CHAPTER ONE
INTRODUCTION

1.1 Preface

IP networks are expected to experience significant data traffic growth in the near future. It is claimed that the current centralized network architecture will face excessive traffic transition through service provider's network elements which increases the possibility of un-optimized routing for users' traffic. The statistics presented in [1] showed that in 2016, global IP traffic will reach 1.1 Zettabyte per year which is equivalent to 64 times the volume of the entire global Internet in 2005. Moreover, author in [2] estimates that in 2018, the total amount of mobile traffic per month will be almost 15.9 Exabyte. The Cisco's [1] above mentioned forecast estimates that IP traffic will reach 400 terabits per second (Tbps) in 2018, the equivalent of 148 million people streaming Internet HD video simultaneously, all day, every day. The number of devices connected to IP networks will be nearly twice as high as the global population in 2018. There will be nearly three networked devices per capita by 2018, up from nearly two networked devices per capita in 2013. Accelerated in part by the increase in devices and the capabilities of those devices, IP traffic per capita will reach 17 GB per capita by 2018, up from 7 GB per capita in 2013 [1].

Triple play service – the delivery of combined IP video, voice and data over a single network – promises to present extraordinary opportunity, as well as heated competition for subscribers. Networks will soon be taxed with geometric increases in traffic, and maintaining service levels will be a top requirement for ensuring customer satisfaction and retention.

The exponential data growth and its unpredictability triggered operator's interest to look for short term optimization solutions to meet the growing demand for services. The ETSI committee gathered operators and vendors to test a series of Proof of Concept (PoC)s [3] with the aim to embrace Network Function Virtualization (NFV) in their live networks. Although it is a very recent technology, NFV rapidly gained operators' trust and has already become a fact in many vendors' solutions.

The NFV technology allows operators to cope with the increasing traffic demands by employing a more flexible network management (easily adapt to software upgrades) and better resource utilization (lowering both Capital Expenditure (CAPEX) and Operating Expenditure (OPEX)). Another benefit of NFV is the usage of less hardware with the elasticity of configuring new services, running tests and production on the same infrastructure.

Network functions Virtualization (NFV) offers a new way to design, deploy and manage networking services. Network Functions Virtualization or NFV decouples the network functions, such as network address translation (NAT), firewalling, intrusion detection, domain name service (DNS), caching, etc., from proprietary hardware appliances, so they can run in a form of a software. It's designed to consolidate and deliver the networking components needed to support a fully virtualized infrastructure – including virtual servers, storage and even other networks. It utilizes standard IT virtualization technologies that run on high-volume service, switch and storage hardware to virtualize network functions. It is applicable to any data plane processing or control plane function in both wired and wireless network infrastructures.

The SDN is referred as a complementary technology to NFV [4], because it can provide the infrastructure which upon VNF software can run. SDN mainly take advantage of decoupling control and data plane of the network.

Software Defined Networking (SDN) is an emerging network architecture where network control is decoupled from forwarding and is directly programmable. This migration of control, formerly tightly bound in individual network devices, into accessible computing devices enables the underlying infrastructure to be abstracted for applications and network services, which can treat the network as a logical or virtual entity.

In the near Future, operators should adopt more flexible cost effective technologies in evolution process of their core network to able to deliver more services customers by increasing the capacity of their networks.

Some traditional operators with legacy infrastructure, NFV and SDN based solution require removing some of legacy hardware so the implementation should go through phases until the full integration achieved. On the other hand, for new emerging market operators, SDN and NFV are considered suitable candidates in terms of cost and easier geographical extension, as well as on-demand capacity fulfillment.

1.2 Problem Statement

Nowadays, triple play services delivery architecture experiences a period of rapid and massive changes. Since NGN Networks are typically designed based on the load foreseen in the peak period, it will undergo extensive scale of usage as more devices connect, more services delivered and allowing more network traffic to transit through. Consequently, current network architecture does not provide any elasticity and on-demand capacity Expansion.

The NGN network entities in triple play network (i.e. Carrier Routing System (CSR), Network Load Balancers (NLBs), session border controller (SBC) and Broadband remote access server (B-RAS)) are based on custom hardware and need to be provisioned and configured on site. Therefore, to increase the network capacity, the deployment of new elements in network sites will be a must. Hereby, the operation of such static networks is heavily not cost-effective, cumbersome and time-consuming process

1.3 Proposed Solution

The NFV and SDN technologies aim to solve these issues, thus a proper integration of these technologies in the existing NGN should be carefully analyzed.

NFV allows the network functions to be deployed on regular x86 servers instead of dedicated hardware which led to massive reduction in total cost of the infrastructure. Virtualized NGN components can be provisioned and can be scaled on-demand based on diverse and time-varying control and data plane requirements.

SDN is an emerging network architecture where network control is decoupled from forwarding plane and it is directly programmable. Open-flow provides the benefit of centralized control over the network by virtualizing the control plane of the network which then will interconnect with NFV system to provide full connectivity.

1.4 Aim and Objectives

The aim of the thesis is to validate the performance of triple play services over a Cloudified system which intended to add the value of below mentioned objectives to the existing triple play services delivery infrastructure.

1. Reduce total cost of ownership (TCO).

2. Improve network elements usage efficiency due to the flexibility of resources allocation.

3. Improve service availability and resiliency.

4. Improve elasticity of the network

5. Higher flexibility and scalability.

1.5 Methodology

The methodology followed by this research takes the advantage of changing the access layer of NGN infrastructure to more intelligent layer by using SDN based devices in order to move the intelligence of the network to the edges which reduces the amount unnecessary transit traffic that passes through the core and aggregation layer of the network.

The aggregation and core layer of the infrastructure were moved from being hardware appliance based to cloud services based. All network function were moved to servers instead of dedicated hardware devices. Each network element is represented by a virtual machine in order to deliver its function as same performance as hardware appliance.

The control functions of the infrastructure is directly connected to the SDN controllers which will reduce the intensity of roles played by the deeper layers (Aggregation and Core).

The new model has been simulated using variety of tools in order to evaluate the performance of triple play services over it.

The results of the performance are evaluated against the requirements of ITU-T in a separate chapter.

1.6 Thesis Outlines

This thesis approaches the aforementioned issues starting from a broader definition of technologies and introduction to the context, followed by a proposed system design, description of the implementation tools and measurements analysis. Hereby, the work has been structured in six main chapters as follows:

Chapter One: Introduction: This chapter outlines the motivation and scope of the work.

Chapter Two: Overview of the Next Generation Network (NGN) and Cloud Technologies Concepts: This chapter presents some basic background of NGN, Triple Play, NFV overview and SDN background and investigation on Virtualization, its benefits, and research challenges also technologies that helped in design process will be introduced. Literature review and related work will be declared in this chapter.

Chapter Three: The Cloudified Model: This chapter presents the proposed cloudified infrastructure. The analysis of proposed system will addressed in this chapter along with technologies used, challenges of the system and possible optimizations will also be presented.

Chapter Four: Simulation Environment, Tool and Technologies: Describes the tools and technologies used throughout the implementation phase of the proposed system. Both NFV and SDN tools were used as well as the configuration of the simulation testbed are included together with explanation of the related commands. The SDN controller architecture is presented along with the different extensions of this controller such as QoS modules.

Chapter Five: Results and discussion: Introduces the expectations regarding the NFV / SDN benefits to the applied use case. The three common services use cases are proposed and their performance is analyzed for different scenarios. This chapter consists of an evaluation of the obtained results and a comparison between the obtained results and the standard expectations of service delivery network.

Chapter 6: Conclusions and Recommendations: Aims to give the final remarks and conclusions of the presented work. Proposed optimizations and complementary future work are also presented.

CHAPTER TWO

OVERVIEW OF THE NGN AND CLOUD TECHNOLOGIES CONCEPTS

CHAPTER TWO

OVERVIEW OF THE NGN AND CLOUD TECHNOLOGIES CONCEPTS

The growing demand for services that rely on IP technology led the operators to search for solutions that will guarantee them a design of a network that provides support for the services on the long term as well as increase network capacity on demand. This chapter presents the triple play based on NGN architecture and the functionality of the main layers elements. Moreover, the possible drawbacks in current networks are identified along with the proposed solutions by researches that have been done related to this field. New technologies like Cloud Computing, NFV and SDN are foreseen to provide more reliable long-term solutions to these issues. Therefore, a study of the benefits of employing these technologies is presented, as well as the interdependencies between them, which might even enhance the advantages to the applied use cases.

2.1 Triple Play

Triple play is the marketing name of the unified telecommunication network which offers three services (Telephony, television and internet) over a single broadband link. Providing triple services over NGN network offers more flexibility in Quality of Service (QoS) policies deployment which led to better quality of experience for the customer. Enabling triple play services within the concept of Next Generation Networks (NGN) over fixed and mobile access networks brings many research issues. One of the most promising researches is related to building IP Multimedia subsystem which allows operators to offer triple play service with quality of service and mobility support. These services could be deployed over copper cable as well as fiber cable with technologies such Point-To-Point Protocol over Ethernet (PPPoE) or even through direct IP connectivity using new innovative technologies such EoMPLS. Offering a competitive triple play services may lead to different challenges at each phase of the network lifecycle. Each of these services has its own unique consideration for testing and maintenance. All the services will discussed separately in the next paragraphs.

2.1.1 Voice Service

Voice over IP (VOIP) is one of the most popular technologies been provided over wire links by the telecom providers or even through internet like Skype. The competition of delivering better user experience pushed the providers to migrate from traditional TDM-based switches to more cost-effective IP-based switches. VoIP comes with two flavors as follows:

DSLAM with POTS: One of the simpler approaches to delivering a VoIP service is to deploy it in stages. Voice services that coexist with DSL connections have used a frequency splitter at the customer premises to separate the lower-frequency voice band from the DSL signals. A VoIP architecture does not need to be IP end-to-end. Instead, a voice switch at the central office (CO) or exchange can provide the interworking between the POTS and IP voice signaling. This avoids the extra complexity of having to deploy SIP-capable CPE. Many DSLAM vendors are integrating voice switch capability into their products, which enables the local loop at the CO to be terminated on the DSLAM for both voice and data services.

This eliminates the need for external splitters and voice switch hardware if a single provider has exclusive use of the copper to the customer [5].

End-To-End VoIP: This kind of connection is used when both parties are VoIP customers where the connection is fully based on IP [6]. Related network components will discussed later in this chapter.

2.1.2 Video over IP

Video over IP is broad term for a group of video services delivered by IP based telecom service provider. This service can be delivered in two form either in Multicast like IPTV service or in unicast form like video on-demand.

2.1.2.1 Internet Protocol Television (IPTV)

IPTV services are generally characterized by efficient transport of television channels over a packet network using multicast. Multicast reduces utilization of network links between the video server and the customer by sending only a single copy of a media stream into the network. The network replicates the stream to individual subscribers closer to the edge, thus saving bandwidth in the core. The components involved before the core are the source video feed receiver and decoder, IP encoder, and encryption process. The media streams are then fed to the IP core. This process is described in the next section [6].

2.1.2.2Video On-Demand

VoD is one of the unicast based models drastically increases the requirements of network transmission, forwarding capacity, and server cluster performance. Each server needs to generate a unique stream for each client, and at 4Mbps for a Standard Definition TV (SD-TV) quality, the requirements quickly add up. Of course, this offers the highest flexibility for the service provider. A profile of each household’s viewing habits can be built and targeted advertising created during the commercial breaks. Also, there are no issues with channel zapping latency [7] due to I-frame interval and subsequent buffer fill. There are additional advantages for the service provider with a unicast stream. For instance, a service for rewinding, pausing, and fast-forwarding a program needs a unicast data stream. Multicast replication can be the standard delivery method until the user requests a pause, rewind, or fast-forward of the channel [6].

2.1.3 Data Services

Data services encompass all services other than voice or video. Triple play terminology gathered multi-play services in data service. Data services start with internet access service which is then extended include more value added services that is IP based and could be delivered by the provider such as premium gaming [8] and walled-garden services [10]. Most of data services revenue comes from two services:

Internet Access: This service connects individual terminals to internet and its services such as E-mail and World Wide Web. Providers deliver the internet over various access techniques with variety of speeds.

Business Connectivity: DSL lines are no longer just for residential access. Business customers are connecting to the Internet and their other offices using DSL access. Frame-Relay, ATM, and ISDN circuits cost a lot more to run than DSL-based ones, and DSL is proving to be a suitable alternative to these older modulations and encapsulations. Broadly speaking, three types of business services in the marketplace use DSL access: Layer 3 VPNs [11], Layer 2 VPNs [10], and enhanced Internet access [12].

2.2 NGN Architecture

Next Generation Network is changes done to providers' access and core architecture to build a unified network that is able to deliver all services by encapsulating all information and data into IP based packets. The conceptual model of NGN architecture contains four basic layer [figure 2-1] based on services delivered by the layer as follows:

2.2.1 Access layer

It is the lowest layer in the model. It supports infrastructure for access of end user devices, like wireless or standard telephones, mobile or desktop computer etc. to aggregation network and vice versa. Physical interconnection can be realized with different type of transport mediums from standard telephone loopback, fiber, xDSL technologies to Fixed Wireless Access (FWA) [86].

2.2.2 Aggregation Layer

Provide IP connectivity between network nodes using high speed links and high performance switches connected through MPLS [13] usually. It is possible to serve to a flows of different character with different requirements on quality of transfer (delay, data loss ...). On interface in direction to access networks and to networks of another operators are mediation gateways (MGW) situated, which are adapting and routing data flows between these networks and unified aggregation network.

2.2.3 Control Layer

Main task of management layer is to control other layers. It is liable for correct functioning of management of aggregation layer (MGW/SGW). It controls service calling (application layer) and also manages user profiles (access layer) [86].

2.2.4 Application Layer

It is also common to call it a service layer, Service layer provides basic blocks of services, from which operators can make their more complex and more usable service. This layer contains all servers that deliver multimedia services over IP packets [86].

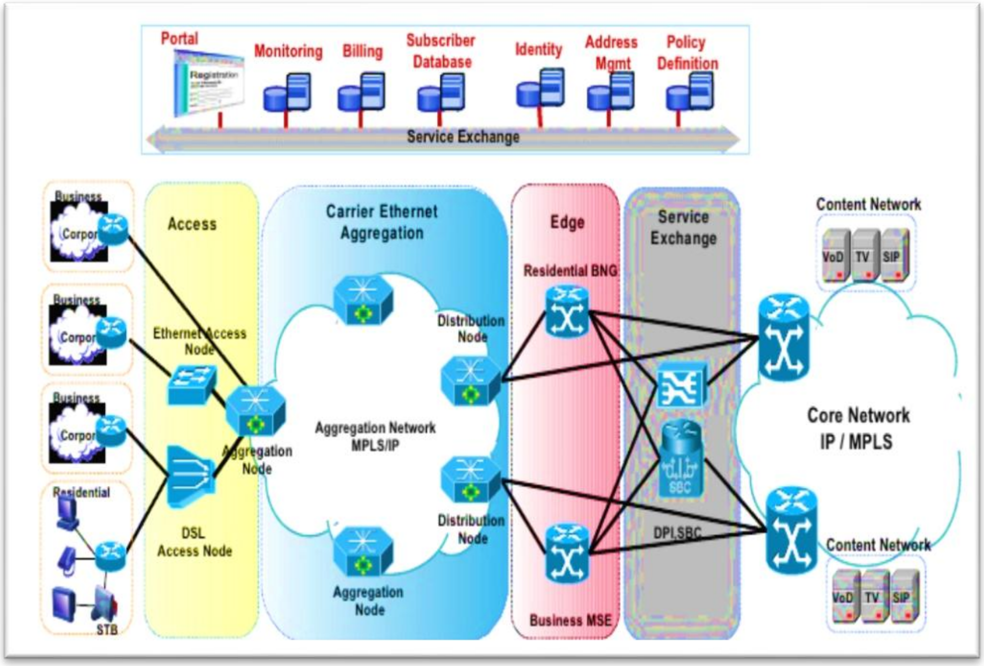


Figure 2-1: NGN architecture [85]

2.3 Architecture Basic Elements and Function

Many network devices work together to build the infrastructure needed to deliver services to end user. Each device has a role to play at each layer of all NGN layers as mentioned above. Here is the explanation of some of these devices:

2.3.1 Digital Subscriber Line Access Multiplexer (DSLAM)

The Digital Subscriber Line Access Multiplexer or DSLAM is the equipment that really allows the DSL to happen. The DSLAM handles the high-speed digital data streams coming from numerous subscribers' DSL modems and aggregates it onto a single high-capacity uplink to Service Provider's core. DSLAMs went through phases of development since ATM DSLAMs until IP-DSLAM and many Features added to the physical DSLAM to support functions such QoS [14].

2.3.2 Multi-Service Access Node (MSAN)

A multi-service access node (MSAN) connects customers’ lines to the network core to provide multiple services such as ISDN, telephony and broadband form single platform. Prior to the deployment of MSANs, providers used multiple DSLAMs to provide multiple services. MSAN offers a cost-effective way to deliver same services form single platform which is extendable to more services since MSAN supports IP and ATM streams of packets [15].

2.3.3 Broadband Remote Access Server (B-RAS)

A broadband remote access server (BRAS, B-RAS or BBRAS) routes traffic to and from broadband remote access devices such as digital subscriber line access multiplexers (DSLAM) on an Internet service provider's (ISP) network. The BRAS can perform several logical functions (e.g. LAC, IP router, or a MPLS PE router) as it aggregates user sessions from the access network. In addition to providing basic aggregation capabilities, the BRAS is also the injection point for providing policy management and IP QoS in the Regional and Access Networks. The BRAS is the last IP aware device between service providers (ASPs and NSPs) and the customer network, and as such is leveraged to manage the IP traffic through the layer 2 Access Network [16].

2.3.4 Softswitch

One of the main equipment that offers voice application in NGN network is Softswitch .The main role of Softswitch is to provide call control functions for VoIP calls. Softswitch enables integration of different protocols within NGN network. Call details for billing are generated in Softswitch also. Another important function is interface creation with existing telephony networks PSTN (Public Switched Telephone Network) through signaling gateway and Media gateway [17].

2.3.5 Media Gateway

It converts multimedia streams between different telecommunication networks such as PSTN, NGN or PBX [18]. It mainly changes transmission and coding technique to be suitable with the destination network. It also could be used within NGN networks to convert streams between NGN-IP based network and the one based on ATM. The media gateway is controlled by media gateway controller. The signaling conversion is done by signaling gateway [19].

2.3.6 Call Agent

The Call Agent takes care of functions such as billing, call routing, signaling, call services and the like, supplying the functional logic to accomplish these telephony meta-tasks. A call agent may control several different media gateways in geographically dispersed areas via a TCP/IP link. It is also used to control the functions of media gateway, in order to connect with media as well as other interfaces. This procedure is utilized to keep the interfaces clear as crystal for receiving calls from any phone lines [20].

2.4 Cloud Computing

Cloud computing is a promising field of research so that it could be the new IP-based business model that can deliver services through shared resources among several servers . One the major advantages is the location independence feature which delivers services to the customers with highest Quality of Experience possible. Delivering the concept of *on-demand self-service* is the ultimate goal of cloud computing through pooling of resources and keeping the human interaction through process flow as low as possible.

Rapid elasticity means that time and space are not constrains and the queries appear to be unlimited and purchased any time. The service can be measured and resources can be monitored, controlled, as well as reported in a complete transparency between the consumer and service [21]. Cloud services do not only refer to convenient storage, accessible by multiple devices, but also include important benefits such as more accessible communication and instant multi-point collaboration.

Cloud Computing Services are typically offered to customers in one of the three service models as defined by National Institute of Standards and Technology (NIST) 800-146 [22] as follows:

2.4.1 Infrastructure as a Service (IaaS)

It is provisioning model in which all equipment that support business operations such as storage, networking, hardware even servers are out-sourced by the organization. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis [23].

2.4.2 Platform as a Service (PaaS)

Provides additional layer for application development frameworks and function which could be integrated with the applications to deliver service for end users. Functions such as databases, messaging and queuing could be offered by the provider and allow the customer to manage his application with some restrictive access to related underlying cloud infrastructure: networks, servers, operating systems or storage as required [24].

2.4.1 Software as a Service (SaaS)

The SaaS is sometimes mentioned as ”on-demand software” in which the data and software resources are usually accessed by users through a web browser over the Internet. This includes the content, its presentation, the application and management capabilities integrated in a self-contained operating environment [25].

The success of cloud computing and SDN / Open Flow in data-centers is attributed to the simple all-IP core networks. In comparison to the multi-technology and complexities in Communications Service Providers (CSP)s' costly transport, the solutions provided by cloud computing are very flexible and demand proper adjustment to the CSP's needs.

The benefits of cloud computing (i.e. virtualization of standard IT computing and storage) are well understood, therefore it is implemented in data centers worldwide. Cloud computing is the virtualization of commodity IT hardware (namely x86 servers) and applications / software, which can run at least up to 99 % of the availability level [26].

On the other hand NFV is the virtualization of telecoms-specific network functions into applications that will run at least 99.999% availability on suitable carrier-grade hardware and software [27].

The PaaS and SaaS cloud computing service models provide software based capabilities that can run over the provided infrastructure (the same infrastructure that may be offering IaaS or Network as a Service (NaaS) service). Major CSPs are now convinced that NFV has matured sufficiently to virtualize the majority of network functions.

2.5 Network Function Virtualization (NFV)

Network Functions Virtualization aims to transform the way that network operators architect networks by evolving standard IT virtualization technology to consolidate many network equipment types onto industry standard high volume servers, switches and storage, which could be located in Datacenters, Network Nodes and in the end user premises, as illustrated in Figure (2-2). It involves the implementation of network functions in software that can run on a range of industry standard server hardware, and that can be moved to, or instantiated in, various locations in the network as required, without the need for installation of new equipment [28].

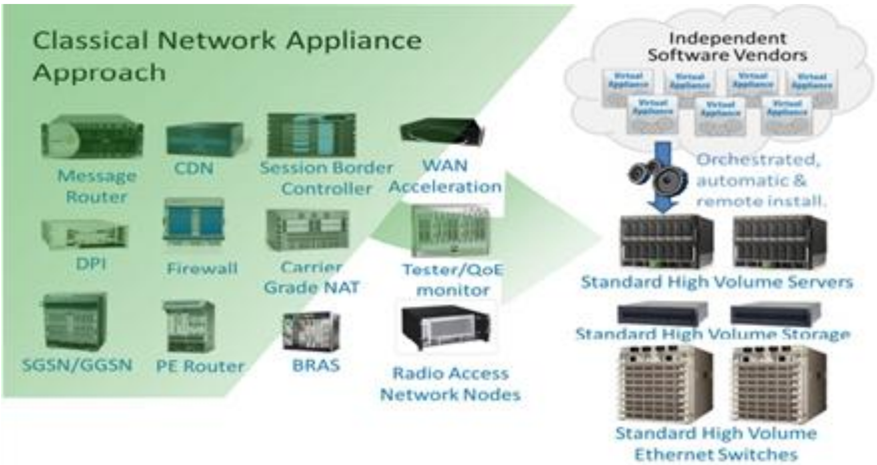

Classical Network Appliance Approach
Message Router
CDN
Session Border Controller
WAN Acceleration
DPI
Firewall
Carrier Grade NAT
Tester/QoE monitor
SGSN/GGSN
PE Router
BRAS
Radio Access Network Nodes
Independent Software Vendors
Orchestrated, automatic & remote install.
Standard High Volume Servers
Standard High Volume Storage
Standard High Volume Ethernet Switches

Figure 2-2: NFV Vision [87]

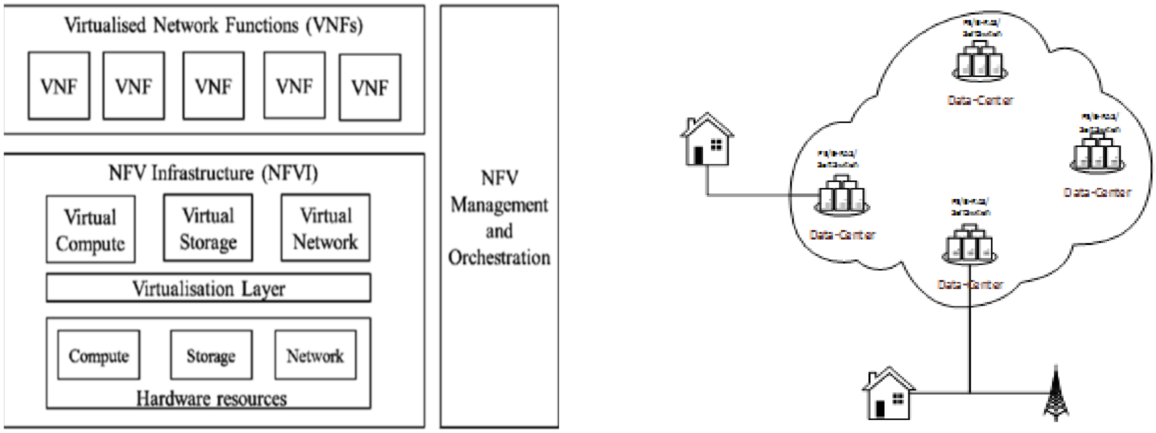
The NFV framework consist of three main components:

Virtualized Network Function (VNF): which represents the software implementation of network function that could deployed on NFVI (Figure 2-3-a).

NFV Infrastructure (NFVI): represents the software and hardware components which build up the platform that VNFs are deployed on.

NFV Management and Orchestration: controls the physical and software resources that support the NFVI and the lifecycle management of VNFs. It allows both horizontal and vertical scalability of the resources based on capacity needs.

The VNF which might fulfill the role of one of NGN functions, although it can scale up both horizontally and vertically according to their specific resource requirements (e.g. the user plane resources can be increased independently of the control plane and vice versa (Figure2-3-b)).



(a) NFV Framework [29]

(b) NFV in NGN

Figure 2-3: NFV architecture and deployment

2.5.1 Benefits of NFV

Part of the major benefits that NFV promises to bring are: lower equipment costs and reduced power consumption through consolidating the equipment and exploiting the scale economies of the IT industry.

