Revisiting Virtual Private Network Service at Carrier Networks: Taking Advantage of Software Defined Networking and Network Function Virtualisation

Luiz Cláudio Theodoro, Pedro Macedo Leite
Hélvio Pereira de Freitas, Adailson Carlos Souza Passos,
and João Henrique de Souza Pereira

Innovation, Research and Development
Algar Telecom
Uberlândia, MG, Brazil
Email: lclaudio@algartelecom.com.br,
pedrol@algartelecom.com.br, helvio@algartelecom.com.br,
adailson@algartelecom.com.br, joaohs@algartelecom.com.br

Flávio de Oliveira Silva, Pedro Frosi Rosa,
João Henrique de Souza Pereira
and Alexandre Cardoso

Federal University of Uberlândia
Uberlândia, MG, Brazil
Email: flavio@ufu.br, pfrosi@ufu.br,
joaohs@ufu.br, and alexandre@ufu.br

***Abstract*—A service commonly offered by telecom operators is the Virtual Private Network (VPN) that allows the interconnection of corporate networks in different geographic localities. To deploy this service, an operator, usually, installs in customer's premises some equipments, such as a router and/or a switch. This deployment increases cost and the complexity of the service. By taking advantage of Software Defined Networking (SDN) and Network Function Virtualisation (NFV), this work presents and details a VPN service architecture that decreases Capital Expense (CAPEX) and Operating Expense (OPEX) and it is open to new innovative service offerings, such as: Quality of Service (QoS) policies, Network Address Translation (NAT) and a multi-homing function. This work also contributes to this research area by going further in the description of a real use case at a carrier network.**

Keywords*—*Software Defined Networking; Network Function Virtualisation; VPN; QoS; NAT.

I. INTRODUCTION

Large computer networks are difficult to manage and are not simple at all in its structure for the fact they involve several equipments, such as switches, routers, modems, servers and others. On these equipments, firewalls, Network Address Translation (NATs), servers load balancers and intrusion-detection systems are configured. The industry has been delivering to the market an infinite of equipment which work in a complex way with a distributed control software closed and proprietary. Such software implements network protocols exhaustively tested during many years that evolved a lot in terms of standardisation and interoperability and generate a big industry based on IP services.

In a traditional scenario, IP Services are provided by a Customer Premises Equipments (CPE), which are the point of contact with the customer facility. All the configuration related to user services resides on the CPE, and in case of any change it must be remotely accessed and updated accordingly. If there is a hardware failure a field technician must be in place in order to substitute the CPE. In this case, the downtime is considerable. An alternative would be to implement a resilient structure, with spare parts and on-line redundancy, thus increasing costs and complexity.

From the operator perspective, this also implies additional costs with technician displacement, keeping spare parts (sometimes from different CPE vendors) and maintenance contracts with third parties.

Normally, administrators configure individual network devices using configuration interfaces that vary among suppliers and even among different products from the same supplier. Though some network management tools offer a central management entity for the network configuration these systems continue to operate at individual configuration protocols, mechanisms and interface levels. Such an operation mode hampers innovation, increases complexity and encumbers companies with high investments and high network operation costs [1][2].

As a proposal to change the way the networks are projected and managed there was Software Defined Networking (SDN) abstractions that separate the control plane (that decides how to control the traffic) from the data plane (that forwards data according to the control plane decisions). By shifting control plane functions to a central place could result in a more proactive management besides optimizing CPE maintenance costs and potentially reducing displacements to customer facilities.

Another important feature SDN has is to use a well-defined Application Programming Interface (API) as the OpenFlow [1], in order to have direct control on the data plane elements; its acceptance has been increasing within the industry and it was the greatest responsible for taking the SDN from the academy to the telecom marketplace. Several commercial switches can already support OpenFlow protocol and several control platforms have been launched [3].

Recently, a new initiative, called Network Functions Virtualisation (NVF), helped to launch virtualisation existent concepts to consolidate network equipment with specific functions in servers with high volume. Switches and storage that can be allocated on the network nodes, on datacentres or on the final user equipment [4][5].

