NFV Virtualisation of the Home Environment

Zvika Bronstein
Huawei Technologies
Zvika.Bronstein@huawei.com

Eyal Shraga
Huawei Technologies
Eyal.Shraga@huawei.com

***Abstract*— NFV Technology facilitates implementation of network functions as SW packages, called Virtual Network Functions (VNF) running over common IT platforms and simple network switches. NFV could be used to virtualize dispersed functions and devices currently deployed as CPEs in the customer home. This new architecture has a major impact on public and home networks. Not only are HW components virtualised, but their location and operational responsibility is shifted to the operator scope. Various security and implementation issues are identified as a result of Home Virtualisation and discussed in this paper.**

Keywords-component; Virtualisation, Home Networks; CPE; RGW; STB; vRGW; vSTB; NFV, VNF, BNG, Home security

I. Introduction

Current business models and architecture of Network Service Providers (NSP) for home services normally imply deployment of new devices within the customer premises - Customer Premises Equipment (CPE). These usually include a Residential Gateway (RGW) for Internet and VOIP services, and a Set-top Box (STB) for Media services normally supporting local storage for Personal Video Recording (PVR) services. This solution is associated with high Capital Expenses (CAPEX) for initiating the service and high Operation Expenses (OPEX) for servicing and maintaining the equipment. This practice has the potential of slowing down the roll out of new services as they are dependent on the revision and capabilities of the installed CPEs. Operators are now looking for ways to reduce the cost associated with new services, and virtualisation technologies offered by NFV have the potential for delivering these capabilities.

The CPE devices mark the operator and/or service provider presence at the customer premises. The availability of high bandwidth access (such as offered by fiber) and the emergence of NFV technology facilitate virtualisation of the home environment, requiring only simple, physical connectivity focused, low cost, and low maintenance devices at the customer premises.

NFV Technology facilitates implementation of Network functions as SW packages, called Virtual Network Functions (VNF) running over common IT platforms and simple network switches. Virtualisation of the home consists of simplifying the home network by removing the RGW and the STB from the home and replacing them by Operator Network provided functionality. This change has the potential for great saving for the operator as well as greatly improving time-to-market of new services, as they can be introduced as required on a grow-as-you-need basis. The benefits derived from avoiding installation of new equipment would be amplified if the home environment is considered with the appropriate NFV approach. In some countries, regulatory restrictions are in place for network based PVR and these will need to be addressed accordingly.

While this new architecture increases the demand for bandwidth between the home and the network, advantages to the operator and the end customer are numerous:

- CAPEX reduction by eliminating the costly STB (one per TV) and RGW.
- OPEX reduction by eliminating the need to constantly maintain and upgrade the CPEs and capacities to make remote diagnostic of the user devices in order to provide direct solutions to problems in the user network.
- Improved Quality-of-Experience (QoE) by functionality such as remote access to all content and services, multi-screen support and mobility.

New service introduction becomes smooth and less cumbersome as the dependency on the CPE functionality and user installation processes is minimized.

II. Description

Figure 1 depicts a legacy home network without virtualisation. In this example, each home is equipped with an RGW and IP STB. All services are received by the RGW, converted to a private IP address and delivered inside the home. The RGW is connected (via a PPPoE Tunnel or IPoE) to the BNG which provides connectivity to the Internet or DC. VoIP and IPTV services bypass the BNG in this scenario.

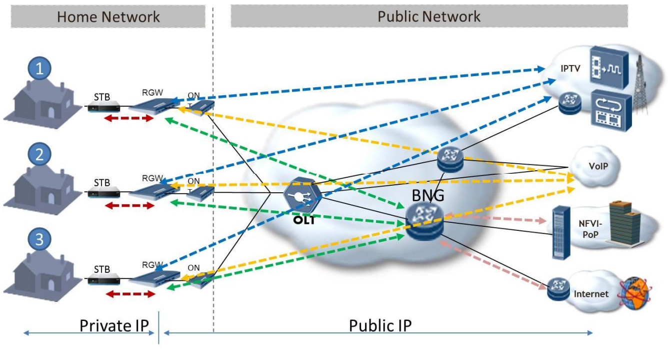

Figure 1: No Home Virtualisation

NFV technology facilitates virtualisation of services and functionality migration from home devices to the NFV cloud as shown in figure 2. In this case, we follow the Virtualised Network Function proposal by NFV and maintain a virtualised replica of the original device, such that the RGW migrates into a vRGW and STB into vSTB. In so doing, we maintain as much as possible the original interfaces to the virtualised devices.

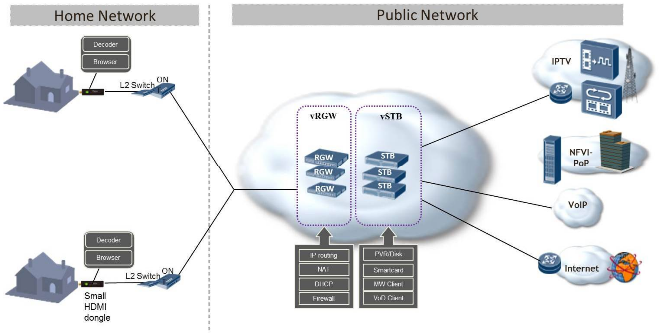

Figure 2: Home Virtualisation functionality

III. VIRTUALISATION TARGET

A. STB – Home Set Top Box

The following functionalities of the Set-Top Box are candidates for virtualisation, and therefore may be removed from the home device and migrate to the virtualised NFV environment.

- **User Interface & Connectivity**
  - ○ Remote UI server – Allows same look and feel to a big variety of home devices including UI automatic negotiation for best possible user experience.
  - ○ Middleware Client – Provide interface for existing middleware servers to query information such as EPG, subscriber rights, etc.

- **Media Streaming**
  - ○ DLNA media server – Expose all media inventory such as: Electronics Program Guide (EPG), VOD catalog, network PVR (NPVR) list, Time-Shift-TV (TSTV) inventory to DLNA devices.
  - ○ VOD, NPVR, TSTV, OTT clients – Provide interfaces to existing content platforms.
  - ○ Streaming methods such as HTTP and Zero Client.
  - ○ Multi-screen – support various, simultaneous screens of varying resolution and formats.
  - ○ Media Cache – Support caching of different content types and formats.

- **Management & Security**
  - ○ Web GUI – to allow subscriber management.
  - ○ Encryption – support different encryption schemes for cached content.
  - ○ Share Content – Possibility for the user to see its contents over any virtualised environment

B. RGW – Residential Gateway

The following functionalities of the Regional Gateway are candidates for virtualisation, and therefore removed from the home device and migrate to the virtualised NFV environment.

- **Connectivity**
  - ○ DHCP server - Provide private IP addresses to home devices.
  - ○ NAT router – Provide routing capabilities to the home. Convert the home addresses to one public IP per home (IPv4/6).
  - ○ PPPoE client – Client for connectivity to the BRAS.
  - ○ ALG – Application Level Gateway to allow Application Specific routing behavior.

- **Security**
  - ○ Firewall, Antivirus, IPS – Provide protection to the home environment.
  - ○ Parental control – Allows control of consumed web content to device level.
  - ○ Port mapping.

- VPN Server – Provide remote accesses to the user LAN.

- **Management**

  - Web GUI – to allow subscriber management.
  - TR-69 – To allow operator's control.
  - uPnP – Discovery of vRGW by home applications.
  - Statistics & Diagnostics.

IV. SECURITYU ISSUES ASSOCIATED WITH VCPE

Displacing the CPE and moving it to the Network Service Provider (NSP) introduces security challenges, especially relating to the RGW that serves as the home security device. Regular Network Functions in NFV environment would normally change from a physical implementation to a virtual implementation (VNF), but otherwise their functionality will not be affected. That implies that the same functionality provide by physical representation will be provided by the virtual one, therefore many of the operational aspects and the security issues associated with this implementation will not be affected. As an example, virtualisation of the BNG, in the NFV environment will imply implementation challenges. It may involve splitting the originally integrated BNG into several elements running on several virtual machines on different servers to overcome scalability and performance issues. A load balancing function might be needed, as well as some changes to the device management to address the fact the function is now virtualised and needs to be maintained and managed as such. Some security issues are associated with normal VNFs (not relating to home virtualisation) having to do with the venerability of the SW implementation of the VNF and are beyond the scope of this paper. However, no new security issues are expected as a result of the NF functionality change.

Virtualisation of the CPE, especially the RGW, is more challenging as it involves several key operational and functionality changes:

- First, the RGW is moved from the home to the NSP. By that the order of the Network functions is changed as described in Section IV below. Functions are moved from Private to Public IP address space, and occasionally the Service Chain is reversed – e.g. between the STB streaming function and the RGW NAT function.

- The vRGW will be implemented on a shared environment, running on the same HW and same CPU as other instances. In some cases, the vRGW will share the same Virtual Machine (VM) with other instantiation of the function. Isolation and protection of the vRGW function is challenging.

- Some RGW functions that were distributed may now become centralized, sharing resources among instances. An example is the DHCP server function implemented in the RGW for allocating IP addresses to home devices. This function, when implemented at the NSP will most likely be centralized with a single DHCP server serving large number of devices. Some security issues arise from the sharing of information on a common database and a common server.

- NSPs are faced with new Security challenges with Home Virtualisation as the responsibility moves from the user to the operator. Devices at home may have various sources, often purchased and owned by the end user. Normally, the end user would assume some responsibility for configuring and physically securing the device, which is not the case when the device is virtualised.

- Another security challenge is introduced by the end user configuration of the device. When the RGW is virtualised, simple operations like Port Mapping or managing IP addresses imply changes to devices and databases in the NSP network, a new challenge altogether.

Subsequently, we categorize security challenges by their cause. The mechanisms for addressing all these security challenges are beyond the scope of this paper, however, the distinction and classification offered by the following table will set the direction of how these security issues need to be handled. The following security causes are suggested:

1. Security issues caused from moving a function from the home to the network - *Location change*
2. Security issues caused by moving a HW based function to a virtualised SW (VNF) – *Physical change*
3. Security issues caused by aggregation, as a result of providing a unified function instead of home distributed function (e.g. DHCP / DNS) – *Aggregation change*
4. Security issue caused by shifting the responsibility from the individual to the NSP – *Responsibility Change*

The following table lists some of the security challenges introduced by the vCPE (especially vRGW) with identification for cause of the security challenge:

	Location Change (home → Network)	Physical Change (HW → SW)	Aggregation Change (Distributed → Centralized)	Responsibility Change (User → NSP)
The NAT function Challenges caused by SW implementation of NAT function		X		
firewall function Beyond L3 – Support L4-L7	X	X		X
L3 firewall function filtering	X	X		
Ingress FW Filtering – Performed at the NSP	X			X
Egress FW Filtering – Challenging when performed at the NSP	X	X		X
Secured Device configuration	X			X
On-premise control - L2 inter-VLAN filtering – Internal Traffic is exposed to network	X			
DHCP Server function	X		X	X
Inter Home communication on failure of Access Link	X			X
Inter Home traffic exposed to network	X			
Home Broadcast exposed to Network	X			
Boot storm at NSP after failure	X	X	X	X
DNS Caching – Information exposure	X		X	
Web proxy caching – Information exposure	X		X	
Special egress rules (e.g., dynamic gaming ports)	X			X
VoIP services – local calls	X			X
User Authentication for configuration	X			X
Virtual Device Configuration - End user configuration of NSP based devices	X			X
UPnP on the vRGW – UPnP is not a secured protocol and needs to be replaced	X			X
Identities of virtual residential gateways – RGW no longer identified by Physical Home address	X	X		
SW Updates of vRGW			X	X
Regulatory considerations	X			X
Cloud based Control functions (DHCP, DNS etc.)		X	X	
Isolation of users sharing NFV Infrastructure		X	X	

Table 1: vRGW Security Issues

V. Coexistence of Virtualised and Non-virtualised Network Functions

Coexistence between Virtualised Home devices and non-virtualised devices is mandatory as the Service Provider is likely to roll out virtualised services gradually based on available access technology and end user requirements. RGW and STB, being the main candidates for virtualisation, may be handled separately opening the door for all possible deployment combinations.

Unlike some Virtual Network Functions in NFV, virtualisation of the home drives a deployment change as the virtualised devices move from the home to the operator network and from the private IP space into the public IP space. The following figures demonstrate some possible deployment scenarios to highlight the complexity of home virtualisation.

Figure 3 depicts an RGW virtualisation for Home #1. vRGW in now implemented in the NFV Network, providing the Private IP address to the home and is directly connected to some services like IPTV and VoIP. For Internet Services, the vRGW uses a tunnel or a session to the BNG. For all services vRGW performs a NAT function (conversion to private IP address).

