A joint Vision on Network Virtualization

China Unicom & Telefonica

2013

A Joint Vision on Network Virtualization

OBJECTIVE

The key objective of the authors for this white paper is to outline the benefits and challenges for deploying on their networks the technologies based in the concepts of Software Defined Networks (SDN) and Network Functions Virtualization (NFV) and to encourage the industry in developing the solutions that the authors demand.

CONTRIBUTING ORGANISATIONS & AUTHORS

China Unicom: Dr. Xiaoyan Pei, Mrs. Xiaoxia Zhou, Mrs. Chuan Jia.

Telefonica: Mr. Antonio José Elizondo Armengol, Dr. Diego López, Mr. Francisco Javier Ramón Salguero, Mr. Santiago Rouco Rodríguez

PUBLICATION DATE

15-18 October 2013 at the "SDN and OpenFlow World Congress", Bad Homburg, Frankfurt, Germany

CONTENTS

Executive Summary

China Unicom and Telefonica recognize that Software Defined Networking (SDN) and Network Functions Virtualization (NFV) are enabling technologies that are going to play a critical role in the next generation of telecommunications and to transform the business economics of the Communication Service Providers (CSP).

Both technologies are highly complementary and, though can be deployed independently on each other, the promised impact on the transformation of the networks would be greater by an overall approach.

The goal of SDN is to separate the control plane from the data-forwarding plane in the network architecture. But making the control plan programmable throughout APIs like OpenFlow that allow a controller to define the behaviour of switches at the bottom of the SDN stack, and APIs that present a network abstraction interface to the applications and management systems at the top of the SDN stack, fuels the whole SDN concept, bringing more flexibility in how networks are deployed and managed.

The NFV goal is virtualizing network functions into software applications that can be run on industry standard servers or as virtual machines running on those servers.

Though there are lot of SDN and NFV uses cases that conceal great attention and efforts by the networking industry, the virtualization of the CPE, Customer Premises Equipment, is considered by the authors as one of the most promising use cases of Network Functions Virtualization technologies because of the relevant network architecture transformation that implies, since all network functions are shifted from

CPE to the network, which is expected to have also a high impact on the economics of the Telco's network operations.

Introduction

For the past years there has been a slow, methodical pace of change in networking where each set of new technologies arrives, surpassing the previous generation in an orderly fashion. The innovation cycle in the Telco industry has had to take up the standardization and equipment amortization cycles. But the challenges over the revenues by the new business models and the regulation, and the huge investments required to deploy technologies (e.g. LTE) ask for a disruption in the networking landscape that virtualization technologies may facilitate in the same way they have facilitated it in the Cloud.

Current limitations of Telco's networks:

- Long innovation cycles driven by standardization processes and the huge scale of investment required for introducing any innovation.
- Deployment of new services often requires re-architecting of the network.
- Hardware is bound to software:
    - Capacity is bound to each function.
    - Vendor's lock in that prevents switching from one vendor to another, when a technology is already deployed.
    - Services time to market is constrained by infrastructure life cycle
- Complexity of network management:
    - Each network has proprietary OSS.
    - Manual intervention usually required across many network layers.
    - Non-uniform semantics along the network.
- New network functions require new interoperability testing.

Network Virtualization Landscape

In a wide sense, the authors consider that Network Virtualization is a paradigm that is composed by two mainstream concepts: Software Defined Networks and Network Function Virtualization.

Software Defined Networks as defined by the Open Network Foundation is an *architecture that decouples the network control and forwarding functions enabling the network control to become directly programmable and the underlying infrastructure to be abstracted for applications and network services*[1]. So the behaviour of the network is not anymore hardwired as it has been till now, but guided by software. This concept means that a network is much more than the sum of each of the building blocks of the infrastructure that compounds it and this added value comes up from the software that defines the behaviour.

In summary, Software Defined Networking means:

- The behaviour of the network is defined via software.
- Separation of the control plane and the forwarding plane in different boxes, or different virtual instances, considering a fully virtualized environment.
- Easy interconnection of network functions.
- Orchestration of the interconnection.

Network Function Virtualization, as it has been stated in the seminal call to action whitepaper delivered by several CSPs in October 2012, Telefonica included, *involves the implementation of network functions in software that can run on a range of industry standard server hardware, and that can be moved to, or instantiated in,*

[1] https://www.opennetworking.org/sdn-resources/sdn-definition

various locations in the network as required, without the need for installation of new equipment[2].

