Virtualization of Residential Gateways: A Comprehensive Survey

Jorge Proença[1], Tiago Cruz[1], Paulo Simões[1] and Edmundo Monteiro[1]

***Abstract*—The Residential Gateway (RGW) is a key device, located in the customer premises, standing between the home network and the access network. It imposes a considerable cost for the operator and constitutes a single point of failure for all the services offered to residential customers – such as Internet access, Voice over IP, IPTV and Video-on-Demand.**

RGW virtualization promises to tackle these issues, but its success has been hampered by scalability and implementation restrictions. However, developments such as the rise of Software-Defined Networking and Network Function Virtualization technologies, together with the evolution of the access network, namely through the deployment of Fiber-To-The-Premises accesses, have finally enabled RGW virtualization in an unprecedented scale.

In this paper we revisit the virtual RGW concept, considering its evolution up to the most recent proposals as well as future challenges and developments.

I. Introduction

The evolution of the access network infrastructures, with the broad deployment of Fiber-To-The-Premises (FTTx) and Data Over Cable Service Interface Specification (DOCSIS) technologies, has brought considerable performance benefits, opening up new opportunities for operators to rethink their role and move towards converged service delivery models (e.g., *n*-Play services). Residential Gateways (RGWs) play an important part in this model, being deployed at the customer premises to connect the home network to the operators network. These devices provide services such as DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol), NAT (Network Address Translation), firewall, URL filtering, Digital Living Network Alliance (DLNA) server, routing, wired and wireless connectivity. They also support services such as IPTV (e.g., via Internet Group Management Protocol proxying [1]), VCI/VLAN (Virtual Channel Identifier/Virtual LAN) management and SIP (Session Initiation Protocol) gateways [2] and/or user agents (for integrated analog telephone interfaces), among other functions [3][4].

The RGW service footprint and complexity have increased over time, resulting in increased costs for the operator both in terms of deployment and maintenance. This cost increase is amplified by the scale factor (one RGW per customer), representing a considerable investment [5][6]. Furthermore, device diversity (vendor, model and even firmware version) and hardware obsolescence further increase management costs and create an obstacle to the quick introduction of new functionalities on the RGW. In the limit, introducing new services may require massive RGW replacement programs whose costs surpass the projected return from those new services.

[1]The authors are with the Department of Informatics Engineering of the Faculty of Sciences and Technology, University of Coimbra, Portugal jdgomes, tjcruz, psimoes, edmundo at dei.uc.pt

With the rise of cloud computing and the virtualization paradigms, together with the evolution of the access network role and supporting infrastructure, RGWs are slowly becoming an anachronism that mostly embodies the legacy access network model. In this perspective, virtualizing the RGW appears as an interesting solution, leading to substantial research efforts. Several operators, equipment vendors and academics have proposed virtual RGW (vRGW) frameworks, each of them with its own specific characteristics, regarding the location of computing resources, the architectural aspects of the virtualized solution or the connection between the home environment and the virtualized components. However, these first approaches suffered from several shortcomings, due to issues such as the need to encapsulate customer data circuits up to the vRGW hosting data center in a scalable way, or because of the increased infrastructure complexity. More recently, the introduction of technologies such as Software Defined Networking (SDN) and Network Function Virtualization (NFV) have enabled more satisfactory vRGW framework approaches, tackling many of the limitations that hampered their wide acceptance in the past.

In this paper we provide a state-of-art analysis on RGW virtualization and overview key existing proposals and possible evolution paths. The remainder of this paper is organized as follows. Section 2 discusses the rationale behind the vRGW concept, as well as its first implementation attempts. Section 3 discusses how the concepts of SDN and NFV became instrumental for the latest evolution of the vRGW concept. Current vRGW developments and proposals, including those from the European Telecommunications Standards Institute (ETSI) and Broadband Forum's (BBF), are presented in Section 4. Section 5 discusses current performance optimizations focusing on networks, virtualization nodes, and their integration. It also addresses standardization efforts. Section 6 provides a wrap-up discussion and Section 7 concludes the paper.t

II. Laying the vRGW foundations

This section presents the rationale for the vRGW concept, starting with a discussion of the problems of the conventional RGW. Next, it delves into an analysis of the initial proposals for virtualizing devices or functionalities, which paved the way for the creation and definition of the vRGW concept.

A. The case for the vRGW

Expansion of high-speed broadband access networks and increased coverage in terms of connected households were instrumental to enable converged *n*-play offers and cloud-based added-value services, which are displacing traditional communication and service delivery models to give place to an *everything-over-IP* approach [7][8]. Consequently, the

residential LAN ecosystem has evolved to encompass a series of devices such as PCs, set-top-boxes, VoIP (Voice over IP) telephones, smartphones, media players, smart TVs and storage devices, providing access to a diversified range of services to broadband customers. This has progressively pushed Telecommunications Service Provider (TSP) players towards a service-centric model, where the RGW stands in the nexus between the connectivity, services and customer environments.

Deployed on the customer premises, RGWs are mostly embedded systems platforms which mediate between the home and the operator's access networks and whose role has not significantly changed over time. As explained in the previous section, the RGW is responsible for the handling of a number of local network services.

The RGW accounts for a considerable share of the broadband network access service deployment costs, also constituting a single point of failure. Deployed right at the intersection of the customer premises and the access networks, an RGW failure may render inoperative services such as TV or fixed telephone – especially in consolidated *n*-play service scenarios. As such, its failure has a potential impact in terms of logistics (due to on-site maintenance, in worst-case scenarios), management and customer loyalty.

Also, RGWs may pose an obstacle for remote diagnostics and troubleshooting of devices and services within the customer premises LAN (for instance, due to NAT translation) also constituting an obstruction for the introduction of new services or adding features to existing ones. In fact, service time to market is frequently dependent on the device manufacturer to introduce support for new services, something often aggravated by the subsequent need to remotely perform a mass update of already deployed RGWs – this may be impossible at all for RGW models past the end of their lifecycle support, or because their capabilities are too limited for the intended purposes.

RGW model and manufacturer diversity is another problem: it is difficult for an operator to maintain a homogeneous set of RGWs as even a single model may have minor firmware and hardware revisions that gradually compromise uniformity and hamper troubleshooting and management operations. Equipment diversity means that even small differences may hamper the deployment of new services (a limited flash memory capacity for embedded firmware may limit update possibilities). Even when they are possible, mass firmware upgrades – a potentially troublesome operation – depend on specific model or vendor-related procedures or the management of different device data models (aggravated by the use of vendor-specific extensions) and pose a significant risk.

This made the case for rethinking the RGW, in order to ease or solve its inherent problems, streamlining its architecture in some way or even removing it completely. In this perspective, virtualizing the RGW comes as an interesting proposition, by moving the bulk of its functionality from the customer premises into the operator infrastructure.

Moving functions such as DNS cache servers, SIP gateways and content caching mechanisms out of the RGW will reduce its footprint, with potential benefits in terms of service manageability and functionality. Moreover, network functionality such as NAT, URL filtering, firewalling or DHCP LAN servers could also be migrated to the operator, being hosted or co-located in a carrier-grade infrastructure. As an example, a DHCP server can be moved outside the RGW, eventually being replaced by a relay agent (implementing DHCP option 82 [9]), located in the access node (i.e., in the OLT) or in a network bridge deployed at the customer premises.

RGW virtualization can make it possible to leave behind a simple device which, in the limit, may consist of a simple bridge (dataplane functionality) eventually equipped with wireless capabilities [10][11]. In this streamlined device, wireless support could be added by using conventional radio System-on-Chip components to implement a thin Access Point (AP), with management/configuration capabilities being ensured by a lightweight agent for remote operator access. Potential alternatives could also be considered, such as CAPWAP [12], using wireless controllers virtualized in the operator cloud or the CloudMAC proposal [13], which allows to further decouple Wi-Fi AP capabilities, by offloading MAC frame processing to the cloud. Regardless of the specific implementation details, it is expected that the removal of function and service dependencies from the RGW, will potentially make it more future-proof, regarding the introduction of new services.

The potential benefits of a Virtual RGW (vRGW) are manifold. Some sources estimate it can reduce up to 90% in call centre costs and up to 46% on the product return cost [5]. Also, a financial study comparing between a physical, a partially virtualized (hybrid) and a fully virtualized CPE [14] demonstrated that virtualization provides an economic benefit for TSPs, which increases along with the number of virtualized functions. In a vRGW scenario, having hardware requirements for new services is no longer a problem since the gateways are software components without a physical dependency to the underlying hardware supporting them. Moreover, failure rates can be lowered [15], software is easier to customize, and it is also easier to introduce new services. However, for the vRGW to be feasible, certain requirements must be satisfied [16][17]:

- *Scalability.* vRGW streamlining and optimization are required, in order to handle the hundreds of thousands or even millions of instances typically required by a single TSP [17][18].
- *Management and orchestration.* For operators, increased service coordination challenges will result from functional dispersion, lifecycle management, resource orchestration, or integration of existing Operations Support Systems and Business Support Systems (OSS/BSS)[1]. Moreover, users are reluctant to relinquish control of the old RGW functionalities, requiring some sort of "shared management" compromise to ease the transition.
- *Resiliency and continuity.* The decoupling of functional and physical components enabled by vRGWs poses significant challenges in terms of service continuity and reliability, introducing additional potential points of fail-

[1]In a telco environment, the OSS are the components that operate the back-office of the telco network, including provisioning and maintaining customer services. The BSS are responsible for maintaining the front-office services, such as billing, customer relationship and call centre operations.

ure and requiring infrastructures to be designed from the ground up to limit the impact of disruptive events.
- *Security.* The evolution to a virtualized paradigm provides an opportunity to improve customer and infrastructure security. However, it can also expose TSPs and/or customers to threats which did not exist in the legacy model, therefore requiring extra care to ensure that the security is not compromised.
- *Service dynamics and elasticity.* To cope with the dynamics of the applications and services, vRGW deployments require efficient orchestration and resource elasticity (especially for computing and networking resources), in order to scale as needed.
- *Component portability.* This is important for two reasons. First, it allows moving software functions across different data centers in an easier manner. Second, it eases the introduction or replacement of third-party components over time, thus enabling true vendor-independence.
- *Coexistence.* Compatibility of virtualized and legacy infrastructure components must be guaranteed, to ensure a smooth migration path.
- *Energy efficiency.* Energy efficiency planing and design targets must attempt to balance the consolidation benefits with the added expense of moving the RGW functionalities to the TSP infrastructure.
- *Improved Quality of Experience (QoE).* Operators must ensure end-users are able to experience QoE benefits from a vRGW migration, both by improving existing services and through the introduction of new, value-added services.
- *Optimization of Value-Added Service (VAS) delivery.* vRGW migration must ease the introduction of new VAS for end-users (e.g., via a self-care portal). Also, resource consolidation and sharing can contribute to reduce VAS operation and maintenance overhead, which can have a positive impact on operational expenditure (OPEX).

If satisfied, these requirements can potentially turn the vRGW into a source of potential benefits in terms of capital expenditure (CAPEX), OPEX and flexibility, pushing the RGW into the service-centric era.

B. vRGW: the First Steps

The first attempts at virtualizing some of the RGW functions started with generic network router devices: [19] and [20] proposed a solution using hypervisor-hosted virtual machine (VM) [21], together with the click modular router and XORP extensible router platforms; [22] studied virtual router migration scenarios using hypervisor hosts. The virtualization performance overhead for network appliances is discussed in [23] and [24], and [25] proposed implementing distributed firewalls using virtualized security appliances. There were also some first proposals using OSGi and virtual machines such as [26]

In 2011, the Eurescom Project P2055 [27] studied the issues associated with the mass virtualization of RGWs for broadband access network environment, from an operator standpoint. It proposed three alternative approaches to displace the physical RGW from the customers premises:

- Moving RGW functionality to the access nodes, by placing packet processing near the subscribers and distributing the load across several dispersed points. This approach requires extensive hardware upgrades in the access nodes, fragmenting resources across the network, increasing complexity and costs.
- Integrating RGW functionality on Broadband Network Gateways (BNG). This approach has the benefit of keeping the network design unchanged, but at the expense of requiring BNG to support mass RGW virtualization, something that is beyond their current capabilities. This would require the need for hardware upgrades and fragmentation of computing resources among BNG.
- Supported in an independent network element (NE) within the operators network. While having the advantage of not interfering with existing network elements, it introduces a new hardware component on the infrastructure, further increasing costs and maintenance requirements.

Physical RGW replacement was also proposed by [28], embedding transport capabilities on the access node (OLT) and decoupling other functionality such as AAA, DHCP and NAT. Other approaches, such as [18], proposed introducing vRGW line cards in the OLT (see Figure 1), also integrating the aggregation switch and edge router functionality (Huawei's MA5600T OLT is such an example) [29]. This was tested on a small scale pilot by the Spanish operator Telefónica.

Also, [30] proposes a vRGW implementation that takes advantage of Broadband Forum's TR-101[31] and TR-156[32] reference frameworks for VLAN Aggregation Topologies in digital subscriber line (DSL) and gigabit passive optical network (GPON) access networks, respectively. This proposal (see Figure 2) uses a mix of Customer (1:1) and Multicast (N:1) service topologies, together with Q-in-Q VLAN encapsulation to provide both service and customer-specific communication channels. Client-VLAN trunks are aggregated at the access nodes and aggregated into VLAN sub-trunks – customer-specific VLANs are then encapsulated within Multi Protocol Label Switching (MPLS) pseudowires at the BNG. The MPLS core network provides circuit abstractions, allowing the customer VLANs to reach the data centers, where the vRGW instances are hosted.

This proposal also included a plan for progressive migration of the vRGW from a standalone virtual machine replicating the RGW system image (and hosted on the operator data center) to a distributed approach, by decoupling and co-locating components, to streamline the vRGW image footprint (see Figure 3). To a certain extent, this approach already suggests some sort of functional decoupling, but without detailing how integration could be implemented, somehow anticipating a solution that is conceptually similar to Network Function Virtualization functional decoupling.

