03

NFV & SDN INNOVATION STRATEGY AT ALTICE LABS

The NFV and SDN concepts are here to stay and significantly impact the communications industry, both in the operational and business dimensions. The adoption of these concepts will provide a significant evolution of the network, bringing with it a set of innovation opportunities and challenges.

Altice Labs is fully aware of this network paradigm evolution in all its technical dimensions and has been exploring these topics mainly through international collaborative RDI projects since 2010. Furthermore, in order to apply the obtained knowledge in the company business units, a process based on short-term Proofs-of-Concept, internally named as planned innovation, has been running in parallel with the RDI projects to evolve our products and solutions towards this new network paradigm. This article focuses on the description of the planned innovation activities, which were recently completed, in particular the virtual Home Gateway PoC, closing the 2010 – 2015 cycle of exploratory innovation through RDI projects, as well as on the description of the recently launched exploratory and planned innovation activities in which Altice Labs is involved towards the challenging 2020: the '5G'.

Rui Calé *(Cale@alticelabs.com)*
Pedro Neves *(pedro-m-neves@alticelabs.com)*
Mário Rui Costa *(MCosta@alticelabs.com)*
Carlos Parada *(carlos-f-parada@alticelabs.com)*
José Bonnet *(jbonnet@alticelabs.com)*

5G, IMT2020, LTE, NFV,
SDN, RAT, LTE, 3GPP, ITU

Introduction

The urge to increase significantly the operational efficiency in service delivery and the agility to create and manage new services lead the traditional communication service providers to begin the adoption of the cloud computing paradigm as a foundation to its service infrastructure [1]. In this context, standardization bodies like ETSI (European Telecommunications Standards Institute) [2] and ONF (Open Networking Foundation) [3] started to define new network and service architectures, using cloud computing to promote the evolution from traditional networks (built over traditional network appliances providing network functions over dedicated specialized hardware – *network ossification*), to new generation networks where the trend is to decouple network functions (software) from the supporting infrastructure and to deploy those functions in geographically distributed telecom data centres (*living networks*). It is the rise of NFV (Network Functions Virtualization) and SDN (Software Defined Networks).

NFV Overview

NFV aims to transform network architectures by implementing network functions in software that can run on common purpose virtualized infrastructure built on top of industry standard hardware. Benefiting from IT Cloud Management evolution, especially the evolution in VIM (Virtual Infrastructure Management) platforms (e.g., OpenStack), the evolution towards an NFV enabled service architecture will lead to the creation of a new service environment, built over a mesh of micro data centres, the new service platforms. These platforms, including advanced virtual infrastructure management platforms, will provide enhanced agility for new services creation and management, being also a contributor for costs reduction due to use of common purpose hardware.

At present time, the creation of a new service requires the setup of an engineering project to coordinate and govern the configuration of several distinct network elements (appliances) and the creation of specific service logic in proprietary service delivery and control platforms. Additionaly, the management of this distributed service intelligence over several network appliances requires the setup of complex management processes. All this together compromises the agility to launch new services.

The migration of service logic to software functions hosted by data centres, the VNF's (Virtual Network Function), will allow the service provider to reduce significantly the operational impact of launching new services. At first, developing a set of software components is, in principle, much more agile and fast than to create new functions in several network appliances (or to deploy new appliances altogether) and additionally will bring much more flexibility to create new functions. Second, but not least important, the virtual infrastructure management capabilities provided by the new service platforms will support through API's (Application Programming Interface) full automated management of the VNFs. This will not only contribute to implement automated management processes (deployment, provisioning, supervision, etc.) but will provide new tools that will streamline the implementation of new service management scenarios like service personalization, service optimization (e.g., service load dynamic adaptation, dynamic QoS management) and service healing (e.g., service replacement and /or reconfiguration to bypass anomalies).

On the other hand, this evolution movement will impose new requirements on the traditional operations management processes, creating the need to explicitly manage new service elements like virtual compute, virtual networking and virtual network functions.

Architectural details about NFV are given in NFV/SDN Architecture Standard Foundations section.

SDN Overview

SDN is another key emerging concept for future networks. SDN assumes the segregation of the Network Functions (NFs) control and data planes, being NF data forwarding process fully commanded by control-level applications through programmatic means (high-level APIs) abstracting the specific network details [4]. This way, the control intelligence resides on upper layer applications, whereas the packet forwarding procedures are kept on the data plane network elements.

SDN stimulate the centralization of control functions in SDN Control Applications, creating a new paradigm for data plane control. Due to the holistic network view, this new paradigm enables the enforcement of control decisions considering the end-2-end state of the controlled network infrastructure. This approach will bring additional flexibility and agility in network control when compared to traditional networks. Centralized SDN Control Applications also act as a central point for the data plane functions configuration, exposing API's for northbound clients such as the operational management processes, contributing in this sense to facilitate end-2-end service management over the controlled domains.

Architectural details about SDN are given in NFV/SDN Architecture Standard Foundations section.

NFV + SDN Key Advantages

NFV and SDN are not dependent on each other and can exist separately. However, the evolution to a virtualized network architecture (NFV) and the implementation of new service scenarios (e.g., personalization, optimization, healing) make SDN an indispensable partner to NFV.

The new service scenarios rely on dynamic and automated virtual network functions reconfiguration, scalability, and even migration between several service provider data centres.

Being a major factor for service enhancement, the network functions lifecycle dynamicity requires the ability to automatically reconfigure the connectivity topology linking the network functions. SDN responds to this challenge.

Additionaly, service personalization, one of the major service enhancements tipically associated with NFV is in fact leveraged on the top of the capability to dynamically and automatically create specific chains of network functions to associate to a specific user service context, a capability powered by SDN.

Architectural details about the combination of NFV and SDN are given in NFV/SDN Architecture Standard Foundations section.

State of the Art on NFV and SDN adoption

This movement is still in its early stages. Network solution providers do not have mature NFV/SDN value propositions and service providers are conducting some "proof–of-concept" (POC) initiatives in order to evaluate NFV/SDN technology maturity and gain insight to define their own NFV/SDN strategy. Altice Labs has been participating in several international RDI (Research, Development and Innovation) projects in the NFV/SDN domains, commonly refered as exploratory innovation, as well as conducting internal PoCs, also known as planned innovation, aiming to evolve our products and solutions towards this new network paradigm and create the necessary knowledge and insight towards an NFV/SDN enabled Service Provider.

This article is organized as follows: NFV/SDN Architecture Standard Foundations section provides the NFV and SDN architectural details. Thereafter, NFV/SDN Innovation Background section provides a short summary about the exploratory innovation background and provides detailed information about the internal PoCs that have been recently completed – virtual Home Gateway (vHGW) PoC, closing the 2010 – 2015 cycle of RDI projects. NFV/SDN Innovation Foreground dives into the future and describes the recently launched exploratory innovation activities (i. Edge computing, ii. Autonomic network management and iii. Network service agility through DevOps), as well as the planned innovation activities in which Altice Labs is involved in the NFV/SDN domains towards 2020. The article closes with a set of conclusions.

NFV/SDN Architecture Foundations

NFV Architecture Basics

The first basic step towards NFV is the "cloudification" of Network Functions creating what is so called Virtualized Network Functions. For this, the NF has to be implemented apart from specialized hardware, and be able to run on top of a cloud platform, using

COTS (Commercial Off The Shelf) standard hardware, as shown in Figure 1.

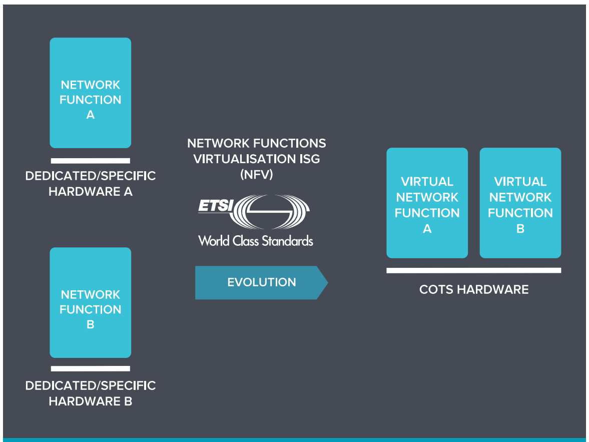
NETWORK FUNCTION A
DEDICATED/SPECIFIC HARDWARE A
NETWORK FUNCTION B
DEDICATED/SPECIFIC HARDWARE B
NETWORK FUNCTIONS VIRTUALISATION ISG (NFV)
ETSI World Class Standards
EVOLUTION
VIRTUAL NETWORK FUNCTION A
VIRTUAL NETWORK FUNCTION B
COTS HARDWARE

FIGURE 1 NF “Cloudification” Concept

Typical examples of VNFs are common routers or firewalls, but it can also be applied to mobile or fixed components, such as Packet Gateways (P-GWs), eNode-Bs (eNBs), Optical Line Terminators (OLTs) or even an entire architecture, like an Evolved Packet Core (EPC).