 ISBN: 978-1-61208-398-8

These two technologies have already crossed the labs barriers and have entered for once on the producer's road-map. Although, SDN has benefited some initial practical successes and it certainly offers necessary technologies to support network virtualisation, lots of work is needed in either to improve the existent infrastructure or to explore SDN's potential in order to solve the problems from a much wider perspectives of use cases. This work is part of such a movement and it points to a real scenario that can be implemented to collaborate on these technologies opportunities and challenges [2].

Both concepts and solutions can be potentially combined in a way to obtain more added value to companies that provide the service and to their customers.

This work revisits the VPN service, a common service, offered by telecom operators that allows the interconnection of networks in different localities. The new service architecture reduces CAPEX and OPEX and also offers innovative functions that can empower the customer by giving the ability to explore new service funcionalities such as different QoS policies, NAT and multi-homing.

The remainder of this paper is structured as follows: Section II describes related work regarding NFV and SDN. Section III presents the current deployment of a VPN service by telecom operators. Section IV revisits the VPN service deployment based on SDN and NFV. Section V describes some innovative service offerings built on top this new service architecture, and finally, in Section VI, we present some concluding remarks and future work.

II. Related Work

Many companies are on the search for solutions to improve their services, to reduce costs and to increase innovation perspectives. Therefore, NFV became an excellent option and thus a great number of researches from allover the world are working for its evolution. In parallel, SDN, as a solution to control the network has been increasing and it can act in consonance with the proposed NFV to give better conditions for implementing new solutions. The NFV is highly complementary to the SDN, but it is not dependent of this one (and vice and versa). SDN aims at dissociating the control plane from the data plane and it was projected as an architecture that uses a centralised control plane in order to ensure better scalability and agility for large networks. Several papers proposed techniques to overcome scalability limitation and they are being effectively implemented by companies looking for obtaining great benefits [4][6][7].

On the other hand, there is a motivation to face NFV and SDN's technical and business challenges with firm intention to clarify functions and interactions from several kinds of commercial entities that act on the market with such technologies. An example can be seen in a use case set shown by European Telecommunications Standard Institute (ETSI) [8].

As the industry closely keeps up with the evolution of these technologies , many have already addressed on the problem and they contribute offering subsides for a better understanding of possibilities from these innovations. From the moment the experiments left the academy and migrated to Wide Area Network (WAN); many use cases and challenges were presented. In this process, network operators were mobilised to disseminate the network virtualisation practice using the virtualisation efficient concepts already intensely adopted by Information Technology (IT) areas and hardware commoditisation for WAN application [9].

Also, considering ETSI's orientations [8] potential use cases were assimilated for the NFV, previously described. They affirm that SDN and NFV are two separated technologies; but, they overlap themselves, each one using the potential of the other one. The orientations mainly point out some challenges to be overcome for these technologies consolidations either on the networks' organisation side or on the IT side, specifically from the cloud.

There are many barriers for the SDN/NFV adoption, for example, the lack of patterns in some areas, the fact the applications have not been projected to be processed in the cloud, the need for interoperability with the infrastructure and legacy systems and others issues but nevertheless, there are high expectations regarding their use [9].

One of the first implementations for functional NFV's concept by means of the forwarding virtualisation function through an OpenFlow network deals with the current IPv4 and IPv6 coexistence and the possibilities brought for the arena by enabled OpenFlow infrastructure. The routing virtualised protocol project is described allowing a simple management and avoiding signalling message overload at the level of the control plane and also avoiding different scenarios considered in order to validate the virtualised function [7].

To help the researchers to accelerate the proposals, in 2014, UNIFY [10] project was born, that aim to open up the potential of virtualisation and automation across the whole networking and cloud infrastructure developing an automated, dynamic service creation platform; thus, leveraging a fine-granular service chaining architecture. This new solution has motivated researchers who will use soon a global orchestrator with optimisation algorithms to ensure optimal placement of elementary service components across the infrastructure. UNIFY launches the NIB (Network Information Base) concept that captures the network aspects and mounts a map of network and processing resources as well as their current state. Interacting with NIB, there are elements responsible for dynamically orchestrating network functions and resources.