Limitations such as the absence of service decoupling mechanisms, flexible infrastructure support for pushing the customer premises boundaries towards the operator data centers, the increased complexity added to the access nodes or even access network restrictions (such as the limit for VLAN or Q-in-Q circuits) have ultimately shown these early vRGW proposals to be still unfeasible for deployment in large scale

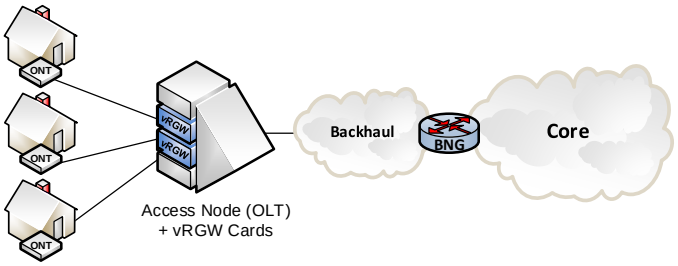


Figure 1. OLT-integrated card-based vRGW [33]

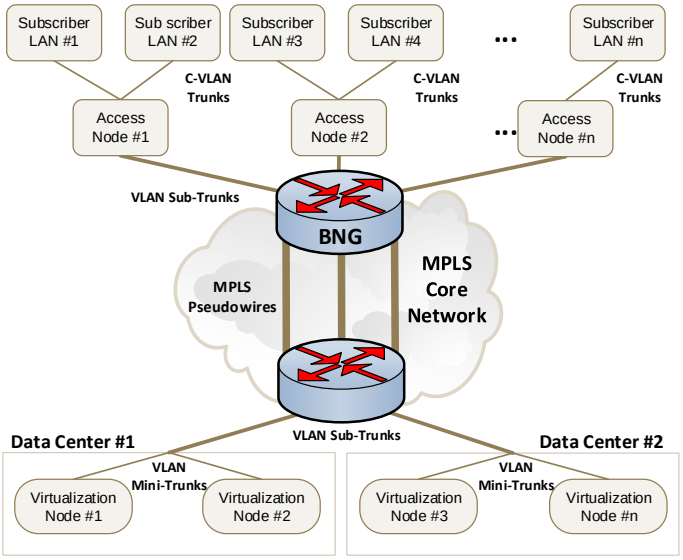


Figure 2. An early vRGW proposal, designed to bring the customer domain up to the operator data center [30]

scenarios. This was aggravated by the fact that most of the proposals practically ignored the vRGW management overhead, opting instead to focus on proof-of-concept scenarios. Meanwhile, developments such as SDN and NFV have the potential to fill some of the gaps of those early proposals and reshape the vRGW concept around more flexible and scalable frameworks, as presented in the next two sections.

III. vRGW-Enabling Developments

The emergence of Network Function Virtualization (NFV) and Software-Defined Networking (SDN) technologies have prompted the industry to start developing standards and solutions to incorporate their benefits within operator infrastructures, with a potentially disruptive effect. The vRGW concept is not immune to these developments, which have rapidly become the main drivers for its recent evolution – despite the fact that most of the work, including specifications, is still in its early stages. Moreover, the fog computing concept can help optimize vRGW function placement at the edge of the operator's infrastructure, where they are most needed, which is important in latency sensitive services. This section provides an overview of NFV and SDN, also presenting several vRGW proposals built on these technologies, with a special emphasis on the ETSI and BroadBand Forum efforts.

A. Software Defined Networking

The term SDN (for "Software Defined Networking") was first introduced in [34], referring to the OpenFlow [35] project being developed at the Stanford University, which eventually became one of the first SDN-enabling standards. SDN breaks with the existing vertical integration that is characteristic of the traditional networking model, by decoupling the control and data planes [36] to introduce direct programmability into the network.

In SDN, the control plane is moved away from the forwarding elements (i.e., routers), and placed in a logically centralized controller. This does not imply a physical concentration of functionality, as the controller functions can be performed by several controller instances to improve, for example, scalability and resilience [37]. The data plane remains in the forwarding elements and their task becomes focused only on traffic forwarding. These changes allow the controller to have a broader view of the network, compared with the narrow view that each individual device (e.g., router or switch) has in traditional networks. The SDN paradigm allows for easier and more flexible network management, especially on complex scenarios [36]. Additionally, packet forwarding is flow oriented, taking into account both origin and destination, instead of just the destination (as generally done in traditional packet forwarding). Flow policies are granted by a centralized controller, which is responsible for management of forwarding element policies – as an example, an SDN-capable switch can be reconfigured on-the-fly over the network, according to network service and application needs. Furthermore, an SDN network can be abstracted into multiple logically isolated networks, allowing multiple users to share the network individually using SDN hypervisors [38]. As control functions are decoupled from forwarding elements and consolidated on the SDN controller, the latter will have a broad perspective of the network domain under its control, contrasting with the narrow view that characterizes standalone forwarding elements in a traditional IP network. Examples of SDN protocols include IETF ForCES (Forwarding and Control Element Separation) [39] and OpenFlow [35].

B. Network Function Virtualization

As network applications and service requirements scale and evolve, both in terms of capacity and complexity, the supporting operator infrastructure needs to resort to specific network management and traffic policies that cannot be provided by the network, in order to keep up with demands. Network Function Virtualization (NFV) [40][41][11] provides a significant contribution to address this problem, by enabling the on-demand creation of flexible network services though a chain-based, composition mechanism that uses network functions implemented in VNF (Virtualized Network Functions)[2], that can comprise functions such as NAT, DHCP, BNG, Firewalls, among other components, implemented as Virtual Machine (VM) or containerized appliances.

The virtualization of the network functions (NF) have the potential to bring several benefits to the TSP. The consolidation

[2]VNF instances are the building blocks that enable the NFV concept

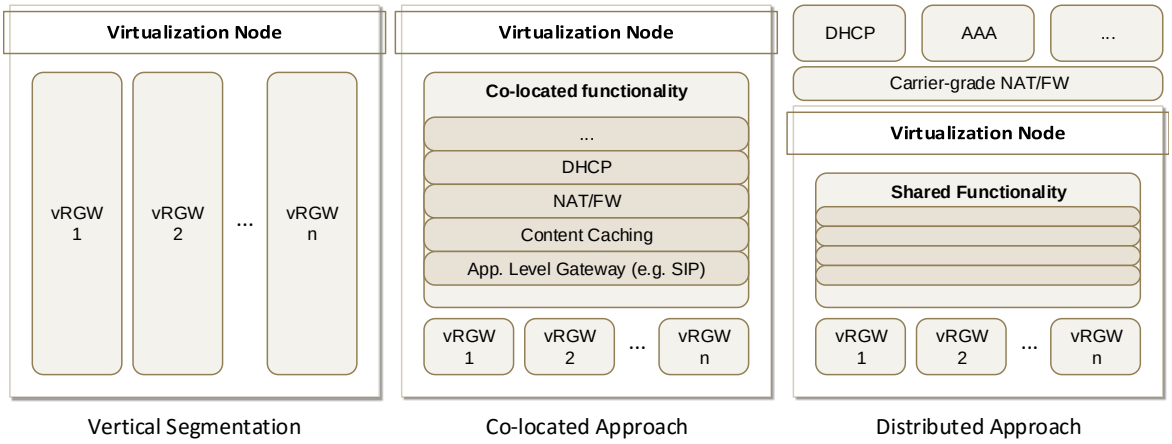


Figure 3. vRGW evolution from a vertical VM to a distributed approach [30]

of network appliances into virtualized software running on COTS (Commercial Off-The-Shelf) hardware is expected to result in the reduction of capital investment as well as energy consumption. In addition to the lowering of the CAPEX and OPEX, NFV can reduce the time to market of new services from months and years to weeks or days [42]. Besides having a faster introduction, the flexibility of NFV also allows for targeted and tailored services [43].

NFV, as standardized by the ETSI NFV Industry Specification Group (ETSI NFV ISG) [44], promotes the decoupling between network capacity and functionality, abstracting end-to-end services as entities using a service chaining approach, where services are modeled and described by composition of elementary VNF (Virtual Network Functions), PNF (Physical Network Functions) and endpoints, chained together by a Forwarding Graph (FG), as shown in Figure 4. This figure shows the virtualization layer performing an abstraction between the physical hardware (hosted in the NFVI point-of-presence, which are datacentres) and the software/virtualized instances. Moreover, FGs can be nested to define complex function blocks.

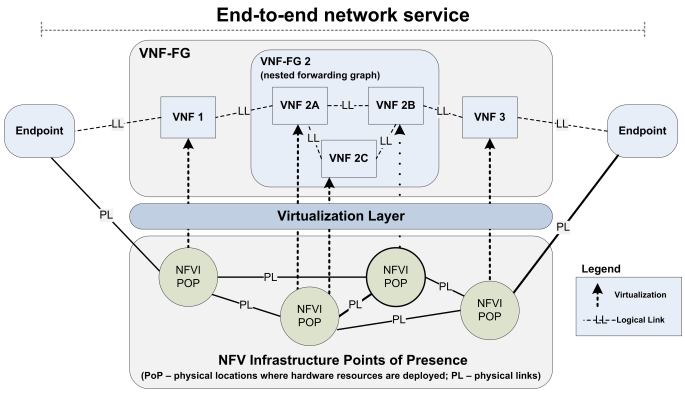


Figure 4. NFV service abstraction on top of NFV Infrastructure (NFVI) resources [45]

While VNFs are implemented in the form of software modules (usually hosted within containers or virtual machine instances, providing reusable function templates), PNFs are conventional network devices with close coupled software and hardware that perform network functions. The logical links in a FG constitute a network overlay, which can be implemented using Software Defined Networking (SDN) or network virtualization technologies such as VLANs [46] or MPLS Pseudowires [47], as depicted in Figure 4.

NFV and SDN are complementary technologies: while the first one attempts to optimize and streamline the deployment of network functions (firewalls, load balancers, etc.), the second one targets the optimization of the network that supports such services.

C. The ETSI Model

The ETSI NFV architectural reference framework is depicted in Figure 5, being composed by several functional modules:

- The NFV Infrastructure (NFVI) domain, which abstracts the computing, storage, and networking resources (provided using COTS hardware, accelerators, hypervisors, among other components) providing support for the VNFs.
- The Virtual Network Function domain, containing the VNF instances (deployed on virtual machines, for instance) which run on top of the NFVI, also including Element Management Systems (EMS) to ease integration with existing Operations Support Systems and Business Support Systems (OSS/BSS).
- The NFV Management and Orchestration (MANO or M&O) domain, which deals with orchestration and lifecycle management of physical and/or software resources that support the infrastructure virtualization and the lifecycle management of VNFs and the services built using them.

Also, NFVI resources may be distributed over different Points-of-Presence (NFVI PoP), geographically spread.

The MANO domain is in charge of the virtualization-specific tasks for the NFV framework, encompassing several components: the NFV Orchestrator, which takes care of network service lifecycle management across the operator domain (data centers included); the VNF Manager(s) (VNFM) which

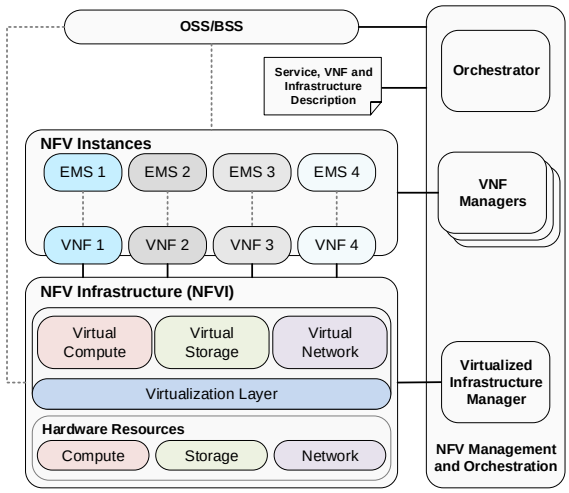


Figure 5. ETSI NFV framework architecture [17]

deals with the lifecycle management for the VNF instances; and the virtualized Infrastructure Managers (VIM), which are responsible for NFVI resource management. A set of metadata sources describe Service, VNFs and Infrastructure requirements, providing the MANO with information about the resources it has to manage. This provides the means for different resource providers (for instance a VNF provider or an Infrastructure provider, such as an hypervisor) to integrate within the NFV framework, by implementing the glue APIs and related descriptions.

In the ETSI model, SDN can play a decisive role to implement the network virtualization mechanisms that support the logical links of a FG service chain, but also to provide what the ETSI describes as the ”NFVI as a Service” use case, enabling operators to lease NFV Infrastructure resources from third-parties, to improve service coverage.

As for the impact on OSS/BSS systems, the MANO components for the ETSI NVFI have been designed and laid out to interact with existing OSS/BSS systems (albeit it is recognized that NFV will most likely have a profound effect on current OSS/BSS architectures). However, the interfaces within the MANO domain and between it and the OSS still need to be standardized to reduce the integration effort in a heterogeneous multi-vendor infrastructure. In order to enable automation and agile management, the NFV MANO and OSS/BSS need to agree on interfaces and associated information and data models, as well as their business processes (such as Billing or Security). The impact on existing OSS will depend on its own nature – in some situations it may be as simple as configuring an integration agent, while in others it might imply profound configuration changes and even roll-out of new OSS components. The ETSI NFV ISG is working to minimize the OPEX and complexity of integration but, once again, this is a work in progress as these aspects will need further development, involving other standardization bodies and organisms.

The ETSI NFV model provides a base for the development of a consensus among operators and vendors. However, as previously described, it is known that some issues were left out in terms of interfaces and data models [17]. The definition missing in some points of ETSI’s architectural framework regarding interfaces and interoperability between vendors and operators reflects on several projects being ”based on the ETSI framework” (such as ZOOM [48], CloudNFV [49], CloudBand [50], ExperiaSphere [51], HP OpenNFV [52], or Planet Orchestrate [53]) but without being compatible between them in terms of functions and services [54].

In the beginning of 2016 ETSI announced a new project: ETSI Open Source Mano (OSM) [55]. The main goal is to develop an NFV MANO software implementation to tackle some of the issues that were left out by the ETSI’s NFV architecture, leading to both initiatives (OSM and NFV ISG) complementing the work of each other. The project’s proof of concept aims at showing that a multi-vendor environment is capable of using and extending open-source based components while being orchestrated by an open-source orchestrator. The OSM orchestrator manages a heterogeneous cloud (composed by OpenStack [56] and OpenVIM [57]) and deploys, connects, and configures the NFV infrastructure that supports VPN and VoIP services. The use case covers a great deal of challenges that real production network would require, such as performance, multi-site orchestration, and multiple vendors. Moreover, it requires configuration of both physical and virtual components.

ETSI is still active in this domain of interface definition. Recent releases, such as [58], specify the interfaces supported over the VIM and VNF Manager elements of the ETSI architectural framework. The document lists and defines interfaces produced by the VIM and consumed by the VNFM. At the moment, there are no interfaces produced by the VNFM.

D. Stretching the Infrastructure to the Edge: Fog Computing

The fog computing paradigm aims at bringing cloud application services near the edge of the operator network. This allows for applications that traditionally run in the core of the network to be dynamically placed closer to the end devices which consume such services. As a result of having the computation physically closer to the end devices, a significant improvement on end-to-end latency can be obtained, which may be critical to different types of services.