The “cloudification” of NFs can be further enhanced by using a complete management environment. In such case, the platform manages the entire lifecycle of VNFs, performing not just the deployment and disposal, but also managing the runtime operations, by migrating or scaling in/out VNFs, according to the function load requirements, leading to an efficient use of resources. Such platform is also able to orchestrate combinations of VNFs according to a given Forwarding Graph (FG), in order to create complex Network Services (NS).

Figure 2 depicts a simplified version of the full ETSI NFV architecture [2]. On the left side, it is shown the execution and control (runtime) operations, while the right side shows management and orchestration. The bottom left shows the “Virtual Infrastructure” (Network Functions Virtualization Infrastructure – NFVI), which comprises hardware resources (COTS), the virtualization layer, (e.g. KVM, VMware hypervisors) and the virtual resources (e.g. Virtual Machines - VMs, Virtual LANs - VLANs). VNFs run on top of one or multiple VMs and use network resources. On the top left, the “Management Support Services” (OSSs/BSSs) interact with the “Management and Orchestration” (right side) and with the VNFs. On the bottom right, the VIM (e.g. OpenStack) interacts with the “Virtualized Infrastructure” (hypervisor) to manage resources. On the top right, the “Orchestrator and VNF Management” module manages the complete lifecycle of VNFs and orchestrate NSs.

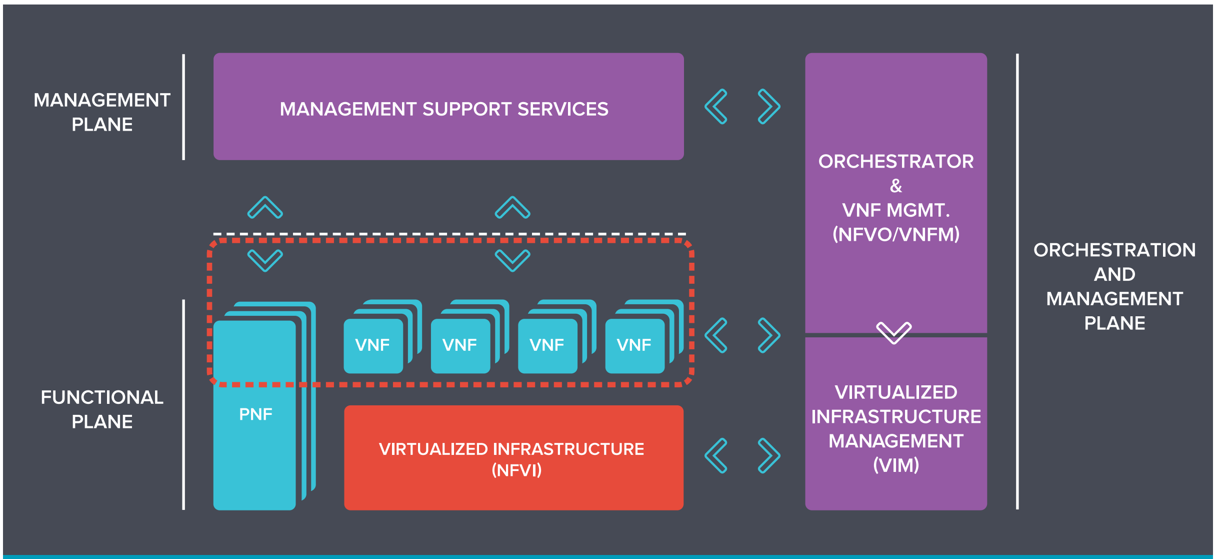
MANAGEMENT PLANE
MANAGEMENT SUPPORT SERVICES
FUNCTIONAL PLANE
PNF
VNF
VNF
VNF
VNF
VIRTUALIZED INFRASTRUCTURE (NFVI)
ORCHESTRATOR & VNF MGMT. (NFVO/VNFM)
VIRTUALIZED INFRASTRUCTURE MANAGEMENT (VIM)
ORCHESTRATION AND MANAGEMENT PLANE

FIGURE 2 ETSI NFV Architecture

SDN Architecture Basics

The SDN concept, promoted by ONF [3], intends to clearly split the network into 3 parts: the user-data plane, the controller plane and the application plane. The user-data plane is composed by basic switching Network Elements (NEs), responsible to forward the user traffic according to basic commands received from the north (controller) interface. The controller plane is an intermediate layer composed by SDN controllers, which provide basic commands to the south (user-data) and high-level APIs to the north (application plane). The application plane use high-level APIs provided by the controller plane to programme the network, simplifying and speeding up the creation of new services.

Figure 3 depicts the basic SDN concept, assuming in this case as the starting point an already virtualized network. Overall, the NEs forwarding process is fully commanded by the applications, which use high-level APIs provided by the SDN controllers. In turn, the SDN controllers interact with the NEs through low-level southbound APIs to enforce basic forwarding rules, using tools like Command Line Interface (CLI), Netconf (Network Configuration) or the most recent OpenFlow. The SDN controllers provide APIs which abstract the programmer from the network details, making simpler the network service creation. This is one of the key advantages of the SDN model.

NFV + SDN Architecture Combination

As NFV and SDN come from different standard organizations, at the time of writing this article, none of them had integrated the concepts into a single architecture. For this reason, herein we try

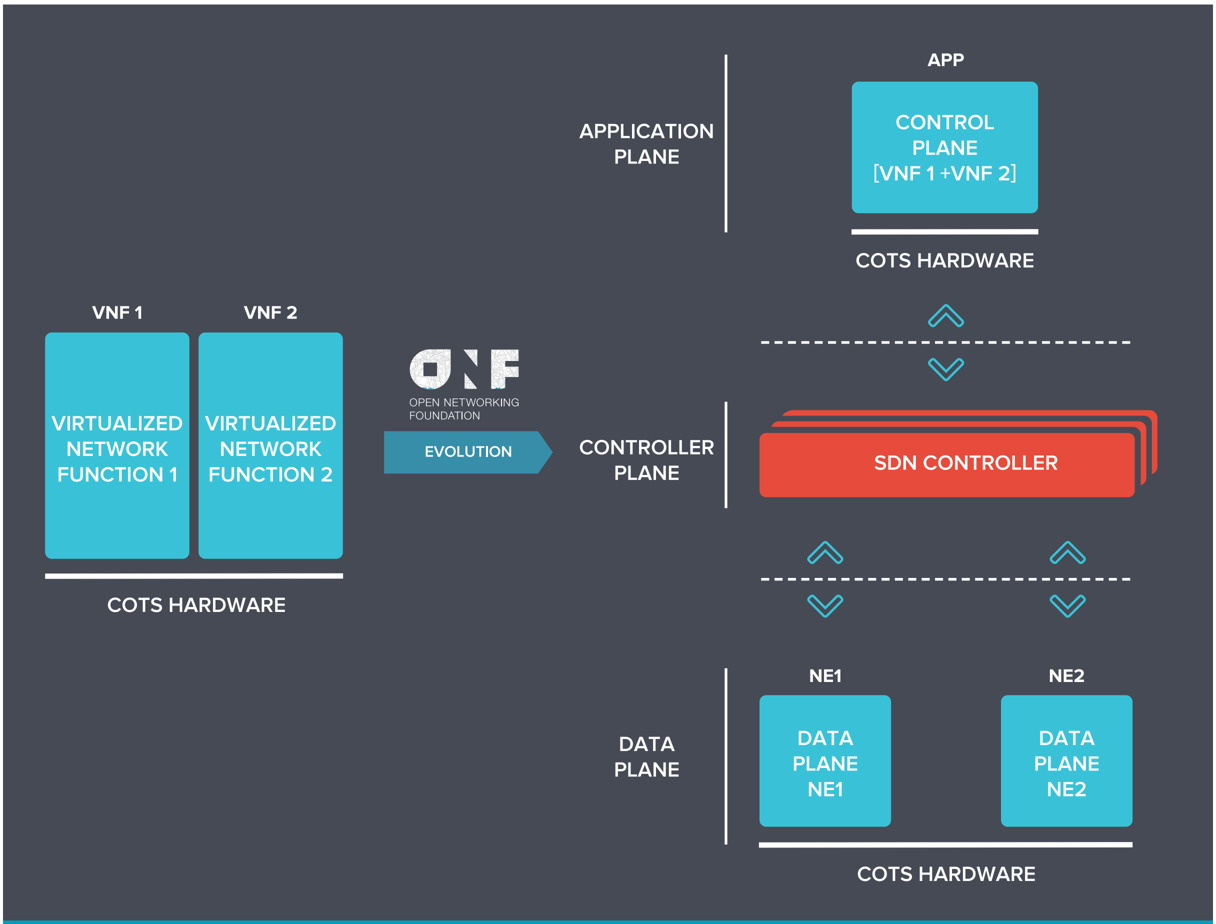

FIGURE 3 SDN concept

to provide our vision on a possible NFV and SDN integration, taking the ETSI NFV architecture as a starting point and introducing the SDN paradigm. Firstly, the NFV architecture, depicted in Figure 2, shows the VNFs (on the left part). Next, according to the SDN model, depicted in Figure 3, the monolithic VNF is separated into three parts (in this example a single control plane is used for both VNFs, whereas the data planes are kept separated). Finally, integrating both concepts, results in the architecture depicted in Figure 4 [5].