Many aspects from the related work are considered on the proposition of the current use case in this paper. Other practises are revealed in other publications as the effort to implement SDN/NFV on Mobile Backhaul Networks. As a conclusion, platforms capable of enabling the SDN/NFV service that show the fact that uniting both these technologies is a current demand [1][2].

III. VPN Current Deployed Approach

Let us take an example a service, such as VPN, that allows to join corporate networks in different geographic localities.

The VPN service requires a very complex structure involving many equipments like switches routers, Firewalls, etc. In a typical VPN L3 scenario (RFC2547 - BGP/MPLS VPNs), a router is installed at customer facility and connected to the nearest border router or Provider Edg (PE) using a Time Division Multiplex (TDM). At the CPE side, separated

 ISBN: 978-1-61208-398-8

routing instances, named Virtual Routing Function (VRF) Lite (which is a logical way of segregating network traffic) handle voice and data traffic; QoS is applied accordingly. In a Metro Ethernet scenario, voice and data are carried using different Virtual Local Area Networks (VLANs) over an Ethernet link, using appropriate QoS marking. At the PE, each VPN has its own VRF (a separated routing table) which handles all the different user traffic. CPE management is accomplished using special policies that allow Management Servers to ping and get SNMP statistics without address conflicts [11].

Some customers require different CPE for voice and data whereas others require high availability or more flexible bandwidth management. A customer activation process is very complex due to the necessity of taking many steps for the effective service implantation: acquisition, installation, configuration and elements operation; also, the operator's team is trained in different owned hardware. The most bureaucratic and delayed activity is the Customer Premises Equipment (CPE) installation at the client's location. This last installation demands operator's time, client's time, adaptation of the structure that will receive the equipment (energy, temperature, cabling, etc.). An infrastructure example to supply this service is shown in Figure 1.

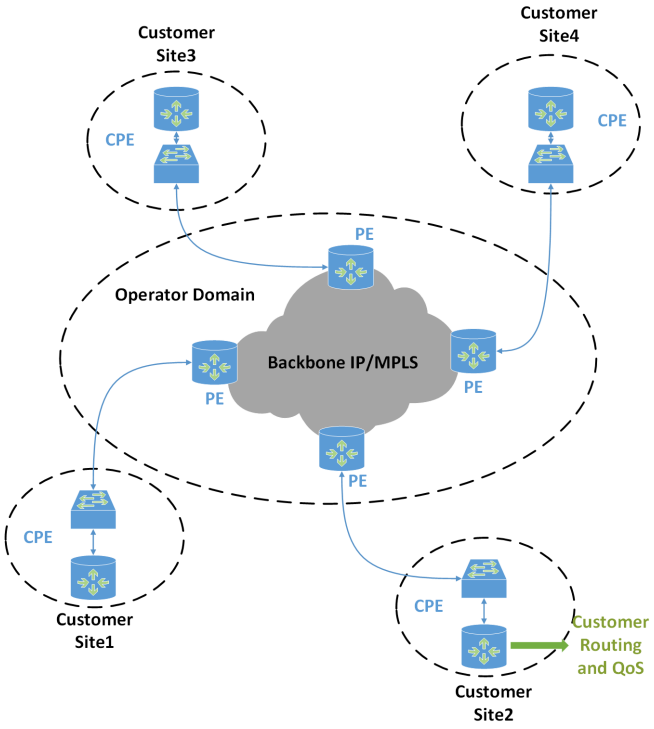

Figure 1. Current Infrastructure of a VPN Service

The image provides a superficial overview and without deepening in the elements we can identify a backbone network on MPLS, a Metro-Ethernet network and the client's CPE. The Multiprotocol Label Switching (MPLS) network, according to RFC 3031, is a framework that allows traffic flow forwarding and its efficient commutation through the network; this means, it is a switch entanglement controlled by MPLS that can supply a broad amount of traffic satisfactory. When it comes to the Metro-Ethernet network, it is a set of switches interconnecting in layer 2; so, by using only the Ethernet protocol [12].

Therefore, in order to have a dataflow from a branch of a certain client for another branch on a geographically separated locality, it is necessary the setting of several switches with different technologies. If in one of these switches the setting is incorrect, the service certainly does not work. The CPE is the equipment located at the client, providing a specific service, which, in this case, is the VPN tunnel and proper client's network routing. Beside both these functions, many others can be added, such as firewall, proxy, WEB server, etc.

The CPE has to be set at the client's location and it also requires maintenance. In case of this equipment's bad functioning, it directly affects the VPN. When VPN does not work, the process inside the operator is to change the CPE, and then, to reconfigure settings. This process has been happening routinely in many operators around the world and a big cost taken on by the operators are the activities in the customer's site to install, configure and mantains the CPEs. The value calculated for this operations is very high and compromises much of the revenue reducing considerably the profit of the carriers and consequently burdening the service value for the customers.

On other hand, due to the increasing costs of the TDM infrastructure, serial links have been gradually replaced by Metro Ethernet access in the last mile. Again, due to licensing costs, an additional switch performing L2 functions, which also provides path redundancy, has been added between the CPE router and the access ring, as shown in Figure 1.

IV. VPN Service Based on SDN and NFV

Taking advantage of SDN and NFV, this section presents a VPN service architecture which reduces service CAPEX and OPEX, and offers innovative functionalities to customers. Considering the most common used VPN service (as described in Section III), this work assumes the SDN/NFV implementation for a VPN service deployed on top of a ring Metro-Ethernet network.

By using virtualisation techniques, CPE functions were moved to the cloud, thus leaving a simpler and cheaper equipment at the customer facility. Handling user traffic would not be constrained by CPU and memory resources, since they can be added on demand, thus leaving room for more innovative services and a better response to the changing and unbalanced traffic (traffic optimisation).

As depicted in Figure 2, at the customer facility, the access switch is replaced by an OpenFlow capable switch. The physical router is removed and its function is virtualised at the *Cloud Router*.

Located at the telecom data centre, the *Cloud Router* is a new network entity. Each physical router is deployed as a virtual machine that runs the Quagga Software Route Suite [13] that provides implementations of Open Shortest Path First (OSPF), Routing Information Protoco (RIP), and Border Gateway Protocol 4 (BGP-4). Each virtualised router offers two Representational State Transfer (REST) based APIs. One is used by Operations Support Systems (OSS) in order to configure the service and its functionalities. This configuration can be done by the operator or by the customer.

 ISBN: 978-1-61208-398-8

The other REST API is used by the *SDN Control Layer* in order to query the *Cloud Router* about the routes and service updates. The *SDN Control Layer* is logically centralised at the operator backbone and is responsible to configure the OpenFlow capable switch accordingly.

Each instance of the *Cloud Router* will handle route exchanges with the PE, eg., RIP, OSPF and also will feed the *SDN Control Layer* with routing updates. The *SDN Control Layer* will handle QoS and NAT accordingly, applying match and action rules to each OpenFlow switch, as depicted in Figure 2.

Customer traffic is carried in a private VLAN tag which maps to a sub-interface on the PE side. This sub-interface belongs to the customer Virtual Routing and Forwarding (VRF) which stores all the routes from customer VPN remote sites. In order to exchange route updates the *SDN Control Layer* has a connection the the customer VRF. This can pose a problem if a single controller is used for different customers where Internet Protocol (IP) addresses overlap. However, this can be overcome by using a reserved IP range for management purposes, thus mitigating IP conflicts, and import/export policies in order to make management servers and CPEs visible to each other.