There are several application fields that can use or take advantage of the fog paradigm, including: Augmented Reality (AR), smart grids, traffic lights, wireless sensor networks, smart building control, Internet of Things (IoT), and Cyber-Physical Systems (CPS) [59] [60] [61]. In one way or another, these are latency-sensitive applications whose experience can be ruined or severely worsen if the end-to-end delay is greater than tenths of milliseconds [59].

Fog computing can be of use in vRGW scenarios as a means to improve the user experience of some services – for instance, network functions can be instantiated at the edge of the network, closer to the RGW devices [62]. For example, if data is being transmitted between devices in the customer premises LAN, and some action needs to be done to that traffic (e.g., pass through a firewall) it will need to be redirected to

the network functions located in the operator side. Different latency results may be obtained if this is done in a data center, which can be quite distant, or at the edge of the TSP network, using fog computing technologies. The latter can result in a significant decrease in end-to-end latency.

IV. Current Virtual RGW Developments

This chapter analyses how the emergence of SDN and NFV enabled a new generation of vRGW proposals, more mature and focused on issues such as functional decoupling, scalability and dynamic accommodation of service and application requirements.

A. Proposals and Initiatives

This section provides an overview of the proposals and initiatives related to RGW virtualization. Its contents will be organized along three different groups, namely: standards-related initiatives, research works, and industry proposals.

1) Initiatives from Standardization Bodies: The ETSI NFV Industry Specification Group has described several use cases for NFV, among which the *Virtualization of Home Environment* scenario [17] is of particular interest, as it describes how the RGW (and even a Set-Top Box) could be virtualized and moved to a service platform in the network. In this scenario, depicted in Figure 6, the vRGW is still responsible for providing private addressing and mediating service delivery to the home LAN.

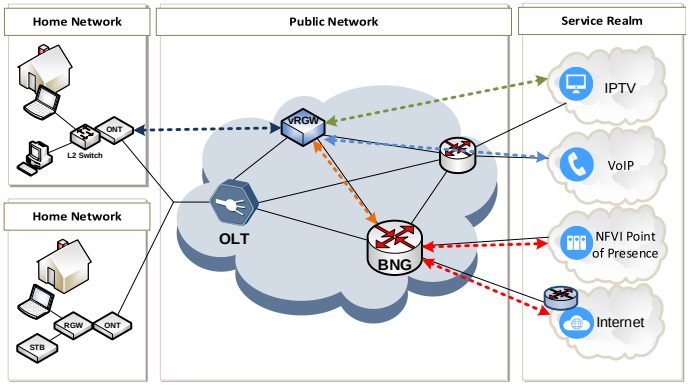


Figure 6. ETSI NFV Virtualization of Home Environment use case (adapted from [17])

Apart from the ETSI, the Broadband Forum (BBF) end-to-end architectures group has also been working on virtualizing Business and Home gateways, an effort documented on working texts WT-317, which includes the architecture for the Network Enhanced Residential Gateway (NERG), and TR-328 (Virtual Business Gateway) [63] [64] [65]. The NERG architecture (Figure 7) splits the vRGW functionality across a virtual Gateway (vG) – in charge of service and network functions such as IP forwarding, NAT and IP addressing – and the Bridged Residential Gateway (BRG), left at the customer premises and responsible for the forwarding plane (which may be an Optical Network Terminal with an integrated Ethernet switch, possibly with SDN support). The NERG is designed to accommodate SDN support in order to enable BRG control from the vG or another controller – such an arrangement requires in-band transport of SDN protocol interactions, demanding special attention to potential security and availability issues.

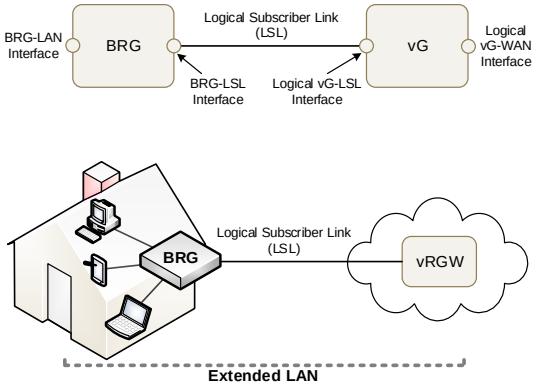


Figure 7. The Broadband Forum NERG concept (Network Enhanced Residential Gateway – adapted from [64])

WT-317 discusses several nodal distribution scenarios to decouple vRGW functionality across the operator infrastructure (Figure 8), using SDN and NFV to ease deployment and maintenance while improving its capabilities.

While some WT-317 scenarios are reminiscent of the Eurescom P2055[3] ideas – contemplating vRGW deployment within the access node, the BNG, or a data center/cloud – there are also new distribution concepts, such as the hybrid boxing model [64]. Hybrid boxing splits the vRGW into a Service-vRG (dealing with services and SDN control) and a Network-vRG (in charge of the forwarding plane), taking advantage of SDN to implement policy-based subscriber traffic forwarding. These proposals fill the void left by the ETSI vRGW use case, as they detail SDN-compatible functional decoupling strategies which are compatible with the introduction of NFV elements. Moreover, the NERG is also envisioned as a platform for leveraging the potential of x86 virtualization advances, pushing for a component-based model akin to an application store, to add new functionalities to the vRGW. Such a solution had already been proposed for conventional RGWs, in the form of TR-157 [66] component management for execution environments such as OSGi [67].

In the wake of the previous developments, TR-328 proposes an even more flexible approach for the vRGW, encompassing three deployment models (Figure 9): within the network (hosted in a Multi-Service Broadband Network Gateway or an elastic virtualization environment); at the customer premises (with the customer providing the NFV infrastructure); or as a set of decoupled functions spread between the customer premises and the network.

Besides the mapping of SDN-based use cases to its own reference network architectures described in TR-101 [31] and TR-145 [68] (and further documented in WT-302: Architecture and Connectivity of Cloud Services for Broadband Networks; and SD-313: Business Requirements and Framework for SDN in Telecommunication Broadband Networks), the BBF has

[3]Project previously mentioned in section II.B.

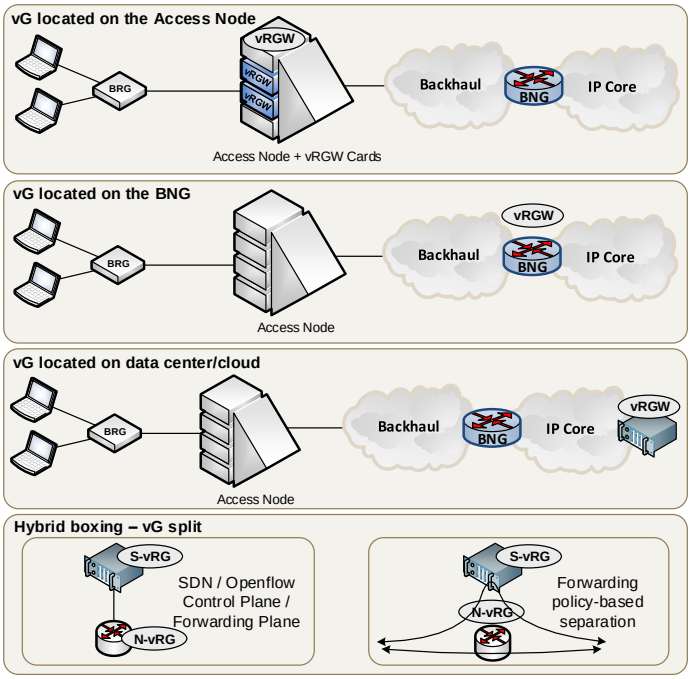


Figure 8. NFV end-to-end service with VNFs (adapted from [64])

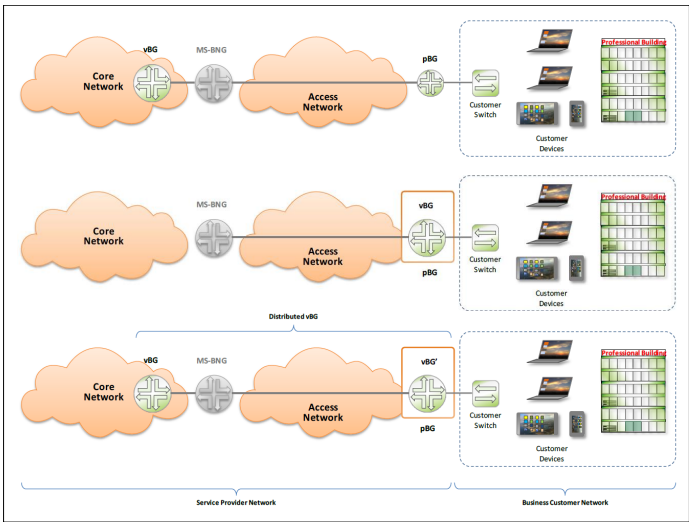


Figure 9. Broadband Forum's NERG vRGW deployment options (adapted from [63])

been working on the concept of flexible service chaining, as suggested by the SD-326 study document [69]. This is a generic concept, in the sense it does not necessarily involve the use of VNFs, going in line with the proposals laid out by [70]–[74].

Another proposal for functional distribution of vRGW components, from [75] and [76], is very similar to the BBF hybrid box model (Figure 10), also splitting the vRGW into a Virtual CPE Packet Forwarder (VPF) and a Virtual CPE Controller (VC), keeping a simple bridge device at the customer premises (although, unlike the BBF proposal, this one is devoid of SDN-like forwarding control).

In this architecture, the VPF is an SDN-enabled packet

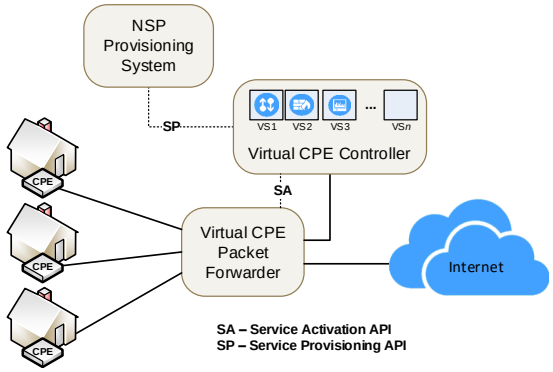


Figure 10. High level architecture for a SDN-based split vRGW (adapted from [76])

processing device, with the VC embedding the control plane controller for the VPF and hosting the Virtual Services (VS) available for subscribers (as well as the service subscription rules used to provide them). Each VS contains the service definitions and respective service logic (for instance, a firewall or parental control service). Operators are supposed to be able to scale VS horizontally, also allocating instances on a per-subscriber basis.

2) Research Initiatives: Current research is also adopting the use of SDN and NFV to tackle RGW virtualization.

In [77], the authors present an NFV and SDN-based vRGW example (the virtualized management and networking domain - vMANDO), with a special focus on the design of a gateway management approach directed at end-users with low or no technological background, enabling them to easily manage the home environment. This can lead to reduced costs on the operator's side (less tech calls and on-site maintenance) and higher user satisfaction rates.

A vRGW concept focused on M2M communications is proposed in [78], which also includes the description of a proof-of-concept gateway for testing based on a composition of open source software. The use of containers to reduce the resource usage in RGW virtualization is addressed by [79]. Authors used full and individual RGW virtualization, with resource savings deriving mostly from having multiple instances sharing the underlying OS. These results can be applied to scenarios where virtualization is integrally performed for each customer instance – not to multi-tenancy scenarios where a network function is shared across multiple customers.

A vRGW implementation based on SDN and NFV, using multiple flow table strategies was also proposed by [80]. For the customer's connectivity, a simple SDN-enabled switch is placed in their premises, while the functions are hosted at the operator's edge. As a strategy for migration between physical RGWs and virtualized instances, [81] proposes to integrate NFV into the RGW using modular gateways. As the gateways are limited devices, the modules installed in the gateway are used to redirect the traffic to virtualized functions.

3) Industry Initiatives: At the moment, several operators are showing interest in the research and development of vRGW solutions [82][83][84][85]. Telefónica, for example, has done a trial in Brazil (where it operates as Vivo [86]) during

2014, with deployments consisting of a simplified gateway to provide basic connectivity, acting as an access point, switch and modem. The adopted approach follows the NFV-based model, with functions moved from the customer's home to the operator's infrastructure [87].

One thing that is common to most industry initiatives is the support of the functions in an SDN-connected NFV infrastructure. However, there are few data published regarding industry initiatives, which indicates that these efforts are still in a somewhat early stage regarding commercial deployments.

In a broader scope, the CORD project [88] [89] aims at providing a reference implementation of a cloud-based service delivery platform for TSPs, combining the use of cloud computing, SDN and NFV. Having started as an ONOS [90] use case, CORD became an open source project of its own, being supported by the Open Networking Foundation (ONF), as well as the Linux Foundation. Its main objective is to provide an unified platform to improve the provision of telecommunication services, using open source software and commodity hardware components such as servers, switches and I/O.

A set of services has been derived from the CORD initiative. Together they form the Residential CORD (R-CORD) service profile [91]. R-CORD variants are being planned and tested by several NSP (Network Service Provider) (e.g., AT&T, Comcast, NTT, DT, Telefónica), being also related with the vOLTHA (virtual Optical Line Termination - Hardware Abstraction) project [92], which deals with the hardware abstraction of passive optical networks (PON). The main services provided by R-CORD are:

- *Virtual OLT (vOLT)* - The main objective is to virtualize the optical line termination (OLT) to replace the proprietary OLT components with a mixture of COTS hardware and open source software [93].
- *Virtual Router (vRouter)* - Placed at the edge of the ISP network, the broadband network gateway (BNG) connects the access networks to the core network of the TSP in traditional environments. In the CORD architecture the vRouter is used to provide the routing functionality between the CORD and the access network [94].
- *Virtual Subscriber Gateway (vSG)* - One of the main use cases of the project is a vRGW implementation designated as vSG (virtual Subscriber Gateway) [95]. The CORD architecture accepts different implementation alternatives, such as having the functions to host the customer's bundle of network functions on a VM, on a lightweight container or on a chain of lightweight containers. Nonetheless, the main idea is that the functions will be located in the central office (CO) and the customer premises is left with a simple device in its home (i.e., a bare-metal switch) simple enough to provide connectivity between the CO and the customer home [96].

Table I summarizes the proposals discussed in this subsection, classified accordingly with their *generation* (before and after the emergence of NFV and SDN technologies), *scope* (standards-related initiatives, research works, and industry proposals) and *focus* (gateway, services, and architecture). This summary will later be complemented with the proposal of a reference taxonomy, in Section IV-D. A more detailed technical summary will also be provided later on, in Table III.

B. Functional Placement

Possibly because the introduction of NFV within carrier environments is still a matter under definition, most vRGW proposals do not encompass a clear description of functional or nodal distribution within the infrastructure, which can be done in several ways.