This integration is compliant with the architecture defined by the ETSI NFV. This integration requires a slightly different naming convention, as some pieces may have different names, depending on the (NFV or SDN) perspective. In order to consider "legacy" components (non-NFV, non-SDN), we kept the physical NFs in the leftmost side of the dashed red square of the architecture, meaning that we may have **Physical Network Functions** (PNF), which do not apply for the NFV and SDN models. In the same way, one may have VNFs, but with no SDN capabilities. For those, the **Virtual Network Functions** naming is kept, as shown in rightmost side of the dashed red square. In the middle, all NFV components are SDN-aware, meaning that they are split into three layers. In the bottom layer (user-data plane), one may have physical or virtualized Network Elements, which can be **Physical Network Elements** (PNEs) or **Virtual Network Elements** (VNEs), respectively. In this case, the names were chosen from the SDN world, since they describe the roles they are performing more clearly. On the controller layer there are the **SDN Controllers (SDN Ctrl)**, assuming here that we may have multiple controllers at different levels. Finally, for the upper part, the application layer, we used the naming **SDN Application** (SDN App). In this case, it is not specified whether it is virtual or physical, as it can be both. However, this layer will be mostly populated by virtual applications, considering that here there are no legacy boxes and hardware specific solutions will be declining.

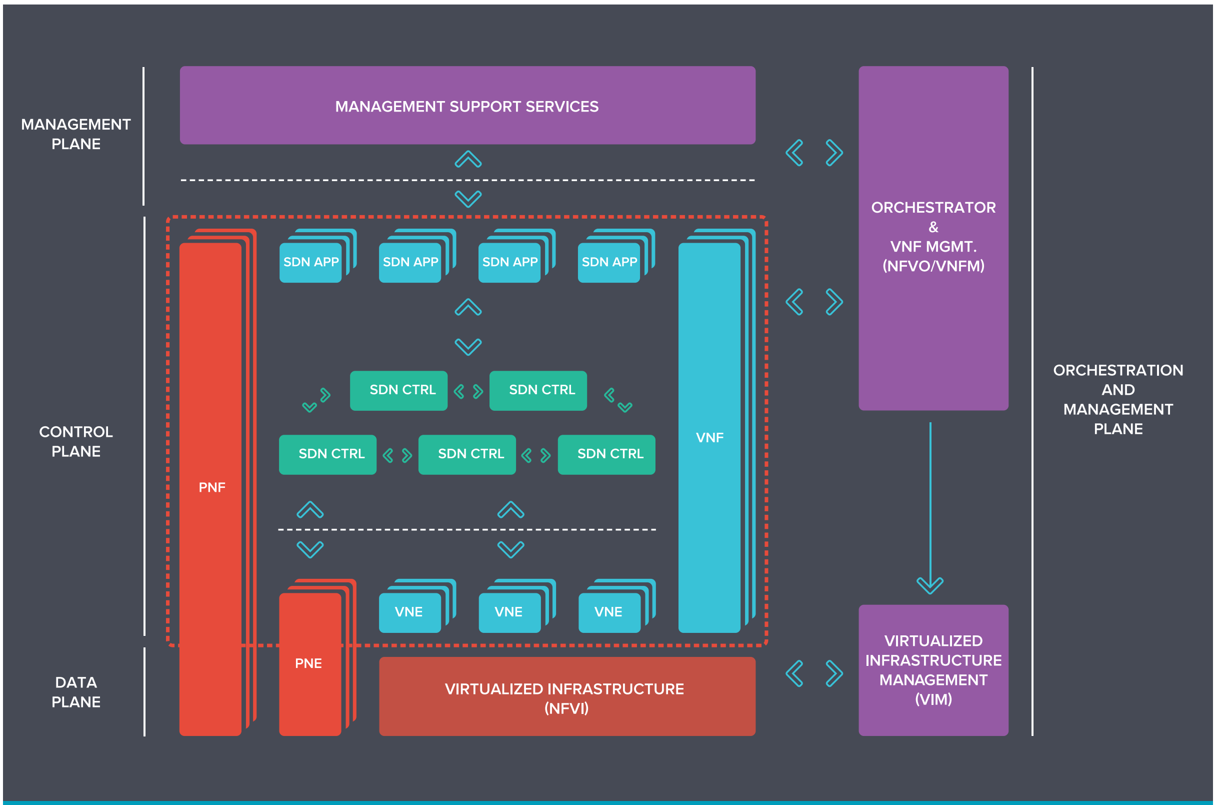
MANAGEMENT PLANE
MANAGEMENT SUPPORT SERVICES
CONTROL PLANE
DATA PLANE
PNF
SDN APP
SDN APP
SDN APP
SDN APP
SDN CTRL
SDN CTRL
SDN CTRL
SDN CTRL
SDN CTRL
VNF
PNE
VNE
VNE
VNE
VIRTUALIZED INFRASTRUCTURE (NFVI)
ORCHESTRATOR & VNF MGMT. (NFVO/VNFM)
VIRTUALIZED INFRASTRUCTURE MANAGEMENT (VIM)
ORCHESTRATION AND MANAGEMENT PLANE

FIGURE 4 NFV and SDN combined architecture

NFV/SDN Innovation Background

This section will briefly outline the RDI activities carried out in the NFV/SDN domains in which Altice Labs has been involved in the last years, as well as describe the recently completed internal vHGW PoC.

Exploratory Innovation

Altice Labs has been studying the network virtualization concept since the end of last decade through international collaborative RDI projects, mostly funded by the European Comission (EC).

Around 2008 we started to study the network sharing concept, nowadays known as network slices, on top of a common infrastructure through network virtualization. Each network is tailored to a particular user or application requirements and takes into account the characteristics of the available networking resources. This work was mainly carried out in the EU-FP7 Programme 4WARD RDI project [6].

In 2010 we started studying and prototyping the coexistence of legacy and new networks via virtualization of resources and self-management, fully integrating networking with cloud computing to produce the "cloud networking" concept. This activity was achieved through the EU-FP7 SAIL RDI project [7].

In 2012, and still prior to the ETSI NFV movement, Altice Labs studied the migration from current mobile networks towards a fully cloud-based mobile communications system, extending the cloud computing concept to support on-demand and elastic provisioning of novel mobile services (e.g. vRAN, vEPC, vIMS). This work was mostly carried out in the EU-FP7 MCN RDI project [8].

Finally, in 2014, and fully aligned with the ETSI NFV evolution, Altice Labs started to design and implement an orchestration platform for the automated provision, configuration and monitoring of network functions (e.g. vHGW, vSBC, vDPI) over virtualized Network/IT infrastructures, as well as exploiting and extending SDN platforms for efficient management of the network infrastructure. This RDI activity is still running within the FP7 T-NOVA project [9].

Planned Innovation: the vHGW PoC

ETSI has identified a number of use cases that unveil the potential of NFV together with SDN [10] and has been supporting PoC proposed by the Industry [11]. The reasons for implementing our own PoC are explained below, but the choice of a specific scenario depended on:

- What use case can we explore in order to:

a) Learn as much as possible about SDN and NFV;

b) Involve as many Business Units as possible in the PoC;

c) Get the attention of the organization ... while investing effort into something that is neither a product nor an research project?

- How can we actually do it?

Motivation

Figure 5 illustrates the rationale that led to the choice of a vHGW as the PoC scenario:

1. Former involvement in exploratory projects [8] [9] showed that NFV and SDN were promising technologies. Competences had been acquired and industry trends called for further trials and validation;
1. The acquired knowledge on SDN and NFV showed that it will bear strong impact to areas of interest to Altice Labs Business Units, namely on products and solutions in the areas of Network Systems, Services, Service Control and OSS;
1. Residential Business was identified as a particularly challenging (and visible) area:
    - High operational costs (e.g. truck rolls) can be cut if the complexity of the home scenario is reduced and if the operator gains more visibility into the home network;
    - The deployment of new, differentiating, services to the residential Internet access clients is strongly boosted by SDN and NFV;
    - High cost of the access network and