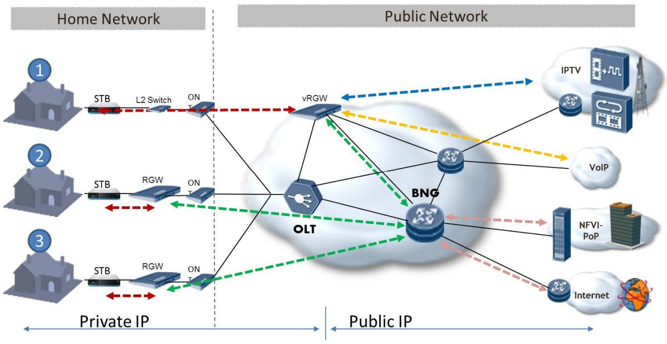

Figure 3: Home Virtualisation – RGW is Virtualised

Figure 4 depicts a Use Case where both RGW and STB for Home #2 are virtualised. The vSTB now uses a Public IP address to communicate with the vRGW and its service platforms (IPTV or Internet platforms via the BNG).

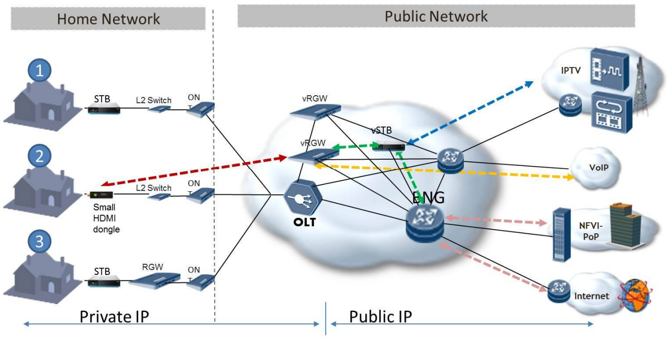

Figure 4: Home Virtualisation – Both RGW and STB are Virtualised – Public IP

In this case depicted in Figure 5, both RGW and STB for home #2 are virtualised and physically connected to the BNG. However, this Use Case more closely emulates the home environment, and logically the vSTB connects to the vRGW using a private IP address. vRGW, similarly to the home environment, provides connectivity to Network services using a Public IP address.

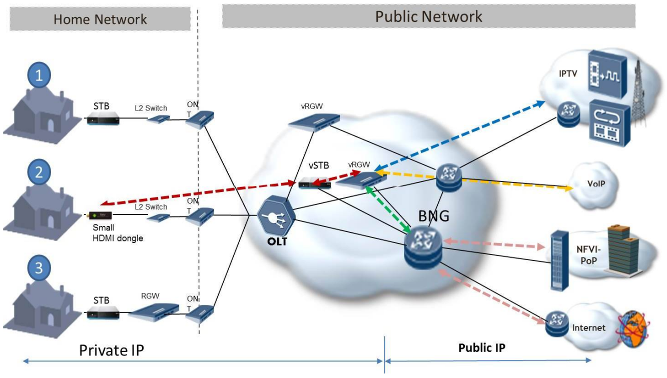

Figure 5: Home Virtualisation – Both RGW and STB are Virtualised in Private IP

In this scenario depicted in Figure 6, the STB services for Home #3 are provided from the NFV network and interoperability with an existing home located RGW is maintained. The vSTB now uses a Public IP address to communicate with its service platforms (IPTV or Internet platforms via the BNG). It also uses a public IP address to communicate with the home located RGW.

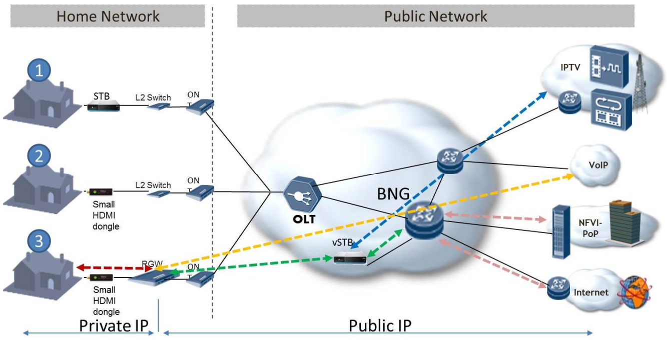

Figure 6: Home Virtualisation – Only STB is Virtualised

In all the above cases, connectivity to the Network Management functions (not specified and not shown here) is kept intact for smooth migration.

VI. Problem description/Issues

In this section we summarize some of the major problems and issues associated with NFV implementation of the Home virtualisation. The resolution and architectures required for resolving these challenges is an on-going task at the NFV standardization and is beyond the scope of the current paper. However we believe that identifying the challenges and classifying them will assist in NFV standardization work.

The Virtualised CPE will be run at from what we refer to as an NFV Front Cloud. It is estimated that hundreds of thousands of virtualised devices need to be supported. A straightforward implementation allocating a Virtual Machine per device would require enormous amount of cloud resources resulting in scalability challenges not easily supported by the relatively constrained NFV Front Cloud.