A first possible approach would be, for example, to have each function from a client being handled by one dedicated VNF. This approach provides a simple and straightforward implementation, but is prone to scalability problems like those already pointed out in previous solutions where each vRGW is individually virtualized as a singe instance [18].

One way to minimize this scalability problem is to improve the efficiency of the software providing the functions [98]. This can be done using software containers to run several different functions in one VM instance, instead of having separate VMs for each function – thus reducing the computational overhead of having multiple OS instances. The computational overhead can be further reduced if the functions become capable of handling multiple tenants. As an example, in a scenario with a function providing DHCP service, the function would provide connectivity for devices from multiple home networks, instead of having a dedicated DHCP function for each home network. However, this poses new challenges that must be addressed to assure the security of the devices in the home networks: when functions become shared between different customers their isolation must be guaranteed. This is necessary when using containers to execute different functions within the same VM, but more importantly, when using the same function to serve multiple clients in a multi-tenant scenario.

In [97], authors presented a hybrid solution supporting network function placement both on the operator infrastructure and on CPEs, making it possible to host complex functions in the operator datacenter while keeping lightweight or latency-sensitive functions running natively on CPEs. However, the use of local functions may affect the future-proof capabilities of the RGW device, in comparison with scenarios where all functions run in the operator infrastructure, depending on which functions are intended to be hosted locally.

C. The role of MANO in the NFV-Enabled vRGW

Apart from functional placement, NFV Management and Orchestration is also a key part of the NFV-enabled vRGW. While the BBF proposes the concept of NERG orchestrator, the ETSI architecture goes beyond by proposing a MANO subsystem (Orchestrator, VNF Manager and Virtualized Infrastructure Manager) with defined APIs, data models and interfaces. However, there are some points still missing in this architecture that should be addressed, such as the management of the VNF life cycle, the service package format and the service template metadata formats (i.e. VNF descriptors and Network Service Descriptors).

Those points are essential to have a standardized or *de facto* management and orchestration that can be used by

Table I
VRGW PROPOSAL CLASSIFICATION

Generation	Proposal	Scope	Main Focus
1st Gen	Cruz et al. [30]	Research Work	Gateway
	Modig [79]	Research Work	Architecture
	Eurescom P2055 [27]	Industry Proposal	Gateway
2nd Gen	Proenca et al. [85]	Research Work	Gateway
	Herbaut et al. [81]	Research Work	Gateway
	OpenCord [95] [90]	Research Work	Gateway
	Dillon [78]	Research Work	Services
	Bonafiglia [97]	Research Work	Architecture
	Nen-Fu [80]	Research Work	Architecture
	NEC [82]	Industry Proposal	Gateway
	Ericsson [83]	Industry Proposal	Gateway
	Telefnica [87]	Industry Proposal	Gateway
	BBF - VBG (TR-328) [63]	Standards Initiative	Gateway
	BBF - NERG [65]	Standards Initiative	Gateway
	ETSI NFV Use Case [17]	Standards Initiative	Gateway

different vendors, manufacturers and operators. It is important to define the guidelines to address these loose ends in the shortest amount of time possible. The main reason for this is that the operators are already investing a lot of effort and resources in the usage of NFV, and if these guidelines take too long to be defined we may reach a point where it becomes impossible (at least at reasonable costs) to reverse the vendor-specific solutions adopted in the meantime [11]. Nonetheless, ETSI is addressing this with ongoing standardization work in the scope of its NFV-IFA workgroup [99][58][100], which addresses interfaces between architectural components such as the orchestrator and VIM, and the VIM and the VNFM. Also, the ETSI is undergoing a collaboration with the Organization for the Advancement of Structured Information Standards (OASIS) to define adequate metadata formats for service and VNF descriptors, based on the Topology and Orchestration Specification for Cloud Applications (TOSCA) language [101].

One of the important aspects of the MANO role is that a large number of instances of virtualized functions must be deployed and configured. For that to be feasible, the management and orchestration must be highly automated and coordinated, in order to provide the necessary provisioning and instantiation. On top of that, those functions will need to be connected using the underlying network architecture in order to create the necessary service chaining to provide the service subscribed by the customer. The high-level orchestration of that layer will also be a responsibility of the MANO, which will coordinate the underlying network components (e.g., OpenFlow controller in a SDN enabled scenario) through its southbound interfaces.

Despite the issues mentioned above, efforts are being made to use NFV in the operator scope. OpenMANO [57] is one example of a framework to manage and orchestrate NFV. This is an open source project created by Telefónica and it is based on ETSIs recommendations and guidelines for NFV. Figure 11 illustrates the relationship and correspondence between the two frameworks. In addition to the MANO capabilities, OpenMANO includes other features as well with its own VIM. The application of these management frameworks to the vRGW use case is addressed, for instance, by [85].

The OpenMANO framework includes three main software components: openvim, openmano[4] (orchestration component), and openmano-gui. The latter provides a web based interface to interact with the framework. This GUI uses an API exposed by the openmano orchestrator to manage the NFV scenarios. The orchestrator will then use the API exposed by the openvim to have the necessary changes made to the infrastructure (both in terms of computing nodes and networking). The connections between the different software components of the architecture are illustrated in Figure 12.

The orchestrator (with the same name as the framework) is the main component of the architecture as it is responsible for NFV orchestration. As illustrated in figure 12, it exposes

[4]For the sake of clarity, the Telefónica project will be referenced as OpenMANO and the orchestrator component as openmano.

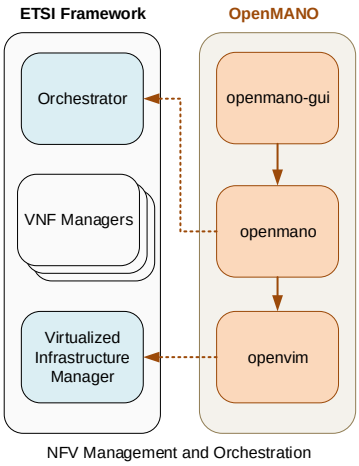


Figure 11. Correspondence of OpenMANO's MANO components to ETSI's NFV Architectural Framework

an API to allow third party applications to use the orchestration capabilities. The southbound side implements the VIM connector that can be adapted or changed to connect to other VIMs such as Openstack [56].

This work has been used as a base for the already mentioned ETSI OSM project (cf. Section III.C). Moreover, OpenMANO has been fully integrated in OSM and has been deprecated as a standalone project in the end of 2016.

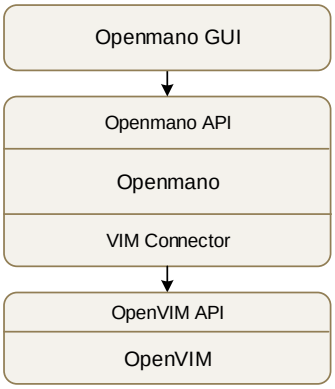


Figure 12. OpenMANO components and their API connections [57]

The openmano framework is an example aimed at a complete implementation of the ETSI framework, but other efforts might implement only part of it. The issues regarding the missing pieces in ETSIs guidelines that were mentioned previously grow in importance in these cases as the different frameworks will need to understand each others' interfaces. Another example of a framework that might benefit from this interoperability is Open Platform for NFV (OPNFV) [102], an open source project announced by the Linux Foundation in 2014. The project was launched with the objective of providing an integrated platform to accelerate the introduction of new NFV products and services. Industry vendors and operators have been supporting the project, which has a considerable number of members at the moment. The first OPNFV release (Arno) rolled out during June of 2015 [103]. Currently, OPNFV is providing consumable releases approximately every six months.

D. Reference Taxonomy

In this subsection we finalize the discussion of vRGW developments with the proposal of a reference taxonomy for classifying past and ongoing initiatives. This taxonomy is organized around four key axis: *Integration with the Operator's Infrastructure*; *Function Distribution*; *Scope*; and *Standards Compliance*. Figure 13 illustrates the proposed taxonomy, along with the categorization of previous works already discussed in this paper.

Integration with the Operator's Infrastructure addresses the relationship of the vRGW with the operator's ecosystem, considering two aspects: integration with current OSS and BSS systems; and the support for coexistence with legacy architectures – an important aspect for allowing smoother, incremental migration paths.

Function Distribution splits into two orthogonal subcharacteristics: *Function Placement* and *Function Coupling*.

Function Placement relates to the physical placement of the functions, for which we identify three main categories. The first is function placement on *Network Equipment*, that includes placing functions on the BNG or even on the bridge device in the customer home as virtualized instances (which has been seen in proposals such as [81], for functions with low resource requirements). Proposals for deploying the vRGW in the datacentres of the operator match the *Operator Cloud* category. Finally, proposals that use a mixture of network equipment and operator cloud placements are categorized as *Hybrid*. NFV-based approaches fit into the two later categories, depending on whether they are exclusively based on datacentre deployment or on mixed solutions.

Regarding *Function Coupling*, the taxonomy considers three categories: *Vertical*, *Co-Located*, and *Distributed*. A *Vertical* approach is used when virtualizing each individual vRGW as is (as done, for example, in initial proposals with a straightforward implementation but with severe scalability issues for real-world deployment). *Co-located* coupling matches scenarios with some shared functionality, such as DHCP or NAT, but on a local domain. *Distributed* approaches apply when the functionalities are massively distributed across geographically dispersed locations.

The proposals can also be classified by their *scope*, considering three main categories: *Research Works*, *Industry Proposals*, and initiatives directly originated from *Standards Bodies*.

Finally, the taxonomy considers *Standards Compliance* for the main standards organizations currently pushing the vRGW developments.

V. Performance Optimization

Performance stands among the various requirements for the vRGW: it must be at least at the same level of traditional

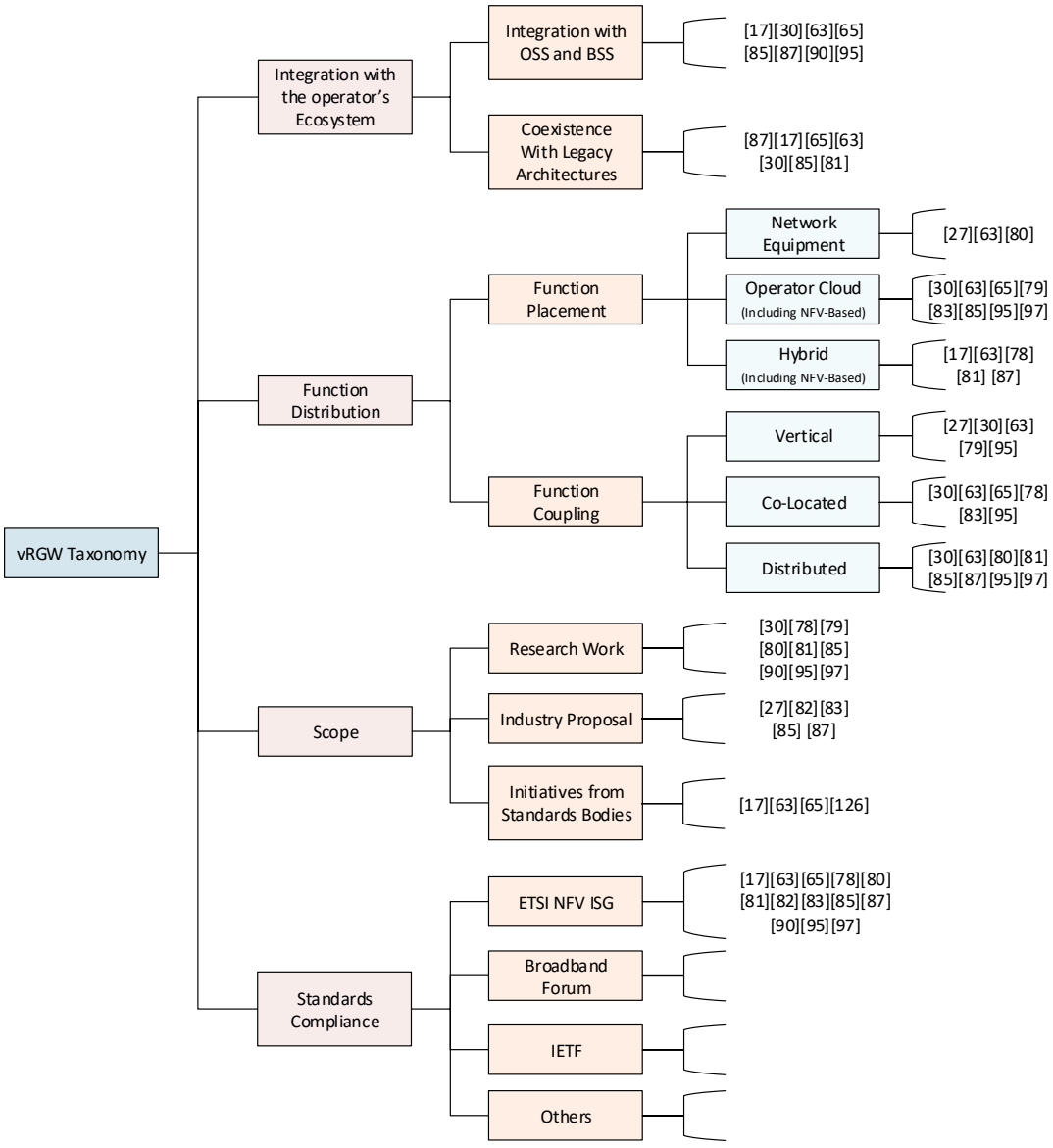


Figure 13. Proposed Taxonomy for vRGW Proposals

counterparts [11]. The vRGW performance is deeply tied to underlying technologies such as NVF. ETSI has published several recommendations and best practices for the deployment of VNFs over a compute host [104]. There have been some research in hardware and software virtualization that directly or indirectly has been beneficial to NFV performance. A while back, there were constraints in network performance in VNF environments that could limit their usability in vRGW scenarios [43][105]. However, recent developments in terms of hardware virtualization and software optimization have made possible to increase the networking performance of the virtualized functions. It is worth noting that additionally to the increase of the VNF performance, the acceleration techniques are also a good way to make the most of the hardware deployed and a way to lower deployment and running costs.

Next, we look into optimizations that can benefit the performance of NFV (and vRGW implementations), divided into three categories: network; virtualization node; and integration of hardware acceleration mechanisms.