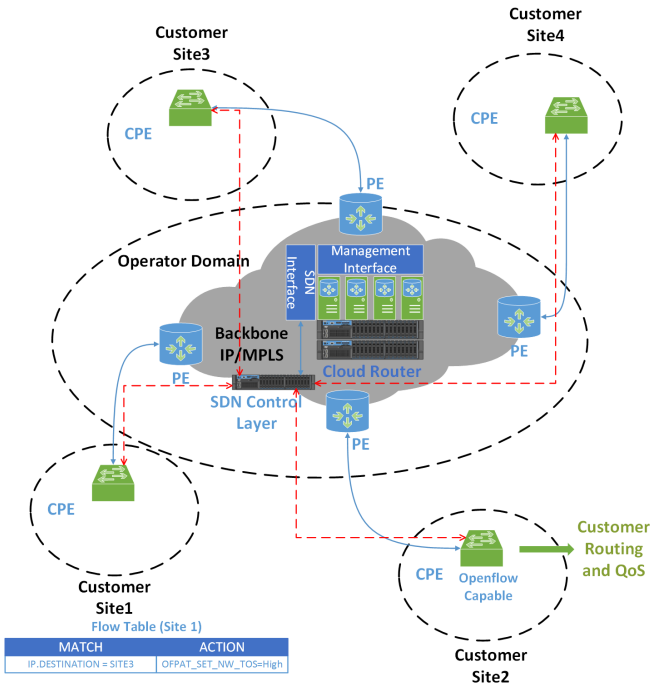

Figure 2. SDN/NFV VPN Architecture

Effectively, the customers stop having a router and can have a smaller device, which can be cheaper allowing them to reach the switch. The final product cost is reduced for the client, the operation becomes simpler, router installation and maintenance is eliminated and this brings huge benefits for the company and the final user.

In the traditional switch, we have the Control Plane that has the entire network intelligence and it owns each supplier. Since Data Plane will not change for the OpenFlow switch; only the smart part of the traditional switch will be centralised and the available protocols on the switch will give place to the OpenFlow secure channel keeping the Data Plane unaltered.

At the real world, a radical implementation is hardly used, thus, the most common way will be the coexistence of traditional protocols with the OpenFlow part on a hybrid composition. This allows this technology to treat the network's resilience, providing security and redundancy, as a result. The switch can support the OpenFlow, and, at the same time, the traditional protocols so the ring resilience to commutating when necessary can be done with the switch's traditional protocols, Spanning Tree, for example. Effectively, the traditional protocol can be used for commuting the ring resilience, and, at the same time, enabling the switch's port to implement the SDN.

To give a detailed vision, the topology containing the interfaces and modules is given below. The client's CPE (router) is virtualised at the central environment; in practice, it is implemented by a Virtual Machine (VM). This VM performs the functions originally executed for the proprietary hardware (routing, QoS, etc.). The details of the functional model that composes the Virtual CPE can be seen in the Figure 3, including the connections.

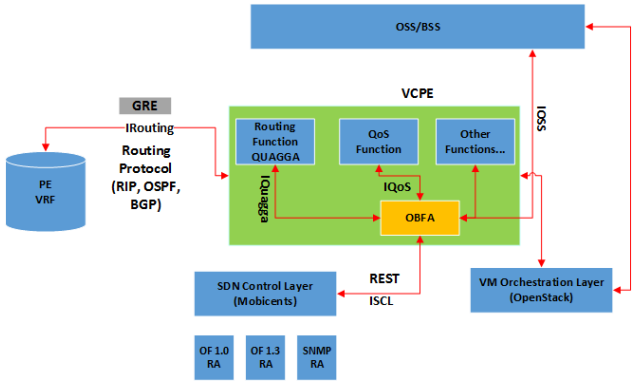

Figure 3. VPN Interfaces diagram

The Virtual Customer Router Function (VCRF) Module interacts with router PE from operator, by using the IRouting Interface and is responsible for exchanging of routes update messages. As the VCPE can be located in some network point not directly connected, a way is required to connect the VCRF to the appropriate PE, so that the routing protocol can establish its adjacency. In this case, the Generic Routing Encapsulation (GRE) is used. The VCRF interacts with the Orchestration and Business Function Aggregation (OBFA) Module trough IQUAGGA interface providing updated information of the routing table. With the respect to QoS requirements related to the client traffic, the module Virtual QoS Function (VQoSF) connected to OFBA Module is used.

The Module OBFA, based on the information received by the VCRF, VQoSF, and IOSS (Interface OSS) creates the suitable flows and communicates to SDN Controller using REST or Interface SDN Control Language (ISCL). Thus, the SDN Controller sends the configuration to the client's switch. The communication with OpenFlows switches is made by the Resource Adaptor (RA) that implements the version of the

 ISBN: 978-1-61208-398-8

protocol suported by customer CPE.

V. USE CASES

The VPN service described in Section IV enables innovative service offerings that can be provided to customers, by giving them the ability to take the control of the service, optimizing operations and reducing OPEX. This section highlights some use these offerings.

A. Quality of Service (QoS) Policies

By using the Management Interface, the customer can deploy different Quality of Service (QoS) policies. For example, let us assume that the traffic from Site 1 destinated to Site 3 will have a higher priority when compared to the traffic destinated to Site 2 or Site 4. The following steps can be run:

1) The customer indicate this policy at the *Management Interface*;
2) Upon modifications, using a REST API callback mechanism, the *SDN Interface* notifies the *SDN Control Layer*;
3) The *SDN Control Layer* translates these modifications to OpenFlow Actions;
4) CPE switch at Site 1 receives an OFPT_FLOW_MOD where the match field is the Site 3 destination IP with an action OFPAT_SET_NW_TOS in order to set DSCP field with a higher priority considering operator forwarding policies;
5) Traffic from Site 1 to Site 3 will be forwarded with higher priority accordingly to the carrier QoS policies.

The example illustrates how QoS policies can be applied to the service. It is important to notice that several other policies can be further deployed based on customer preferences in a programmable way, as long as the OSS system supports these new functionalities.

B. Network Address Translation(NAT)

Sometimes, it becomes necessary to modify the destination address of the packets coming from a particular site (Site 2 for instance) when destination server is out for maintenance (for example at Site 3). In this simple situation, we want to move traffic to an alternative server (at Site 4), momentarily, until the original server comes up again. Thus, we can use the strategy described below using the Management Interface:

1) The customer indicates the new policy at the *Management Interface*;
2) Upon modifications, using the REST API, the *SDN Interface* notifies the *SDN Control Layer*;
3) *SDN Control Layer* translates this new configuration to OpenFlow actions;
4) CPE switch at Site 2 receives an OFPT_FLOW_MOD where the match field is the Site 3 destination IP with an action OFPAT_SET_NW_DST in order to set IP Destination with the new IP address belonging to Site 4.
5) Traffic from Site 2 to will now be forwarded to new server at Site 4.

C. Multihoming Function

Let us consider a situation where the customer has an alternate router from other operator for backup purposes. This router will be connected to the Openflow switch and it will be used when Site 3 link fails, for example, and its network stops being advertised. In this case, the virtualised CPE from Site 2 will be notified by a Route Update message from the PE routing protocol, e.g., RIP, OSPF. When a Management program receives this event it will ask the SDN Controller from Site 2 (in our example) to set a new rule to deviate the traffic to a pre-defined backup Site (Site 4 for example, which also has an alternate connection), using the following steps:

1) Using a REST API the *Management Interface* communicates with the SDN Control Layer;
2) *SDN Control Layer* translates this context to OpenFlow actions;
3) CPE switch at Site 2 receives an OFPT_FLOW_MOD where the match field is the Site 3 destination IP with an action OFPAT_SET_NW_DST in order to set IP Destination with the alternate IP address belonging to Site 4.
4) Traffic from Site 2 to will now be forwarded to Site 4 using the alternate router.