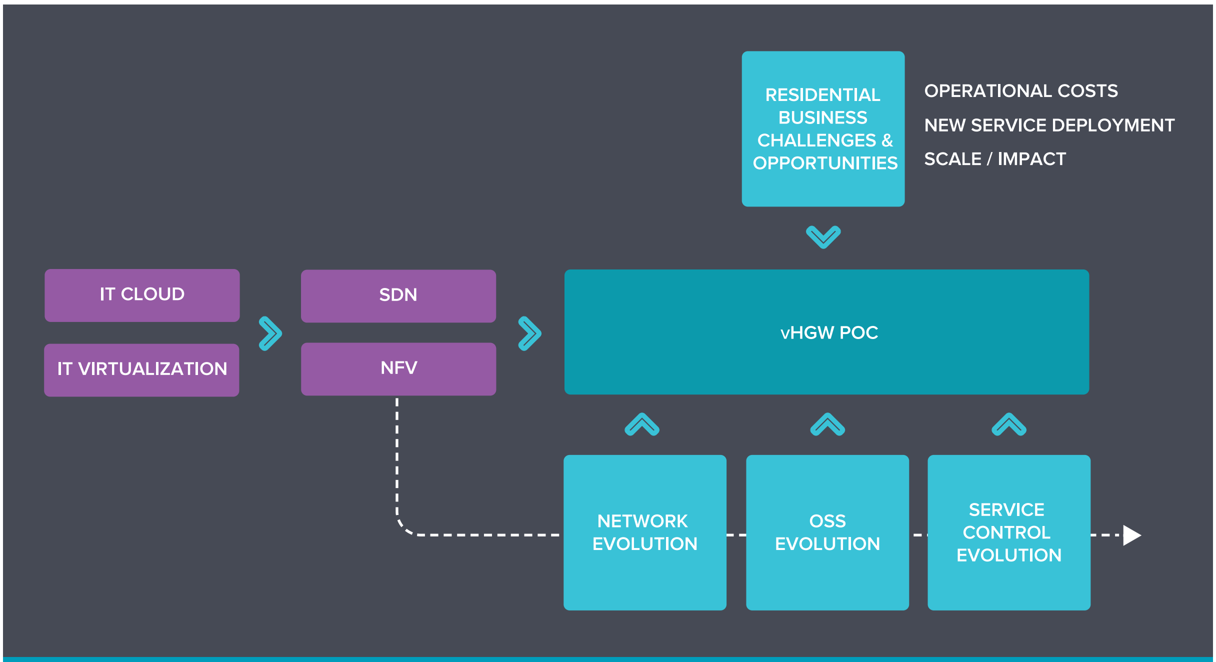

FIGURE 5 vHGW PoC rationale

home infrastructure guarantees that a PoC related to the possibility of saving money in this area gets the attention of the organization;

1. As a result of 1., 2., and 3., the idea of implementing a PoC that addressed the virtualization of the HGW came naturally, as a planned innovation project, building on the results of exploratory innovation projects and on the needs of the Business Units.

To keep the PoC within a feasible scope, the services evolution area has not been addressed at this stage. A particular service has been elected for the PoC: High Speed Internet (HSI).

As a result of all this, the PoC initial goal was fixed in setting up a scenario where specific HGW functions like Firewall or Parental Control could be run on a remote data centre and personalized using a common Self-Management Portal.

PoC Technical Goals

The overall scope of the PoC was limited, keeping a principle of short runs with visible results which were called “PoC Phases”, with limited and well defined scope:

Phase 1

- Extending the home network broadcast domain to the data centre;
- Implementing a virtual infrastructure in the data centre;
- Migrating HGW functions to the virtual infrastructure in the data centre;
- Implementing software defined service chains;
- Performing basic orchestration;
- Allowing basic self-management, with per device personalization (one device = one user);
- Implementing the mechanisms to support seamless session establishment and self-configuration activities.

Phase 2

- Enabling policy-driven service chaining;
- End-2-end service activation, encompassing integrated provisioning of physical network functions and of virtual network functions;
- Enhanced personalization. Per service per user configuration;
- A first approach to mobility across households.

Phase 3+

Further phases are described in the end of the next section.

PoC Technical Description

Herein the detailed technical aspects of each one of the PoC phases is described.

Phase 1

As a first approach to a PoC for a vHGW, a minimum scenario was established as illustrated in Figure 6.

Home Domain: To setup a home network domain, an Altice Labs ONT RGW (Optical Network Terminator Remote Gateway) was used. RGW functions like Routing, NAT (Network Address Translation) or Firewall were stripped out, and the equipment was left with a minimal set of capabilities, those related to the local Wi-Fi AP and the L3 functions needed to establish and keep a GRE (Generic Routing Encapsulation) tunnel to the data centre.

Data Centre PoP: A virtual infrastructure was built, relying on COTS Hardware and open-source software, namely:

- Hypervisor: Linux KVM (Kernel-based Virtual Machine);
- Switching: OVS (Open V Switch);
- SDN Controller: ODL (Open Day Light);
- Virtual Infrastructure Manager: OpenStack.

Adjustments were made to ODL to support the chaining of functions that were required.

A homebrew orchestrator with the NFVO role was adopted.

Two open-source, off the shelf functions were “elected” to be run on the PoP, on a per-household virtual environment, as VNFs:

- Firewall (Alpine Linux);
- Parental Control (DAN’s Guardian).

NAT and DHCP (Dynamic Host Configuration Protocol) for the home network were ran from OpenStack.

A self-management portal was built to support the demonstration of the PoC, featuring the personalization aspects that highlight the possibilities of the scenario.

Access Network and Transport: In a first approach, access network features were left out of the PoC. ONT/OLT/BNG configuration was statically prepared to setup a tunnel between the home domain and the data centre.

Service Control: Altice Labs AAA product was used as a combined DHCP+AAA server for authenticating, authorizing and managing IP addresses for the ONTs. Another instance of Altice Labs’ AAA was used as a

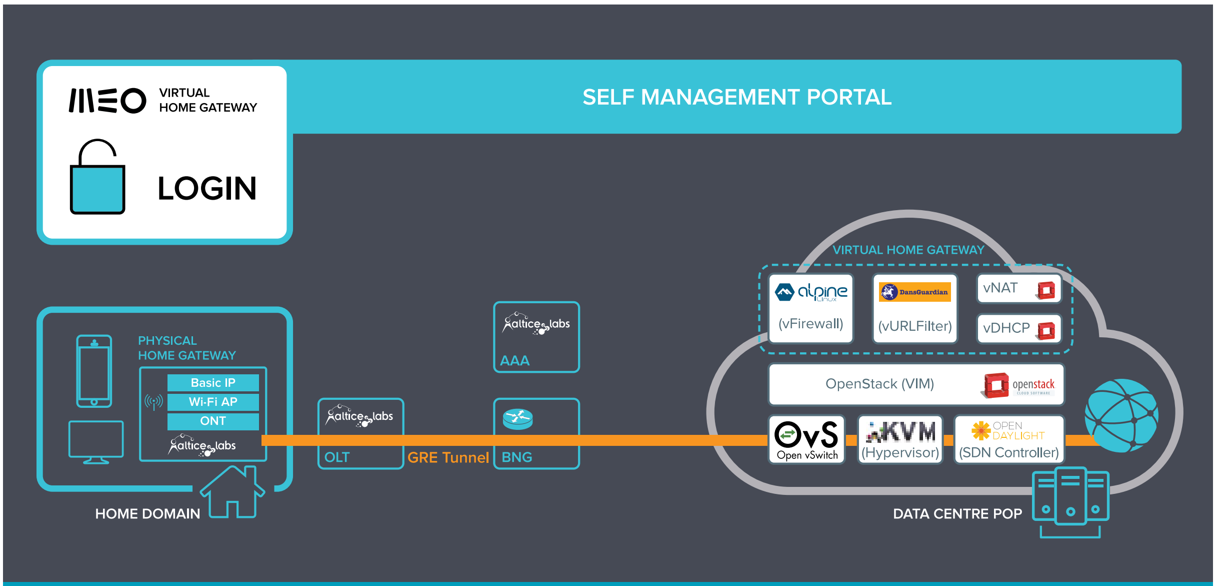

FIGURE 6 PoC phase 1

centralized transparent authorization endpoint for user sessions, keeping the chain configuration and attachment status of devices, to be read/written by the portal and queried by the DHCP server. Both AAA servers generate notifications to the orchestrator.

Management: In phase 1, a strictly functional approach was tried. No managerial issues were involved, apart from the user's self-management of the Internet access service.

For the phase 1 demonstrator, an authenticated home network user was able to:

- View the attached devices;
- Block access to a particular device (MAC);
- Characterize a device and assign it to a user;
- Configure functionalities for the user/ device (different service chains were chosen according to the selected functionalities – URL filtering for Parent Control, service blocking using Firewall).

Phase 2

Figure 7 illustrates the PoC phase 2.

