Jussi Torkko

Feasibility of NFV in Consumer Broadband Services in Fixed Network Domain

Metropolia University of Applied Sciences

Master's Degree

Information Technology

Master's Thesis

19.5.2016

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Jussi Torkko Feasibility of NFV in Consumer Broadband Services in Fixed Network Domain 41 sivua 19.5.2016
Tutkinto	Ylempi Ammattikorkeakoulu Tutkinto
Koulutusohjelma	Information Technology
Ohjaaja	Yliopettaja Ville Jääskeläinen

Verkon funktioiden virtualisointi (NFV) on yksi kiinnostavimmista tekniikoista telekommunikaatio alalla. Sen pää periaate on muuttaa mahdollisimman monia verkon toiminteiden funktioita fyysisiin laitteisiin pohjautuvista ratkaisuista ohjelmoiduiksi virtuaalisiksi applikaatioiksi. Virtualisoiduilla toteutuksilla mahdollistetaan säästöjä laitteiden jäähdytyksestä, virransyötöstä sekä tilan käytöstä. Myös operatiivisia säästöjä saavutetaan virtuaalisten toteutuksien dynaamisuuden ja skaalautuvuuden kautta.

ETSI:n NFV Standardisointi työryhmä on tehnyt töitä vuodesta 2012 lähtien mahdollistaakseen tämän teknologian standardoimisen. Tämä työ tutkii ETSI:n NFV käyttö esimerkin ”Kodin ympäristö virtualisoiminen” soveltuvuutta toteutettavaksi TeliaSoneran verkossa Suomessa. Työ on tehty paperi tutkielmana ja lopputuloksena se esittää suosituksensa jatko toimenpiteistä asian suhteen.

NFV tuo CAPEX sekä OPEX säästöjä laaja mittaisten toteutusten yhteydessä. Se myös mahdollistaa nopeamman kehitystyön erottamalla laitteiston ohjelmistosta. Nopeampi kehitystyö johtaa nopeampiin kaupallisiin julkaisuihin sekä helpottaa uusien arvoa lisäävien palvelujen kehitystä.

Loppu tuloksena työ ei suosittele ”Kodin ympäristön virtualisoimista” ainoana toteutuksena mutta osana laajempaa toteutusta yhdessä useampien virtuaalisten toiminteiden kanssa. Työ suosittelee myös jatkamaan virtuaalisten RGW:n ja STB:n yksityiskohtaisempaa tutkimusta ja painottamaan työtä näiden lisäpalveluiden kehittämiseen.

Avainsanat	NFV, NFVI, RGW, vRGW, STB, vSTB

Author(s) Title Number of Pages Date	Jussi Torkko Feasibility of NFV in Consumer Broadband Services in Fixed Network Domain 41 pages 19.5.2016
Degree	Master of Engineering
Degree Programme	Information Technology
Instructor(s)	Ville Jääskeläinen, Principal Lecturer

The Network Function Virtualisation (NFV) is one of the most interesting new technologies in telecommunications. The main principle of the NFV is to have software based network functions running as virtual instances instead of having numerous hardware based specific network elements doing the task. By doing this there one should save in cooling, power and space. Also operational savings should be achieved with a more dynamic and scalable environment.

ETSI NFV Standardization Group has been working with this technology since 2012 to lead the development towards a standard. This thesis studies the feasibility of implementing the ETSI's NFV use-case of "Virtualising the Home Environment" in TeliaSonera's network in Finland. This study was conducted as a paper study and as a result it gives a set of recommendations for the future work.

The NFV provides CAPEX and OPEX savings in large scale implementations. It also accelerates development work by decoupling hardware and software. Faster development enables faster time to market and helps creating value added services (VAS).

As a result the study does not recommend implementing "Virtualisation of the home environment" alone but as one of the many virtualised network functions to reach a large enough scale of implementation. It also recommends to continue more specific studies of virtualizing the Residential gateway (RGW) and Set-top-box (STB) and how new VAS can be created on top of them.

Keywords	NFV, NFVI, RGW, vRGW, STB, vSTB

Table of Content

Acronyms

ALG	Application Layer Gateway
API	Application Program Interface
ASIC	Application Specific Integrated Circuit
BNG	Broadband Network Gateway
BSS	Business Support System
CAPEX	Capital Expenditure
COTS	Commercial Off-The-Shelf
CPE	Customer Premises Equipment
DC	Datacenter
DHCP	Dynamic Host Configuration Protocol
DLNA	Digital Living Network Alliance
DNS	Domain Name Service
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
EMS	Element Management System
EPG	Electronic Program Guide
ETSI	European Telecommunications Standards Institute
FG	Forwarding Graph
FIB	Forwarding Information Base
FTP	File Transfer Protocol
GUI	Graphical User Interface
HDMI	High Definition Multimedia Interface
HW	Hardware
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPoE	IP over Ethernet
IPS	Intrusion Prevention System
IPTV	IP Television
ISG	Industry Standardization Group
ISP	Internet Service Provider
L2	Layer 2 (Referring to OSI model and Ethernet)
L3	Layer 3 (Referring to OSI model and IP)

LAN	Local Area Network
NAT	Network Address Traslation
NF	Network Function
NFV	Network Function Virtualisation
NFVI	NFV Infrastructure
NPVR	Network PVR
NTP	Network Time Protocol
OLT	Optical Line Termination
ON	Optical Network termination
ONF	Open Networking Foundation
OPEX	Operational Expenditure
OS	Operating System
OSS	Operations Support System
OTT	Over-the-Top
PoC	Proof of Concept
PVR	Personal Video Recorder
QoS	Quality of Services
RGW	Residential Gateway
ROI	Return of Investment
SDN	Software Defined Networking
STB	Set-Top-Box
SW	Software
SWOT	Strengths, Weaknesses, Opportunities, Threats
TSTV	Time Shifted TV
uPnP	Universal Plug and Play
VAS	Value Added Services
Wi-Fi	IEEE 802.11b wireless networking
VIM	Virtual Infrastructure Management
WLAN	Wireless LAN
VM	Virtual Machine
VNF	Virtual Network Function
VoD	Video on Demand
VoIP	Voice over IP
VPN	Virtual Private Network
vRGW	Virtual RGW
vSTB	Virtual

1 Introduction

Today's telecommunication operator services are mostly hardware based appliances. The hardware is dedicated to serve one purpose and for other purposes it is required to have more devices. Every device requires space, cooling and power that all cost. The life-cycle of the hardware is also becoming shorter every year. As a solution to this challenge the telecommunication industry has invented the network function virtualization (NFV) concept. The virtualization of server platforms has become a standard technique in modern datacenters and now it is applied in producing network functions.

The idea of NFV is to use standard industry volume servers and by means of virtualization to pool computing, storage and networking capacity that is then allocated to virtual machines which execute the network functions. On the same server hardware there can be running several network functions and therefore resources can be used in more effective way. The virtual network functions are software based and can be started, stopped, scaled or moved without moving or installing new hardware. Of course using common of the shelf (COTS) servers instead of optimized and application specific integrated circuits (ASIC) based special routers has an impact on performance that needs to be taken into account. In Figure 1 there is illustrated the NFV principle how several network specific devices could be consolidated to virtual instances running on the same infrastructure created by virtualizing and pooling server resources and managed with one orchestration and management system. [1]

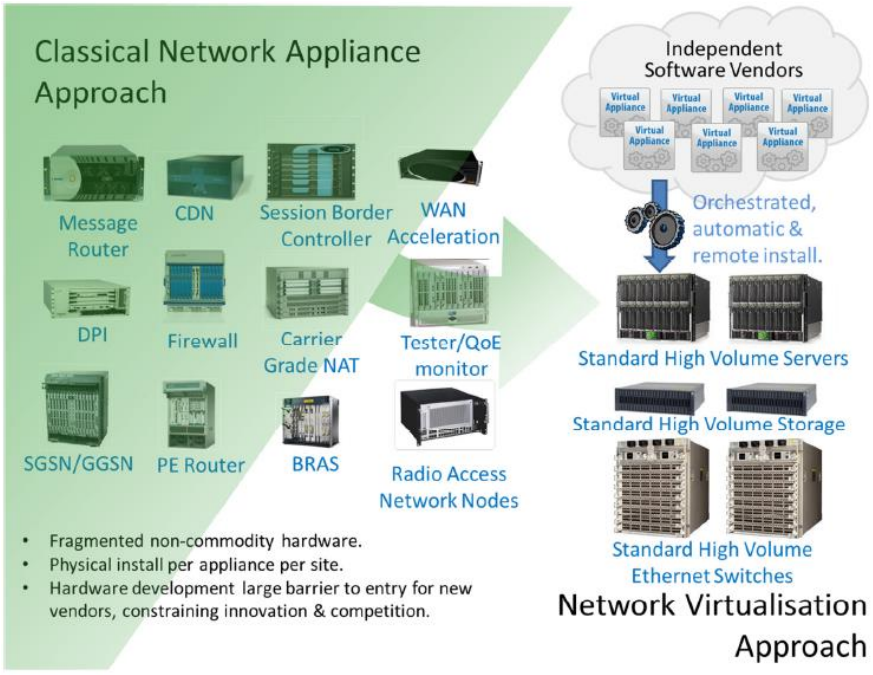

Figure 1. ETSI NFV ISG vision pictured. [1]

The industry started to discuss NFV in the beginning of this decade and that is also approximately when a workgroup under ETSI supervision was formed to standardize the technology. The ETSI industry standardization group (ISG) was formed by leading telco operators and device manufacturers.

One of the many publications of ETSI NFV ISG is a list of the most promising use-cases for NFV [2]. Two of these use-cases are directly related to the topic of the present study. These use-cases are No.7 “Virtualisation of the home environment” and No.9 “Fixed access network function virtualization”. This study focuses on the first one, the virtualization of home environment, and evaluates the feasibility of implementing it in the Finnish market and in TeliaSonera’s network.

The principle in the use-case is to move as many of the customer premises equipment (CPE) functions as possible to the network. Leaving only simplified and cheap equipment to customer premises. In the network functions can be centralized and run in a more efficient manner then today as distributed to homes of the customers. This will have an impact on service delivery and design.

Figure 2 shows ETSI NFV use case No.7 where many of the Residential Gateway (RGW) and the Set-Top Box (STB) functionalities have been moved up in to the network. [2]

Only simple L2 switch and a HDMI dongle is left in home network to provide connectivity to services.

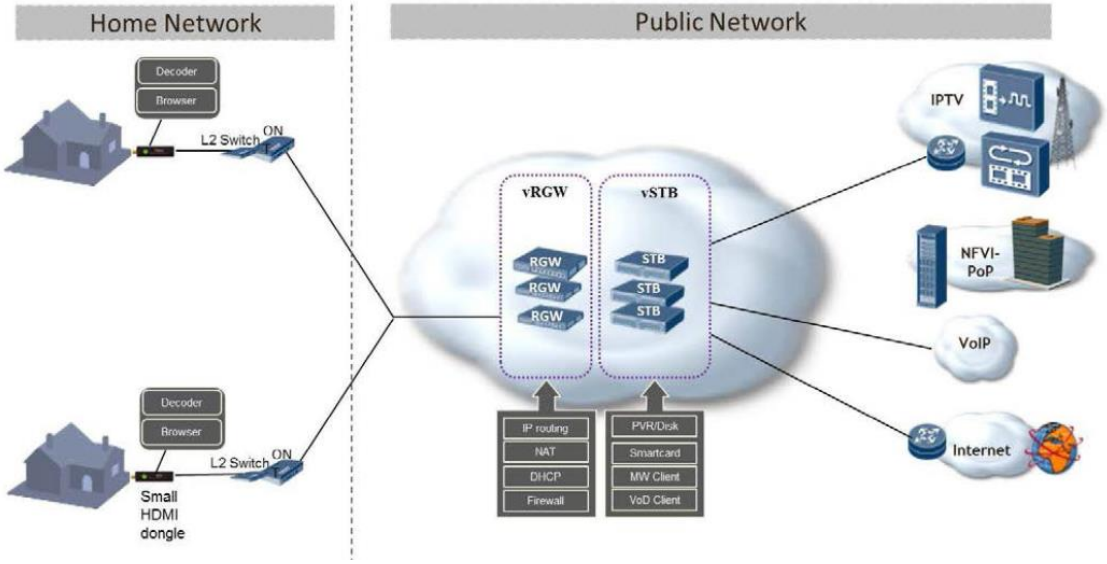

Figure 2. The ETSI NFV Use-Case #7 Virtualisation of the Home Environment. [2]

The goal of this study is to evaluate the benefits and drawbacks of this use-case of virtualising the home environment and to determine would it be feasible to implement it in TeliaSonera's network in Finland. As a result this study presents a set of recommendations for future actions.

This study was conducted as a paper study. It evaluates the solution with given specifications and compares it to the existing service model. The evaluation is based on ETSI publications, TeliaSonera specialist interviews and opinions, the company's internal work related to NFV and own observations. The structure is as follows:

- Chapter 1 introduces and describes the study.
- Chapter 2 explains the NFV in more in detail and gives an overview of the SDN.
- Chapter 3 explains how today's services work and introduces the ETSI use-case of "Virtualising the Home Environment" and how it differs from today's model.
- Chapter 4 evaluates the feasibility and examines the possible impact on the network
- Chapter 5 summarizes the work done and presents the final recommendations for future work.

2 Network Function Virtualization

This chapter explains the basic concept of Network Function Virtualisation (NFV), the reference architectural framework and NFV's relation to Software Defined Networking (SDN).

2.1 NFV and Services

Telecommunication services can be presented as an end-to-end service or broken into a set of functional components that create this entity. For example the Internet access typically consist of the following components: DHCP, DNS, NAT, Transport, Security (of some level) etc. Connecting these components together in a specific order creates the end-to-end service. This order of connected services can be expressed by means of a Forwarding Graf (FG). Forwarding graph is a great way to illustrate service components and information flow order. As shown in Figure 3 below, the forwarding graph is nested in a graph that also shows us the infrastructure network segments related to the service. [3]

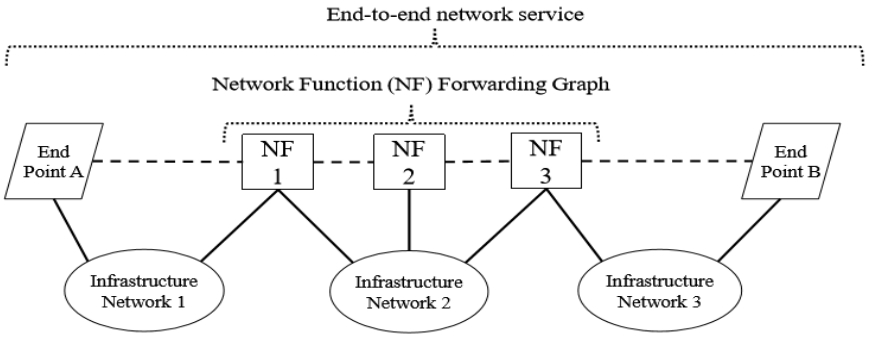

Figure 3. Graph presentation of an end-to-end service. [3]

The Network Function Virtualisation is a big change to telecommunication in many ways but the main idea and purpose is rather quite simple. The idea in NFV is to decouple software and hardware from each other by means of standard IT virtualisation technology and running network specific functions as a software on high volume servers, storage and switches. When a Network Function (NF) is not restrained to one physical hardware

device it gives a lot more flexibility to its operation and management. Non-physical NF can be moved, copied, scaled up or down when needed or one can create triggers that start these dynamic new features. Non-physical existence also minimizes the impact of single HW failure for the service itself.

When a service is implemented by means of NFV the use of FG becomes more useful describing decentralized end-to-end services. Figure 4 shows an example service that is composed of three virtualized network functions and one of these is implemented as the sum of three sub-functions and only two out of five components are located at the same physical location. [3] Without means of a FG describing this service and mapping it to corresponding execution locations would be difficult.

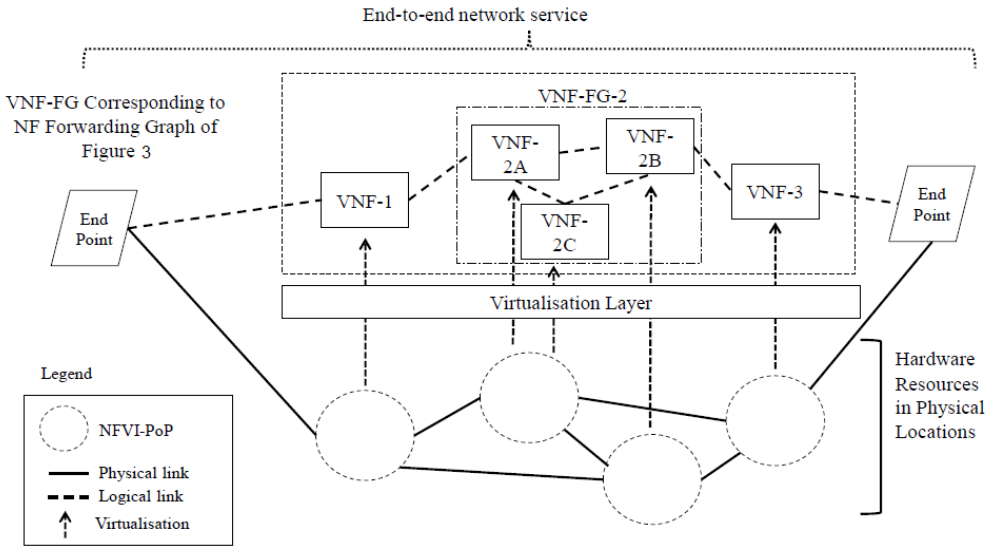

Figure 4: When a NF is virtualized it is not restrained to one physical location. [3]

The list of claimed benefits of network function virtualization is long. Many of these are listed in ETSI NFV ISG White paper I released in October 2012. [1] On top of the list there are reduced costs that is maybe the most weighted feature today when creating new services.

The cost reduction is based on consolidated equipment and exploitation of the IT industry COTS servers and storage. Using the same HW for producing different services helps building future capacity without a need to know exactly for what purpose it is going to be used. Therefore in a NFVI environment a buffer of resources are kept always above production requirements.

Installations of new funtions is also fast. These free resources can be used to install any new software based function in seconds or minutes when today installing a new device can take days or weeks.

Virtualised services and infrastructure can be divided into domains like networks. This enables testing of new features and services on the same shared infrastructure with the production.

The fast implementation and testing also shortens greatly time-to-market when launching new services. The decoupling the HW and the SW opens market for new business. The small software companies could enter the market of virtual appliances without huge investments in the hardware production. Openness is encouraged to keep interoperability with all HW vendors and SW development.

The dynamic SW based services could be also targeted geographically and resources could be prioritized periodically or for critical incident handling when needed.

The virtualisation of network functions together with Software Defined Networking (SDN) represent so big and drastic change to communication networks that they are described as revolutionary technologies within the industry. When talking about changes in this scale there are many thing that can go wrong. Today there is no standardization for NFV nor for SDN. Luckily this has been acknowledged and a few big open organizations have started to drive these initiatives towards standardization and open ecosystems to provide best possible interoperability across the industry.

The following paragraph will explain the network function virtualization with an example of ETSI architectural framework.

2.2 NFV Reference Architectural Framework

ETSI NFV ISG started their work with painting their vision of NFV on a White Paper I released October 2010 [1]. In the following years with White Paper II (2013) [4] sharpened the plan for delivering this vision and other more detailed documents were published on how it should be done in domain levels. One of these more detailed documents

is ETSI GS NFV 002 v1.1.1 Network Function Virtualising; Architectural Framework published in October 2013 [3]. These papers are not standards defining exact details but guidelines for industry consensus of best practice and defining a high level architecture and interfaces between the main building blocks to keep everything compatible and interoperable between different vendors. Interoperability in NFV is highlighted because locking into one vendor specific environment would strip away many benefits of virtualizing and might lead into vendor lock-in when seeking new features for development. Multivendor environment or possibility for it and decoupled SW from HW ensures easy individual development and replacement of different sections of the virtualization environment.

The architectural framework in Figure 5 introduces most of all the different sections referred as building blocks and the interfaces between them. [3] The following text explains them in more detail.

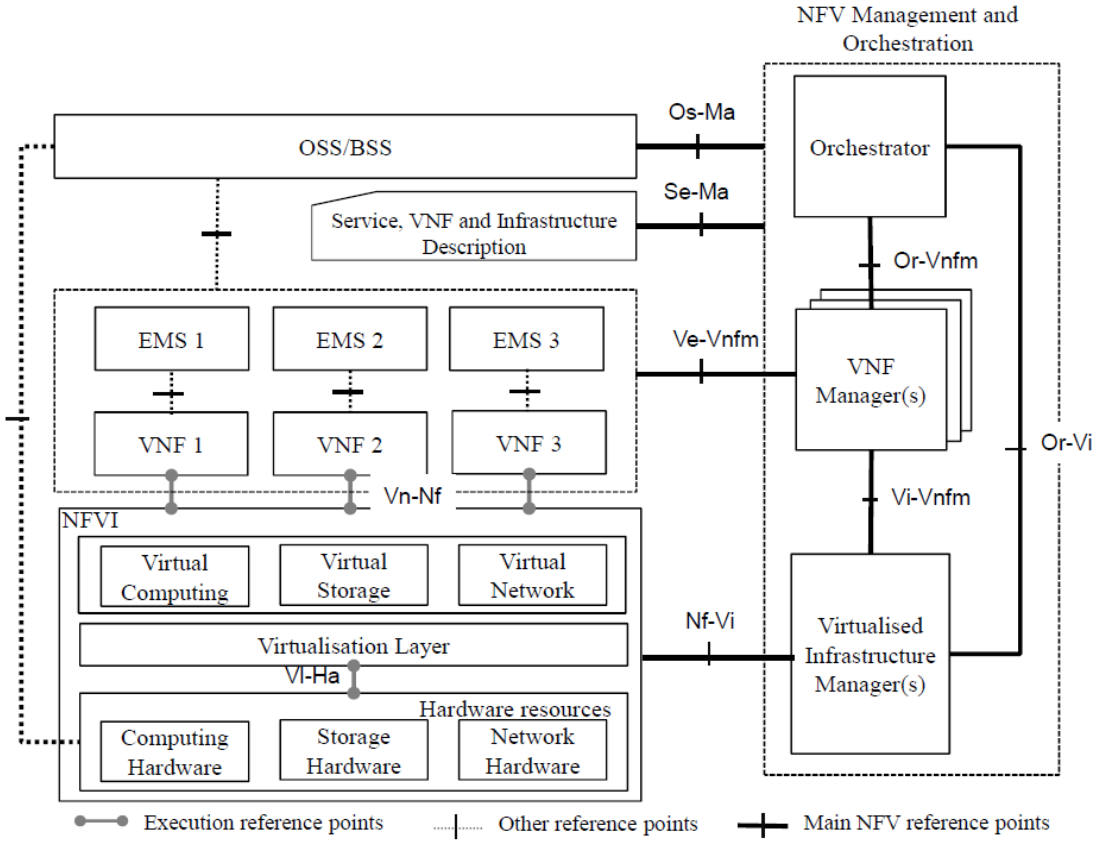

Figure 5. The ETSI NFV reference architectural framework [3]

Network Function Virtualisation Infrastructure (NFVI). This is where the magic happens; where physical becomes virtual. This is the most complex part of the NFV. But within the

scope of this study it is not necessary to cover it in very detailed. The overall picture is adequate to understand for the service focused approach in this study.

The NFVI can be roughly divided into two parts. The hardware resources and the virtualization layer with virtual resources. The hardware resources are the physical equipment; servers, storage and switches. Individual and physical devices. The virtualization is done by means of Hypervisors. Hypervisor is software, hardware or firmware that takes control of hardware resources underneath and runs virtual machines (VM) on top. A VM, also called a guest, can run its own operating system (OS) or software and is not aware of the hypervisor underneath it. Hypervisors are managed by an orchestrator or a virtual infrastructure manager and together they create virtualization layer that pools all resources of underlying HW. The HW is connected to a network with physical switches and VMs are connected by virtual switches. Virtual switching can be a hardware feature or software based. VM's recourses and connections are managed by the orchestration/management system that allocates resources and arrange the network connectivity needed. How this all is done exactly varies between different vendors. Some have more proprietary and closed ecosystem while some rely on open ecosystems. This does not make a great difference if interfaces of NFVI are interoperable with a common framework and a specification.

The Virtual Network Functions (VNF) are running on VMs that are created on virtualization layer. VNFs are only aware of resources and connections that VM is related to by the orchestration and management system. This feature is the basis for something called abstraction layer. Abstraction layer is a network and a resource overview of a given operational network environment. Abstracting parts of network gives an opportunity to isolate services run on shared resources. This provides more simplified picture that makes it easier to manage and it also provides additional level to security. It also makes it possible to do testing on the same production platform without a need of creating exact lab environment of it. VNF is a software based functional application executing its described function just as it would be on a dedicated HW. More complicated VNFs include databases and are a sum of several child functions. To communicate with orchestration and management entities VNF has an *Element Management System* (EMS). EMS could be a software agent on the same VM that handles communication towards management. How NFV's are compiled and how they are chained is stored in dedicated "Descriptions" -database.

Operation Support System (OSS) and Business Support System (BSS) are the same as they have been in traditional telecommunication networks. OSS represents service provider's network inventories, provisioning and device configuration system that work together with BSS which handles product and customer relations. OSS and BSS are usually mostly automated to handle customer orders and handling related information flow to and from the network. With virtualized network parts it is possible to choose what kind of abstraction view of network is shown to OSS and BSS.

NFV Management and Orchestration is composed of the orchestrator, VNF managers and Virtualisation Infrastructure Manager (VIM). The VNF Manager and VIM are sub systems that handle communication on their specific area and respond to Orchestrator. Orchestrator is the management for the whole environment. From here it is possible to supervise performance and assign resources and initiate other management functions or create new networks and services.

All parts of this architectural framework have also specified interfaces between them providing communication channel between segments. Having these interfaces specified makes it possible to use multi-vendor environments without great tailored integration of different systems. This build in interoperability is really important part of this framework. Most of today's Telco's have some legacy devices in their networks with proprietary management systems. This creates additional burden to integrate these to other systems.

2.3 NFV's Relation to Software Defined Networking

Network Function Virtualisation is not the only new innovation the industry is buzzing about. Software Defined Networking (SDN) has been equally groundbreaking news for networking. NFV and SDN are not depended on each other, however, they can be highly complementary together.

NFV aims at consolidating many network equipment types running on COTS IT servers, storage and switches. This is claimed to enable great savings on costs, power, space and cooling. At the same time it brings benefits of decoupling SW and HW accelerating innovation, implementation and time to market with high-level of automated management of the NFV environment.

The principle of SDN is to separate the control plane and the data plane in devices. This is a somewhat similar approach that NFV has decoupling SW & HW but the goal is different. By separating control and data planes SDN strives to enhance network performance, simplify compatibility of existing implementations and to facilitate operations and maintenance procedures. For those who are not familiar with concepts of data and control plane there is Figure 6 describing traditional router control and data planes and their functionality.

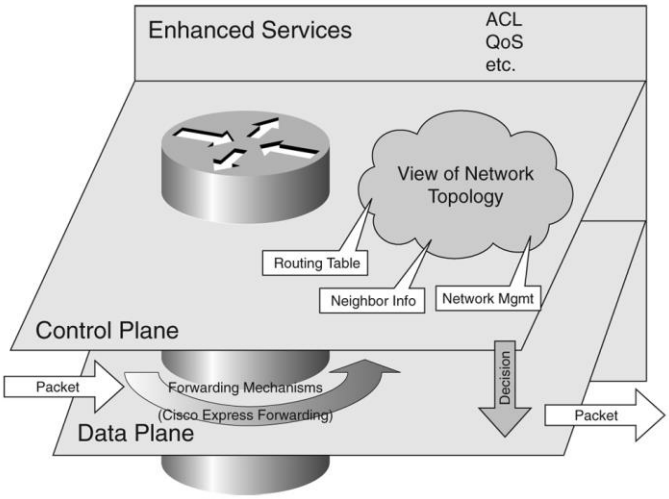

Figure 6. Router's control plane and data plane. [5]

When packets enter the router they are processed on the data plane whose function is merely to pass packets to the right direction. The decision is based on the forwarding information database (FIB) that is filled by the control plane. One could say that the control plane is the intelligence of a router. This part holds routing information, network information and other traffic treatment related instructions. When a router gets a packet for which it does not have a FIB entry it is passed to control plane for further processing. On the control plane the decision is made on how it should be forwarded and this information is added to FIB. After this control plane is capable to forward this type of traffic to a right destination again.

Now with SDN devices control planes would be centralized to a controller that would hold the whole network view and could therefore make more optimal traffic routing decisions.

The SDN high-level architecture is illustrated in Figure 7. [6] The infrastructure layer refers to network devices forwarding information. The devices communicate with the controller software using a certain defined interface and protocol such as OpenFlow. The software based controller is aware of both the network and the services and therefore capable in doing highly optimal traffic management decisions. Above the control layer is the application layer. The application layer is populated by business applications that have some interaction with the network. This interaction could be provisioning of new customer connections or just monitoring and information gathering. Communication between the control and application layer is done over standard APIs. On the control layer this communication towards the application layer can be restricted in order to provide required level of security. The control layer can be used to make abstraction views of the network for simplification of maintenance or security reasons.

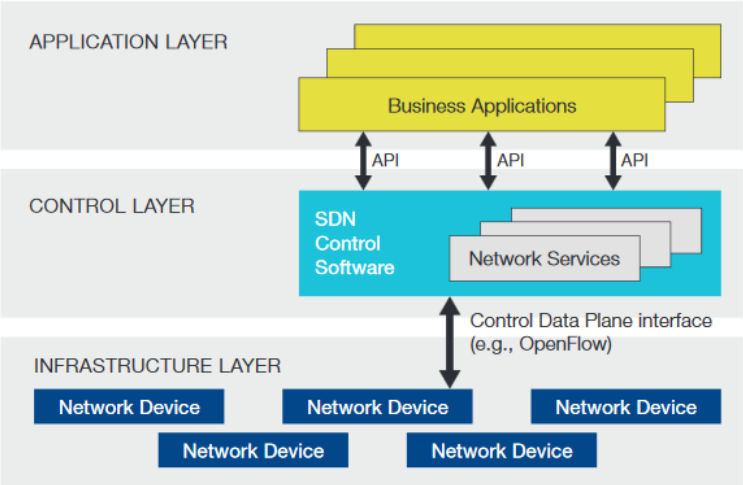

Figure 7. NFV complementing SDN [6]

The main drivers for new network architecture and SDN are listed in ONF Whitepaper 2012 as follows. [6] Change in traffic patterns: Traffic in networks has shifted from traditional “north-south” type client-server communication towards “east-west” type from machine to machine traffic where client query can travel between several servers and databases gathering information before returning to client. The “Consumerization of IT”: Users have more devices of great variety and access to networks and content is expected to be always available. IT is under pressure to fill these expectations while protecting intellectual property and meeting other security demands. The rise of cloud services:

Clod services have become ubiquitous both in business and personal lives. Industry has embraced both private and public cloud resulting a huge growth of the business. In addition to accessing data enterprise business services require more enhanced services such as self-provisioning and elastic scaling all with increased security. The “Big Data”: Handling todays “Big data” requires massive scale of resources in datacenters. Even thousands of servers needing direct connection to each other to process the huge amounts of data.

In addition to these requirements of today the existing networks set limitations in performance. SDN promises by using centralized software based network controller and common APIs to achieve: improved vendor independent automation and management with finer granularity of control. The acceleration of new service innovation is enabled with programmability by operators, enterprises, independent vendors and users without waiting particular network device vendor releases.

Together NFV and SDN could provide whole network wide centralized control and management, consolidate many devices on IT server HW and provide automation and programmability of a kind that simply cannot be achieved in today’s networks. However, they are not required to have both and that gives ISPs freedom to make the change in smaller tiers towards the fully applied SDN and NFV implementation.

3 ETSI NFV Use-case ”Virtualised Home Environment”

This chapter describes the service architecture commonly used to deliver internet access and related services (The Triple-Play) and the architecture ETSI use-case proposes. First here is explained todays architecture and some of its functions related to this use case. It is also equally important to clarify what is meant here with the Home environment. The Home environment equals in following context the Residential Gateway (RGW) and the Set-Top-Box (STB) which are required devices usually to deliver Internet services and IPTV.

3.1 Today’s Service Architecture

The internet access and related services that ISPs offer today is often called as Triple-play service. This is because they consist three services: the internet access, IPTV and VoIP. In Finland the VoIP service is not a profitable service and most of the operators are not even offering it. This is also the case with TeliaSonera on which this study is focused and therefore this service will be just ignored here even though it is mentioned on some of the pictures. The triple-play services are basically delivered as described in Figure 8 [2] and with help of the named elements. This traditional architecture is also what TeliaSonera is currently using.

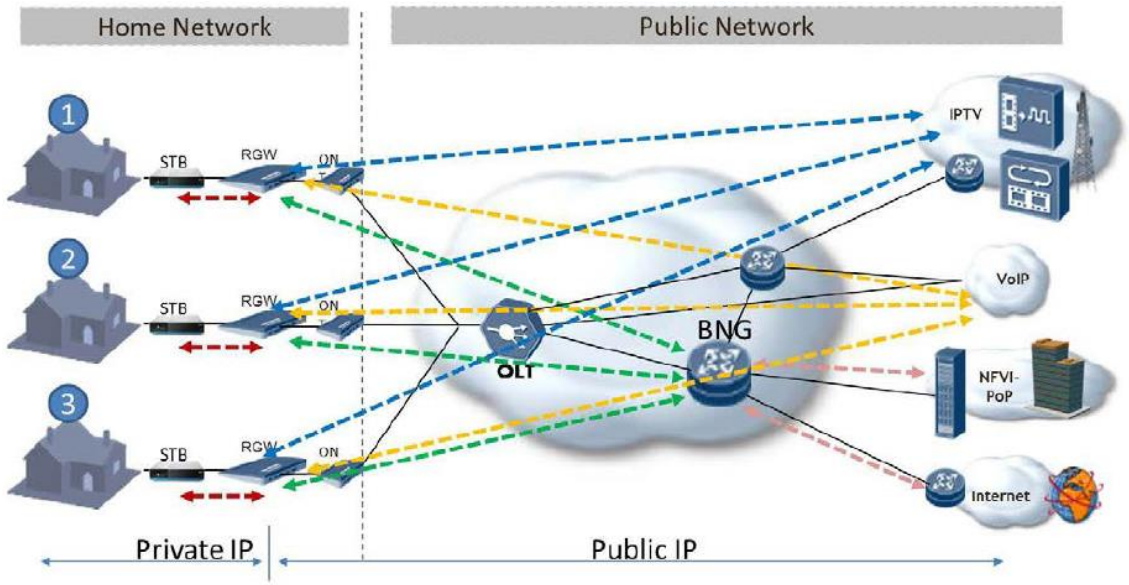

Figure 8. Common triple-play service architecture. [2]

In the customer home network there is a STB for IPTV stream reception, decoding and interaction with service backend. A local storage Personal Video Recorder (PVR) is often integrated on set-top box for recording content in addition to Network PVR (NPVR) service. A small router RGW creating home LAN and providing IP connectivity over L2 transport segment to ISP network, routing and policing traffic, handling Dynamic Host Control Protocol (DHCP) and Network Address Translation (NAT) between private and public IPs, Firewall and possibly other functions depending on service provider. A RGW is the most complex and expensive equipment in home network for operator to provide and maintain. The transport network is mostly irrelevant for this study. In figure 8 it has been described with Optical Network termination (ON) and Optical Line Termination (OLT) pair. This could be DSL modem and a DSLAM pair or pure Ethernet. The transport function is only to create safe and transparent connection for user and aggregate traffic over available media to ISP's network. Of course it has many features and it does make a difference for the service but it is ignored here for the sake of simplicity. The Broadband Network Gateway (BNG) is a router functioning as a termination point of customer connection. It terminates customer L2 connection and provides customer L3 connectivity and routing toward ISP backbone and eventually to the internet. It also the point where the Qality of Service (QoS) policy is enforced for the customer. Backend services produce the actual service and can be located in ISP network (IPTV, VoIP) or in the internet

(Over the top (OTT) applications e.g. YouTube and NetFlix). The RGW can connect directly to right service backend or it can be routed with help of the BNG towards the right direction.

The border of public and private IP domains is here at the RGW level. Internet uses IP addresses for unique identification of connected devices. Today the IP version 4 addresses that are running low are still mainly used. Therefore part of the address space is reserved as so called private addresses (RFC1918). Private addresses are used in closed routing domains such as in ISP internal networks and in homes and by these means saving public addresses. These private addresses are not valid in public internet for routing because they are in free usage and the user could not be identified or there could be many destinations. Public addresses are maintained by official authorities, registries that provide ISPs the address blocks for requested purposes. ISPs track the use and are obligated to follow and log users IP information for possible lawful interception. Section 4.1.1 below describes how the network functions work in more detail.

3.1.1 RGW functions

When the RGW is powered for the first time it will soon start creating connections for preconfigured services. First it needs a public IP for internet connectivity. This is done with DHCP queries. DHCP protocol sends a broadcast querying where the DHCP server is. To suppress unnecessary broadcasting in network access devices such as DSLAM or switches ISP network relay this query directly to the DHCP servers. DHCP servers reply with IP address and other possible information related to RGW management such as FTP, NTP, and DNS addresses etc. DHCP options are also often used in way or another to identify customer to which IP is given. In many countries law and regulations obligate ISPs to track customer IP information if misusage lead to lawful interception. Due to general IPv4 depletion in most of the cases only one or few public IPs are granted for the RGW or CPE querying the IP. Today it is expected that the end-user has more than one device on LAN that require IP connectivity. Then NAT together with local DHCP function need to be used. When a device connected to LAN queries for IP the RGW local DHCP server replies with a private address. Private addresses cannot be routed to internet and therefore NAT function translates the private one to public IP when traffic is passed to network side and wise versa. The traffic to original source is mapped by tracking port and source/destination information.

Often RGW is also capable of creating wireless LAN (WLAN) for home environment and provide basic firewall services. Additional features can be application and port mapping for traffic and parental control features.

In TeliaSonera's case what is not visible for the customer is that the RGW also does a so called policy routing and QoS. Certain protocols or purpose reserved address blocks are treated with pre-defined actions. For example multicast related address area and protocols are marked to priority class of traffic and mapped with certain Virtual Local Area Network (VLAN) tag to be able to connect ISP IPTV service and provide required quality of service. There are also own classes and VLANs for device remote management and other data traffic where all the rest will be added if no special treatment. What this policy routing enables is that the customer has the freedom to choose the way the devices are connected with respect to networking fundamentals and TeliaSonera does not need to change configurations (e.g. port configuration) for different set-ups and avoids some unwanted calls from customer service.

3.1.2 STB Functions

The STB is the other important device in home environment for the use-case of virtualisation. A STB is also a requirement for IPTV reception for most ISPs. The IPTV is equated to the broadcast TV in Finland and under same tight requirements and regulations. The STB box has a remote control and interface to connect the home's big screen. This gives people the same user experience as with the standard broadcast TV. STB often has a bootstrap configuration that helps it to solve in DHCP fashion server addresses and to load recent SW for itself. After this the customer authenticates over Graphical User Interface (GUI) and the STB resolves from servers what content and channels customer is entitled to.

IPTV traffic uses control protocol IGMP for signaling ordered channel to be viewed and changes. IPTV is a bidirectional service where traffic can flow in both directions. This enables video on demand (VoD) services and other content selection and 3rd party services on top of TV broadcasts what creates richer user experience. The users are used to demand recording features for TV service. In IPTV service this is handled with local hard drive in STB called private video recorder (PVR) service or with network PVR which

would be network storage service attached to IPTV. In Finland and in many other countries there are a lot of laws, regulations and content right management right related matters that dictate what can be recorded in network and what can only be recorded in customers physical device at home premises.

Like all video material streamed from network today, IPTV is also encoded to save bandwidth and correct transmission errors. This sets a requirement for STB to have encoding capability and for pay channel case also decryption to display secured content.

3.2 ETSI NFV Use-Case “Virtualised Home Environment”

It has been seen that this traditional way of providing services to consumers could be virtualized from most of the parts saving CAPEX and OPEX and enabling new customer experience enhancing features. In the ETSI SG NFV Use-case document the workgroup proposes the following list of traditional functions to be virtualized [2]:

1) RGW

- Connectivity
    - DHCP server – to provide private IP addresses to home devices
    - NAT – Provide routing capabilities for traffic by converting home network addresses to one public
    - IPoE client – Client for connectivity to the BNG
    - ALG – Application level gateway to allow application specific routing behavior
- Security
    - Firewall, antivirus, IPS – Provide protection to home environment
    - Parental control – Allows control of consumed web content
    - Port mapping
    - VPN Server – Provide remote access to the user LAN
- Management
    - Web GUI – to allow subscriber management
    - TR-69 – To allow operator control
    - uPnP comparable technology with augmented security – Discovery of vRGW by home applications
    - Statistics and diagnostics

2) STB

- User Interface and 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 EPG, VOD, NPVR, TSTV 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 and Security
    - Web GUI – to allow subscriber management
    - Encryption – support different encryption schemes for cached content
    - Share Content – Possibility to share content

For the main parts the proposed list is pictured in Figure 9. RGW and STB are copied as SW appliances and located to a so called service provider front cloud. Home network connectivity is handled with simple bridging L2 switch and a HDMI dongle to connect the TV screen.

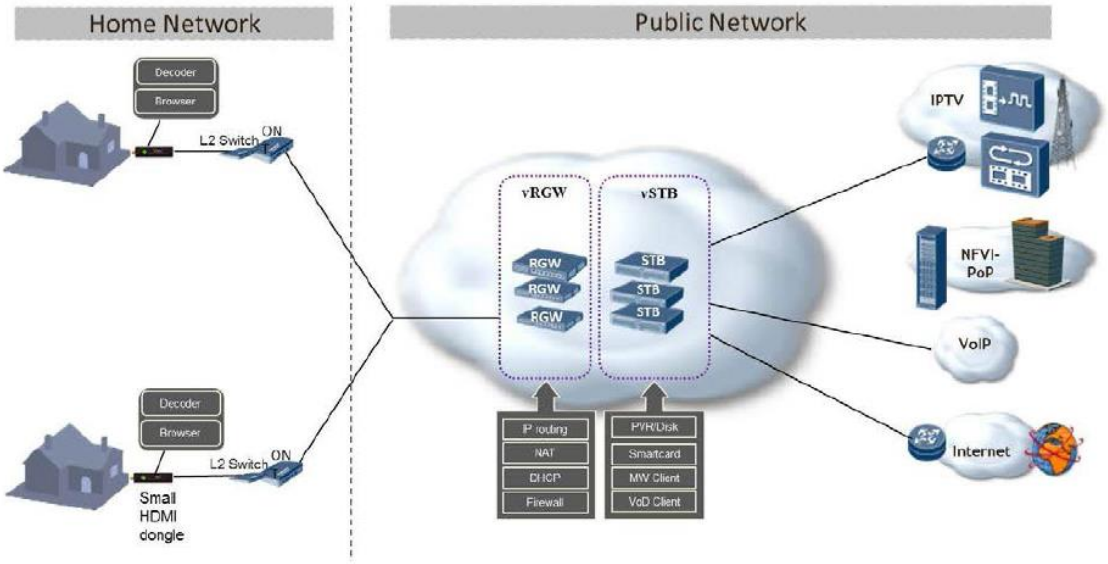

Figure 9. vRGW and vSTB located in ISP Front Cloud [2]

If the reader is not a network engineer this list does not give a clear picture of what is changed. Many of the functions are still the same and there for the same purpose. However, there are significant changes in some functions. Changes from a traditional architecture to a virtualized architecture is discussed next.

3.2.1 Home Network Equipment Functions

The STB and RGW were the devices providing user interfaces to connect services. Now that these two devices are moved to network as virtual instances there is a need to provide something else to connect end user devices at homes. Here in the use-case it is proposed to introduce a simple L2 switch/modem to provide connectivity to ISP network and to connect home network devices. Basic L2 switch could be very simple with WLAN capability, a few Ethernet ports and basic QoS support. Its function is merely bridge user end-devices to ISP network. DSLAM or aggregation switch on ISP network side can mark and tunnel traffic as chosen to transport to front cloud located vRGW. For IPTV service it would be good that the switch in home premises would have support for QoS so that video stream could be prioritized in case of congestion of bandwidth.

Today's TV screens have Ethernet interfaces but this not the main interface for video stream and also legacy devices must be supported. The HDMI interface has become the main standard and can be expected to have. A small HDMI dongle can be capable of

taking video transport stream from Ethernet and decode it into HDMI interface. The dongle can also be used to provide a radio, infrared or Wi-Fi interface to interact with TV remote controller. This way it is possible to provide a similar user experience the customers are expecting to have. However the dongle would not have the full middleware client, the software communicating to backend service, instead it would have a browser based remote UI client that connects to vSTB in network and display chosen content.

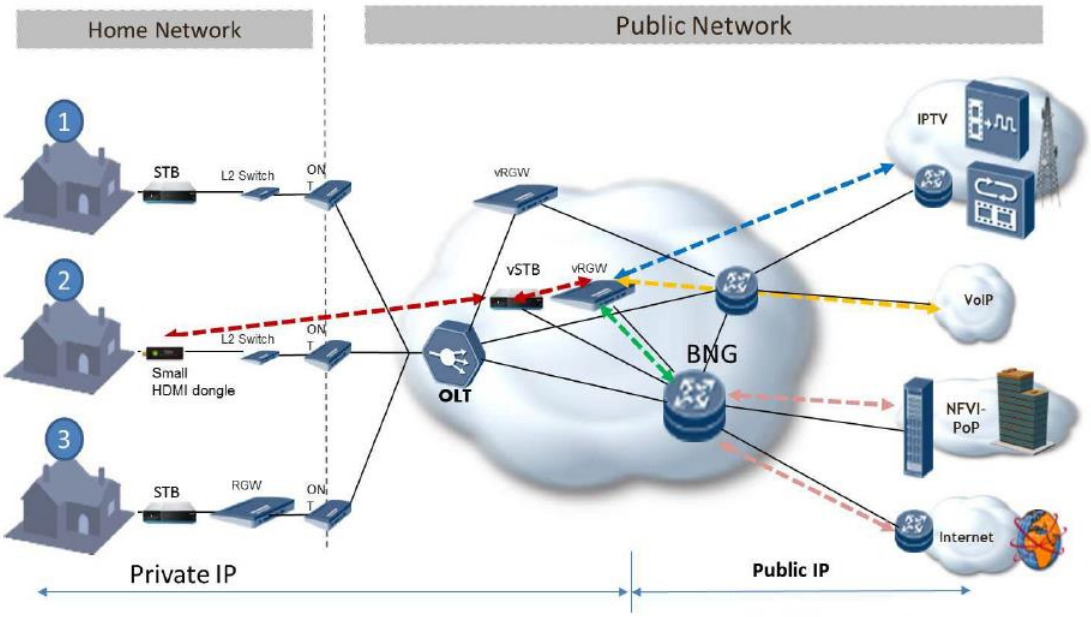

Figure 10. Both vRGW and vSTB in private address domain. [2]

Here in Figure 10 [2] one has virtualized STB and virtualized RGW functioning in private address space much like in home environment. This schema where both vRGW and vSTB are using private addresses could help save IPv4 addresses. However, if it is required the devices could be using public addresses. These requirements depend a lot on more detailed service and network architecture decisions.

3.2.2 vRGW Functions

As in the traditional solution the vRGW functions as local DHCP server for the home environment providing private addresses for home devices, providing NAT function to outbound traffic, Aplication specific routing and IPoE connectivity to BNG as before.

For security the same functions apply; firewall, parental control and port mapping. However, these can be made richer with the assumption that there is NFVI with more computing resources than an average CPE. Of course services should be implemented so that high demand for computing and other resources is only a momentarily and preferably interleaved for optimal resource use. As an example one could take the antivirus and a VPN services that could be too complicated to implement on consumer CPE HW. Here with consumer product in mind the VPN would be used to provide connectivity to user home network and content from remote location. End user could have web GUI to manage vRGW functions and statistics & diagnostics as today and operator management could be implemented for example according to TR-69 standard.

3.2.3 vSTB Functions

As said before the home HDMI dongle would have a web remote GUI and to pair the vSTB would have remote UI server. Network UI server would be responsible for scaling screen for optimal size for any home device working together with multiscreen function. The middleware client is required to handle the signaling with backend service.

For media streaming a DLNA media server could be added to the connected DLNA equipment at home to all media. This of course is impacted with regulation, laws and copyrights. But the technology is there for even a secure connection from server to client to protect all content. For TV the video is streamed as before and decoded at the end by the dongle. Encoding of video stream is a must for saving bandwidth and avoid of errors. But videos could be cached for some point depending of service to prevent jitter if end user and backend service is further from each other. The network location of STB could enable multiscreen service for more than one simultaneous connected devices for same or different content. Here on the vSTB most of it even basic functions have some aspect that is touched by local regulations, laws and copyrights. Therefore biggest challenges is on encryption and all traffic securing in respect to these.

3.2.4 Coexistance of Virtualized and Traditional Network Functions

For ISP it is necessity to be able to migrate step by step to virtualized functions and be able to run old and new virtualized services simultaneously. Virtualising STB or RGW

does not take effect on existing service model and it is even possible to virtualize just one device without the other without any particular order. This coexistence of traditional solution and new virtualized architecture is also illustrated in Figure 10.

Another important aspect is that this should not have an impact on legacy networking devices. This does not require any more resources or new features but could even simplify service from access device perspective if it would not be required to be IP aware at all and L2 capability would be enough.

3.2.5 Known Problems/Issues in Solution

In such a big change there is of course some known problems or issues. The ETSI working group already raised the following in the Use-Case document. [2]

When user devices with their functions are virtualized in ISP front cloud not all of them can be mapped 1:1 on own VM per server. Running several VMs on same pooled resources is the way but it will still require management of tens or even hundreds of thousands of VMs at same operational area. Some functions adapt to centralization better than others for example DHCP is reasonable to be centralized rather than run as instance per customer. Pooling resources and sharing network functions lead into another challenge of keeping the customer notion as service is scattered on across the system. The orchestration needs to be aware of customer service elements and functionalities need to be instantiated only on an on-demand basis.

The work group also rises the adequate bandwidth for future media stream demands as an issue but this is a general issue in networking for ISPs. The technology evolves faster than ISPs are capable of migrating legacy platforms with healthy return of investment while new more bandwidth requiring OTT services are adopted yearly that also cut ISP revenues simultaneously (e.g. NetFlix).

Then there is concern of adopting to service dynamics. Users and application usage are forever changing and NFVI will need to adopt to changes preferably automatically. Also operating several thousand of customer devices in the same domain presents new security threats. The virtualized customer devices and traffic must remain transparent to

each other and internal links need to be protected against new threads when physical differentiation does not exist no more.

4 Evaluating Feasibility

This chapter is addressed to evaluate the feasibility to virtualize RGW and STB elements in TeliaSonera's network in Finland following the principle of the ETSI use-case.

4.1 Cost Requirements

Internet service providers are profit driven companies and therefore the return of investment (ROI) is always one of the most important things when something new is planned to be implemented. This applies also to the virtualizing of home environment use-case.

When a model of a physical device is changed to another physical model the main issue is to compare the prices. This is not the case when a physical device is changed to a virtual appliance in a service provider cloud infrastructure. There are several things that have an effect on the final cost per device. The scope of this study was to evaluate the technical implementation from a service point. Therefore this study does not go into details on the cost structure of the NFVI. But the price is such a significant factor for the feasibility of this new potential solution and a high level evaluation is given in this chapter.

What TeliasSonera uses today is a customized Technicolor RGW and a STB from Arris. The average price for the RGW TG799vac is 71 USD and for the STB Arris VIP2853 with Mpeg license the price is 66 USD. This STB does not have a hard drive for a local videorecorder so it is comparable to vSTB. The virtualization of the RGW and the STB will have no physical changes to the access or aggregation networks nor on the BNG. The vRGW and vSTB prices are not simple to calculate. First of all, one should know more about how the NFVI would be implemented and calculate expenses for the estimated amount of resources consumed by one user device. This share of NFVI is the most difficult part to estimate because it has so many different functional parts as shown in Figure 5 earlier and possible actual outcomes of implementation according to service provider's wishes. Then one needs to add costs from SW appliance that probably will have a pricing model tied to volumes and implemented features.

But after the virtualization is done it is likely to have reduced OPEX that should compensate the investment costs. These expected savings from the OPEX are mostly from easier management and operation and troubleshooting. When for example the RGW is a SW appliance running on virtual machine inside the ISP network it can be investigated easier. If the service gets broken it can be instantly recreated as it is only a SW appliance instead of sending a new HW to a customer (meanwhile the service would be down). Of course the home environment is left with few simple devices that can get broken or misconnected and might require a new device to be sent or a technician to solve it. But with simple devices it should be easier to create a more robust setup for homes. The new virtual services are also expected to bring new revenue from new value added services (VAS). This amount of expected new revenue can tip the calculation either way. If not positive enough the virtualization looks to be too expensive to implement.

If dressed in a mathematical form this simplified cost comparison would look something like this:

$$\left(Existing\ device\ cost + \frac{OPEX}{device}\right) \geq \left(vDevice + \frac{NFVI\ resource\ cost}{virtual\ instance} + \frac{OPEX - new\ revenues}{vDevice}\right)$$

To justify the start of virtualizing the home environment as in this use-case the costs of virtualization should be less than the current ones or at least close to the same with strong belief that new revenues will add up at given time-frame.

The NFV also enables the use of shared resources for different functions. There might be a case when virtualizing the RGW and STB would not be alone cost efficient enough but together with other network functions it might be. Nevertheless, an efficient use of NFVI platform will be a key factor to cost efficient virtualized network functions.

4.2 Network Need to Adapt to the Virtualization

The virtualization of the RGW and the STB will make some changes to the network and the traffic flows. It will also highlight the role of datacenters in consumer services. The datacenters today are mostly hosting business services and the service provider's internal services. These are more demanding than consumer services by nature but with residential services the number of hosted virtual instances will grow remarkably. This needs to be taken into account in management and operations in DCs.

All Internet traffic in a traditional service is routed from RGW to the BNG and from there to the backbone of ISP. Now with a vRGW the internet traffic flow would go from home premises to DC where the vRGW is and from there to BNG. There are bypassing mechanisms for this to avoid overloading of virtual instances but at minimum all new sessions would need to go first to the vRGW and after that the traffic can be routed through the shortest path. Bypassing mechanisms will help with big data flows such as video streams from OTT services but there will be additional increase of bandwidth usage for DCs.

TeliaSonera uses multicast routing for broadcast IPTV. The multicast extends end to end from the super headend to the STB of a customer. This offloads access and aggregation networks when TV broadcast is sent only once regardless of number of customers watching TV. This has made it possible to use fairly small uplinks in the access network. Most common uplink capacity for a DSLAM or a switch is 1Gb. Another on-demand and personal content is unicast traffic. Now when a STB is virtualized and moved up into the network the multicast stops there. At best multicast could be used to optimize backbone traffic to DCs. From vSTB the TV stream would need to be unicast traffic to the home premises of the customer. This means that the same live TV stream should most likely be send individually to all the customers behind one DSLAM or a switch. This would create a significant traffic load to the access network and would likely require masses of link upgrades in the network.

Datacenters are big and demanding physical installations in a network. They require large amounts of redundant cooling and electricity that already sets a certain requirements for the location. The location must also be such that the network can provide sufficient connections for redundant connectivity and bandwidth. To justify these costly requirements the datacenter services are often centralized to optimize the usage. The centralization of services suits for most of the traditional DC services. Now when the RGW and the STB are virtualized in to a datacenter the distance between end user and a centralized DC might become a concern. Some delay in web services is within tolerance but if, for example, every TV remote interaction needs to travel to a distant DC and the returning response might exceed a customer patience. All delay in services is negative and centralizing the RGW and the STB functions will add some delay. One solution to this is to create a so called front cloud. Front cloud is a mini-datacenter with few racks of

server HW and other basic components for the services and possibly a remote operational and management connections to a bigger DC. The implementation can be decided by the service provider and the idea of the solution is just to bring cloud services closer to customers. Decentralization could mean less effective production but that is the cost for lower latency and better performance.

Changing the physical RGW and STB into a SW based instances could also have a possible impact on the IT side. With the RGW and the STB running as a SW it should be easier to create interfaces from a self-service portal and other systems directly to devices. This could enable a possibility for customers to make changes themselves to the services they use making them more personalized. This could apply to services such as parental control, content filtering, anti-virus or storage services. These can be called in general as Value Added Services (VAS). VAS is not a new thing but traditionally adding them has been restricted with physical restrictions or software versions of devices. Now with vRGW and vSTB physical HW restrictions don't exist. And SW versions can easily be updated. This could significantly shorten time to market when new services are introduced.

4.3 Assumptions Made for Evaluation

As concluded in Chapter 5.1 the price is an important criteria for the feasibility of virtualizing the RGW and the STB. However, at this point without having the exact figures for NFVI costs and with no exact knowledge of the virtualization solution the costs are impossible to determine. Due to this fact that the costs for the virtualization are not known at this point the costs are assumed to match the requirements and ignored in the further evaluation.

As already mentioned, the exact NFVI and the used vendor solution for virtualization are undecided and therefore another assumption was made for the study. It is assumed that a fully functioning virtualization solution is available and there is no functional restrictions to virtualize the RGW and the STB as proposed in the ETSI use-case.

These assumptions regarding price level and functionality enable to continue evaluating the technical feasibility of the virtualization.

4.4 SWOT Analysis

A traditional way of evaluating a solution is the SWOT analysis. The acronym SWOT stands for the words Strengths, Weaknesses, Opportunities, and Threats. This is a simple method where one writes down the internal strengths and weaknesses and external possibilities and threats into a four field chart. Then the content is analyzed further, e.g. how to use the strengths, can some of the weaknesses turned into strengths, how to exploit the future opportunities in a best way and how to avoid the threats.

Strengths	**Weaknesses**
• Efficient use of resources • Dynamic and Elastic • Decoupling HW and SW • Functional block structure & APIs • Reusability of functions	• Complexity of NFVI • Costs for first implementations • Unknown operational environment • Lack of internal coding capabilities
Opportunities	**Threats**
• Agile development • Fast Time to Market • Easy implementation of new vendors • VAS	• Security • Latency • Effect on the network • ISP Employees • Regulations and content rights

Figure 11. The SWOT chart for Virtualising the Home Environment use-case.

The key findings of the SWOT analysis of this virtualization use-case are displayed in Figure 11 in a form of a chart. The SWOT analysis was based on the company's internal work related to NFV, conversations and interviews of colleagues and the author's observations. Each topic is analyzed further in following chapters.

4.4.1 Strengths

The Efficient use of resources is one of the main features NFV promises. Using the same physical HW makes an installation of new capacity easier without a specialized HW for

a specific service and no possibility to mix them. High volumes of the same HW also decreases costs. When all services on the same domain of NFVI use shared resources it easier to reallocate resources for other services. The resources can be planned well before if the same resources are needed repeatedly and regularly. For example, if one business service requires more resources during day and less or none during evenings these resources could be freed and reallocated to TV services that have a peak time in late evenings. Or during a night time some of the NFVI servers could be put down to sleep to save electricity and cooling and awaken on morning when NFs need more resources again. This makes the NFV dynamic and elastic.

This dynamic and elastic nature of NFV extends from the resource use to the services. As said the services are scalable up or down by reallocating resources. VMs can also be copied and moved without using the state information. This could be used to react on geographical changes in the network. For example if one major incident makes the traffic to travel to the other site the services could follow the new optimized routes. NFV is based on a SW executing network functions on VMs. These functions are managed and operated by an orchestrator software. When everything is SW based and the orchestrator is aware of NF states it is possible to program traps that trigger an automated changes to the network. One could be a capacity issue of a service. If a service is exceeding 90% of allocated resources more resources could be given automatically without human interaction. Or when a failure or an error occurs it could trigger an automated fix to solve it.

Decoupling the hardware and the software enables different lifecycles for HW and SW. The VNF features are described in its SW and not restricted by the hardware support. Today a new network device with new features may require latest microchips that have the support for the new SW instruction set making the new feature possible. Also new HW has required latest SW nevertheless if only the HW capabilities are needed. For example ISP wants to upgrade 10GB interface card of a router to 100GB. The new HW can require the latest OS software to work properly. Therefore ISP needs to update router SW to have access to higher capacity interfaces. Now with NFV one can change or mix HW and it has no impact on SW. Only the amount of resources change from the service point of view. SW can be written to a specific OS or a hardware platform but when it is operated in a virtual environment the required platform is chosen and VM emulates this regardless of what hardware it is running on.

The Functional block structure with standardized APIs brings significant benefits. Different functional parts of NFV environment such as the management & operations, the infrastructure or a VNF SW can be seen as building blocks of the environment. The architectural framework defines roles for all functional parts and defines APIs for interactions between them. The functional block structure gives operator freedom to pick building blocks from different vendors and to compile an environment that suits best for them. Interoperability is granted if definitions of APIs are respected. This is highly desirable for the lifecycle management, the development and the financial point of view. Legacy ISP IT systems today are a sum of smaller systems and decades of development and they have complicated internal dependencies. One small change for HW support can trigger a whole system wide series of changes leading to long development cycles. NFV offers now a shortcut to this by restricting changes to one functional area at the time. Open ecosystem with defined APIs and roles for different parts enables new innovation from the IT industry. Also small companies and academies can create new network functions or extend existing ones when it is decoupled from a dedicated HW.

Reusability of functions. Services are often a series of network functions in certain order. If network functions are virtualized in feasible size they can be reused when designing a new service. For example CPE routing capability is valid for business and consumer services and so is the firewall function. Just to name a few. Network functions are kept as a library from where it is easy to pick required functions for the service.

4.4.2 Weaknesses

Complexity of the NFVI. The NFVI is a rather complex platform with many components to manage. This cannot be denied. Some vendors offer a whole solution and some only components for it. More complete solutions often have dependencies to certain other solutions of the vendor but in return might offer special features and help the operational work. This is a trade that all ISPs have to think when building own infrastructure for NFV. Regardless of the complexity of the choices in establishing NFVI it should have standard APIs to other systems if the architectural framework is respected. These APIs should guarantee the interoperability with the other functional blocks built on top of it. And once all details have been solved and the system is running the complexity should not be visible to outside systems.

The costs for the first implementations. Without a doubt the costs for the first implementations will be very high. But so is any other network and a new IT system if it is built only for one purpose. The more NFs are virtualized the more cost efficient it will become. Also the DC efficiency can be increased with high volumes.

Unknown operational environment. The NFV is often seen as an unknown operational environment. This is true for many ISPs. But few big operators e.g. Deutche Telecom, British Telecom, and Telefonica haw openly claimed to be virtualized some of their NFs. This serves as an example but all operators have different network environments that make all implementations slightly different. Also customers and pricing makes a difference if a service will be a success. The NFV differs from traditional networking. This will probably lead ISPs to problems that have not existed before. But this is known to happen with all new technologies and does not mean a failure.

Lack of internal coding capabilities. Many ISPs have outsourced many parts of operations during the past years of economic depression. If an ISP has outsourced internal coding capabilities to SW companies this may be seen here as a problem or even an obstacle. This does not mean that it always is. If cooperation with partner companies works well this is not an issue. With the virtualization networking is shifting towards SW implementations and IT systems with automation having a greater role in all of it. In most cases with the virtualization it is enough to understand the basics of Python and Pearl coding languages and Yang modeling language. These are just the few most popular coding languages the industry has chosen to use with the virtual appliances. It could be any other language also. For some of the networking personnel of an ISP this might not be that great change since these languages are often used with a scripting configuration for devices and on interfaces to management systems. But this knowhow should be secured or an ISP should prepare to train its personnel. Also securing networking skills at the same time is crucial. Just mastering coding skills for writing an application is not enough for understanding how the VNF should work. Nevertheless the trend is that SW coding is becoming more valuable to the telco business in future years.

4.4.3 Opportunities

Agile development. The dynamic and elastic nature on the NFV together with decoupling of HW from has SW enabled opportunity for more agile development of services and features. Some ISPs have burden of legacy networks and IT systems. This has led the development of services into long self-iterating cycles where one small change to IT or HW triggers a broad impact to all neighboring systems. With virtualization these dependencies between HW and SW are gone and one can be developed without changes for the other if interfaces between them remain the same.

Fast time to market. as the above mentioned development of new services and products has not been easy due to legacy networks and systems. Sometimes HW restrictions force an ISP to drop a new idea just because migration of restrictive old platform is just too expensive. NFV together with the IT transformation could bring an ISP closer to OTT service providers when measuring time to market numbers. Now there is a huge gap between and ISPs with their networks are far beyond OTT services in developing and launching something new for customers.

Easy implementation of new vendors. Continuing the finding of opportunities in HW & SW decoupling. Due to the dependencies between HW and IT systems it has always been cheaper to keep the same vendors for HW platforms to minimize the impact of changes to IT systems. Sometimes it would be technically better to change vendor or there could be just investment savings to buy HW from another vendor, however, the cost of developing IT support might favor keeping the old vendor. Now with the SW decoupled HW platform development and investments can be based more direct to its performance, features and cost. The same of course apply to SW as they have their own lifecycles.

Value added services (VAS). This brings us to the VAS. Now that services are created by compiling VNFs together it is easy to add more features to create premium value services for the demanding customers. Today the physical RGW is the same for all customers nevertheless of services they have need for. This forces an ISP in to a compromise to offer only the most required services to keep the RGW cost feasible. vRGW doesn't have these physical restrictions. The only restrictions are related to the available resources of virtualization platform and software. If it is required practically any feature

can be allowed in software for a customer and these can be cashed as VAS. Here in context of vRGW and vSTB this could be for an example a remote access to NPVR recordings and to the home network or enhanced security services to protect the home network.

4.4.4 Threats

Threats. In telecommunication and IT in general there have always been security threats. When a new device or SW is released to the markets it doesn't take too long before some level of backdoor or a bug is found that compromises the security of the system. The vendors release updates and batches to block these threats. The industry is starting to understand the flaws and weak points in a network and know to anticipate attacks to them. Also security countermeasures have been developed to minimize or block security threats when occurred. However the NFV is representing a new combination between IT and networks where functions of networks are taking place in a virtual shared domain. This will create a great number of new security threats. Some help for fighting against these security issues can be got from existing experience from DC virtualization. Virtualisation has been done in DCs for a decade and most of the HW and virtualization level security issues have already been solved.

Latency. Longer latency is an outcome from centralizing services. For consumer customers this has never been as high criteria that it has been for business customers. But it will have an effect to consumers also. Online gaming is one rising trend and a form of a service that is highly sensitive for latency. A 10ms latency can be unacceptable for demanding gamers and a long latency may push them to choose another service provider. For TV services latency is not that critical if it remains static and doesn't create jitter. Latency would affect the user experience with vSTB when only a dongle would be within home premises and all content including EPG and menus would be streamed from the network. Long latency could delay response from the system to menu selections and channel changes leading to series of button presses causing unwanted results.

Effect on the network. Latency and capacity are just a few aspects that should be taken into account and optimized when centralizing and virtualizing network functions. The ISPs must iterate and match their network architecture to respond to the new traffic patterns and volumes.

Conservative employees. Any new venture can fail if employees implementing it are not fully committed to it. During last few years the writer of this thesis has observed that many working with networks tend to have negative attitude to virtualization and they don't want to even evaluate the potential. This conservative attitude might be just a lack of information or some might need just more proofs of the concept. These attitudes are an obstacle for an open evaluation of the technology, virtualized or not. These negative anticipations should be handled with sufficient trainings and communication to ensure that the key personnel making decisions and creating the first implementations have a complete view of NFV.

Regulations and content rights. Within TV-services regulations and content rights of material can make a great impact on service. A national regulations can include certain must-carry channels that are always needed to be available for the customer. Regulations also state the minimum quality for services and possibly force injection of geographically local content such as local news or advertisements. Also the law may dictate that emergency information must be broadcasted on all channels in some circumstances. Big cities have a great number of customers and therefore services are centralized to these locations. When moving the IPTV service to use a vSTB could increase a level of centralization. For more rural areas of habitation this could mean even longer distances. The ISP must have these regulatory obligations in mind when centralizing services to DCs. There might be cases where the regulation will force to use smaller remote sites to produce these services. The content rights protect the content from illegal changes and rights of its owner to it. For IPTV service the content rights need to be negotiated always before recoding the transport stream. Therefor if a channel content is given to an ISP as a stream from a source the transport stream can't be re-encoded e.g. for more efficient bandwidth saving or for higher quality. Also transporting an IPTV stream to another platform such as a mobile device is seen as an own service that requires renegotiation. Therefore one can expect to have problems to create a new multiscreen or a remote access content for customers and keeping the service as a whole and intact experience. Another aspect is when the content is streamed to a customer. The primary IPTV stream is to the dongle that handles the decoding. But how are the streams secured all the way to secondary screens and mobile devices so that it is impossible to copy un-encoded streams? There are solutions to this, for example DLNA standard, but it requires careful

planning to get wide enough end user equipment support. When relied on general technology standards that are expected to exist in consumer devices has often lead into increasing unwanted calls to a customer service. It is irrelevant if it is a technical problem with SW version mismatch or a user fault. The customer is still unhappy.

4.5 Specialist Opinions from TeliaSonera

For this study a group of senior technical specialists from TeliaSonera were asked for opinions and views for the NFV and virtualizing the RGW and STB. Based on the answers one can summarize the following.

Everyone interviewed were familiar with the concept of the NFV. There was strong consensus that vRGW and vSTB would have lower acquisition costs but with customer migration to a new service they were doubtful if it would bring savings from CAPEX. If the lifecycle for virtual devices is longer than with physical devices then CAPEX saving are likely to realize.

Saving from OPEX were taken granted with virtual instances. Simplified installations and upgrades together with a minimized troubleshooting were expected and this would also improve the customer experience.

Whether a new service development would be faster and introduction smoother there were more conservative thoughts. But if it would be possible to launch a new service without reconfiguring an on-premises equipment it might be true. The doubt here was that can one really have that simple customer devices that this would be possible.

More uncertainty was present when asked if QoE could be improved with a new VAS like multiscreen and a remote access service. But here it was seen as a positive thing that these would be provided as a managed service for a broader customer base. Today these type of features are customer dependent 3rd party device based technical solutions. Nevertheless, if QoE was not increased the development of a VAS would be faster and more flexible. The VAS were seen as an enabler for new revenues that is the key target of the business development.

For the big question whether the use-case of virtualizing the home environment would be feasible in Finland there were no direct answers. This was seen more as a network strategic question that should cover more than just consumer targeted services. It was agreed though that one could have PoC environment already this year if wanted and candidate SW implementations have already been found.

Some concerns were also highlighted during the interviews. The virtualisation would have an impact on the network and would cause some new problems. One of the few one knows to expect is the losing of some of the multicast benefits in routing IPTV and having more unicast type of traffic. The capability to manage home WiFi connectivity was also raised. A managed WiFi can be used today for enhanced voice services and off-loading mobile networks. If one virtualizes managed devices and have only simplified L2 switch for providing home connectivity the exploiting WiFi possibilities will be difficult. For the IT development virtualization was seen to solve some of current difficulties but was expected to equally rise new ones. And for last but not least all interviewed were worried about new kind of security threats and doubting if all are known to be fought against.

4.6 Enhancing NFV with SDN

The NFV would consolidate many networking devices into virtual appliances. But all devices cannot be virtualized at least not fully. One needs to have a transport network to deliver services to the customer premises. If today's functionality of CPE devices are virtualized in to the network at least some customer awareness is required from the first ISP access network device to be able to identify the customer. This means that some configuration is required to be done when provisioning customer's connection to the network. This is usually done by OSS system or manually. The SDN could improve a system to a system interaction by providing a centralized network controller that VIM could talk to directly. The process would be automated from an order to a business system from where it would travel to a VIM and a SDN controller and network could provision the connection and services automatically in most optimal way. This does not differ from today's OSS system that much but one could create more intellectual automation process when the SDN controller is aware of the network state all the time. Today's OSS systems also need programmed instructions what to do per device type and per product type. Manual work is always more human resources consuming, slow and vulnerable for

human errors. With the SDN having a network state information and VNFs being portable, scalable and dynamic the end-to-end service could be made reactive to network changes. For example the service could in case of congestion recalculate an optimal path to match a set of SLA demands or just to dissolve the congestion. The SDN also uses a standard communication language (e.g. Openflow) in interaction with devices and a standard API in northbound interface towards other systems. This should enable a more agile and simple service development than with traditional OSS systems with case sensitive development needs.

5 Results and Conclusions

The NFV is coming fast. There are no standards developed yet but one can constantly see new announcements in the industry of ongoing PoCs or applications or even some production implementations. There does not seem to be doubt if NFV is going to be the new direction, it is more what is the best approach and scale of implementation for each operator. The ETSI NFV industry standardization group has done a lot of work since 2012 bringing vendors and service providers together to harmonize the development and paving the common road towards standardization. Now ETSI has released a great number of documents describing in detail the architectural framework and its components. Within a few years the industry should have come to an agreement to set the standards for this novel technology.

The main principle of the NFV is to have software based network functions running as virtual instances instead of having numerous hardware based specific network elements doing the task. By doing this one should get savings from cooling, power and space. Also operational savings can be achieved with a more dynamic and scalable environment.

Amongst ETSI publications there is a document describing numerous use-cases for NFV. One of them is “Virtualising the home environment”. This use case introduces the idea of virtualizing the RGW and the STB. This thesis focused on studying the feasibility of implementing this use-case in TeliaSonera’s network in Finland and providing a set of recommendations for future work. This study was made as a paper study and the evaluation was based on the background information, the SWOT analysis and specialist opinions.

Since there was no actual implementation that could have been evaluated the costs were not available for comparison and this matter was mostly left out from the study. However, it is clear that costs for virtualization should not be much higher than the existing implementation with the physical devices. And it can be considered as a fact that the first implementations of NFV are going to be costly due to all the IT systems and other possible changes required to the network to establish the NFVI and management and operations for it. Therefore it is clear that NFV becomes more feasible when more functions

are virtualized. Running multiple VF simultaneously makes also the use of the DC resources more efficient.

When functions are run on virtual SW based appliances instead of physical devices it decouples SW and HW lifecycles. This decoupling enables a faster and a more agile development of new features and services. New VAS are also easy to develop since the physical CPE device is not a restriction anymore. The available resources are limited only to the NFVI resources allocated to the service or the function. The NFV architectural framework defines the environmental requirements and features. This architectural framework is designed so that there are standard APIs between internal parts and towards BSS and OSS systems. This makes it possible to select parts for the system from different vendors and to create highly automated processes to provision or change services.

There are also threats and risks related to the NFV. This is a new technology and it differs from the existing networking in many ways. It will change the architecture a bit and definitely the traffic patterns in networks. This will likely lead into new problems in networks before it is understood better. The idea is combining DC, telco networks and IT technologies in a new way. It will take some time before all employees of an ISP working with NFV are trained to an adequate level to master this new technology. As for the security, the NFV exposes the network into new kinds of threats. New ways of attacks are expected and today's means can be applied against new elements. Another aspect of security is to design all simultaneous services and connections that are operated in the same virtual domain so that there is no possibility in any case for customers to get access to others' personal data.

TeliaSonera is looking into a telco cloud platform that can serve as the NFVI for VNFs. Also the strategy regarding actions related to NFV and SDN is being constructed. This work is required to be finalized before network functions can be virtualized. At the same time other work streams are being started to recognize the most potential virtualization use cases and to do the vendor selections related. This study supports these decisions to be taken. The decision for virtualizing the RGW and STB, however, is not that clear and no decisions have been taken at TeliaSonera today. According to this study and all benefits presented here it is strongly recommendable to take these into the roadmap but

not as the first implementations. The consumer business is based on high volumes and low revenues. It would not be wise to go forward in this before the costs are equal or less than today with a physical equipment. On the other side this should be further studied with actual tests of virtualized home environment and focusing on VAS and network traffic changes. It is clear and proven by the industry that RGW could be virtualized but creating a suitable offering of IPTV and other VAS on top of it is the key to new revenues in consumer markets.

TeliaSonera, like many other ISPs, have their share of legacy network and IT systems. With a great variety of device models and several IT systems interacting the development work has become rather slow and resource consuming. The NFV as well as SDN will bring eventually big value to this by solving many relations and accelerating the development work.

The List of References

.

Some internal company documents and information have been used to gain knowledge but are not available for public reference.

1 ETSI NFV ISG (2012) Network Functions Virtualisation – Introductory White Paper (October 22, 2012), https://portal.etsi.org/nfv/nfv_white_paper.pdf (Accessed May 17, 2016)

2 ETSI NFV ISG (2013) Use Cases, (October 2013), http://www.etsi.org/deliver/etsi_gs/nfv/001_099/001/01.01.01_60/gs_nfv001v010101p.pdf (Accessed May 17, 2016)

3 ETSI NFV ISG (2013) Architectural Framework, (Oct 2013), http://www.etsi.org/deliver/etsi_gs/nfv/001_099/002/01.01.01_60/gs_nfv002v010101p.pdf (Accessed May 17, 2016)

4 ETSI NFV ISG (2013) Network Functions Virtualisation – Update White Paper (October 15, 2013), https://portal.etsi.org/nfv/nfv_white_paper2.pdf (Accessed May 17, 2016)

5 Website: www.Netwokworld.com (2007) A generic picture describing router control&data planes, http://core0.staticworld.net/images/idge/imported/article/nww/2007/09/11fig01-100279788-orig.jpg (Accessed May 17, 2016)

6 ONF (2012) White Paper (April 13, 2012) https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf (Accessed May 17, 2016)