NFV aims to break up the current network infrastructure architecture model, where building blocks are black boxes vertically (hardware and software functions) integrated by each vendor. This current model drives a hard vendor lock-in that has kidnapped the network innovation and new service delivery by the long lifecycle and slow pace of rigid roadmaps.

In summary, Network Functions Virtualization means:

- Separation of hardware and software.
- Providing network functions implemented by software.
- Use of general-purpose hardware.
- Management of the hardware resources as a pool of resources.

Why are both SDN and NFV technologies needed jointly by CSPs?

Transforming current CSP networks to achieve a flexibility and efficiency similar to the same achieved by cloud computing infrastructures requires having SDN and NFV technologies in place. NFV will decouple the network functions from specific hardware implementations to general-purpose hardware and will allow moving those functions to the most convenient location in the infrastructure.

But this capability won't address the networking requirements of the network functions themselves; namely, network functions must be interconnected in a proper way to deliver their service and the interconnections must remain the same way after being

[2] Network Functions Virtualisation – Introductory White Paper. http://www.tid.es/es/Documents/NFV_White_PaperV2.pdf

moved around. SDN technologies will be the tools to keep the proper networking for virtualized network functions on. Taking off the control plane from network boxes and moving it to a centralized controller will sweep along the connectivity logic of network functions while being reconfigured in an NFV infrastructure, avoiding a heavy burden currently quite common in network infrastructures.

As the previously mentioned whitepaper states, *Network Functions Virtualisation is highly complementary to Software Defined Networking (SDN), but not dependent on it (or vice-versa). Network Functions Virtualisation can be implemented without a SDN being required, although the two concepts and solutions can be combined and potentially greater value accrued.*

Which is the promise of Network Virtualization for Telcos?

Network Virtualization is not just about throwing away the vendor lock-in and the proprietary hardware; it is an opportunity to overcome many of the current limitations of the network infrastructures operated by telcos.

- It will make the infrastructure to be more uniform, shifting from dedicated boxes by network function to general-purpose high-end servers running network functions software.
- It will allow extending the same network for different services.
- It will provide flexibility to develop new services and will speed up the time to market of those new services.
- It will foster innovation and competition by opening up the technology vendor ecosystem to new agents.
- It will allow testing new network functions in a simpler way.
- It will allow better risk management in a changing and uncertain landscape.
- It will provide capabilities to increase capacity in an easy and flexible way.

Maturity level of Network Virtualization Technologies

The Open Network Foundation leads SDN standardization and the current OpenFlow specification is at version 1.3.2. But the main indicator of the maturity level of SDN is the widespread availability of products in the industry, not just from start-ups and industry challengers, but even by leaders of the networking industry and moreover the adoption of the technology by the CSPs or some of the big players of the internet industry as Google, that are deeply committed with SDN standardization.

Agile provision of connectivity in data centres is one of the use cases that receive more attention by the whole industry. Facebook has recently announced an open source switch project as part of its Open Compute Project that *will focus on developing a specification and a reference box for an open, OS-agnostic top-of-rack switch*[3]. Google uses a combination of Quagga open source software along with OpenFlow to optimize its data center interconnects[4] so datacenter-to-datacenter WAN successfully runs on an SDN enabled network.

On the other hand, NFV is a very recent concept, as it was formally described in 2012 and is in the early stages of standardization. Anyway several demonstrations of the base technologies have been available along the past years and some products are being recently announced as implementing network functions based on NFV concept.

Work Areas and Uses Cases

These two technologies come up with the promise of transforming the CSP networks and so the authors are contributing to the different ongoing standardization efforts and

---

[3] http://www.opencompute.org/2013/05/08/up-next-for-the-open-compute-project-the-network/

[4] Google: SDN based Inter-datacenter WAN using OpenFlow

want to encourage to the industry to achieve a fast development of the both technologies.

In this regards, the authors consider the following uses cases of high interest:

- ***Virtual IP Edge towards a Unified IP Edge:***

  The IP edge virtualization use case aims to propose a different paradigm of the access network. This new paradigm aims to leverage on unifying the IP edge of the network (e.g. BRAS, CG-NAT, GGSN, EPC, PE routers, etc.) to have a common pool of resources that can be used for playing the different IP edge functions, with enhanced efficiency taking advantage of the NFV solutions.

  This new paradigm will provide great benefits such as:

  - Making independent software and hardware installation
  - Making possible to deploy and configure a new "virtual node" in minutes
  - Moving into a new network functions architecture
  - Virtualization opens the door to operator differentiation

  The virtualisation of a mobile core network is a natural sub-case of the IP Edge virtualization, with just the mobile blocks (e.g. GGSN, EPC, etc.)

