Service oriented cloud CPE as a means of a future terminal

Christos Tsirakis
OTE Academy S.A.
Athens, Greece
ctsirakis@oteacademy.gr

Panagiotis Matzoros
OTE Academy S.A.
Athens, Greece
pmatzoros@oteacademy.gr

George Agapiou
OTE S.A.
Athens, Greece
gagapiou@oteresearch.gr

Abstract—**The current CPE deployment model, which is based on deploying "intelligent" independent equipment in the customer premises, has important challenges that have been limiting the profitability of services for telecommunications service providers. Cloud CPE model provides a win for cost and service performance for the future, as it reduces onsite CPE complex requirements to a minimum and moves these features into the cloud, under service provider control. The financial analysis proves that the cCPE is a viable solution for the operators and also it is proved that can bring costs down for the operator but also for the end user and can be a viable solution for the 5G ecosystem.**

Keywords—Cloud CPE, NFV, OPEX, CAPEX.

I. INTRODUCTION

The speed at which communications technology changes seems to be exponentially increasing. New protocols and technologies have become enablers of innovation and value creation, so new standard versions keep constantly appearing into the market. One of these technologies is the Customer Premises Equipment (CPE) [1].

CPE is the device that attaches both residential and business customer sites to the telecommunications service provider (SP). There are many types of CPE devices, like telephones, switches, residential gateways (RG), cable modems, set-top boxes, and Digital Subscriber Line (xDSL) routers that enable consumers to access communication SP's services and distribute them around their house via a local area network (LAN).

Unlike the early "foolish" DSL modem used for the Internet access, today's home broadband router is a standalone, relatively complex but intelligent box that perform networking function a plethora of services and functions such as routing, switching, firewalling, amongst several others. More specifically, it does not only terminate the signals coming from the provider (Layer 1 and 2), but it also serves as a router (Layer 3), a NAT firewall, an Ethernet switch, a wireless access point (AP), a DCHP server, a Web server, a telephone and a VoIP server. All these current CPE's features are shown in figure 1.

These devices are also considered to be "service enablers" because the customer just values the Quality of Service (QoS) (the VPN connection, the IPTV service, the internet connectivity) and not the box itself. However, the

CPE is the presence of the service in the home and often overlooked in its importance.
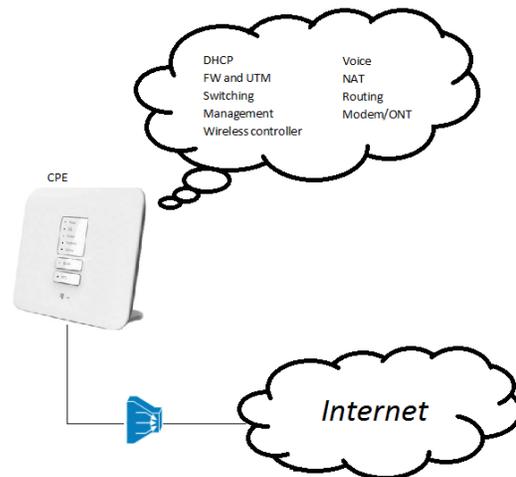

Figure 1. Current full featured CPE

Furthermore, different services with diverging requirements, such as voice, video, Internet, and even cellular communications (through femtocells) are now transported on top of these CPEs. This means that the device must be able to intelligently classify each packet flow travelling across it. All these features must be performed locally at the customer premises, and build up into a complex list of features that translate into a large amount of logical functions that have to be implemented in large amounts of complex software.

Additionally, as more complex IP services are introduced (e.g. Corporate Security, Parental Controls or IPTV), more demands are made of this legacy hardware and in many cases this demand may be beyond the devices' capability, requiring a new device or such a change to the existing software that it usually takes many months to develop and distribute an upgrade.

However, most of times, the device, which will implement these functions, has to be built into cost-effective and commoditized hardware, so as not to eat up the small margins operators receive through subscriptions. This leads to failure-prone and loosely maintained devices, unavoidably leading to numerous failures and service disruptions. SPs have been looking for ways to effectively centralize the logic

of these services in a location under their control and simplify the device located in the customer premises.