VI. CONCLUSION AND FUTURE WORK

SDN was adopted by the research community and has had a considerable evolution. Besides this, SDN is present in the roadmap from various manufacturers. Concomitantly, NFV was also widely accepted and gained momentum, especially by applied research that can be exploited by telecom operators. These two promising technologies bring a number of benefits to end users, carrier networks and service providers being essential in innovative scenarios and demonstrating consistent results regarding the feasibility to implement these new solutions.

This work presented an implementation of a VPN service that is currently widely deployed by telecom operators. The service architecture detailed reduces CAPEX and OPEX and may be used to add innovative functions on top of this service, which can empower corporate customers, giving them the control of their service.

The paper also contributed with this research area by presenting to the community a solution deployed at a real telecom operator, thus, fostering NFV and SDN adoption, acting as a blueprint for a VPN service based on these technologies.

Future work will detail results presenting measurements regarding the service and functions in a production environment. Also, new use cases and functionalities will be created and detailed using the presented service architecture as a framework. From this, one can think in future studies aiming at the implementation of new cases and further use of new platforms, such as the recent UNIFY.

ACKNOWLEDGMENT

This work has been partially funded by ALGAR Telecom and the Brazilian agencies: CAPES, CNPq, FAPEMIG and PROPP/UFU.

 ISBN: 978-1-61208-398-8

REFERENCES

[1] N. McKeown et al., "Openflow: enabling innovation in campus networks," ACM SIGCOMM Computer Communication Review, vol. 38, no. 2, 2008, pp. 69–74.

[2] N. Feamster, J. Rexford, and E. Zegura, "The road to SDN: An intellectual history of programmable networks," SIGCOMM Comput. Commun. Rev., vol. 44, no. 2, Apr. 2014, p. 87–98.

[3] F. Schneider, T. Egawa, S. Schaller, S.-i. Hayano, M. Schöller, and F. Zdarsky, "Standardizations of SDN and its practical implementation," vol. 8, no. 2, Apr. 2014, p. 6.

[4] ETSI, "Network functions virtualisation - an introduction, benefits, enablers, challenges e call for action." Whitepaper, 2012.

[5] D. King and C. Ford., "A critical survey of network functions virtualization (nfv)," 2013.

[6] M. F. Bari et al., "Dynamic controller provisioning in software defined networks," in 2013 9th International Conference on Network and Service Management (CNSM). IEEE, 2013, pp. 18–25.

[7] J. Batalle, J. Ferrer Riera, E. Escalona, and J. Garcia-Espin, "On the implementation of NFV over an OpenFlow infrastructure: Routing function virtualization," in Future Networks and Services (SDN4FNS), 2013 IEEE SDN for, Nov. 2013, pp. 1–6.

[8] E. Group Specification. Network function virtualisation (nfv); use cases. [Online]. Available: http://docbox.etsi.org/ISG/NFV/Open/Published/gs_NFV001v010101p%20-%20Use%20Cases.pdf [retrieved: May, 2013]

[9] S. Perrin and S. Hubbard. Practical Implementation of SDN & NFV in the WAN. [Online]. Available: https://networkbuilders.intel.com/docs/HR-Intel-SDN-WP.pdf [retrieved: May, 2015]

[10] A. Császár et al., "Unifying cloud and carrier network: Eu fp7 project unify," in Utility and Cloud Computing (UCC), 2013 IEEE/ACM 6th International Conference on. IEEE, 2013, pp. 452–457.

[11] E. Rosen and Y. Rekhter. BGP/MPLS VPNs. Published: RFC 2547 (Informational) Obsoleted by RFC 4364. [Online]. Available: http://www.ietf.org/rfc/rfc2547.txt [retrieved: Mar., 2015]

[12] E. Rosen, A. Viswanathan, and R. Callon. Multiprotocol label switching architecture. Published: RFC 3031 (Proposed Standard) Updated by RFCs 6178, 6790. [Online]. Available: http://www.ietf.org/rfc/rfc3031.txt [retrieved: Jan., 2015]

[13] OpenSourceRouting. Quagga software routing suite. [Online]. Available: http://www.nongnu.org/quagga/ [retrieved: Mar., 2015]

 ISBN: 978-1-61208-398-8