- ***Virtualization of the CPE (customer premises equipment):***

  ETSI NFV whitepaper points out *the virtualisation of services and capabilities that presently require dedicated hardware appliances on customer premises (home environment to small branch office to large corporate premises)*. This use case is closely related to the previous one, as the new access network architecture is based on the virtualization within the network of the layer-3 functionality. In this way, value added services (VAS) currently provided by the CPE can be clearly enhanced by offering layer 2 visibility within the access network, and home environment simplification aiming to shift all dispensable devices to the access network without lacking any functionality or service.

Due to the relevance of this use case for the authors, it will be considered in depth, in the next epigraph.

- ***Virtualization of Mobile Network***

  It is a fundamental tool for making the network manageable without precluding the incorporation of new technologies and features (CoMP, interference shaping,…). It may also be a tool for modifying (opening) the mobile network infrastructure ecosystem.

  The mobile network virtualization should address the following requirements:

  - Supporting mobility of network functions between different locations in order to adapt to different deployment options
  - Supporting different sets of functionalities by means of software over the same generic hardware

  The first step should be the virtualization of the base station and the radio access network.

  - Pooling base stations' baseband processing capabilities allows for supporting advanced features that require tight synchronization and/or the exchange of large quantities of information (e.g., quantized IQ signals)

- ***Virtualization of mobile backhaul***

  With the 3G and LTE deployment, more and more IP equipment are deployed to carry mobile backhaul service. In a local area, there might be more than thousands of IP equipment. It is very difficult to deploy and maintain such a huge IP network. The virtualization of mobile backhaul aim is similar to VCPE, simplifying the access equipment of mobile backhaul to a nearly hardware, the route, maintenance, deploying, etc. will be done in core routes, so the designing, planning, expanding, maintenance of mobile backhaul will be greatly simplified and the stability of network will be also improved.

Other areas and use cases such as deployment of SDN in data centres and virtualization of network control plane functions such as IMS, UDB, PCRF, etc. are hot topics, though the authors consider the previously mentioned uses cases of higher priority. Nonetheless, the networking industry is very committed with these approaches, and it is expected to deliver first serious deployments of these control plane functions on the following months, which will be useful for demonstrating network virtualization potential and obtaining significant savings in terms of Opex and Capex.

Network Virtualization is still something that it is necessary to mature and the authors recognize that it is a process that must be guided carefully to achieve the promises. In this regards, some of the challenges that this process may have to face are:

Avoid vertical integration while assuring performance

- It is needed to assure the hardware and software effective independence, avoiding the traditional vertical approach.
- The performance of software must be guaranteed in a predictable way and comparable to the performance of the current state of the art appliances.
- Software appliances (network functions) must be portable in the same way that software applications are in cloud environments.

Orchestration and management of the Network

The challenge for service providers is how they can build the experience for deploying network functions running on virtualized infrastructures instead on appliance hardware. But also achieve management systems that provide high performance and reliability at the data plane, solving issues such as deterministic resource allocation, exclusive network cards allocation, OS bypass, etc.

Foster a new ecosystem

The authors consider that the development of SDN & NVF technologies will transform the current ecosystem of cooperation between networking industry and CSP and the expected benefits will require the development of a new more flexible and open ecosystem; an ecosystem that will involve ISV (Independent Software Vendors) to provide differential network functions and deliver the innovation in the network through the competition.

Case of Study: virtual CPE

Because of the expected high impact onto the economics of the Telco's network operations, the virtualization of the CPE is considered by the authors as one of the more promising use cases of Network Virtualization technologies.

The authors consider anew access architecture based on the virtualization within the operator's network of the layer-3 home routing gateway functionality. This approach would translate into:

- CAPEX Savings. The operator will not only save on these installations but also in future HW upgrades for new services (IPV6 functionality, for example, can be added in the network and not in the home gateways).
- OPEX Savings. Operations will be simplified, as a simpler home gateway will have fewer incidences. The operator will have a complete Layer 2 visibility of home networks. SW upgrades will be done at operator's premises.
- Making easier the development and deployment of new services over the network.

vCPE Network Architecture

Current state of the art in home and access network architectures relies on a layer-3 device (the routing gateway) in home premises that performs different network functions, depending on the access technology (DSL modem, PON modem, etc.) and/or the services provided (Internet access, IPTV, VoIP, etc.). Such network functions comprises local NAT, local DHCP, IGMP proxy-routing, PPP sessions, routing, etc. This routing gateway is the base equipment for CSP services, enabling Internet access. Advanced services rely on deploying additional boxes at home(e.g. IPTV needs a set-top-box, generic VAS need a home gateway). This model, based on the installation of different devices in home premises, entails a high cost for service providers in both initial installation and operational support, as they are typically responsible for the end-to-end service.