Cloud computing, combined with software defined networking (SDN) and network function virtualization (NFV) can help solve this issue. Cloud computing represents a paradigm for information technology (IT) services, which can now be delivered in an on-demand and self-service manner. SDN brings new capabilities in terms of network automation, programmability, and agility that facilitate integration with the cloud. On the other hand, NFV accelerates the innovation of networks and services, allowing new operational approaches, novel services, faster service deployment (shorter time to market), increased service assurance, and stronger security [2].

The goal of this model is to "move the CPE to the cloud". This is achieved by making CPE smaller by removing the software complexity from the device located at the customer premises and put it in a cloud hosted in SP's premises. As a result, the future CPE will be a standard device with minimal capabilities of voice telephony, wireless access point, and Ethernet switching. Anything beyond that, should be executed as software in a customer-specific virtual instance in the SP's cloud.

These functions, which will be put into the cloud, could include:
- Routing
- NAT and firewall
- DHCP
- Virtual Router Redundancy Protocol (VRRP)
- Wireless controller
- Centralized management and provisioning
- Reporting

The Cloud CPE is easily extensible to include new and adjacent provided services:
- Network-based storage
- Virtual desktop infrastructure
- Remote maintenance
- Physical site security and automation

All of the control plane functions can be handled with general-purpose CPUs, without the need for specialized hardware. These functions can be virtualized and moved as workloads into the SP cloud, while the data plane can be running in a much simpler and cost effective device in the customer premises.

Cloud CPE model splits the CPE device into two entities: a control plane representing the software service logic and complexity, and a data plane entity performing the actual traffic manipulation and the local enforcement of the service logic. The control plane is removed from the device sitting in the customer premises and implemented in a virtual machine in the SP datacenter that can be easily managed, upgraded or troubleshot by the SP. The data plane then is remotely controlled by the virtualized control plane. But it is able to provide locally in the customer premises all data plane functions required for the service, such as firewalling, NAT, QoS, DHCP, DNS, etc. Therefore, the cloud CPE solution is depicted in figure 2.

From the perspective of the provider and the router vendor, the benefits of the cloud CPE model are the following:
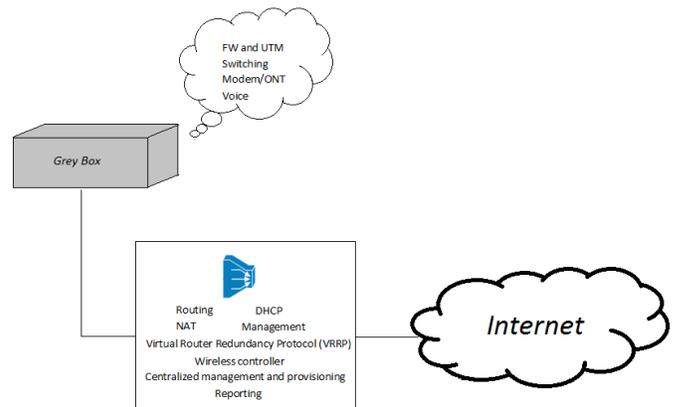

Figure 2. Cloud CPE model

- *Cheaper CPE / CapEx reduction* – Currently, the several different CPE capabilities make the equipment more expensive. In future, a simple standard CPE would reduce the cost of the equipment significantly/dramatically. The list of requirements on the device is reduced and standardized, thus making them more cost effective and stable. Furthermore, as customers migrate between services, the hardware that needs to be changed to support new features is minimal.
- *Cheaper support / OpEx reduction* – a single standard CPE results in much less steps to follow in case of a fault, providing lower dependency on end-customer interaction (power, location, maintenance). For example, if something goes wrong at the CPE, reboot is much faster in the cloud than in the CPE. Also, software bugs can be easily fixed if the software runs in the provider's Central Office. By keeping the service implementation complexity in their centralized location, operators can have tight control of the service and perform any maintenance required without the need of making any changes in the customer premises, which would mean logistic problems in the form of technician visits or device swap-outs.
- *Security* – All the security functions can be put into the provider network, so the device cannot be electronically compromised. Also, in case of security vulnerabilities, the new firmware is automatically flashed to the cloud CPE without leaving home broadband users on their own to flash any new firmware to their routers.
- *Upgradeability* – Several times, the current CPEs are not able to perform every configuration task required for some complex services. This could result in an installation process that requires a technician visit. Additionally, CPE firmware rollouts can take weeks or months. However, the

ability to offer new services, which can be created in the cloud (e.g. cloud storage, a home video server, and home automation), avoids the need to send out new routers, reduces the time to market, and allows service providers to try and scale new functions with market demand. It also enables upgrades and adoption of new standards as they come out. Configurations and changes are simplified, as the service can be configured once in the cloud, and implemented in a huge number of CPEs automatically.

- *Manageability* – Currently, service providers are forced to support and maintain a device that is located in the customer premises. It will be commonly misconfigured, unplugged, hacked. With cloud CPE, the end users have limited access to the device and a small set of features to change. However, the service provider can offer management services without having to try and access the customer's device. Remote reconfiguration capabilities and efficient remote management become possible and easier to implement. The service provider has full control, so all monitoring, metering, and support functions are simplified.

- *Customization* – Software can be provided by a different vendor than hardware. The procurement phase is long and complex, as service providers are forced to contact hardware vendors with long lists of features, issuing RFx processes, and performing in depth testing and certification processes. Additionally, they have to deal with customized firmware loads from all software vendors, due to the high complexity of the software functions to be implemented in the device, and the difficulty of later upgrading a device that is running in the customer premises.
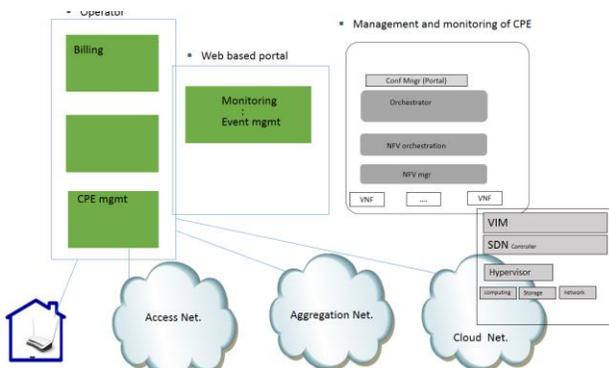
II. ARCHITECTURE

Figure 3: Architecture for configuring, managing and operating a cCPE

The cloud CPE architecture presents the different layers involved for provisioning and managing the cCPE. When a user is asking for a service then multiple domains like SDN network, VNFs deployed in NFVI domain and the Orchestration layer plays the role of a high level managing and orchestrating different tasks. The different functional elements are virtualized in the cloud and when a user is asking for a service then a series of elements is formulated to produce a chain of virtualized elements capable to run the service.

III. FINANCIAL ANALYSIS

The techno-economic analysis produces three scenarios: the classical CPE or physical CPE, the grey CPE-which is a hybrid one with some network functions being virtualized and the white box which is fully virtualized. For the above three CPE models, a financial analysis is performed. For this analysis, the net present value, the return of investment and cash flow are important parameters which are considered.
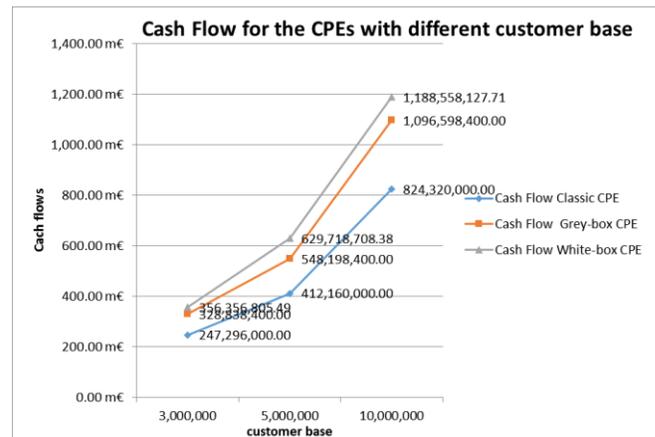