For phase 2, two major developments took place:

- **Service Control:** A policy-driven approach to service chaining was developed, including:
  - **Subscriber and Policy Repository:** to keep the information that is needed for policy enforcement;
  - **Policy Server:** to determine what policies to apply based on context and subscription information. Controls a Classifier, a Traffic Accounter and a Traffic Shaper to enforce policies regarding service chain selection, gating and QoS control;
  - **Classifier:** Deep packet inspection of traffic allows the classification of service flows;
  - **Traffic Accounter and Traffic Shaper:** VNFs that are controlled by the Policy Server, to count traffic and to enforce QoS rules;
- **Management:**
  - **Service Activation:** NFV orchestration and the "traditional" fulfillment activities were combined into a "Multidomain Service Activator" in charge of coordinating configuration across all platform;

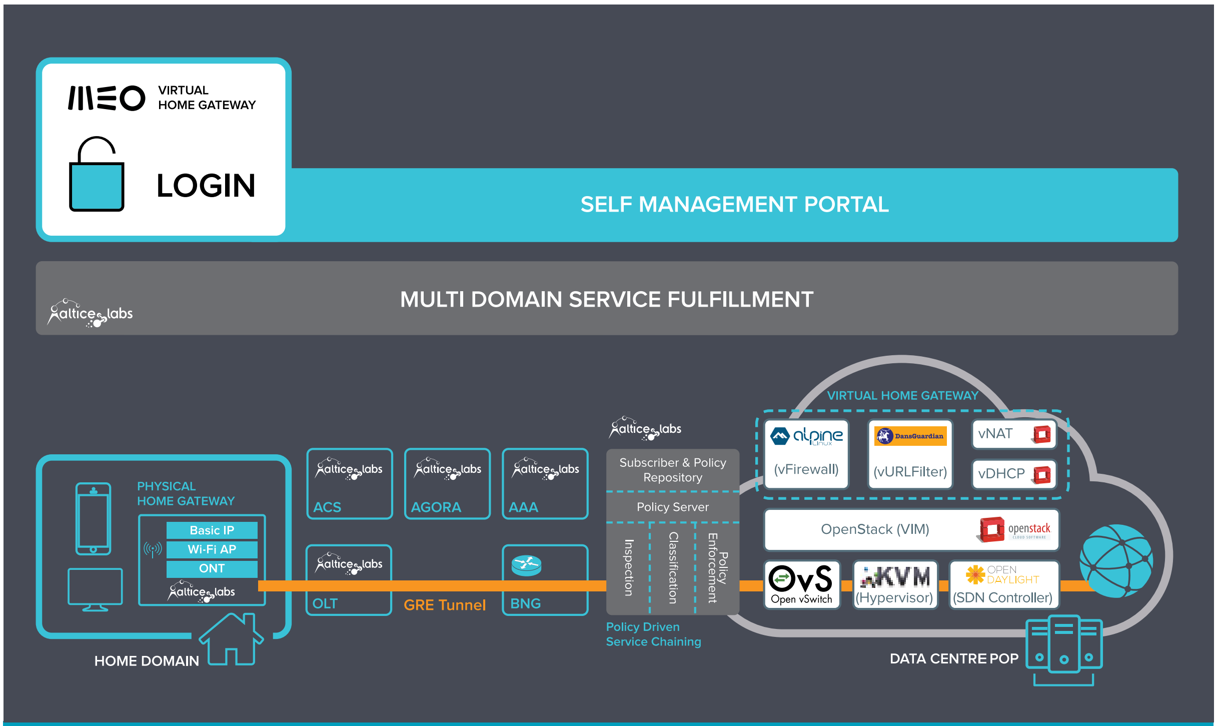

FIGURE 7 PoC phase 2

- **Self-Management** portal was enhanced with per user configuration capabilities and session context awareness.

NFV/SDN Innovation Foreground

This section describes the NFV/SDN domain innovation activities for the upcoming years. In detail, the major NFV/SDN related RDI activities are highlighted in the next section, whereas the subsequent section depicts the NFV/SDN related planned innovation roadmap.

Exploratory Innovation

This section describes three major RDI areas that will be impacted and significantly evolved due to the adoption of the NFV/SDN networking paradigm. These areas are: i. autonomic network management, ii. network services agility through DevOps and iii. edge computing. Altice Labs is actively working on these areas under the scope of the Horizon 2020 programme RDI collaborative projects.

Autonomic Network Management

The current networking paradigm, illustrated in Figure 8, poses a number of challenges to network operators, in particular, the management of anomalies and upgrades in the regular behaviour of the network are one of the main sources of increasing both capital and operational expenditures. Nowadays, operators have to do their best to detect and mitigate all sorts of problems in the networks, such as link failures, performance bottlenecks, security attacks, QoS degradation, software bugs, and hardware faults, among others. Existing solutions typically require manual re-configuration of the equipment, and in some cases, the only solution is the installation of new equipment and functionalities such as routers, NATs, firewalls, intrusion detection systems, load balancers, probes, etc. These tasks cannot be performed without affecting even for limited time the normal operation of the network. This causes disruptions in the services and violations in SLAs (Service Level Agreement), thereby incurring in increased operational and capital costs and compromised end users' QoE (Quality of Experience).

Research in recent years in the area of SDN and NFV has resulted in the emergence of new capabilities

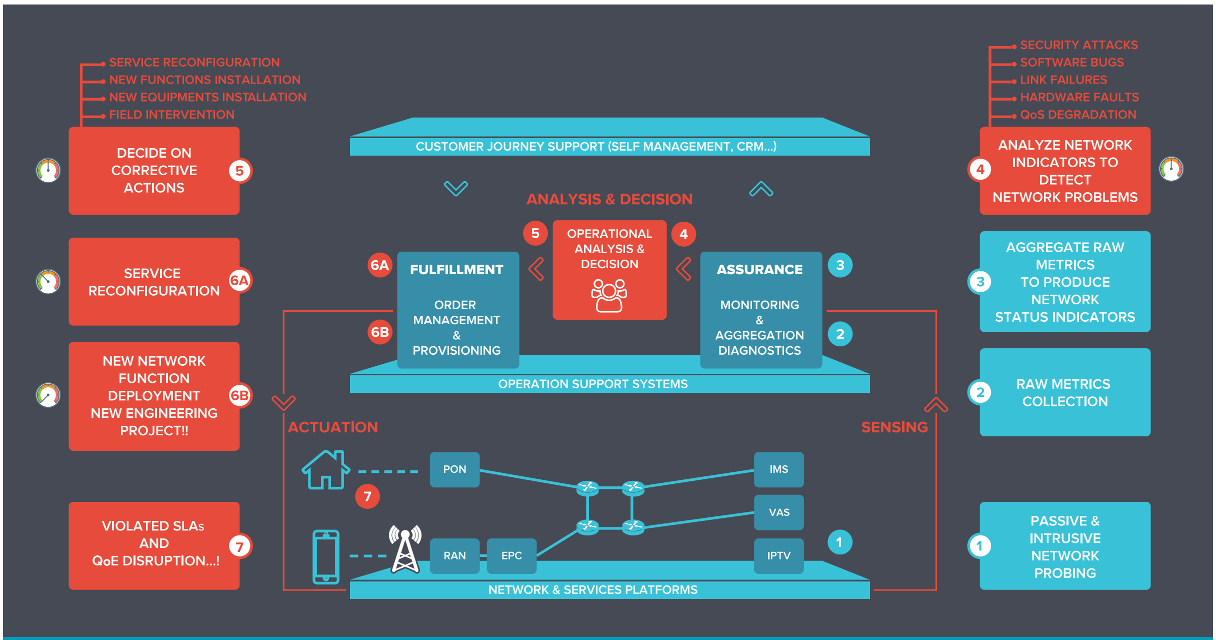
SERVICE RECONFIGURATION
NEW FUNCTIONS INSTALLATION
NEW EQUIPMENTS INSTALLATION
FIELD INTERVENTION
DECIDE ON CORRECTIVE ACTIONS
5
SERVICE RECONFIGURATION
6A
NEW NETWORK FUNCTION DEPLOYMENT NEW ENGINEERING PROJECT!!
6B
VIOLATED SLAs AND QoE DISRUPTION...!
7
CUSTOMER JOURNEY SUPPORT (SELF MANAGEMENT, CRM...)
ANALYSIS & DECISION
5
OPERATIONAL ANALYSIS & DECISION
4
6A
FULFILLMENT
ORDER MANAGEMENT & PROVISIONING
6B
ASSURANCE
MONITORING & AGGREGATION DIAGNOSTICS
3
2
OPERATION SUPPORT SYSTEMS
ACTUATION
SENSING
PON
7
RAN
EPC
IMS
VAS
IPTV
1
NETWORK & SERVICES PLATFORMS
SECURITY ATTACKS
SOFTWARE BUGS
LINK FAILURES
HARDWARE FAULTS
QoS DEGRADATION
4
ANALYZE NETWORK INDICATORS TO DETECT NETWORK PROBLEMS
3
AGGREGATE RAW METRICS TO PRODUCE NETWORK STATUS INDICATORS
2
RAW METRICS COLLECTION
1
PASSIVE & INTRUSIVE NETWORK PROBING

FIGURE 8 As-Is Network Management Paradigm – Human-based, Machine-assisted

that significantly improve the agility, flexibility and cost efficiency to manage network functions. These capabilities are the foundations to trigger a paradigm shift in the way network operations are planned and deployed, called autonomic management – Figure 9.

This new management approach will explore SDN, NFV and cloud computing technologies, together with innovative algorithms, to achieve a highly intelligent paradigm for smart self-management of complex networking scenarios.

One of the main impacts of introducing autonomic capabilities is to significantly reduce the operational costs directly related to the management of the network. Essential network management tasks are automated, which will enable remarkable reduction in the complexity of the network management, currently being manually conducted. Proactive and reactive actions are automated in order to resolve/mitigate networking problems, thereby minimizing the current labour-intensive maintenance and troubleshooting tasks for network operators, leading to more significant decrease in OPEX.

In order to provide a fully-automated and highly intelligent autonomic management system, three key properties must be addressed by the architecture. The first one is related with **automated network monitoring**. The architecture should enable the automatic deployment of NFV applications, typically known as probes or sensors, in the network infrastructure to facilitate system-wide distributed monitoring. These virtual applications are spread across the access and backbone network infrastructures to enable end-2-end user, service and network awareness through the collection of metrics from all required elements in the network architecture. The collected information must feed data analysis algorithms (e.g., data analytics, data mining, machine learning) in order to create key indicators that may translate to (1) service affecting conditions (network failures, performance bottlenecks, security braches, intrusions, etc.),

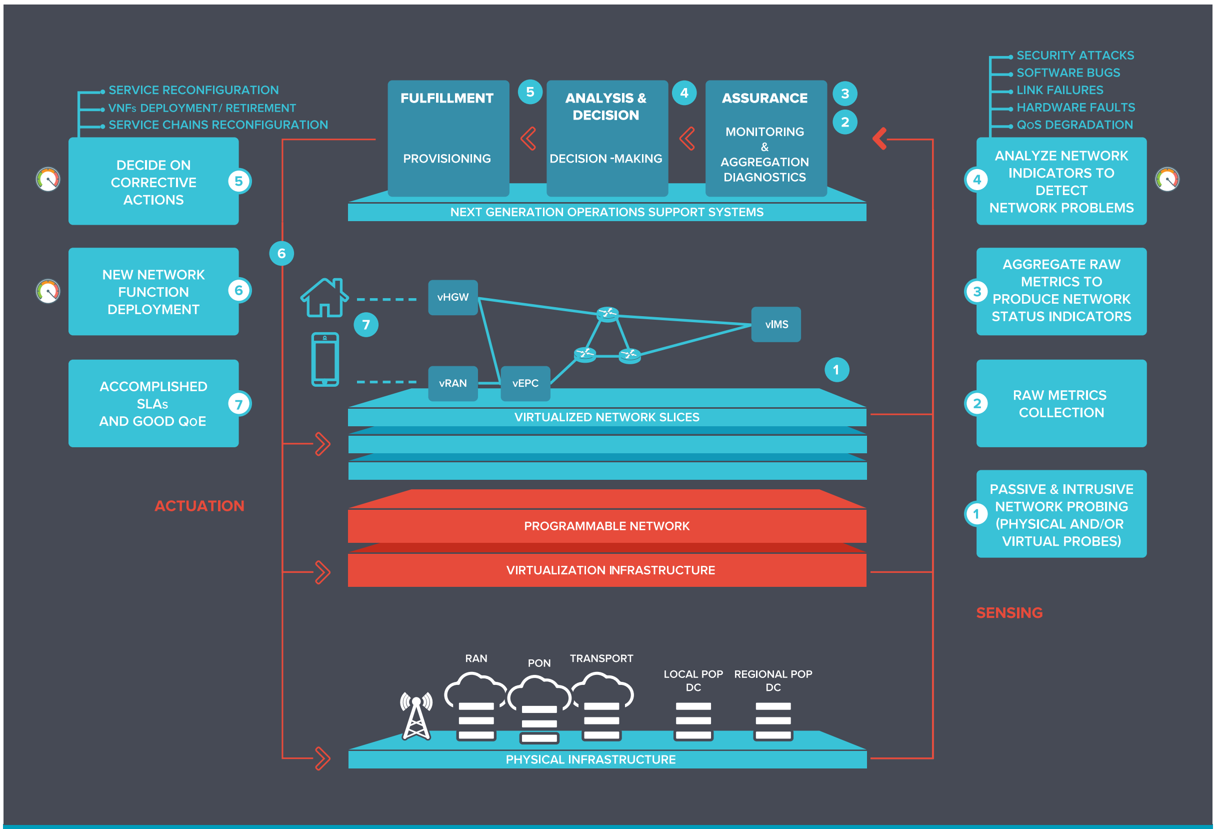
SERVICE RECONFIGURATION
VNFs DEPLOYMENT/ RETIREMENT
SERVICE CHAINS RECONFIGURATION
DECIDE ON CORRECTIVE ACTIONS
5
NEW NETWORK FUNCTION DEPLOYMENT
6
ACCOMPLISHED SLAs AND GOOD QoE
7
ACTUATION
FULFILLMENT
PROVISIONING
5
ANALYSIS & DECISION
DECISION -MAKING
4
ASSURANCE
MONITORING & AGGREGATION DIAGNOSTICS
3
2
NEXT GENERATION OPERATIONS SUPPORT SYSTEMS
6
vHGW
7
vIMS
vRAN
vEPC
1
VIRTUALIZED NETWORK SLICES
PROGRAMMABLE NETWORK
VIRTUALIZATION INFRASTRUCTURE
RAN
PON
TRANSPORT
LOCAL POP DC
REGIONAL POP DC
PHYSICAL INFRASTRUCTURE
SECURITY ATTACKS
SOFTWARE BUGS
LINK FAILURES
HARDWARE FAULTS
QoS DEGRADATION
4
ANALYZE NETWORK INDICATORS TO DETECT NETWORK PROBLEMS
3
AGGREGATE RAW METRICS TO PRODUCE NETWORK STATUS INDICATORS
2
RAW METRICS COLLECTION
1
PASSIVE & INTRUSIVE NETWORK PROBING (PHYSICAL AND/OR VIRTUAL PROBES)
SENSING

FIGURE 9 NFV/SDN-ready Network Management Paradigm – Machine-based, Human-assisted

(2) conditions thay may evolve to service affecting conditions in the future, (3) non optimal service delivery to specific users, i.e., detection of situations where the service topology being used to deliver a service to end users can be optimized in order to minimize the resources being used or the service QoS. Packet inspection tools such as intrusion detection systems, selective packet processing tools, user profiling tools and network monitoring tools are some examples of software used to gather measurements to derive these high-level metrics.

The second key aspect that must be fulfilled by the new management architecture is the **autonomic network maintenance**, i.e., the ability to define high-level tactical corrective and preventive measures to respond to the diagnosed conditions. These tactical measures may correspond to reactive actions of the network in response to fix/mitigate existing network issues of various kinds, or may correspond to proactive actions to prevent the evolution of the diagnosed condition to an effective anomaly affecting services. These actions may be mapped to request for automated configuration, scalability, migration of existing VNF's, the deployment of new VNF's or the reconfiguration of services' connectivity logical topology.

The combination of automated network monitoring with the automated network maintenance is the backbone of the autonomic service management, contributing to maximize the chances of sustaining the healthy operation of the network (and services) enabling intelligence-driven responses even in scenarios unknown *a priori* and without requiring human decisioning and intervention.

Finally, the third key feature is the **automated and dynamic service provisioning** taking into account not only the service type characteristics but also the status of the network architecture. This comprises dynamic smart selection of the best locations where the services should be deployed (or migrated to) considering the requirements associated with the specific service instance being provisioned (for instance the contracted QoS) but also the key indicators produced by the automated network monitoring applications that translate the network health (anomalies, performance), in order to guarantee that the provisioning of new services also contributes to maintan the required levels of network performance, health and security.

This research activity is currently being addressed in the EU-H2020 SELFNET RDI project [12].

Network Services Agility using DevOps

Nowadays, deploying a Network Service may imply lengthy hardware procurement processes, as well as usually complex 'hand-over' of the newly developed service to the operations team and acceptance tests that depend also on the knowledge handed over from development teams and the hardware availability. This is even worse when further activities like training affects many employees, for which training environments have to be put in place, increasing even more the network services' time-to-market.

Two recent trends dramatically change this: on one side, the above mentioned NFV/SDN, which enables the quick (re-)configuration of the network, to accommodate new services, and a merge of the software development and operations teams, known as DevOps, which eliminates the hand over time gap mentioned above.

Furthermore, a collection of objectives implying improvements in Telecommunications set for 2020, known collectively as '5G', also address this, namely to dramatically reduce the time-to-market of new services ('from 90 days to 90 minutes'). Telecom operations must thoroughly review its processes in order to be in line with this objective. '5G' also strongly pushes into significantly lowering barriers to entry of service developers/providers, not necessarily coming from infrastructure providers, which means that Telecoms will probably have to open their infrastructures to these new service providers, without negatively affecting services already deployed.

These '5G' drivers, together with the NFV and SDN trends, lead Altice Labs to rethink development and operations internal processes, namely with the objective of making them more agile.