A. Networking

One way of increasing networking performance is by optimizing the libraries that the applications use to interact with the NIC. Released by Intel, the Data Plane Development Kit (DPDK) is a set of libraries for the development of applications that require intensive network packet processing. DPDK processes network packets in polling mode instead of the default interrupt mode. This mode reduces the usage of CPU cycles per processed packet by continuously checking the NIC for state changes, which mitigates the CPU interruption

in packet processing. DPDK is able to provide substantial improvements of packet processing performance compared with traditional libraries on COTS hardware, by allowing applications to access the NICs without the overhead of the OS [106]. On the other hand, when using this library, there is no interrupt when packets are available in the NIC. Traditional libraries (e.g., Linux's LibPCAP) limit performance, while DPDK allows a greater use of the hardware. For example in [107], packet processing of a virtual Deep Packet Inspection (DPI) application on a 10Gbps NIC was capped at around 1Gbps using LibPCAP. On the other hand, it provided near line rate when the same application was using DPDK.

Hardware virtualization techniques can also play an important role to improve the performance of NFV by reducing processing overheads. Single Root I/O Virtualization (SR-IOV) specified by the Peripheral Component Interconnect Special Interest Group (PCI-SIG) [108] can divide a piece of hardware into multiple PCI Express Requester IDs (virtual instances of PCI functions) and allocate each one directly to a VM. This will reduce the interactions between the hypervisor and the VM, as the VM has direct access to the hardware and enables near native performance. As an example, while performing packet processing operations on a 10Gb link, [107] managed to reduce performance degradation in a virtualized deployment to 19%, comparing with a physical deployment, by using SR-IOV. Despite the performance benefits that SR-IOV can bring to NFV, care must be taken as there are deployment scenarios where it might not be a good option. For example, [109] describes a Docker-enabled container scenario where packet forwarding between VNFs in an intra-host could have up to 100% more round trip time (RTT) when using SR-IOV, than with macvlan, bridged, or OVS-enabled interfaces. The reason for the increased RTT is that the switching is offloaded to a PCIe device and the effects are greater with a larger number of chained functions and an increased packet size.

Another recent networking optimization in packet switching is the SnabbSwitch. This is a virtual switch for the KVM hypervisor running in user space (it is planned to be extended to other architectures such as ARMv8). SnabbSwitch is aimed at high performance packet processing in NFV environments. In tests, SnabbSwitch proved capable of processing packets at near line rate in some scenarios [110].

Some proposals have a more specific target, and use hardware acceleration to provide better performance to NFV. For example, [111] proposes the replacement of NICs with FPGA boards with on-board networking interfaces (such as NetFPGA [112]). The authors propose shifting some of the processing logic directly to the hardware responsible for handling network packets. When a packet arrives at an interface, it may be processed by the FPGA and sent directly to another network interface inside the FPGA board, or sent to the software appliance to be further processed. This way the network function can be a software based, hardware based, or a mixture of both.

B. Virtualization node

The usage of container technologies to host the different VNFs, instead of individual guest OS instances for each virtualized function [109][113][114][115], has also been addressed by recent research efforts. Containers provide a way to reduce the overhead associated with hosting several OS instances, providing lightweight OS-level virtualization instead of a full, hypervisor-based approach [116], allowing for the deployment of a higher number of instances within the same hardware. Modig [79] has studied the resource usage in a container-based RGW virtualization approach using OpenVZ. Testing showed that using containers can increase the performance and reduce resource usage, specifically in terms of memory and storage.

Container-enabled virtualization has been compared with VM virtualization in the literature. In [109], the networking performance of Xen and Docker enabled functions has been compared, with a special focus on latency and jitter. They have also measured the CPU cycles impact of these virtualization techniques when using a range of networking technologies (direct, macvlan, SR-IOV, bridge and OVS). Their research showed that the use of OS-level virtualization (i.e., using containers) can increase performance, when compared with hypervisor virtualization using the same hardware. This advantage in terms of latency and jitter has also been pointed out by [114]. The authors of [113] also found Docker to have a lower latency, when compared with KVM deployments in chained VNF scenarios.

Another point that must be considered is the maturity of large-scale container orchestration. Compared with large-scale VM management, container management at scale is fairly recent with tools such as kubernetes [117] and CoreOS [118]. Also, security and isolation must be guaranteed [119].

Improvements in some NFV scenarios might also be obtained by exploring alternative server architectures. [106] notes that the traditional server architecture may not be the best one to fully exploit some NFV scenarios. Traditionally, server architecture follows a model of having a small number of powerful CPU cores. However, looking specifically into the vRGW scenario, many of the involved VNFs are not CPU-bounded, focusing instead on network I/O. As a result, these functions may benefit from an approach with a higher number of low power cores instead of a small number of powerful cores. Mellanox's [120] TILE-Mx100, an ARM-based SoC with 100 cores, is an example of such architecture. Architectures using a large number of small cores together with mechanisms such as DPDK may increase the efficiency of network I/O intensive VNFs [106].

C. Integration and Standardization of Hardware Acceleration Mechanisms

Table II summarizes the main performance-enhancing techniques for NFV environments that might be relevant for vRGW scenarios.

ETSI has also done some work related with the use of hardware acceleration techniques to improve the NFV performance, which resulted in a set of documents [121][122][123][124] from the ETSI GS NFV-IFA group.

Table II
NFV PERFORMANCE OPTIMIZATIONS FOR VRGW SCENARIOS

Technique	Scope	Type	Main Impact
DPDK [106] [107]	Network	Network Library	Reduced latency
SR-IOV [108] [107] [109]	Network	Hardware_driver	Hardware slicing
Snabswitch [110]	Network	Software switch	HHigh-performance packet processing
NetFPGA [111] [112]	Network	FPGA-based NIC	Handling packets at HW-level
Container-based VNFs [109] [113] [114] [115] [116] [117] and CoreOS [118] [119]	Virtualization node	VNF host	OS overhead reduction
Mellanox TILE-Mx100 [120]	Virtualization node	High core-count architectures	Increase efficiency in I/O intensive VNFs
ETSI VNF accelerator	Integration and standardization	Development architecture	Improve the interoperability of VNFC and accelerators

Some preliminary work on the subject has been made with a proposal of a common architecture and an abstraction layer. This type of acceleration aims at helping VNFs with special performance needs, for instance to meet certain latency or service-level agreement (SLA) requirements.

This work is largely related with the NFVI section of ETSI's architectural framework for NFV, since it covers all the hardware and software components that compose the environment supporting the deployed VNFs. Moreover, it covers the use of acceleration in all domains covered in the NFVI: compute, network, and storage. Also, this includes hardware acceleration, software acceleration, and any combination of the two.

ETSI is aiming at an architectural approach that uses an abstraction layer (Acceleration Abstraction Layer, or AAL) to enhance the interoperability between the Virtual Network Function Component (VNFC) and the accelerators (see Figure 14). VNF acceleration implementations may range from tightly-coupled software and hardware (passthrough model) to loosely-coupled software that takes advantage of an acceleration abstraction model. This model shows some advantages over the passthrough model. With passthrough, the drivers for the hardware are contained in the VNF. This way, a new hardware release will require vendors to update the VNFs. In the abstraction model the hardware drivers are a responsibility of the NFVI that will provide the functionality for the VNF. The VNF will have a generic driver that will not make any assumption about the underlying NFVI.

ETSI also presents an accelerator taxonomy, based on the use cases presented in [121]. The taxonomy classifies the accelerators based on a number of criteria, such as the software that makes use of the accelerator, it's type, location, and functionality [121]. The taxonomy is based on use cases organized in three categories: compute, network, and storage acceleration. Some of the example use cases for computing acceleration are key for vRGW scenarios, such as IPSec tunnel termination, Next Generation Firewall (NGFW) Acceleration,

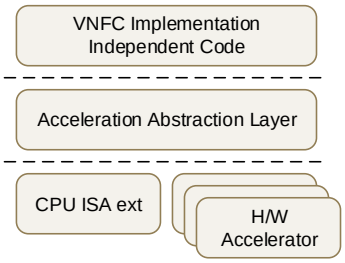


Figure 14. ETSI layered architecture for VNF accelerator [121]

Virtual Acceleration Interface for VNFs, Transcoding and Deep Packet Inspection. Network acceleration can be used in scenarios of Load Balancing and NAT, NFVI Virtual Networking Offload, NFVI Secure Overlay Offload, and in Dynamic Optimization of Packet Flow Routing.

This work has been carried further in [122] to give more detail to the proposed concepts and architectures. Among the developments there is the identification of common design patterns to enable an VNFC instance to set-up and use accelerators in run-time. Additionally, the document also describes how VNF vendors can take advantage of the accelerators without being dependent on the implementation. Finally, it defines methods and requirements that enable VNF independence from specific accelerator implementations.

ETSI has also approached some aspects related to virtual switch (vSwitch) performance [123]. This is a critical point of the NFV infrastructure due to being a convergence point for VNF traffic, whether it is from VNFs of the same compute node or different compute nodes. This work also describes some characteristics of the usage of vSwitches in these environments, listing some of the functions they may perform (such as load balancing). It also describes some use cases and deployment scenarios, as well as the specific characteristics

needed for the measurement and benchmarking of the virtual switching environment.

Other proposals exist in the literature to enhance the performance of NFV, such as fast path offloading (FPO) [125], which is also beneficial for vRGW scenarios. FPO may be used to improve the performance of an L7 load balancer, by offloading the flow redirection to the fast path, and performing only the flow configuration at the VNF level. This method is similar to the Open vSwitch slow path/fast path architecture, where a forwarding rule is executed at kernel level (fast path) after being processed the first time at user level (slow path).

VI. Discussion

The previous sections provided an overview of the existing proposals for virtualizing the RGW, with Table III summarizing the main features of each one. Looking at those proposals, it is clear that current RGW architectures are quite different from the new proposals, designed for emerging/future architectures and services. Next, we will discuss some of the key aspects and open challenges related with the vRGW concept.

A. Moving away from vertical segmentation

Most of the earliest vRGW proposals relied on some sort of vertical segmentation of RGW instances (cf. Figure 3). These were used as baseline for performing initial tests and implementing proof-of-concept demonstrators. However, they had considerable limitations in terms of applicability. They were a good start to validate the virtualization idea, but were not applicable to real world scenarios where thousands of instances would need to be deployed. We can point out two distinct vertically segmentated type of proposals: those based on dedicated vRGW line cards, and those using virtualization. The latter being a rather simplistic approach which took the traditional RGW and virtualized it as a full RGW implementation. Both have limitations in terms of scalability to the millions of instances that one single provider might have deployed [17][18].

B. Scaling and performance

As mentioned in the previous subsection, the initial proposals were focused mostly on functional aspects, with little attention paid to scaling issues. Moreover, at the time they were devised there were still few hardware acceleration solutions for the data path. Later approaches have paid more attention to scalability and performance, trying to combine more efficient vRGW segmentation solutions with the recent advances on virtualization and hardware acceleration, significantly decreasing the overhead imposed by the underlying support infrastructure while also taking advantage of the acceleration mechanisms provided by the hardware to streamline and optimize the operation of VNF instances. Some of the these optimizations (introduced in Table II) are related with aspects such as networking, containerization of software instances and virtual switches. Nonetheless, this is still work-in-progress with considerable space for improvement.

Still in this scope, it should also be mentioned that there is a remarkable lack of quantitative data publicly available. In fact, very few projects released quantitative data, even at partial level – presumably due to its strategic value for involved operators and manufacturers. Without this quantitative data it becomes considerably more difficult to assess the overall performance and scalability of vRGW platforms, as well as their economical impact.

C. Novel vRGW-enabled services

In addition to more flexible deployments and cost reductions, the virtualization of the RGW can also drive the introduction of new services, some of which may have not been possible with current gateways. In the past, TSPs have increased their service portfolio as the infrastructures grew. When broadband access allowed for operators to provide high speed Internet to their costumers, new services appeared to take advantage of it, such as IPTV and VoIP. More recently, these services have expanded to a broader range, including smart-home applications and utilities such as the ones mentioned in [127], in M2M communication scenarios [78] and in healthcare Ṅow, the flexibility of instantiating network functions and easily interconnecting them, without waiting for expensive and slow hardware and firmware updates, has the potential of driving a new wave of novel services.

In addition to the RGW, more extensive virtualization of other CPE devices can be expected, including for instance Set-Top Boxes (STB), which that can take advantage of most of the vRGW benefits and also consolidate storage capacity in the data centre (for example, when a show is recorded by a large number of customers, only one instance needs to be saved in the operator infrastructure, instead of having one copy in each customer premises, as with traditional STBs). Gaming consoles are also expected to benefit from virtualization: the most technologically limiting factor for a good gaming experience is latency, which with current FTTH architectures is significantly reduced when compared with older broadband network architectures. Finally, more general services such as VPN for both business and home markets are more easily deployed. For instance, in a business environment where a company has several branches, each one with a virtualized gateway, setting up a VPN connection can be as simple as creating a link between the virtual gateways in the datacenter(s). Nonetheless, these are just the more obvious Use Cases, and extensive scouting and exploitation of novel applications is expected in the next years – especially because the introduction of NFV (discussed next) makes it possible to explore customization and niche markets which were not economically attractive before.

D. The impact of NFV on Service Design and Customization

As already mentioned, the emergence of the NFV concept was one of the most significant developments for the vRGW concept. By providing a flexible way to deploy network functions as individual VNFs, a service can be split into several distinct functions that, altogether, represent a customer gateway service. Providers have a pool of functions that can

Table III
COMPARISON OF RGW VIRTUALIZATION APPROACHES

Proposal	vRGW Use Case	Type	VIM	Coexistence	OSS/BSS	Multi Tenancy	Status
Open-Cord [95] [90]	Yes	Open-source NFV project	OpenStack	–	Includes Northbound Interfaces	Yes	Under active development
Telefónica [87]	Yes	NFV-based vRGW PoC	OpenStack	Coexists with legacy infrastructure	Includes API to use existent OSS/BSS	Yes	Commercial deployment were planned for 2015
ETSI NFV Use Case [17]	Yes	Proposed use case for NFV-based vRGW	Yes, using ETSI's NFV reference architecture	Mandates coexistence with virtual and non-virtual functions	Recommends integration with existing BSS/OSS	Mentioned with issues to be resolved	Published in ETSI GS NFV 001 [126]
BBF NERG [65]	Yes	vRGW proposal	–	Expects the coexistence of legacy clients	Expects BSS/OSS to be integrated	–	Technical report released
BBF - VBG (TR-328) [63]	No	vBG system architecture proposal	Specifies Infrastructure management reference points	Requires backwards compatibility	Specifies reference points to existing systems	–	Technical report released
Eurescom P2055 [27]	Yes	Study on RGW virtualization	–	–	–	–	Finished project
Ericsson [83]	Yes	Whitepaper Proposal	–	–	–	Yes	–
NEC [82]	Yes	Whitepaper proposal	–	–	–	–	–
Cruz et al. [30]	Yes	Architecture Proposal	OpenStack	Assumes coexistence for ease of deployment	Recommends integration with existing BSS/OSS	No, but opens Multi Tenancy possibility in the future	Proposed architecture
Proenca et al. [85]	Yes	NFV-based vRGW PoC	Custom Openstack	Integrates with legacy components	Integrates with current OSS/BSS	–	Published PoC results
Herbaut et al. [81]	Yes	NFV-based vRGW PoC	–	Yes	–	–	Published PoC and results
Dillon [78]	No	M2M Gateway PoC	–	–	–	–	PoC proposal
Bonafiglia [97]	Yes	Architecture options	–	–	–	–	Published PoC results
Huang [80]	Yes	Multiple Flow Table vCPE Framework	–	–	–	–	Published PoC results
Modig [79]	Yes	Container based virtualization	–	–	–	–	Published results

be used to build an end-to-end service. Graph-like Service Function Chains provide a guideline path for traffic steering, enabling the customer's network flows to reach each of the individual network functions that compose the service, such as URL filters and firewalls. Traditionally, service design is a task that can take a significant amount of time from since it starts until it becomes ready for customer use. However, using the NFV's flexibility, the creation of tailor-made services to smaller customer groups can be done on-demand, by structuring the needed functions and building the respective service chains.

The NFV concept is also partially responsible for the horizontal segmentation of current vRGW proposals. By providing a flexible way to instantiate and deploy network functions, it made it easier to develop flexible multi-tenant functions, such as those used in [85] – e.g., instead of having one URL filter for each customer a broader service serves multiple customers.

From a research point-of-view, this deep connection between the NFV and vRGW concepts opens both new prospects and new challenges. For instance, the definition of metadata formats and interfaces for VNF and service templates must be flexible enough to easily accommodate the introduction of new elements or the the nesting of already defined service abstractions within existing vRGW instances, in a seamless way.

E. OSS/BSS integration

While earlier vRGW proof-of-concepts focused on other functional aspects, large scale deployment of vRGWs is not possible without the solid management capabilities currently provided by the operator's OSS and BSS systems (for operations and business management, respectively). As these are often mature systems that operators have long used and extensively refined for their operations, it is important that

new vRGW architectures are capable of integrating with them (either directly or using some sort of adapters).

When using an NFV-based approach, the VNF lifecycle operations should be able to be integrated into current OSS/BSS systems, ideally using automated management techniques to reduce error rates, and avoiding vendor lock-in to maximize the operator's acceptance.

Undergoing efforts in this specific direction include for instance the OASIS/TOSCA metadata formats [101], whose objective is to support the automated deployment of applications as well as their management. It uses an XML-based format to model an application architecture, its components, and the relationships among them in a topology graph.

F. Migration paths/coexistence of legacy and vRGW

In addition to the operators' OSS and BSS systems, the acceptance of new vRGW architectures requires the co-existence between current (legacy) and new architectures. This arises from the fact that the large infrastructure already deployed and the high number of customers served by it, which sometimes reaches millions of customers for a single service provider, make it difficult (if not impossible) for the vRGW to be deployed without taking care of its coexistence with existing architectures.

RGW/vRGW coexistence encompasses several aspects, with OSS/BSS integration being one of the most important. From this perspective, the integration of the vRGW within the current OSS/BSS systems could ease such integration (as already suggested in the previous point), for which there are current efforts in terms of function data models and interfaces (described in the previous section). This would allow for a gradual and smooth deployment of new vRGWs and enabling physical devices, in parallel with the decommissioning of the current classic RGWs. ETSI's proposal for NFV goes in line with this, pointing out the need for coexistence between virtual and physical functions in the same environment [17], [126]. A proof of concept following this mindset, with an NFV-based vRGW integrated with an existing legacy infrastructure, is presented in [85].

G. Security and User acceptance

Operators must assure that the security levels that exist currently are maintained as much as possible in the vRGW scenarios. Current containerization technologies such as Docker can be configured to provide a satisfactory amount of security [128][129]. Moreover, there is a great research effort being put into improving the security in this area. The security issues include having proper isolation among individual customer domains, especially in cases where multi tenant-supported functions are involved. Moreover, the connection between the customer premises and the datacentre should also remain secured with proper encryption and encapsulation.

The way operators offer these services to their customers may influence their acceptance to this new paradigm. Some clients may be suspicious of having less equipment in their houses, fearing a loss of control or property – even though legacy equipment such as the RGW and the Set-Top-Box are already partially managed directly by the operator. This can be counteracted with offering sufficient control of their environment in the user portals provided to customers. Current RGW configuration management requires a level of technical knowledge higher than the average user has. Changing the RGW management paradigm to one more focused on the users [130] [77] can help them be more involved in the management and configuration of their network. Finally, some operators may include new services in the customers service package to make them more susceptible of accepting the new paradigm. Moreover, if the service charge is not increased, customers may benefit from a cost reduction in their electricity bill, as the bridge devices that support a vRGW scenario have lower power requirements.

H. Impact of emerging paradigms such as Fog Computing

As the supporting infrastructure becomes more homogeneous due to the functions being abstracted and capable of running in non-specialized hardware, it also becomes easier for them to be decoupled geographically. Thus, the deployment location of the functions required for the vRGW can be optimized by instantiating them in smaller datacenters closer to the end customer. Some services can take advantage of this, specially for latency-sensitive applications such as cloud-based gaming [131] (e.g. video streaming Gaming-as-a-Service (GaaS)). Another example is the case of the virtual Set-Top-Boxes (vSTB) [132], where part of the components of the service may be moved to the operator datacentre in a thin/zero-client fashion [133]. Also, Desktop-as-a-Service (DaaS) services providing on-demand applications and desktops may take advantage of having low latency from the datacentre to the customers premises [134]. They can also benefit from this flexibility to launch the services as close to the customers as possible, providing a better experience [135].

I. Future Trends/Research Directions

From the previous discussion, it has become clear that the majority of the current proposals rely on NFV and SDN as crucial building blocks to implement the vRGW concept.

An aspect overlooked by current research is related to the requirements, strategies and implications of providing network functions closer to the customer premises, in order to improve device-to-function latency. While a few authors do provide some insights (e.g., [62]), they are rather limited. However, it is expected that the development of 5G mobile networks will prompt further developments in this domain, eventually leveraging the potential of fog computing to improve latency and quality-of-experience for service consumption.

The simplification of the RGW device, along with the flexibility provided by the SDN-enabled data plane, is key for several proposals, allowing operators to improve QoE for multimedia applications, such as gaming or streaming, by having a more controlled flow prioritization [136]. In a similar fashion, such capabilities can be used to improve QoS, by allocating the available bandwidth using SDN flow [137] classification.

Another promising trend concerns the scalability and performance enhancement of vRGW approaches based on SDN and NFV, where some of the intrinsic performance and scalability limitations of the Openflow protocol are expected to be mitigated by the emerging P4 (Programming Protocol-Independent Packet Processors) [138] programming language – a notable development which has been subject of considerable advances in the past few years. P4 is a language designed for programming network device dataplanes, allowing to express how packets are processed by a forwarding element. Unlike Openflow, which is a protocol that provides the means for describing flow-oriented rules, P4 is a domain-specific programming language designed in a protocol-neutral fashion. Support for P4 programmable data planes is gaining traction both in the ONOS and CORD project communities.

The already mentioned lack of publicly available quantitative data regarding the scalability, performance and cost-effectiveness of vRGW frameworks also opens a fundamental field for future research. While we believe this lack of public data is essentially related with the strategic business value of such data for operators and manufacturers directly involved in proof-of-concept implementations and trials – motivating them to hold its public release – the truth is there is a considerable gap that still needs to be filled before wider acceptance of the vRGW concept.

After the introduction of the virtualized gateways in production, we can expect to witness the emergence of new services (and improvements on existing ones). With the increased service independence regarding physical gateway functionalities, operators and researchers should have more freedom to exploit new services and improving existing ones.

The introduction of virtualized residential gateways is also expected to benefit other domains beyond the scope of the telecom operator services, improving support for other types of service providers and use cases, including smart metering scenarios from utility providers or health-care services.

VII. Conclusion

It is clear that the virtualization of the residential gateway can bring benefits to both customers and operators. Factors such as the reduction in CAPEX and OPEX expenses and reduced time to market of new services are contributing to the acceptance of the concept within the industry.

This paper presented an overview of virtual residential gateway approaches, proposals and enabling technologies. It started with a presentation of the rationale behind the ideia of virtualizing the RGW, followed by the analysis of the first generation of vRGW proposals – including implementation attempts and corresponding shortcomings and limitations. These first vRGW attempts were not mature enough to gain traction in the market but highlighted the potential of the paradigm.

Meanwhile, the telecommunications industry adopted a number of enabling technologies which are key for the successful adoption of vRGW concepts. Among these technologies, SDN and NFV stand out for their impact on addressing the scaling, performance, deployment and life-cycle management issues that plagued the first vRGW approaches. In fact, these technologies are fundamental for a new set of vRGW proposals that have appeared more recently, more closely integrated into the operators environment and easing design, deployment and management operations. This is a result of the flexibility that NFV and SDN bring to network functions and their interconnections.

In the future other paradigms, such as fog computing, are also expected to bring significant advances to the vRGW concept, contributing to further stretch the RGW function placement domain to the edge of the operator network (closer to the customer premises) and allowing to increase service quality, especially in latency-sensitive services.

Despite this positive scenario, there are still several open challenges associated with the vRGW concept. There are conceptual and societal issues that may arise in the shifting the concept. User-related issues such as data privacy and control of vRGW functions. On the technological side, scalability problems present in some of the initial proposals due to the large number of instances need to be properly addressed and planned. Also, to make the most of SDN and NFV paradigms with interoperability between the different vendors, resource management and function orchestration must be properly standardized, including their interfaces.

On the whole, the vRGW is a promising concept, which is undergoing active development from industrial, research and standardization bodies.

Acknowledgment

This work was partially funded by the MobiWise P2020 Project (reference P2020 SAICTPAC/0011/2015) and the "Mobilizador 5G" P2020 Project (project 10/SI/2016 024539).

References

[1] B. Cain, S. Deering, I. Kouvelas, B. Fenner, and A. Thyagarajan, "Internet Group Management Protocol, Version 3," RFC 3376 (Proposed Standard), Internet Engineering Task Force, Oct. 2002. [Online]. Available: http://www.ietf.org/rfc/rfc3376.txt

[2] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, "SIP: Session Initiation Protocol," RFC 3261 (Proposed Standard), jun 2002. [Online]. Available: http://www.ietf.org/rfc/rfc3261.txt

[3] D. Waring, "Residential gateway architecture and network operations," *International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) document: JTC*, vol. 1, 1999.

[4] F. den Hartog, M. Balm, C. de Jong, and J. Kwaaitaal, "Convergence of residential gateway technology: analysis of evolutionary paths," in *Consumer Communications and Networking Conference, 2004. CCNC 2004. First IEEE.* IEEE, 2004, pp. 1–6.

[5] H. Xie, Y. Li, J. Wang, D. Lopez, T. Tsou, and Y. Wen, "vrgw: Towards network function virtualization enabled by software defined networking," in *Network Protocols (ICNP), 2013 21st IEEE International Conference on*, Oct 2013, pp. 1–2.

[6] Bell Labs Consulting, "Building the case for virtualized residential gateways (strategic white paper)," 2016. [Online]. Available: https://resources.ext.nokia.com/asset/191454

[7] Y. Royon, "Environnements d'ex'cution pour passerelles domestiques," Ph.D. dissertation, INSA de Lyon, 2007.

[8] A. De Smedt, H. Balemans, J. Onnegren, and S. Haeseleer, "The multiplay service enabled Residential Gateway," *Broadband Europe*, 2006.

[9] M. Patrick, "DHCP Relay Agent Information Option," RFC 3046, Internet Engineering Task Force, Jan. 2001. [Online]. Available: http://www.ietf.org/rfc/rfc3046.txt

[10] Z. Bronstein and E. Shraga, "Nfv virtualisation of the home environment," in *Consumer Communications and Networking Conference (CCNC), 2014 IEEE 11th.* IEEE, 2014, pp. 899–904.

[11] R. Mijumbi, J. Serrat, J. Gorricho, N. Bouten, F. De Turck, and R. Boutaba, "Network function virtualization: State-of-the-art and research challenges," *Communications Surveys Tutorials, IEEE*, vol. 18, no. 1, pp. 236–262, Firstquarter 2016.

[12] P. Calhoun, M. Montemurro, and D. Stanley, "Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification," RFC 5415 (Proposed Standard), Internet Engineering Task Force, March 2009. [Online]. Available: http://www.ietf.org/rfc/rfc5415.txt

[13] J. Vestin, P. Dely, A. Kassler, N. Bayer, H. Einsiedler, and C. Peylo, "Cloudmac: Towards software defined wlans," *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 16, no. 4, pp. 42–45, Feb. 2013. [Online]. Available: http://doi.acm.org/10.1145/2436196.2436217

[14] C. Tsirakis, P. Matzoros, and G. Agapiou, "Service oriented cloud CPE as a means of a future terminal," *2017 56th FITCE Congress, FITCE 2017*, pp. 40–44, 2017.

[15] F. Sanchez and D. Brazewell, "Tethered linux cpe for ip service delivery," in *Network Softwarization (NetSoft), 2015 1st IEEE Conference on*, April 2015, pp. 1–9.

[16] L. Xia, D. King, Q. Wu, and H. Yokota, "Use cases and Requirements for Virtual Service Node Pool Management," Internet Engineering Task Force, Internet-Draft draft-xia-vsnpool-management-use-case-01, Apr. 2014, work in Progress. [Online]. Available: https://tools.ietf.org/html/draft-xia-vsnpool-management-use-case-01

[17] ETSI NFV ISG, "Network Functions Virtualisation (NFV); Architectural Framework, v1.2.1," 2014.

[18] J. J. Dustzadeh, "SDN: Time to Accelerate the Pace," p. Keynote presentation, 2013. [Online]. Available: http://www.sdnap.com/wp-content/uploads/2013/04/SDN-TIME-TO-ACCELERATE-THE-PACE-huawei.pdf

[19] N. Egi, A. Greenhalgh, M. Handley, M. Hoerdt, L. Mathy, and T. Schooley, "Evaluating xen for router virtualization," in *Computer Communications and Networks, 2007. ICCCN 2007. Proceedings of 16th International Conference on*, Aug 2007, pp. 1256–1261.

[20] N. Egi, A. Greenhalgh, M. Handley, M. Hoerdt, F. Huici, L. Mathy, and P. Papadimitriou, "A platform for high performance and flexible virtual routers on commodity hardware," *SIGCOMM Comput. Commun. Rev.*, vol. 40, no. 1, pp. 127–128, Jan. 2010. [Online]. Available: http://doi.acm.org/10.1145/1672308.1672332

[21] P. Barham, B. Dragovic, K. Fraser, S. Hand, T. Harris, A. Ho, R. Neugebauer, I. Pratt, and A. Warfield, "Xen and the art of virtualization," *SIGOPS Oper. Syst. Rev.*, vol. 37, no. 5, pp. 164–177, Oct. 2003. [Online]. Available: http://doi.acm.org/10.1145/1165389.945462

[22] P. S. Pisa, M. D. Moreira, H. E. Carvalho, L. H. Ferraz, and O. C. Duarte, "Migrating xen virtual routers with no packet loss," in *Proc. of the First Workshop on Network Virtualizaton and Intelligence For Future Internet-WNetVirt*, vol. 10, 2010.

[23] A. Bazzi and Y. Onozato, "Feasibility study of security virtual appliances for personal computing," *Information and Media Technologies*, vol. 6, no. 3, pp. 950–960, 2011.

[24] S. Zeng and Q. Hao, "Network i/o path analysis in the kernel-based virtual machine environment through tracing," in *Information Science and Engineering (ICISE), 2009 1st International Conference on*, Dec 2009, pp. 2658–2661.

[25] D. Basak, R. Toshniwal, S. Maskalik, and A. Sequeira, "Virtualizing networking and security in the cloud," *SIGOPS Oper. Syst. Rev.*, vol. 44, no. 4, pp. 86–94, Dec. 2010. [Online]. Available: http://doi.acm.org/10.1145/1899928.1899939

[26] M. Ibáñez, N. M. Madrid, and R. Seepold, "Virtualization of residential gateways," *Proceedings of the 5th International Workshop on Intelligent Solutions in Embedded Systems, WISES 07*, pp. 115–125, 2007.

[27] D. Abgrall, "Virtual home gateway, how can home gateway virtualization be achieved?" *EURESCOM, Study Report P2055*, 2011.

[28] R. Da Silva, M. Fernandez, L. Gamir, and M. Perez, "Home routing gateway virtualization: An overview on the architecture alternatives," in *Future Network Mobile Summit (FutureNetw), 2011*, June 2011, pp. 1–9.

[29] H. T. C. Ltd. (2010) SmartAX MA5600T Series Product Website. [Online]. Available: http://enterprise.huawei.com/en/products/network/access-network/olt/en_ma5600t.htm

[30] T. Cruz, P. Simões, N. Reis, E. Monteiro, F. Bastos, and A. Laranjeira, "An architecture for virtualized home gateways," in *Integrated Network Management (IM 2013), 2013 IFIP/IEEE International Symposium on*, May 2013, pp. 520–526.

[31] E. Cohen and E. Shrum, "Mitigation to Ethernet-Based DSL Aggregation," BroadBand Forum, Technical-Report 101, 2006. [Online]. Available: https://www.broadband-forum.org/technical/download/TR-101.pdf

[32] T. Anschutz and L. Yeheskiel, "Using GPON Access in the context of TR-101," BroadBand Forum, Technical-Report 156, 2008. [Online]. Available: https://www.broadband-forum.org/technical/download/TR-156.pdf

[33] T. Cruz, P. Simões, and E. Monteiro, "Optimizing the Delivery of Services Supported by Residential Gateways: Virtualized Residential Gateways," *Handbook of Research on Redesigning the Future of Internet Architectures*, pp. 432–473, 2015.

[34] K. Greene, "Tech Review 10 Breakthrough Technologies: Software-Defined Networking." 2009. [Online]. Available: http://www2.technologyreview.com/article/412194/tr10-software-defined-networking/

[35] B. Pfaff, B. Lantz, B. Heller *et al.*, "Openflow switch specification, version 1.3. 0," *Open Networking Foundation*, 2012.

[36] D. Kreutz, F. Ramos, P. Esteves Verissimo, C. Esteve Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: A comprehensive survey," *Proceedings of the IEEE*, vol. 103, no. 1, pp. 14–76, Jan 2015.

[37] S. Yeganeh, A. Tootoonchian, and Y. Ganjali, "On scalability of software-defined networking," *Communications Magazine, IEEE*, vol. 51, no. 2, pp. 136–141, February 2013.

[38] A. Blenk, A. Basta, M. Reisslein, and W. Kellerer, "Survey on Network Virtualization Hypervisors for Software Defined Networking," *Communications Surveys Tutorials, IEEE*, vol. PP, no. 99, p. 1, 2015.

[39] ForCES, "Forwarding and Control Element Separation (forces) -." [Online]. Available: https://datatracker.ietf.org/wg/forces/charter/

[40] M. Chiosi *et al.*, "Network functions virtualization, an introduction, benefits, enablers, challenges and call for action," in *SDN and OpenFlow SDN and OpenFlow World Congress*, October 2012. [Online]. Available: http://portal.etsi.org/NFV/NFV_White_Paper.pdf

[41] ——, "Network functions virtualisation–network operator perspectives on industry progress," *Updated White Paper*, July 2013. [Online]. Available: http://portal.etsi.org/NFV/NFV_White_Paper2.pdf

[42] A. Lemke, "Alcatel Lucent - Why service providers need an NFV platform: Strategic White Paper," 2015.

[43] B. Han, V. Gopalakrishnan, L. Ji, and S. Lee, "Network function virtualization: Challenges and opportunities for innovations," *Communications Magazine, IEEE*, vol. 53, no. 2, pp. 90–97, 2015.

[44] ETSI. (2012) ETSI - Industry Specification Group for NFV. [Online]. Available: http://www.etsi.org/technologies-clusters/technologies/nfv

[45] M. Ersue. (2013) ESTI NFV Management and Orchestration - An Overview. [Online]. Available: http://www.ietf.org/proceedings/88/slides/slides-88-opsawg-6.pdf

[46] IEEE, "802.1Q-2014 - IEEE Standard for Local and metropolitan area networks–Bridges and Bridged Networks," IEEE - Institute of Electrical and Electronics Engineers, Standard, 2014.

[47] S. Bryant, P. Pate *et al.*, "Pseudo wire emulation edge-to-edge (pwe3) architecture," RFC 3985, March, Tech. Rep., 2005.

[48] TM Forum. (2016) Zero-time Orchestration, Operations and Management (ZOOM) - Webpage. [Online]. Available: https://www.tmforum.org/zoom/

[49] T. Nolle. (2016) CloudNFV - Webpage. [Online]. Available: http://www.cloudnfv.com/

[50] Nokia. (2016) CloudNFV - Webpage. [Online]. Available: https://networks.nokia.com/solutions/cloudband

[51] T. Nolle. (2014) ExperiaSphere: Take The First Step to Open Orchestration. [Online]. Available: http://blog.experiasphere.com/

[52] (2015) HP OpenNFV Reference Architecture. [Online]. Available: https://www.hpe.com/us/en/networking/nfv.html

[53] blueplanet. (2014) Planet Orchestrate - Overview. [Online]. Available: http://www.blueplanet.com/about/newsroom/Cyan-Introduces-Planet-Orchestrate-the-Industrys-First-Orchestration-Application-that-Integrates-Cloud-Services-NFV-and-WAN.html

[54] R. Mijumbi, J. Serrat, J.-L. Gorricho, S. Latré, M. Charalambides, and D. Lopez, "Management and orchestration challenges in network function virtualization," 2015.

[55] ETSI. (2016) ESTI Open Source Mano (OSM) - Project Homepage. [Online]. Available: https://osm.etsi.org/

[56] OpenStack. (2010) OpenStack Open Source Cloud Computing Software. https://www.openstack.org/. [Online]. Available: https://www.openstack.org/

[57] Telefónica. (2015) OpenMANO project page. https://github.com/nfvlabs/openmano. [Online]. Available: https://github.com/nfvlabs/openmano

[58] ETSI, "ETSI GS NFV-IFA 006 "Network Functions Virtualisation (NFV); Management and Orchestration; Vi-Vnfm reference point - Interface and Information Model Specification (2016-04)"," 2016.

[59] S. Yi, C. Li, and Q. Li, "A Survey of Fog Computing: Concepts, Applications and Issues," in *Proceedings of the 2015 Workshop on Mobile Big Data*, ser. Mobidata '15. New York, NY, USA: ACM, 2015, pp. 37–42. [Online]. Available: http://doi.acm.org/10.1145/2757384.2757397

[60] I. Stojmenovic and S. Wen, "The Fog computing paradigm: Scenarios and security issues," in *Computer Science and Information Systems (FedCSIS), 2014 Federated Conference on*, 2014, pp. 1–8.

[61] A. B. Garcia Hernando, A. Da Silva Farina, L. Bellido Triana, F. J. Ruiz Pinar, and D. Fernandez Cambronero, "Virtualization of residential IoT functionality by using NFV and SDN," *2017 IEEE International Conference on Consumer Electronics, ICCE 2017*, pp. 86–87, 2017.

[62] A. Lombardo, A. Manzalini, G. Schembra, G. Faraci, C. Rametta, and V. Riccobene, "An open framework to enable NetFATE (Network Functions at the edge)," in *Network Softwarization (NetSoft), 2015 1st IEEE Conference on*, 2015, pp. 1–6.

[63] R. I. G. Fabregas, "Tr-328 virtual business gateway," Tech. Rep., July 2017. [Online]. Available: https://www.broadband-forum.org/technical/download/TR-328.pdf

[64] C. Alter, "Broadband forum work on "network enhanced residential gateway" (wt-317) and "virtual business gateway" (wt-328)," *Broadband Forums liaison letter to the IETF*, 2014.

[65] D. M. G. Dalle, "Tr-317 network enhanced residential gateway," Tech. Rep., July 2016. [Online]. Available: https://www.broadband-forum.org/technical/download/TR-317.pdf

[66] J. Carey and H. Kirksey, "Component objects for cwmp, tr-157 issue 1 amendment 5," Broadband Forum Rech Report, Tech. Rep., November 2011.

[67] OSGi. (2012) OSGI Service Compendium, Release 4, version 4.3. OSGi Alliance Specification. [Online]. Available: http://www.osgi.org/Specifications/HomePage

[68] Cui, A., and Hertoghs, Y, "Tr-145: Multi-service broadband network functional modules and architecture, issue 1," Broadband Forum Rech Report, Tech. Rep., November 2012.

[69] Alter, C., and Daowood, S., "Broadband forum work on flexible service chaining (sd-326)," Broadband Forums liaison letter to the IETF, Tech. Rep., February 2014.

[70] L. Niu, H. Li, Y. Jiang, and L. Yong, "A Service Function Chaining Header and Forwarding Mechanism," Internet Engineering Task Force, Internet-Draft draft-niu-sfc-mechanism-01, Oct. 2014, work in Progress. [Online]. Available: https://tools.ietf.org/html/draft-niu-sfc-mechanism-01

[71] T. Nadeau and P. Quinn, "Problem Statement for Service Function Chaining," IETF RFC 7498, Nov. 2015. [Online]. Available: https://rfc-editor.org/rfc/rfc7498.txt

[72] M. Boucadair, C. Jacquenet, Y. Jiang, R. Parker, and Kengo, "Requirements for Service Function Chaining (SFC)," Internet Engineering Task Force, Internet-Draft draft-boucadair-sfc-requirements-06, Aug. 2015, work in Progress. [Online]. Available: https://tools.ietf.org/html/draft-boucadair-sfc-requirements-06

[73] L. Dunbar, C. Jacquenet, M. Boucadair, and R. Parker, "Service Function Chaining: Design Considerations, Analysis & Recommendations," Internet Engineering Task Force, Internet-Draft draft-boucadair-sfc-design-analysis-03, Apr. 2015, work in Progress. [Online]. Available: https://tools.ietf.org/html/draft-boucadair-sfc-design-analysis-03

[74] Y. Jiang and L. Hongyu, "An Architecture of Service Function Chaining," Internet Engineering Task Force, Internet-Draft draft-jiang-sfc-arch-01, Aug. 2014, work in Progress. [Online]. Available: https://tools.ietf.org/html/draft-jiang-sfc-arch-01

[75] Y. Lee and R. Ghai, "Problem Statements of Virtual Home Network," Internet Engineering Task Force, Internet-Draft draft-lee-vhs-ps-02, May 2015, work in Progress. [Online]. Available: https://tools.ietf.org/html/draft-lee-vhs-ps-02

[76] Y. Lee and C. Xie, "Virtual Home Services Use Cases," Internet Engineering Task Force, Internet-Draft draft-lee-vhs-usecases-02, May 2015, work in Progress. [Online]. Available: https://tools.ietf.org/html/draft-lee-vhs-usecases-02

[77] R. Flores Moyano, D. Fernández, L. Bellido, and C. González, "A software-defined networking approach to improve service provision in residential networks," *International Journal of Network Management*, vol. 27, no. 6, pp. 1–19, 2017.

[78] M. Dillon and T. Winters, "Virtualization of Home Network Gateways," *Computer*, vol. 47, no. 11, pp. 62–65, nov 2014.

[79] D. Modig and J. Ding, "Performance impacts on container based virtualization in virtualized residential gateways," in *2016 39th International Conference on Telecommunications and Signal Processing (TSP)*, jun 2016, pp. 27–32.

[80] N.-f. F. Huang, C.-c. C.-h. C. H. Li, C.-h. H. C.-c. Chen, I.-h. H. Hsu, C.-c. C.-h. C. H. Li, and C.-h. H. C.-c. Chen, "A Novel vCPE Framework for Enabling Virtual Network Functions with Multiple Flow Tables Architecture in SDN Switches," in *2017 19th Asia-Pacific Network Operations and Management Symposium (APNOMS)*, sep 2017, pp. 64–69.

[81] N. Herbaut, D. Negru, G. Xilouris, and Y. Chen, "Migrating to a nfv-based home gateway: Introducing a surrogate vnf approach," in *Network of the Future (NOF), 2015 6th International Conference on the*, Sept 2015, pp. 1–7.

[82] NEC, "Virtual home environment," *Whitepaper*, Nov 2014, accessed: 2016-03-11. [Online]. Available: https://www.sdxcentral.com/wp-content/uploads/2015/10/virtualized-customer-premises-equipment-brochure.pdf

[83] Ericsson, "Virtual cpe and software defined networking," *Whitepaper*, 2014, accessed: 2016-03-04. [Online]. Available: http://www.ericsson.com/res/docs/2014/virtual-cpe-and-software-defined-networking.pdf

[84] NEC, "Virtualized customer premises equipment - turning your cpe into a future-proof competitive advantage," *Whitepaper*, 2015, accessed: 2016-03-21. [Online]. Available: https://www.sdxcentral.com/wp-content/uploads/2015/10/virtualized-customer-premises-equipment-brochure.pdf

[85] J. Proença, T. Cruz, P. Simões, G. Gaspar, B. Parreira, A. Laranjeira, and F. Bastos, "Building an NFV-Based vRGW: lessons learned," in *14th IEEE Consumer Communications and Networking Conference (CCNC 2017)*, January 2017.

[86] ViVo. (2016) Vivo Telecommunication Operator - Homepage. [Online]. Available: http://www.vivo.com.br/

[87] R. Cantó Palancar, R. A. da Silva, J. L. Folgueira Chavarría, D. R. López, A. J. Elizondo Armengol, and R. Gamero Tinoco, "Virtualization of residential customer premise equipment. Lessons learned in Brazil vCPE trial," *it-Information Technology*, vol. 57, no. 5, pp. 285–294, 2015.

[88] ON.LAB. (2017) Open CORD - CORD. [Online]. Available: http://opencord.org/

[89] R. F. Moyano, D. Fernandez, L. Bellido, N. Merayo, J. C. Aguado, and I. De Miguel, "NFV-based QoS provision for Software Defined Optical Access and residential networks," *2017 IEEE/ACM 25th International Symposium on Quality of Service, IWQoS 2017*, 2017.

[90] P. Berde, M. Gerola, J. Hart, Y. Higuchi, M. Kobayashi, T. Koide, B. Lantz, B. O'Connor, P. Radoslavov, W. Snow, and G. Parulkar, "Onos: Towards an open, distributed sdn os," in *Proceedings of the Third Workshop on Hot Topics in Software Defined Networking*, ser. HotSDN '14. New York, NY, USA: ACM, 2014, pp. 1–6. [Online]. Available: http://doi.acm.org/10.1145/2620728.2620744

[91] CORD. (2017) R-CORD - Guide. [Online]. Available: https://guide.opencord.org/profiles/rcord/

[92] CORD Project. (2018) VOLTHA Project Overview. [Online]. Available: https://wiki.opencord.org/display/CORD/VOLTHA

[93] CORD. (2017) CORD Virtual Optical Line Termination - Guide. [Online]. Available: https://wiki.opencord.org/pages/viewpage.action?pageId=1278086

[94] ——. (2017) CORD Virtual Router - Guide. [Online]. Available: https://wiki.opencord.org/pages/viewpage.action?pageId=1278093

[95] L. Peterson, A. Al-Shabibi, T. Anshutz, S. Baker, A. Bavier, S. Das, J. Hart, G. Palukar, and W. Snow, "Central office re-architected as a data center," *IEEE Communications Magazine*, vol. 54, no. 10, pp. 96–101, October 2016.

[96] CORD. (2016) CORD Virtual Subscriber Gateway - Guide. [Online]. Available: https://wiki.opencord.org/pages/viewpage.action?pageId=1278090

[97] R. Bonafiglia, S. Miano, S. Nuccio, F. Risso, and A. Sapio, "Enabling NFV Services on Resource-Constrained CPEs," *Proceedings - 2016 5th IEEE International Conference on Cloud Networking, CloudNet 2016*, pp. 83–88, 2016.

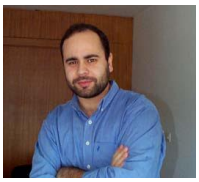
[98] B. Kozicki, N. Olaziregi, K. Oberle, R. Sharpe, and M. Clougherty, "Software-defined networks and network functions virtualization in wireline access networks," in *Globecom Workshops (GC Wkshps), 2014*, Dec 2014, pp. 595–600.

[99] ETSI, "ETSI GS NFV-IFA 005 "Network Functions Virtualisation(NFV); Management and Orchestration; Or-Vi reference point

- Interface and Information Model Specification V2.1.1 (2016-04)," 2016.
[100] ——, "ETSI GS NFV-IFA 010 "Network Functions Virtualisation (NFV); Management and Orchestration; Functional requirements specification (2016-04)"," 2016.
[101] "TOSCA simple profile for network functions virtualization (NFV) version 1.0," May 2017. [Online]. Available: http://docs.oasis-open.org/tosca/tosca-nfv/v1.0/csd04/tosca-nfv-v1.0-csd04.html.Latestversion:http://docs.oasis-open.org/tosca/tosca-nfv/v1.0/tosca-nfv-v1.0.html
[102] Linux Foundation. (2014) Open Platform for NFV (OPNFV). https://www.opnfv.org/. [Online]. Available: https://www.opnfv.org/
[103] ——. (2015) OPNFV Delivers Open Source Software to Enable Deployment of Network Functions Virtualization Solutions. Accessed: 2016-01-10. [Online]. Available: https://www.opnfv.org/news-faq/press-release/2015/06/opnfv-delivers-open-source-software-enable-deployment-network
[104] ETSI, "ETSI GS NFV-PER 001 "Network Functions Virtualization(NFV); NFV Performance & Portability Best Practises V1.1.2 (2014-12)," 2014.
[105] G. Wang and T. S. E. Ng, "The Impact of Virtualization on Network Performance of Amazon EC2 Data Center," in *INFOCOM, 2010 Proceedings IEEE*, 2010, pp. 1–9.
[106] I. Cerrato, M. Annarumma, and F. Risso, "Supporting Fine-Grained Network Functions through Intel DPDK," in *Software Defined Networks (EWSDN), 2014 Third European Workshop on*, 2014, pp. 1–6.
[107] M.-A. Kourtis, G. Xilouris, V. Riccobene, M. J. McGrath, G. Petralia, H. Koumaras, G. Gardikis, and F. Liberal, "Enhancing VNF performance by exploiting SR-IOV and DPDK packet processing acceleration," in *Network Function Virtualization and Software Defined Network (NFV-SDN), 2015 IEEE Conference on*, 2015, pp. 74–78.
[108] PCI-SIG. (2010) Peripheral Component Interconnect Special Interest - Special Interest Group Homepage. [Online]. Available: https://pcisig.com/
[109] J. Anderson, H. Hu, U. Agarwal, C. Lowery, H. Li, and A. Apon, "Performance considerations of network functions virtualization using containers," in *2016 International Conference on Computing, Networking and Communications (ICNC)*, 2016, pp. 1–7.
[110] M. Paolino, N. Nikolaev, J. Fanguede, and D. Raho, "SnabbSwitch user space virtual switch benchmark and performance optimization for NFV," in *Network Function Virtualization and Software Defined Network (NFV-SDN), 2015 IEEE Conference on*, nov 2015, pp. 86–92.
[111] J. F. Zazo, S. Lopez-Buedo, Y. Audzevich, and A. W. Moore, "A PCIe DMA engine to support the virtualization of 40 Gbps FPGA-accelerated network appliances," in *ReConFigurable Computing and FPGAs (ReConFig), 2015 International Conference on*, 2015, pp. 1–6.
[112] NetFPGA. (2016) NetFPGA Project Homepage. [Online]. Available: http://netfpga.org/
[113] R. Bonafiglia, I. Cerrato, F. Ciaccia, M. Nemirovsky, and F. Risso, "Assessing the Performance of Virtualization Technologies for NFV: A Preliminary Benchmarking," in *Software Defined Networks (EWSDN), 2015 Fourth European Workshop on*, 2015, pp. 67–72.
[114] J. Evens, "A comparison of containers and virtual machines for use with NFV," *M.Sc. Thesis*, 2015. [Online]. Available: http://hdl.handle.net/1942/19367
[115] M. Raho, A. Spyridakis, M. Paolino, and D. Raho, "KVM, Xen and Docker: A performance analysis for ARM based NFV and cloud computing," in *Information, Electronic and Electrical Engineering (AIEEE), 2015 IEEE 3rd Workshop on Advances in*, nov 2015, pp. 1–8.
[116] R. Cziva, S. Jouet, K. J. S. White, and D. P. Pezaros, "Container-based network function virtualization for software-defined networks," in *2015 IEEE Symposium on Computers and Communication (ISCC)*, July 2015, pp. 415–420.
[117] Kubernetes. (2016) Kubernetes - Production-Grade Container Orchestration Homepage. [Online]. Available: http://kubernetes.io/
[118] CoreOS. (2016) CoreOS - Open Source Projects for Linux Containers - Homepage. [Online]. Available: http://coreos.com/
[119] C. Rotter, L. Farkas, G. Ny\'\iri, G. Csatári, L. Jánosi, and R. Springer, "Using Linux Containers in Telecom Applications," *Innovations in Clouds, Internet and Networks, ICIN*, 2016.
[120] M. Technologies. (2016) Mellanox Website. [Online]. Available: http://www.mellanox.com/
[121] ETSI, "ETSI GS NFV-IFA 001 "Network Functions Virtualisation(NFV); Acceleration Technologies; Report on Acceleration Technologies & Use Cases V1.1.1 (2015-12)," 2015.
[122] ——, "ETSI GS NFV-IFA 002 "Network Functions Virtualisation(NFV); Acceleration Technologies; VNF Interfaces Specification V2.1.1 (2016-03)," 2016.
[123] ——, "ETSI GS NFV-IFA 003 "Network Functions Virtualisation(NFV); Acceleration Technologies; vSwitch Benchmarking and Acceleration Specification V2.1.1 (2016-04)," 2016.
[124] ——, "ETSI GS NFV-IFA 004 "Network Functions Virtualisation(NFV); Acceleration Technologies; Management Aspects Specification V2.1.1 (2016-04)," 2016.
[125] D. Touitou and E. Roch, "Accelerating NFV with fast path offloading," in *Consumer Communications and Networking Conference (CCNC), 2014 IEEE 11th*, jan 2014, pp. 893–898.
[126] ETSI NFV ISG, "Network Functions Virtualisation (NFV); Use Cases v1.1.1," 2013.
[127] E. Park, S. Kim, Y. Kim, and S. J. Kwon, "Smart home services as the next mainstream of the ICT industry: determinants of the adoption of smart home services," *Universal Access in the Information Society*, pp. 1–16, 2017. [Online]. Available: http://dx.doi.org/10.1007/s10209-017-0533-0
[128] A. R. Manu, J. K. Patel, S. Akhtar, V. K. Agrawal, and K. N. B. S. Murthy, "A study, analysis and deep dive on cloud paas security in terms of docker container security," in *2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT)*, March 2016, pp. 1–13.
[129] T. Combe, A. Martin, and R. D. Pietro, "To docker or not to docker: A security perspective," *IEEE Cloud Computing*, vol. 3, no. 5, pp. 54–62, Sept 2016.
[130] R. F. Moyano, D. F. Cambronero, and L. B. Triana, "A User-Centric SDN Management Architecture for NFV-based Residential Networks," *Computer Standards & Interfaces*, 2017.
[131] X. Liao, L. Lin, G. Tan, H. Jin, X. Yang, W. Zhang, and B. Li, "Liverender: A cloud gaming system based on compressed graphics streaming," *IEEE/ACM Transactions on Networking*, vol. 24, no. 4, pp. 2128–2139, Aug 2016.
[132] T. Cruz, P. Simões, P. Cabaco, E. Monteiro, and F. Bastos, "On the use of thin-client set-top boxes for iptv services," in *38th Annual IEEE Conference on Local Computer Networks*, Oct 2013, pp. 771–778.
[133] K. Suksomboon, M. Fukushima, and M. Hayashi, "Optimal virtualization of functionality for customer premise equipment," in *2015 IEEE International Conference on Communications (ICC)*, June 2015, pp. 5685–5690.
[134] T. Guo, P. Shenoy, K. K. Ramakrishnan, and V. Gopalakrishnan, "Latency-aware virtual desktops optimization in distributed clouds," *Multimedia Systems*, pp. 1–22, 2017. [Online]. Available: http://dx.doi.org/10.1007/s00530-017-0536-y
[135] K. Fanning and D. M. Cannon, "Daas: A cost-savings strategy," *Journal of Corporate Accounting & Finance*, vol. 26, no. 5, pp. 15–20, 2015. [Online]. Available: http://dx.doi.org/10.1002/jcaf.22058
[136] M. Amiri, H. A. Osman, and S. Shirmohammadi, "SDN-enabled Game-Aware Network Management for Residential Gateways," *2017 IEEE International Symposium on Multimedia (ISM)*, pp. 330–333, 2017. [Online]. Available: http://ieeexplore.ieee.org/document/8241626/
[137] N. F. Huang, S. J. Wu, I. J. Liao, and C. W. Lin, "Bandwidth distribution for applications in slicing network toward SDN on vCPE framework," *18th Asia-Pacific Network Operations and Management Symposium, APNOMS 2016: Management of Softwarized Infrastructure - Proceedings*, pp. 3–6, 2016.
[138] P4 Language Consortium. (2017) P4 Language Specification, version 1.0.0. [Online]. Available: https://p4.org/p4-spec/docs/P4-16-v1.0.0-spec.html

Jorge Proença is a PhD student in Information Science and Technology at the University of Coimbra. He received his M.Sc. degree from the same institution in 2012. He is a junior researcher in the Centre for Informatics and Systems of the University of Coimbra (CISUC), participating in several research projects in the fields of network virtualization, security and critical infrastructure protection.

Tiago Cruz is Assistant Professor at the Department of Informatics Engineering at the University of Coimbra since December 2013, where he obtained his PhD in Informatics Engineering, in 2012. His research interests cover areas such as management systems for communications infrastructures and services, critical infrastructure security, broadband access network device and service management, internet of things, software defined networking and network function virtualization (among others), being the author of more than 70 publications, including chapters in books, journal articles and conference papers. He is member of the IEEE Communications Society and IEEE Senior member.



Paulo Simões is Assistant Professor at the Department of Informatics Engineering of the University of Coimbra, Portugal, where he obtained his doctoral degree in 2002. He regularly leads industry-funded technology transfer projects for companies such as telecommunications operators and energy utilities. He was also founding partner of two technological spin-off companies. His research interests include Network and Infrastructure Management, Security, Critical Infrastructure Protection and Virtualization of Networking and Computing Resources. He has over 150 publications in refereed journals and conferences of these areas. He is also member of the IEEE Communications Society.

Edmundo Monteiro is Full Professor of the University of Coimbra (UC), Portugal. He has more than 30 years of research experience in the field of Computer Communications, Wireless Networks, Quality of Service and Experience, Network and Service Management, and Computer and Network Security. He participated in many Portuguese, European rand international research projects and initiatives. His publication list includes over 200 publications in journals, books, and international refereed conferences. He is also co-author of 9 international patents. He is member of the Editorial Board of Springer Wireless Networks journal and involved in the organization of many national and international conferences and workshops. Edmundo Monteiro is Senior Member of IEEE Communication Society, and Senior Member of ACM Special Interest Group on Communications. He is also the Portuguese representative in IFIP TC6 (Communication Systems).