# Virtualizing Customer Premises Equipment

Jorge Proença, Tiago Cruz, Paulo Simões
*University of Coimbra, CISUC, DEI*
Coimbra, Portugal
{jdgomes, tjcruz, psimoes}@dei.uc.pt

Miguel Freitas, Rui Calé
*Altice Labs, EIT*
Aveiro, Portugal
{miguel-r-freitas, cale}@alticelabs.com

***Abstract*— Business and residential gateways are customer premises equipment (CPE) devices that connect the customer network to the operator network. Being hampered by a traditional, device-centric, deployment approach, these devices are regarded as candidates for partial or full virtualization, with envisioned benefits in terms of simplified management, hardware costs, and streamlined service design. This demo presents a prototype vCPE environment demonstrating two distinct service models. First, a residential service with the virtualization of all functions on the operator's infrastructure, representing most service deployments, which can easily scale to millions of customers. Second, a more business-oriented service model that uses a hybrid deployment scheme with a mixture of virtualized functions deployed both the operator side and in the customer premises, using physical gateways that still have some computational capacity. The seamless subscription of value-added functions to the service (for instance an ad blocker function) is also demonstrated.**

***Keywords— NFV, SDN, Broadband Networks, vCPE***

## I. Introduction and Motivation

For internet service provider (ISP) scenarios targeting the residential and business sectors, the customer premises gateway, often called the "home router", establishes the main connection between the customer and the provider domains. This gateway allows user equipment (UE) devices such as personal computers to be connected to the internet using cabled or wireless LAN connections, also providing direct and/or indirect support for VoIP, IPTV and IoT services.

Overall, the customer gateway is a significant part of the deployment costs for an operator, as well as being a single point of failure, whose misconfiguration or failure may leave a client isolated and without service. Moreover, the complexity of dealing with a multitude of heterogeneous gateways with variations in vendor, model, and firmware versions creates an additional overhead in operational costs and in the complexity associated with their management [1][2], as gateway devices in use are replaced when their expected lifetime ends, and not when new models are released.

Gateway service virtualization can benefit the operator in different ways. Virtualized functions decouple software components from hardware platforms, enabling service/component offloading from the gateway. Thus, when a function is updated, all users benefit from it and the operator does not need to develop and maintain different versions of the same function for different hardware configurations. Troubleshooting processes is also improved for operators in a virtualized environment. As most functions are instantiated in the operator domain, it is easier to troubleshoot if a function needs to be reinstalled or have its configuration values reset to the default parameters. In a traditional service, malfunctioning functions may render the premises isolated from the operator, which often requires costly and slow truck roll solutions. On the other hand, in a virtualized environment, premises isolation is less likely to happen, as the functionality in the customer premises device is reduced to little more than tunnelling – greatly reducing the chances of the gateway becoming a point of failure and allowing the operator to quickly solve the problem, with less expense.

This work is funded by the project POWER (grant number POCI-01-0247-FEDER-070365), co-financed by the European Regional Development Fund (FEDER), through Portugal 2020 (PT2020), and by the Competitiveness and Internationalization Operational Programme (COMPETE 2020).

## II. vCPE Prototype Demo Scenario

This demo showcases a service delivery scenario with virtualized residential and business gateway instances. Virtualized instances are referred as vCPEs (Virtualized Customer Premises Equipment), with pCPEs (physical CPEs) being the physical gateway devices deployed in the customer premises (see Figure 1).

In a **residential scenario**, all functions typically supported by the home router are instantiated in the operator environment, either in the core datacentre or at the edge. The pCPE simply extends the client domain to the datacentre by establishing a L2 tunnel (VXLAN).

**Business scenarios** may require specific and feature-rich functions that may benefit from being hosted in the customer premises. To address those functions, it is possible to follow a hybrid approach, with some services deployed locally and other services deployed at the operator's environment. To enhance flexibility, instead of a typical CPE with limited computing capabilities, we use a device with some computational power and virtualization capabilities, so that both centralized and local functions become virtualized (thus simplifying management and making it possible, according to the circumstances, to decide where each function is located).

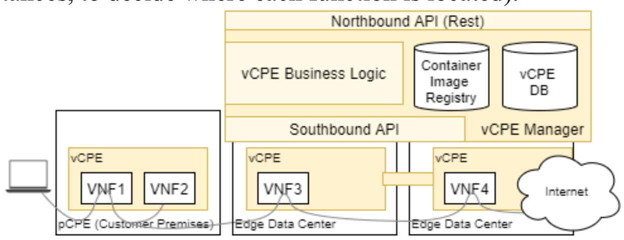


*Figure 1- Functional Architecture*

This results in two distinct types of devices to be deployed, depending on the service being delivered:

- **vCPE Small (for residential scenarios)** – all functions are virtualized at the datacentre, with a basic pCPE.
- **vCPE Large (for business scenarios)** – hosting of the virtualized functions is spread between the operator infrastructure and the pCPE.

Figure 1 provides a high-level view of the functional architecture used in this demo. The vCPE Manager provides the business logic, stores the function images, the data related with the vCPEs and client information, managing all operational tasks for clients, services and vCPE instances

The demo is divided into two scenarios, for residential and business customers. The first uses the *vCPE Small* as pCPE, leading to an environment where the physical device deployed at the customer premises is the most stripped and simplified, without local virtualization of functions. This device is used when all functions are instantiated at the operator infrastructure, which could be in an edge or core datacentre. This simplifies the physical device requirements to a minimum, needed to provide a basic set of functionalities:

- Establish VXLAN tunnels for L2 connectivity between the customer premises and the operator infrastructure.
- Providing wired and wireless LAN connectivity to the user equipment (UE) devices within the customer premises.
- Bridging capabilities to forward packets within the local UE devices, and between the customer premises and the datacentre, through the VXLAN tunnel.

For business environments with higher service requirements, we use the *vCPE Large*. In addition to the basic functionality provided by the *vCPE Small*, the pCPE used in this scenario has increased computing capabilities, allowing it to instantiate virtualized network functions locally at the customer premises. This enables to further extend Virtualized Network Function (VNF) [3] location deployment options for function instantiation: cloud (centralized), edge (central office) and customer premises. Functions can be deployed at the operator infrastructure and at the customer premises, depending on their specific requirements. As an example, functions such as routing should be deployed on the operator side, considering that the VXLAN tunnel extends the edge of the customer's L2 domain from the customer premises to the datacentre. Other functions might benefit the customer and/or the operator by being moved to the customer premises, due to stricter latency requirements or to reduce operator infrastructure traffic.

In this business scenario, the service offered to the customer may have more advanced features, and distributed services to be deployed when there are multiple branches associated with a business customer. The Adkill VNF is used in this demo as an example of a function that reduces the load on the operator network, as some DNS queries are filtered locally in the customer premises, offloading the burden from the operator's side, both in terms of traffic and associated service load.

## III. Scenario Setup

The demo is deployed in a testbed (see Figure 2) from the University of Coimbra and Altice Labs. All the devices are being emulated by virtual machines (VM) running in a virtualization server using VMware ESXi as a hypervisor. The hardware of the server is based on a dual setup Intel Xeon Gold 5120 @ 2.20GHz, and 256 GB of RAM, and each VM uses 4GB of RAM and 2 CPUs (vCPE manager, each CPE Small, each CPE Large, and each user equipment instance).

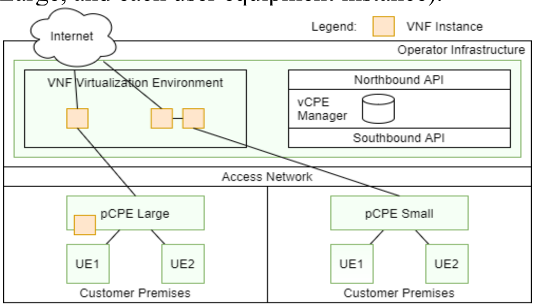


*Figure 2 - Virtual machines setup*

Figure 2 illustrates two customer premises (one residential and one business), and the operator's infrastructure, which are connected by an access network (e.g., fibre). In the operator's infrastructure, besides the vCPE Manager there is also a VNF environment hosting the VNFs required for each customer. In the figure, both customer services are composed using two VNFs. The residential service has both VNFs hosted at the operator's infrastructure, and the business service has one VNF in the operator's infrastructure and the other in the local premises, virtualized in the pCPE Large. Scenarios where some of the VNFs in the operator's infrastructure are shared among multiple customers are also possible, although not used in this specific demo. L2 VXLAN tunnels connect the pCPEs to the operator infrastructure, and each customer premises has dedicated private networks to connect their UE devices.

## IV. Demo Plan and Objectives

The demonstration is focused on highlighting the functionality of a vCPE-enabled scenario, showing the two service models and pCPE devices described in the previous sections. The operator infrastructure is represented by the VNF virtualization environment and the vCPE manager, which manages customers, the catalogue of available VNFs, the active VNF instances for each vCPE, and the lifecycle of the provisioned vCPE devices and instantiated VNFs.

The two service models are demonstrated, representing residential and business scenarios. In both cases, the CPE device is connected to the datacentre using VXLAN tunnels to extend the L2 domain from the customer premises to the operator's infrastructure. When the service is fully established, the client's UE devices can be connected to the pCPE. The device performs a DHCP broadcast request, which is received by the VNF handling these requests.

There are two VNFs that provide the basic connection service: vRouter and DHCP/DNS. Access to the internet is done through the vRouter VNF. This function is based on an Alpine Linux-based container, a lightweight Linux distribution that only needs 8MB for a minimal installation. The DHCP/DNS is handled by an Alpine-based container using Dnsmasq as a DHCP and DNS servers. This is a known lightweight and opensource DHCP and DNS server. Depending on the service model (i.e., pCPE small or large), this function is instantiated in the datacentre or locally at the physical gateway. When the UE receives an IP address lease, it can communicate with the devices connected to the private network as well as access the internet through the vRouter function. All the VNFs expose a webservice that customers can use to manage their functions. Each function provides a set of parameters that can be configured, with some configurations available only for the operator.

## V. Conclusions

This demo shows a prototype of a virtualized customer premises equipment (vCPE) gateway capable of virtualizing network functions in the datacentre, and in a mixed scenario with functions virtualized in the datacentre and in the customer premises. This allows operators to have a uniform set of software pieces, simplifying the management and provisioning of services, and enable easier service design to introduce new services.

## VI. References

[1] J. Proença, T. Cruz, P. Simões and E. Monteiro, "Virtualization of Residential Gateways: A Comprehensive Survey," IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1462-1482, 09 Oct 2018.

[2] J. Proença, T. Cruz, P. Simões and E. Monteiro, "Revisiting the Concept of Virtualized Residential Gateways," in Design Innovation and Network Architecture for the Future Internet, IGI Global, 2021, pp. 272-304.

[3] R. Mijumbi, J. Serrat, J. Gorricho, N. Bouten, F. D. Turck and R. Boutaba, "Network Function Virtualization: State-of-the-Art and Research Challenges," IEEE Communications Surveys & Tutorials, vol. 18, no. 1, pp. 236-262, 04 Sep 2016.