This problem is even worse in PON deployments as nowadays its home premises modems, the ONTs, do not include layer-3 functionality themselves and delegate those in a separate routing gateway within the customer's premises. As a result, an additional box must be installed for fiber accesses.

The fact of having a new (layer-2) device in the home, the ONT, is a driver to propose a different paradigm for the home network. Since fiber deployments are in an early deployment stage, this could be the right moment for a disruptive breakthrough in the way broadband fiber services are delivered.

On the other hand, DSL services are usually bound to legacy CPE with very limited network functions that prevent the service provider capability of upgrading or providing new services, as IPv6 limitations of the current CPE installed base proves. A virtualized CPE would facilitate the provision of new services to customers with legacy CPEs, throughout virtualized network functions deployed at the IP edge and minimal reconfiguration of the legacy CPE.

The architecture proposal for home virtualization is based on the following requirements:

- Home and access networks should be layer-2 based networks with layer-2 visibility among them, where the need for routing gateways in the home network is suppressed.
- Installation and maintenance procedures should be simplified and Plug & Play client architecture should be achieved.
- Devices and services should have self-provision capabilities.
- Most (if not all) of the layer-3 network functions should be moved from the home network to the service provider network, and hosted in a pool of resources.
- Devices in the home network should have visibility among them to minimize the bandwidth usage in the access network.

In order to remove and virtualize the CPE functions from customer premises, all the necessary functionality has to be carefully studied and implemented within the network so the perception of the user is, at least, as good as if the physical home router would be at his home.

This new network access architecture will have a great impact on the different services.

Services within home

In vCPE Network Architecture, services interconnection within home will be greatly influenced. Some of the control signal within home will be route to network, but the service traffic will be required keep in home mandatory.

Internet service

The virtualisation of the CPE implies changes on the IP edge that will perform as a pool of resources and will receive most of the CPE functionalities, such as routing, firewall, Network Address Translation (NAT) functionalities, and IP address allocation.

Voice service

Voice service is partly affected by these changes. In this service, it's needed to consider two scenarios:

- Either it is required to support POTs as a legacy service, and then to have dedicated hardware for VoIP (i.e. IAD or ATA) in the remaining home gateway.
- Or it is possible to use SIP phones connected to Ethernet ports, and then it would be the IP edge the responsible for routing VoIP traffic to the VoIP core network.

IPTV and video services

IPTV service would experience significant changes in a vCPE scenario as well. For example, in some scenarios the IPTV service is provided over a different VLAN of the one used to deliver the Internet service. But in a vCPE scenario, there would not be an IPTV dedicated VLAN but an Ethernet VLAN shared among all Ethernet devices (e.g. Set Top Boxes), which would receive an IP address from the same DHCP. The virtualization of the CPE would open the possibility of the virtualization of other boxes such as the STB, extending the Smart TV concept.

Conclusions

In summary, all these ambitious efforts allow envisioning the networks of the service providers shifting towards a much more software-centric world and service-model partnership between SDN and NFV. Finally the authors encourage the networking industry to address all these new challenges. To accelerate progress, the authors are committed to contribute actively in the NFV ISG of ETSI and other standardization bodies.

Contact Information

China Unicom:

Mrs. Xiaoxia Zhou zhouxx1@chinaunicom.cn

Telefonica:

Dr. Diego López, diego@tid.es

Mr. Francisco Javier Ramón Salguero, fjrs@tid.es

Glossary

API	Application Programming Interface
BRAS	Broadband Remote Access Server
CAPEX	Capital Expenditure
CG-NAT / NAT	Carrier Grade Network Address Translation
CoMP	Coordinated Multi-Point
CPE	Customer Premises Equipment
DHCP	Dynamic Host Configuration Protocol
DSL	Digital Subscriber Line (typically ADSL2/+, VDSL2, G.fast)
EPC	Evolved Packet Core
ETSI	European Technical Standards Institute
GGSN	Gateway GPRS Support Node
IGMP	Internet Group Management Protocol
IPTV	IP Television
IPv6	Internet Protocol version 6
ISG	Industry Specification Groups
NAT	Network Address Translation
NFV	Network Functions Virtualization
ONT	Optical Network Termination
OPEX	Operating Expenditure
PE routers	Provider Edge Router
PON	Passive Optical Network
PPP	Point-to-Point Protocol
SDN	Software Defined Network

STB	Set Top Box
VAS	Value Added Services
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol