cloud owner, the roundtrip delay can be significantly reduced. Thus, the latency-sensitive applications and services can benefit from distributed cloud architecture. This is similar to the common practice to implement content distribution networks (CDNs) and push static and often demanded contents towards the users at the edge of the network. Additionally, layer 1 VPNs that provide dynamic connection provisioning directly in the optical domain can be used to further reduce network latencies close to the minimum achievable value, i.e., the signal propagation time.

D. Energy Consumption

The energy consumption of cloud computing infrastructure is expected to increase in the future mainly due to the trends described in IV.B. However, the energy consumption and the environmental influence of cloud computing is not easy to estimate. In a recent study, it has been shown that the main contributor to the total cloud energy consumption might not be data centers, as one would intuitively expect, but rather the wireless access networks [8]. Additionally to data centers and network infrastructure, end user equipment and usage intensity of cloud services should also be taken into account when evaluating energy efficiency of cloud computing.

The energy consumed during the use phase is only a part of the whole story. In addition to the operational energy consumption, energy consumed and resources used within other phases of the system's life cycle, i.e., the material extraction, manufacturing, transportation and recycling phases, influence the overall environmental sustainability of cloud computing. Thus, there is a need for a holistic approach in addressing energy consumption and environmental impacts of cloud computing [9]. Such an approach should take into account current and future developments in energy-efficient component and system design, virtualization, consolidation, efficient room cooling, use of alternative and regenerative energy sources as well as network elements and end-user devices [10,11]. An example of such a holistic approach is presented in [9,12]. The approach combines the concept of exergy, i.e., available energy, with the life cycle assessment (LCA) analysis. The overall lifetime exergy consumption is an effective measure of system's environmental sustainability and can be used to identify the main sources of inefficiency.

E. Security and Privacy Issues

With the deployment and an intensive use of cloud infrastructure and services both security and privacy issues

become increasingly important. There are two main questions to be addressed: (i) how to transmit and store client data and (ii) where to store data [7].

Traditionally, data are transmitted through the core network using secure VPNs, which can be either IPsec VPNs, secure sockets layer (SSL) VPNs, point-to-point tunneling protocol (PPTP) VPNs secured with Microsoft point-to-point encryption protocol (MPPE), or layer 2 tunneling protocol (L2TP) VPNs secured using IPsec. It should be noted here that data transmitted within the data center are usually not encrypted at all, which present a possible security leak. Data privacy, integrity and cryptographic isolation can only be guaranteed when strong encryption and authentication of each packet or frame is established on the end-to-end basis, i.e. between customer devices and servers.

F. Legal Constraints

Privacy laws determine how data can be stored. There are a number of regulations that govern how data are to be stored and who has access to it. Examples of such regulations in the United States (U.S.) are the Health Insurance Portability and Accountability (HIPAA) [13], which governs patient information, the Family Education Right and Privacy Act (FERPA) [14], regulating the access to student records and the Gramm-Leach-Bliley Act (GLBA) [15] that is about sensitive financial data. In the Europe, the European Union‘s Data Protection Directive (DPD) governs sensitive private data [16]. This directive restricts data storage of sensitive private data of EU citizens outside the EU, but has actually no limitations on the storage and movement of data within the EU.

The rules on where data can be stored are determined by transborder data laws. The movement of data originating from one jurisdiction to another jurisdiction is sensitive, but often required to be performed in a global cloud. Thus, the implementation and operation of global cloud infrastructure is strongly influenced by transborder data laws. A large number of countries have already enacted legislation that determines how data may cross borders. As of December 2011, there were almost 100 countries across the world that are regulating transborder data flows in some form, or have the possibility of doing so [17]. In general, the regulations can be divided in (i) those presuming that data flows should be allowed, but leaving the option for permitting or limiting some of them and (ii) regulations saying that transborder data flows should not take place unless they are explicitly allowed. An example of the latter is the EU’s DPD.

Due to the large number and diversity of transborder data laws and regulations it is difficult to establish and efficiently operate large centralized data centers that conform to all laws, rules and regulations. Sometimes transborder data regulations are in conflict with some other regulations and acts such as those enacted to intercept and obstruct terrorism. Important are not only data transfers and what jurisdictions the data is located in, but also the origin of the company that owns the cloud infrastructure. For example, the USA PATRIOT Act gives the US government broad powers to collect private data stored inside and outside the United States of America if stored and managed by U.S. companies. This may stand in contradiction with some other regulations on transborder data flows such as the EU’s DPD.

V. MULTI-LAYER SDN

Already for many years now, multi-layer integration has been a wish of networking industry. Since multi-layer SDN provides centralized network intelligence, it makes possible to inspect all network layers concurrently to determine a path and transport technology best suited to carry traffic. Even on a single path, a data flow can be transported using different technologies and using different layers. For example, using multi-layer SDN, a network can establish a transport path partly over OTN and partly over GMPLS. Additionally, multi-layer SDN could monitor and evaluate the performance at each layer and across several network areas and dynamically reroute traffic or add some bandwidth from a lower layer to avoid congestions and find an optimal solution in milliseconds. This can avoid the need for hold-down timers, which are provisioned waiting periods defined and used by upper layers to provide enough time for lower layers to react to failures. Multi-layer SDN can open the way for dynamic network optimization as well as for automated congestion control and cost management.

Current SDN implementations focus mainly on Ethernet networks for data centers. It is essential to extend and apply the SDN concept to transport networks on layer 0/1 (e.g. DWDM, OTN, HOS, EON), layer 2 (e.g. Ethernet) and layer 2.5 (e.g. MPLS-TP), where there is currently a lack of standards and products providing automated provisioning across these layers.

Modern optical transport networks already provide a relatively high level of flexibility and controllable attributes. Some of the attributes can be controlled by software, so a SDN controller can control them. Many optical transport systems available on the market today implement the path computation element (PCE), which is standardized in IETF RFC 4655 as a control protocol for MPLS and GMPLS networks. PCE engine can be implemented in a SDN controller as a software module to provide path computation across several layers (Layers 0, 1, 2 and 2.5). Topology management and virtual routing modules are also available. However, additional standardization is required to allow the SDN controllers to directly manage optical transmission components such as variable bandwidth transceivers (VBTs) and reconfigurable add/drop multiplexers (ROADMs). New-generation optical coherent transceivers with digital signal processing provide a high level of flexibility and adaptability to support trade-offs between bit-rate, spectral efficiency and reach. They can provide different modulation formats such as binary phase shift keying (BPSK), quadrature phase shift keying (QPSK) and quadrature amplitude modulation (QAM) together with forward error correction (FEC) [19]. Within the network, the available spectrum can be flexibly handled by allocating one, two or more spectral slices to a data flow. Some of realizations of ROADMs are very flexible and allow the control of the wavelength (color), ingress/egress direction and wavelength reuse without restrictions [20]. Such ROADMs are called colorless, directionless and

contentionless (CDC) add/drop multiplexers. These are examples of components that can be used to implement software defined optical transport networks.

VI. Business Aspects

The main driver for introducing NFV and carrier clouds is their potential not only to reduce costs, but also to increase revenue. There are many possible ways how network providers, i.e., communication service providers (CSPs) can utilize network virtualization to expand their business and improve processes in the areas of network management and control. A recent study and survey [21] outlined some benefits of using NFV in the network and at customer premises, which are summarized in Table I. The survey indicated the interest of CSPs in a long-term vision for NFV and that policy servers, switches, routers, application servers and IMS nodes will be first affected by virtualization. They are also interested in reducing the complexity of management systems required to support IMS nodes as well as to evaluate how virtualization will influence the evolved packet core (EPC).

Opposite to these benefits network providers are exposed to costs and risks related to the introduction of NFV and carrier clouds. The costs include network equipment costs, integration services costs and own manpower costs. The risks with the introduction of such a significant architectural change in the network have to be mitigated, which often also results in additional costs.

A business case calculation, taking into consideration both, benefits and costs, has to give among other things a clear figure in which timeframe the return of investment (RoI) can be expected. However, there is no general rule and recommendation for all network providers and it has to be considered on case by case basis. Therefore, prior to introduction of NFV and carrier clouds a deeper analysis of specific conditions for a network provider is recommended, resulting in an individual business case which should be the basis for the final decision.

TABLE I. Benefits of NFV for Communication Service Providers (reproduced from [21]).

Reduced Costs	Increased Revenue
• Lower on-site installation, maintenance and energy costs • Faster service introduction, activation and upgrade • Longer product lifecycle • Effective deployments • Reduced equipment footprint at customer site	• SLA assurance • Increased quality of experience • Policy compliance • More premium services • Reduced time-to-market • Ubiquitous services over any access • Higher service adoption

Suppliers of network equipment are aware of the potentials of NFV and carrier clouds. There are already a number of solutions being developed and offered by leading vendors. Without the claim of completeness we list in Table II recent efforts in the area of NVF platforms [22].

TABLE II. Recent Efforts in Providing Solutions for NFV and Carrier Clouds (reproduced from [22]).

Solution	Main Provider	Partners
CloudBand: a management system for orchestrating and automating NVF platforms	Alcatel-Lucent	CloudBand Ecosystem Program: Deutsche Telecom, Telefonica, Citrix, Intel, Vyatta, Radware, Red Hat, HP, Nuage Networks, Gigaspaces, StackIQ, Inktak and Nominum
Open Network Environment, Quantum	Cisco	HCL Technologies, Leap Wireless
Cloud System: virtual network system mooving toward NFV paltform	Ericsson	Joined OpenStack to contribute to development of solutions
Cloud Services Automation, Matrix, Aggregation Platform	HP	Optus, Connectem
Liquid Net : virtualized elements for radio networks, applications and management	NSN	IBM, Intel, CD Networks, India Sevice Providers, SK Telecom

While CSPs are still mainly interested in virtualizing core network functions, virtualization of customer premises equipment (CPE) may also become an important role in the near future. It is because virtual CPEs would eliminate the need of replacing the old CPE with a new one every time when a new service is introduced. This could improve the time-to-marked and reduce the cost, but also reduce inventory, installation time and errors. Thus, locating some of virtual network functions at the network edge seems to be a possible approach for the future. The virtual functions that could be located at the customer premises include firewalls, network address translators (NATs), diagnostic tools, rate limiters and traffic accelerators. The main challenge that arises from using distributed virtual functions is implementing a management system that is able to efficiently manage and orchestrate in a centralized manner both distributed and centrally-located virtual network functions together with virtual machines and traditional servers.

VII. Conclusions

Carrier cloud is a new business model that allows communication service providers (CSPs) to offer high-quality cloud services to private and business users. It becomes possible by implementing distributed data centers as well as managing and orchestrating virtual network functions together with virtual machines and traditional servers in data centers. Thus, network function virtualization (NFV) and multi-layer software-defined networking (SDN) are enabling technologies for carrier clouds. Multi-layer SDN provides centralized network intelligence and makes possible inspection of all network layers concurrently to determine a path and transport technology best suited to

carry traffic. In order to achieve high level of security, encryption and authentication on the entire transmission path between end devices, i.e. users and servers, is required. Both system vendors and service providers are already developing and offering NFV platforms. CSPs are currently engaged in proof of concepts with many NFV use cases within the core network. In the near future, virtualization of customer premises equipment (CPE) may also become an important role because it offers large potential cost and time savings while keeping the implementation within limits. Even though all involved parties are pushing the development and standardization of NFV, the lack of an appropriate business case showing a clear and concrete figure for business value for CSPs can slow down the momentum for adoption.

REFERENCES

[1] D. Cai and S. Natarajan, “The Evolution of the Carrier Cloud Networking”, 2013 IEEE Seventh International Symposium on Service-Oriented System Engineering, March 2013, San Francisco, CA, USA, pp. 286 – 291

[2] Cisco Visual Networking Index, "Global Mobile Data Traffic Forecast Update, 2013-2018", 2014.

[3] D. Evans, "The Internet of Everything", Cisco IBSG, 2012.

[4] C. Lange D. Kosiankowski, C. Gerlach, F.-J. Westphal, A. Gladisch, "Energy consumption of telecommunicationnetworks", In ECOC 2009, Vienna, Austria, Sept. 20-24. Paper 5.5.3.

[5] Cisco white paper: “Cisco Global Cloud Index: Forecast and Methodology, 2011-2016,” October 2012.

[6] Dell white paper: “Data Center Design Considerations with 40GbE and 100GbE,” August 2013.

[7] Y. Ben-David, S. Hasan, and P. Pearce, “Location Matters: Limitations of Global-Scale Datacenters”, Technical Report, 2012, pp. 1-11.

[8] CEET, “The Power of Wireless Cloud: An analysis of the energy consumption of wireless cloud,” Centre for Energy-Efficient Telecommunications, Tech. Rep., April 2013.

[9] S. Aleksic, M. Safaei, „Exergy Consumption of Cloud Computing: A Case Study”, (invited), 19th European Conference on Network and Optical Communications (NOC 2014), Milan, Italy, June 2014, pp. 1 - 6.

[10] S. Aleksic, M. Deruyck, V. Vereecken, W. Joseph, M. Pickavet, and L. Martens, „Energy Efficiency of Femtocell Deployment in Combined Wireless/Optical Access Networks”, in Computer Networks Journal, ELSEVIER, Vol. 57, No. 5, April 2013, pp. 1217–1233.

[11] S. Aleksic, „Energy-Efficient Communication Networks for Improved Global Energy Productivity”, in Telecommunication Systems, Springer, Vol. 54, No. 2, pp 183-199.

[12] S. Aleksic, „Energy, Entropy and Exergy in Communication Networks”, in Entropy Journal, MDPI, Special Issue on Entropy and the Second Law of Thermodynamics, 2013, pp. 4484 - 4503.

[13] The Health Insurance Portability and Accountability Act of 1996, August 21, 1996.

[14] Office of Family Policy Compliance, Family Education Rights and Privacy Act (FERPA). Retrieved October 17, 2004. Online: http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html.

[15] Financial Privacy: The Gramm–Leach–Bliley Act, Federal Trade Commission, 1999. Online: http://business.ftc.gov/privacy-and-security/gramm-leach-bliley-act.

[16] Europea Commision, Protection of personal data, http://europa.eu/legislation_summaries/information_society/data_protection/l14012_en.htm.

[17] C. Kuner. Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future. OECD Digital Economy Papers, No. 187, pages 39, 2011.

[18] H.R.3162 -- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Online: http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.3162.ENR.

[19] K. Roberts, C. Laperle, ``Flexible Transceivers”, European Conference and Exhibition on Optical Communication (ECOC), September 16-20, 2012.

[20] S. Gringeri, B. Basch, V. Shukla, R. Egorov, and T. J. Xia, “Flexible Architectures for Optical Transport Nodes and Netowrks”, IEEE Communications Magazine, Vol. 48, No. 7, July 2010, pp. 40-50.

[21] T. McElligott, “A Step Forward Operations in Virtual Networks”, Stratecast Perspectives & Insight for Executives (SPIE), Vol. 14, No. 6, 2014.

[22] M. Sullivan-Trainor, “Network function virtualization: Where’s the business case?”, TBR Special Report, 2014.