Figure 4. Cash flow for the three CPE types

The EBITDA for the year 2021 for the three type of CPEs is seen in figure 5.
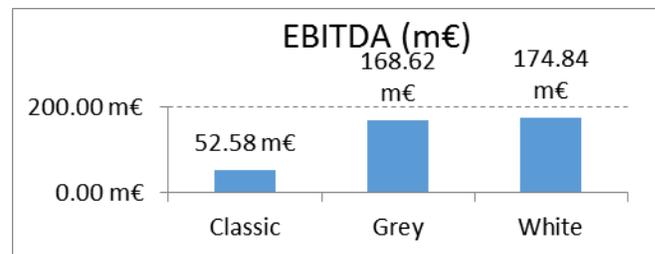

Figure 5. The EBITDA at year 2021 for the three CPEs

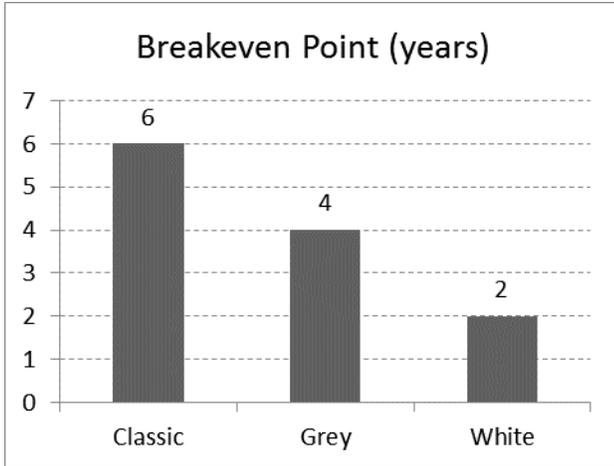The breakeven point for the considered three CPE types is seen in figure 6

Figure 6. The breakeven point for the three CPEs

A sensitivity graph that show how the data of figure 6 can be altered is depicted in figure 7 where the value of each CPE is increased by 2 euros.
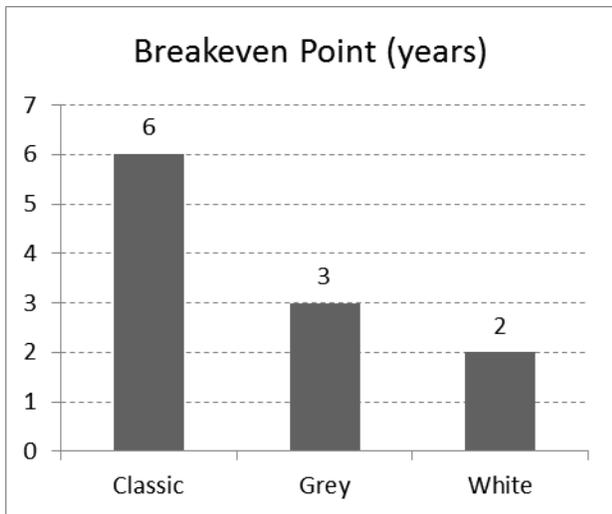

Figure 7. The breakeven point for the three types of CPEs by changing the value of each CPE by two euros

IV. IMPLEMENTATION OF A CCPE IN THE 5G CONTEXT

According to a number of surveys about the 5G eco-system [3], the achievement of the performances of 5G (throughput, latency, etc.) demands an increase in the elements of the network and the provision of heterogeneous network. However, this increase cannot be stemmed only in terms of the number of different base stations (BS), but also in terms of different radio access technologies. A 5G network should integrate the LTE network, the new radio access technologies (mmWave, massive MIMO), and the WLAN radios. This integration of different radio technologies needs a cloud-based network approach which introduces the technologies of software defined networks (SDN) and network function virtualization (NFV). These offer the important flexibility and control of the upper layers. The virtualization on the core network and the cooperation between the BSs at the radio access network (RAN) offers an E2E control of the future networks.

The proposed approach of cloud CPE gives the opportunity for successful integration of the WLAN as access point in the 5G eco-system. Moreover, the Wi-Fi access point is a costless indoor densification solution of the network. The aggregating resources of the Wi-Fi can be available through a consolidate cloud system of the radio access network, which communicates well with the core network.
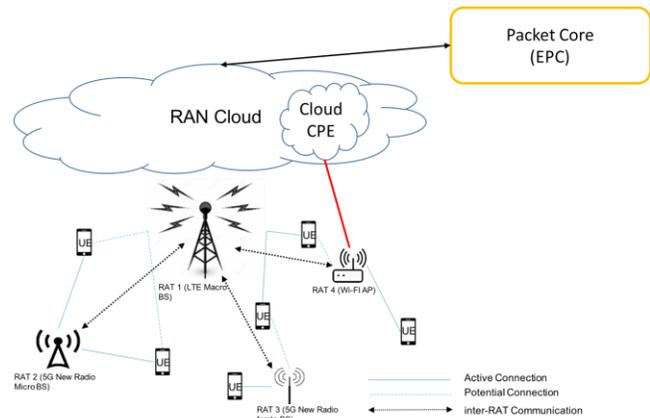

Figure 8. Multi-RAT connectivity and cloud CPE integration

The integration of the cloud functions of the CPE (figure 8) in the cloud radio access network allow the control plane to consider the Wi-Fi access point as part of the whole network. This combination of the control plane for both the BS and the Wi-Fi allow the operator to steer the functions of the devices according the on-demand needs of the network, support the mobility between different access point (LTE, 5G New radio, WLAN), to offload and to distribute the traffic equally for better QoS [4].

In the introduction section there was a description of the functions, which can be moved to the cloud. Some of these functions are common functions for all the radio technologies. This allows the combination of these functions under a common framework as part of the cloud RAN. Figure 9 illustrates the common functions.
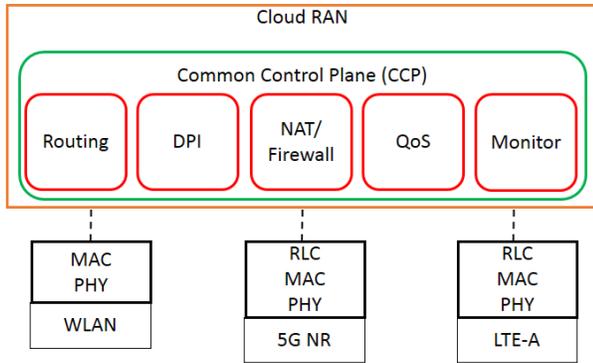
Figure 9. Common multi-RAT functions

The common functions between the different radio access technologies are:

- Routing
- Deep Packet Inspection
- NAT and Firewall
- Quality of Service
- Data inspection

This unified control plane allows the cloud RAN to monitor, reroute and offload the network traffic across all the different elements faster, using less processing time, in order to offer better quality of service according to the on–demand needs of the network.

V. CONCLUSIONS

This paper presents a financial analysis for the cloud CPE, which allows telecommunication providers to offer new features and services easier as a result of the flexibility that is offering. Additionally, the financial analysis that was presented, demonstrated that the adoption of cCPE option could be profitable in economic terms. The total CPE cost is decreasing as the number of services that are located in the cloud is increasing since there is less amount of costs that have to be invested by the operator when most of the network functions in the CPE are moved to the cloud. In addition, the provisioning costs are higher when the CPE is the classic one since any change that has to be done in the CPE affects the provisioning to all the terminals that have been provided to customers. Thus, telecommunication providers should take under consideration the possibility to invest in this type of terminal equipment.

REFERENCES

[1] Fernando Sánchez, David Brazewell, "Tethered Linux CPE for IP service delivery", *IEEE Conference on Network Softwarization (NetSoft)*, Apr. 2015

[2] João Soares, Carlos Gonçalves, Bruno Parreira, "Toward a telco cloud environment for service functions", *IEEE Communications Magazine*, vol. 53, no. 2, Feb. 2015, pp. 98-106

[3] Jeffrey G. Andrews, *et. al*, "What will 5G be?", *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 6, Jun 2014

[4] Subramanya Chandrashekar, *et. al*, "5G Multi-RAT Multi-Connectivity Architecture", *IEEE International Conference on Communications Workshops (ICC)*, May 2016