Virtualisation of the CPE eliminates the physical connectivity and the Physical port identification of the home device. DHCP option 82 needs to be replaced by an NFV based identification of the VNFs. Every VNF should be uniquely identified for service chaining to other VNFs. Communication among NFV entities should be secured and authenticated (e.g. between orchestration and the NFV Infrastructure for creating and connecting VNFs etc.)

It is possible to decompose the vCPE function into two parts. One part handles the Data Plane (such as packet forwarding, NAT and filtering). Additional control functionality such as DHCP, DNS, Web cashing etc. could be implemented as a centralized function (supporting multiple vCPEs).

Shifting per customer functionality to a network located one is well suited to be treated with specialized server pools on a per-functionality basis (e.g. centralized DHCP) rather than full virtual instances on per-customer basis. The challenge is to keep the customer notion when customer functionalities are scattered across different server pools. Some level of orchestration is required to make sure that on a per-customer level, the required functionalities are instantiated coherently on an on-demand basis and the solution remains manageable.

Virtualisation of Media services such as those provided by the vSTB may require a significant processing power from the NFV Infrastructure. Some performance sensitive functions are the result of the following:

- While currently the average bandwidth per home is less than 1Mbps, in 3-5 years, with the deployment of Virtualised Media functions, each home may source an order of 2-4 HD (or higher) streams at peak time, which adds up to more than 10-25 Mbps per home. This number will grow with the higher Media resolution in future services.
- Some operators will choose, in order to simplify the home decoding function, a VDI (Bit Stream coding) streaming which is more computation intensive than HTTP on the server side.
- For content protection, streamed media may need to be encrypted per home

To contain the cost and scale, a large number of virtualised devices need to be integrated on limited number of CPUs. While Moore's law will address the growing needs for bandwidth, careful design and optimization of content distribution and streaming load balancing is required.

The vCPE is required to support a large number of applications and services driven by the end user dynamics. In addition, there will be many topologies and network configurations during the migration from current to virtualised networks. In the virtualised environment, the responsibility for ensuring proper behavior of every scenario is the remit of the network operator.

Users expect to manage and configure their CPE devices even when they are virtualised and provided as a service. This new capability required from the operator is unique to the vCPE. An additional challenge is to guarantee service continuity at the home during network or access link failure (to match current network behavior).

Integration of existing management and OSS technologies must be considered.

Optimal functional splitting depending on the required functionality performance level has to be assessed (e.g. control plane and data plane functionalities, self-care and operator management access, etc.).

The virtualised environment needs to guarantee complete isolation among users. Data Encryption of cached content and link security is mandatory.

Acknowledgment

Many individuals and entities are involved in the Home Virtualisation work. Initial requirements and architecture were done in conjunction with a Tier-1 operator in a joint innovation project. Various research & development groups in Huawei Network Product Line were involved in various parts of the vRGW and vSTB research. Definition of the Home Virtualisation Use Case was done by the authors as part of NFV ISG End-to-End use case definition. Significant contribution was made by Adi Molkho from Huawei as part of his research on vSTB. Identification of Security issues listed in Table I were in large contributed by Robert Moskowitz from Verizon and Bob Briscoe from British Telecom and others from NFV ISG Security EG.

References

[1] ”Network Function Virtualisation” at http://portal.etsi.org/NFV/NFV_White_Paper.pdf.

[2] “GS NFV 009 V012 (2013-08) Network Function Virtualisation Use Cases;” at http://docbox.etsi.org/ISG/NFV/INF/70-DRAFT/INF2/NFV-INF001-2v030.docx

[3] Badger, et al., “Draft Cloud Computing Synopsis and recommendations”, NIST- SP800-146 (May 2011), pg. 2-1,5-4,5-5,7-2

[4] HGI, Home Gateway Initative “Home Gateway Technical Requirements: Residential Profile” Version 1.0

[5] Diego R. López, Borja Iribarne, “Business Cases for Virtual Customer Premises Equipment (vCPE) for end users”

[6] Minoves, P. ; Frendved, O. ; Bo Peng ; Mackarel, A. ;Wilson, D., “ Virtual CPE: Enhancing CPE's deployment and operations through virtualisation,” Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference on

[7] Mario Ibáñez, Natividad Martín, Madrid, Ralf Seepold, “Virtualisation of the Residential Gateway,” Fifth International Workshop on Intelligent Solutions in Embedded Systems WISES'07 Universidad Carlos III de Madrid, June 21-22, 2007