DevOps is a set of procedures, tools and techniques that allow organizations to dramatically streamline software development and operations (hence the name) processes, by bridging the gap that usually exists between those two groups. The whole idea is to accelerate the delivery of value, minimizing waste - of time, of software that is built, tested, delivered and only partially used and of software that is delivered with errors and has to be corrected.

Adopting DevOps implies a series of techniques and procedures already used in Agile development, applying them to the deployment of software, taking advantage of the virtualization of resources. These techniques and procedures are:

- **Automated tests:** to increase the quality of the delivered software, tests have to be executed very often (for each change in software), which is impossible to do with the traditional manual testing procedures. Therefore, code is written to test code, making it possible to execute those tests without human intervention and as often as needed. These tests should consider a layered approach, in which lower level tests are run more often (often using techniques that fake dependencies, specially if those are slow, like databases, network, file systems, etc.) and are faster to run, while higher layer tests are slower (because no fakes are used) and consequently ran less often;
- **Continuous integration:** reduce risks by integrating often, and therefore a smaller number of changes on each integration: if the integration breaks, it is a lot easier to spot the offending change or code. Depending on the technology stack used (programming language, frameworks, etc.), a **continuous build** process that compiles and links dependencies may also be needed;
- **Continuous delivery:** having a continuously integrated system is only a small step from having it delivered also continuously. Some kinds of systems and some kinds of changes to those systems must have human intervention for the delivery to effectively take place. Sometimes continuous delivery is also called **continuous deployment**;
- **Infrastructure as code:** when the infrastructure is virtualized, it is common to be able to define it through code. When this happens, a completely new dimension is opened, since techniques that are more usually used in software development, like version control, automated tests, etc., can also be used in defining the infrastructure. This activity then becomes a **repeatable** process, through which hundreds or even thousands of servers can be provisioned in a consistent way and in relatively short times;
- **Configuration management:** manages systems' configuration lifecycle, including dependencies between different **configuration items**. In its broadest sense, configuration management also covers functions like **root cause analysis** (of a detected problem), **impact analysis** (of a planned change), etc., making it a crucial asset in today's IT infrastructure.

The most common metaphor to DevOps is a 'pipeline' that is fed by development, passes all the planned phases of that pipe without human intervention (unless a problem is detected), and delivers the value added by the developed software to the 'customer'. Each stage of this pipeline applies quality control measures before any change proceeds to the next stage.

The main impact for Altice Labs of such an approach for developing software is much beyond a mere **change of culture**. Agile Methodologies, to which a DevOps approach is very closely connected to, are supported in many principles (see 'The Agile Manifesto', http://www.agilemanifesto.org/) that somehow are still strange and difficult to accept by many developers, as leaving them the responsibility to define the infrastructure on which the developed software will run seems really strange for more traditional organizations.

Nevertheless, Altice Labs and Altice Group operations will surely benefit from adopting such processes, since those are the most efficient known at the time of writing, delivering value to the 'customer', whoever he/she is. DevOps forces the organization to streamline and automate software development and delivery processes wherever possible, even in scenarios where the Ops are from an external entity. Activities like **test automation**, which have already started in Altice Labs, will be of great advantage, but also evolve a lot as well, when used in a DevOps process.

One of the approved EU-H2020 projects under the ‘5G’ call, SONATA (Service Programming and Orchestration for Virtualized Software Networks) [13] addresses precisely the issue of applying DevOps in NFV and SDN environments. What has been known as ‘5G’ pushed down barriers to market entry, delivery times (services), etc., so organizations really have to change if they want to keep doing business successfully in this market. Lowering barriers to market entry means that telcos will have to host services that have been brought up by other players, in a much faster way than what is still the todays’ current practice. This significant increase in delivery speeds implies much more Agile cultures, and new processes and tools that are not easily adopted or adapted to the organizations. This explains the importance of such projects, in which experimentation e.g. trial and failure are relatively inexpensive, while allowing for on job training.

(Mobile) Edge Computing

The emerging cloud paradigm is increasingly replacing IT servers traditionally located on enterprise premises, and moving them to centralized clouds. Big data centres (DC) are able to hold a large amount of COTS resources at a very low cost, taking advantage of economies of scale. With the NFV advent, the same paradigm can be applied to network functions, which can be virtualized and moved to a data centre. However, because of its nature, not all VNFs can be centralized. For this reason, the deployment of local/regional micro-DCs is under discussion and becoming a consensual belief in the telecom community.

Today, many services are able to run efficiently from centralized DCs, taking advantage of high data rates provided by modern broadband technologies. However, some other services would benefit if placed on the edge of the network, closer to clients. Edge computing provides four main advantages:

- **Ultra-low latencies:** many applications, such as augmented reality or gaming, benefit from very low latencies, which can be obtained by placing services closer to clients, fostering new services;
- **Backhaul bandwidth efficiency:** edge computing can promote an efficient use of local communication, minimizing backhaul capacity when local/regional communication is kept on the edge, not requiring to be forwarded outside (core), which is especially relevant for data intensive services. Examples are the delivery of video streaming on sport events to spectators on the stadium, or video analysis of surveillance cameras (IoT), which can be performed locally on the edge, sending outside only notifications of relevant events (e.g. car accident detection) or small video chunks;
- **Location awareness:** the information about client’s location can be used to customize the delivery of certain services - location based services;
- **Network context information:** network context information can be used to leverage the user experience, e.g. by adapting the quality of the content (video) according to the actual network conditions.

In this context, by the end of 2014, ETSI has created the MEC (Mobile Edge Computing) ISG (Industry Specification Group) [14], which intends to standardize a service execution framework, capable of offering to developers and service providers an IT service environment on the edge of mobile networks.

Although the focus of ETSI MEC is the mobile environment, this concept can be applied to any non-3GPP network, like Wi-Fi or even wired technologies such as DSL, Fibre, Cable, etc. The rationale is the same: to take advantage of the unique environment that only operators can offer and to provide better and new services. Candidate services can be provided by the operator, but mainly come from OTTs, from which operators expect a significant interest, trying to recover some revenues recently taken away.

Figure 10 shows the basic components of the MEC architecture, that are being developed under MEC ISG.

Although the MEC environment can be anywhere between the client and the core, eNBs seems the

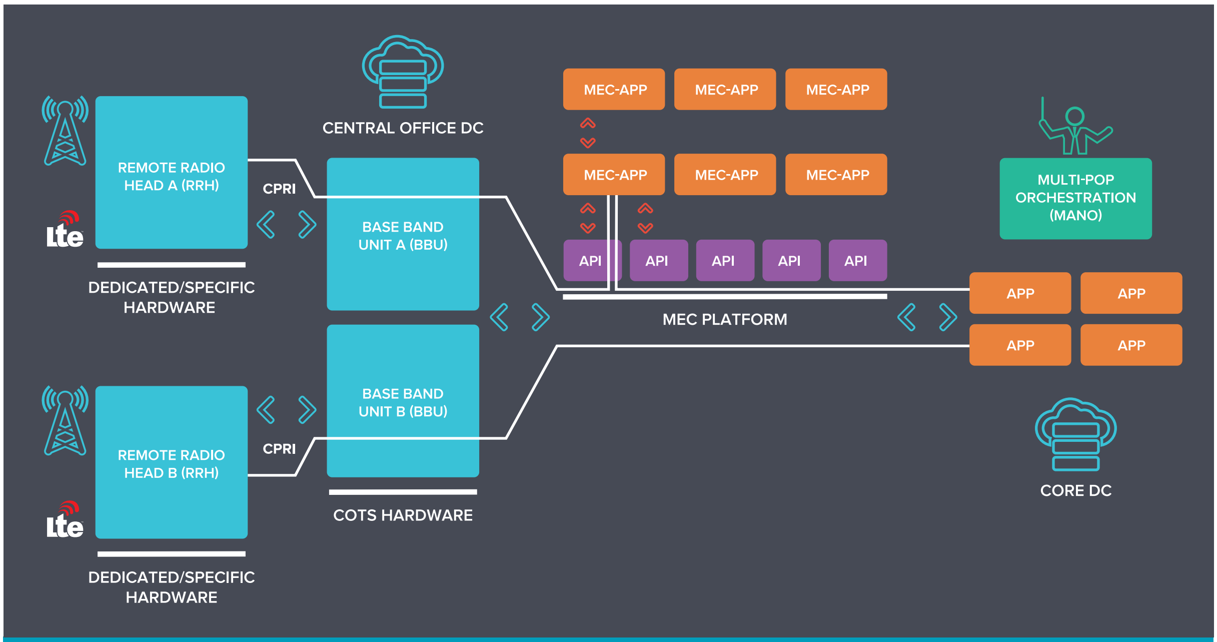

FIGURE 10 MEC basic architecture

most suitable target. MEC environment is composed by a main entity, the **MEC Platform**, which is responsible for the integration with the mobile network and provides APIs to allow applications to interact with the network. Examples of APIs are:

- User-data plane traffic uplink/downlink traffic interception (breakout);
- Access to network information (NSIS);
- Access to client’s location.

MEC Applications run on top of an IT infrastructure, likely to be virtualized, and use APIs to programme services to clients. On top of this, there is a **Management and Orchestration** layer, responsible to manage the Apps lifecycle and orchestrate the placement of the different application on multiple edges.

The MEC concept imposes significant requirements to operators, especially regarding the creation of small IT/cloud infrastructures on the edges, which is quite more expensive when compared to the same capacity in a single central DC. However, some other trends may act as enablers for the edge computing success. The ongoing process of virtualization of access network functions on mobile networks (C-RAN) will impose the separation of the eNBs into RRHs (antennas) and BBUs (signal processing), deploying the BBU components into small local micro-DCs. In the same way, with the evolution of wired networks, some equipment is expected to face similar evolution (OLT, CMTS, etc.), ending up by converging wired and wireless access functions into common micro-DCs. In such an environment, where operators are already spreading IT resources along the edge for NFV purposes, MEC solutions become affordable, as edge computing environments can share resources with NFV. Figure 11 depicts this convergence and evolutionary view of MEC environment.

Altice Labs is part of the H2020 RDI Superfluidity project [15], which intends to develop the MEC concept, among other research subjects.

Planned Innovation: Upcoming PoCs

After the implementation and demonstration of the vHGW POC, Altice Labs is currently working in the analysis of new problem spaces relevant to be addressed regarding the services and network evolution using NFV and SDN, and on the specification of new solution prototypes, namely:

- New generation of enterprise services: evolution of the current generation of

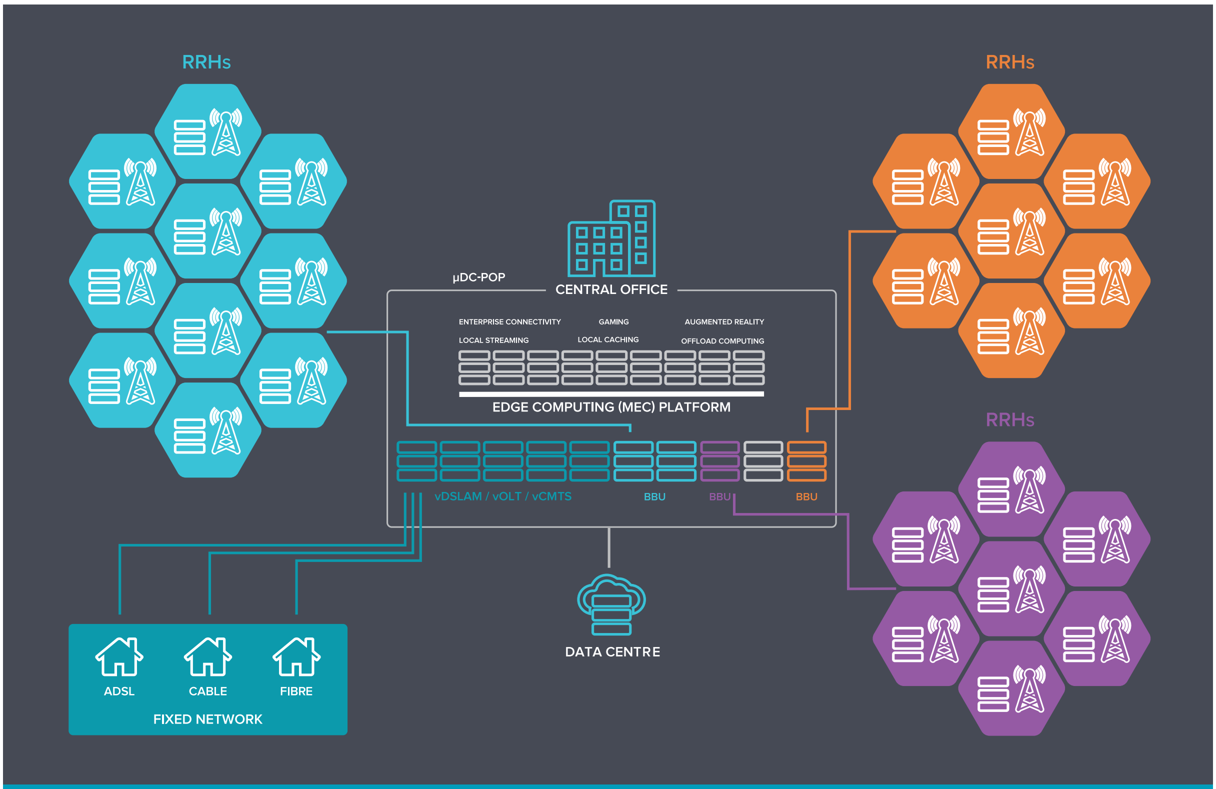

FIGURE 11 MEC evolutionary context

enterprise services to provide self managed programmable VPN services to enterprises, complemented by virtualized CPE services and virtualized IT services;

- Convergent central office architecture: full virtualization of fixed access PON network and mobile 4G network, convergent policy driven network control architecture, convergent policy driven service chaining. This PoC, aside from network virtualization, intends to addresses the current Gi-LAN network evolution and goes beyond promoting fixed mobile convergence through a unified control and service chaining;
- Assurance architecture for NFV and SDN network: definition of the architecture basis for end-2-end assurance over new NFV and SDN networks architectures.

Other PoCs, covering a wider scope than the vHGW will extend to other areas, such as the corporate vCPE.

Also planned, as the PoCs matures, is the set up of joint field trials involving Service Providers network operational teams, addressing field requirements which will be a further step towards the validation of the chosen approaches.

Conclusions

More than a trend or hype, NFV and SDN paradigms will for sure be adopted by the telecommunications industry. We can go further and say that NFV and SDN adoption will be major transformation forces, driving the evolution of traditional Communication Service Providers to a new generation of Digital Service Providers, emerging over a new generation of Service Platforms.

The new generation Service Platforms will have in its core a “network of data centres”, where the vast majority of service funcionalities will reside. Being the access networks a valuable asset inherited by the telco operators, this new generation Service Platform will be complemented with managed access connectivity which is a considerable differentiating factor as compared to Internet players.

The new generation Service Platforms will boost the speed, agility and flexibility for new digital services creation and, at the same time, will furnish the means to dynamically control, in near real time, the configuration and topology of the service functions, managing effectively service loads, service quality levels and anomalies affecting services. In the end, the ultimate purpose is to achieve unmatched levels of operational efficiency and improve significantly the customer experience.

Altice Labs has been following and contributing to the most relevant SDO's and industry organizations that have been specifying and implementing NFV and SDN architectures and technologies since the early stages of this technology. Due to this, Altice Labs has developed internal critical skills and reached a maturity level that supports the current engagement in the most relevant international exploratory innovation projects, the capability to implement internal Proofs-of-Concept and to feed the Altice Labs' product business units with the knowledge and experience required to evolve its product roadmap, thus future-proofing the company's portfolio by adapting it to new technological frameworks, like SDN and NFV. ○

References

[1] Portugal Telecom Inovação, “An NFV/SDN Enabled Service Provider: A New Generation of Digital Services”, http://www.ptinovacao.pt/content/WP-An-NFV-SDN-Enabled-Service-Provider.pdf, Public PTIN whitepaper, January 2015

[2] ETSI NFV, Network Functions Virtualization, http://www.etsi.org/technologies-clusters/technologies/nfv

[3] ONF, Open Networking Foundation, http://www.opennetworking.org

[4] Fernando Bastos, Jorge Carapinha, Mário Rui Costa, Pedro Neves, Rui Calé, “NFV & SDN: Arquiteturas de Rede Emergentes”, Revista Saber & Fazer PTIN, 2015

[5] Pedro Neves et. al, “The SELFNET Approach for Autonomic Management in an NFV/SDN Networking Paradigm”, International Journal of Distributed Sensor Networks Volume, 2016, Article ID 2897479

[6] Pedro Gutiérrez, Martina Zitterbart, “D2.31 Final Architectural Framework”, FP7 4WARD project, June 2010

[7] Azimeh Sefidcon, “D.D3 Refined Architecture”, FP7 SAIL project, October 2012

[8] Andy Edmonds, “D2.5 Final Overall Architecture Definition, Release 2”, FP7 MCN project, April 2015

[9] George Xilouris, “D2.21 Overall System Architecture and Interfaces”, FP7 T-NOVA project, August 2014

[10] ETSI Group Specification NFV 001 v1.1.1, “Network Functions Virtualization (NFV); Use Cases”, ETSI, October 2013

[11] ETSI NFV PoCs, http://www.etsi.org/technologies-clusters/technologies/nfv/nfv-poc

[12] H2020 SELFNET project, https://5g-ppp.eu/selfnet/

[13] H2020 SONATA project, https://5g-ppp.eu/sonata/

[14] ETSI MEC, http://www.etsi.org/technologies-clusters/technologies/mobile-edge-computing

[15] H2020 Superfluidity project, http://www.superfluidity.eu