NFV provides increased velocity of time-to-market and mitigates the typical network operator cycle of innovation. Economies of scale required to cover investments in hardware-based functionalities are no longer applicable for software-based development, making feasible other modes of feature evolution. The NFV should enable network operators to significantly reduce the maturation cycle.

Targeted service introduction based on geography or customer sets is possible. Services can be rapidly scaled up/down as required. In addition, service velocity is improved by provisioning remotely in software without any site visits required to install new hardware.

The virtualization of NGN core network is a great opportunity for cost efficient production environment. This will allow network operators to cope with the increasing traffic demand in NGN networks and acquire better resource utilization (including energy savings). Other advantages are: more flexible network management (no need to change hardware for upcoming upgrades), hardware consolidation, as well as easier multi-tenancy support and faster configuration of new services.

The NFV might help optimizing network configuration and topology in real time based on the actual traffic patterns and service demands. Another important capability is the possibility of running production, test and reference facilities on the same infrastructure [28].

2.5.2 Differences between SDN and NFV

The NFV's main goal is to reduce equipment cost and decrease time-to-market by providing scalability, elasticity and a strong ecosystem. The OpenFlow-enabled SDN proposed by the Open Networking Foundation (ONF) aims to achieve the same benefits. While NFV is intended to optimize the deployment of network functions (such as firewalls, DNS, load balancers, etc.), the OpenFlow-based SDN solution is more focused on routing and optimizing the underlying networks [30].

As shown in Figure 2-4, the NFV is highly complementary to SDN, but not dependent on it (or vice-versa). The NFV can be implemented without a SDN being required, although the two concepts and solutions can be combined and potentially greater value obtained.

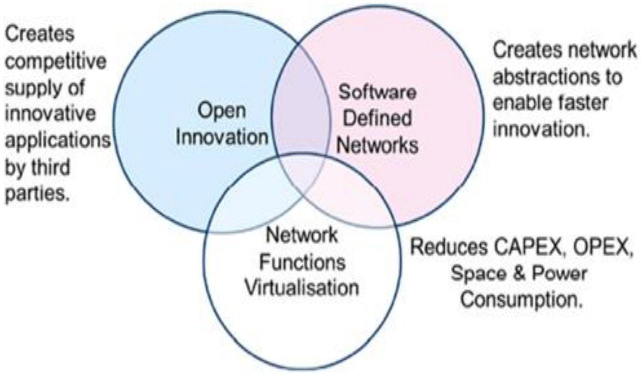

Creates competitive supply of innovative applications by third parties.
Open Innovation
Software Defined Networks
Creates network abstractions to enable faster innovation.
Network Functions Virtualisation
Reduces CAPEX, OPEX, Space & Power Consumption.

Figure 2-4: Network Functions Virtualization Relationship with SDN [29]

2.6 Software Defined Networking

SDN is an emerging network architecture where network control is decoupled from forwarding plane and it is directly programmable. This technology has been promoted by the ONF which is a nonprofit, mutually beneficial trade organization, founded by some of the largest IT companies in the world: Deutsche Telekom, Facebook, Google, Microsoft, Verizon, and Yahoo.

The ONF was organized for the purpose of standardizing a protocol between the controllers and the network elements. This protocol is called OpenFlow protocol and runs on the *Southbound* interface. With SDN, enterprises and carriers main benefit is to gain control over the entire network from a single entity, which reduces the network complexity and operation. The SDN also simplifies the network devices themselves; since they no longer need to understand and process thousands of protocols standards, but rather accept instructions from the SDN controller [31].

2.6.1 SDN Architecture

Figure (2-5) depicts a logical view of the SDN architecture which consists of three main layers: *infrastructure, control and application layer*. Network intelligence is (logically) centralized in software-based SDN controller, which maintains a global view of the network:

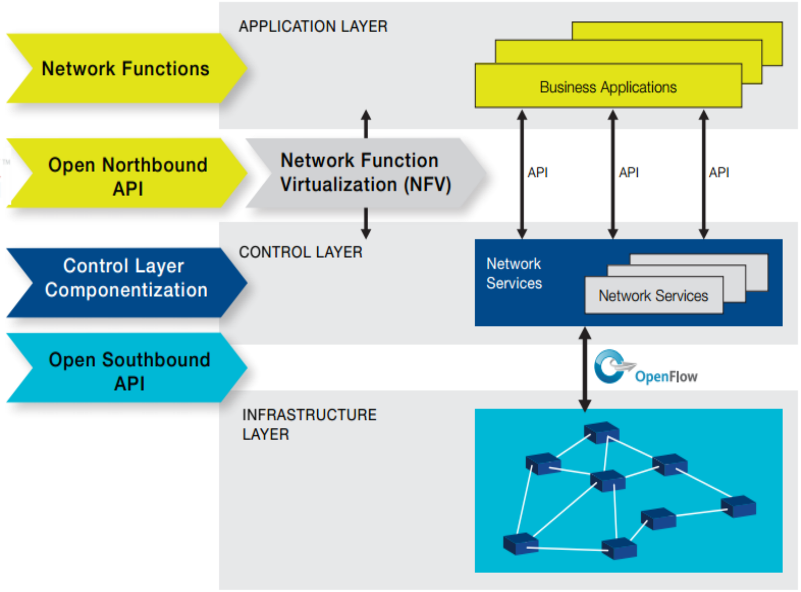


Figure 2-5: The Open SDN architecture [32]

Application layer and Northbound Application Programming Interface (API):

The *Northbound Open API* is defined as a software interface between the controller platform and the VNF applications running on the top. These interfaces are open to customers, partners, and the open source community for development. One of these open source providers is OpenStack, a development committee which aims to bring NFV API into the SDN picture.

Control layer:

Figure 2-5 shows an open controller (i.e. “OpenDaylight”) in the core of the Open SDN architecture, which will be further presented in the next chapter. Nevertheless, any of the existing controllers can be used as a controller platform. These controllers consists of programmable modularized structure.

Infrastructure layer:

The *Southbound Protocols* define the control communications between the controller platform and data plane devices, including physical and virtual switches. Support for a wide range of physical and virtual switches, ensure that customers have the maximum choices and flexibility in designing and deploying their software-defined network. One of the protocols defined for the *southbound interface* is OpenFlow, but the flexible Open SDN architecture also supports delivering configuration for other standardized protocols (e.g. Border Gateway Protocol (BGP), SNMP).

Figure 2-5 shows SDN and NFV as complementary technologies: OpenFlow-based SDN focuses to optimize the underlying infrastructure, whereas NFV concentrates on the deployment of network functions (e.g. firewalls, DNS, etc.) in the application layer [32].

2.6.2 OpenFlow Protocol

The OpenFlow protocol constitutes a mean for the SDN controller to add, update, and delete new entries in flow tables, both reactively (in response to packets) and proactively.

The ***Reactive flow instantiation*** happens when a new flow comes into the switch, the OpenFlow agent does a lookup in the flow tables and if no match for the flow is found, the switch creates an OpenFlow (OF) PACKET_IN message and forwards it to the controller for instructions. Reactive mode reacts to traffic, consults the OpenFlow controller and creates a rule in the flow table based on the instruction.

In contrast to that, ***proactive flow instantiation*** implies there is no lookup into the flow table and the flows are defined in advance, eliminating the latency introduced by interrogating the controller.

The ***hybrid flow instantiation*** is a combination of both reactive and proactive flow instantiation. Employing this flow instantiation mode will allow the flexibility of reactive mode for a granular traffic control, while preserving a low-latency forwarding for the rest of the traffic [33].

The most recent OpenFlow Switch version (1.4.0) has been defined by ONF in paper [34] and it is composed of three main modules (Figure 2-6):

1. *OpenFlow Channel* connects the switch to a controller and allows commands and packets to be sent between the controller and the switch. The controller manages the switch via the OpenFlow protocol running over Secure Sockets Layer (SSL). That is the reason why *OpenFlow Channel* is also referred as *Secure Channel*;
2. *A Flow Table* with an action associated to each flow entry which dictates the switch how to process the flow. Each flow table contains a set of flow entries (i.e. match fields, counters and a set of instructions);
3. *Group Table* contains group entries and each entry has a list of *actions buckets*. These actions are applied to packets which are sent to the group entries [34].

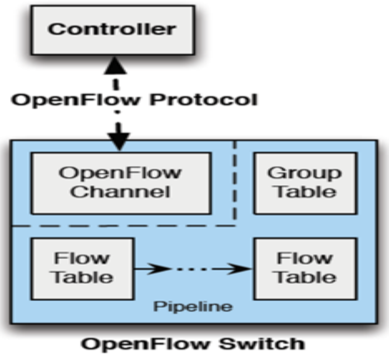


Figure 2-6: OpenFlow switch [34]

2.6.3 OpenFlow Switch

An OpenFlow switch is modeled as a group table and a collection of flow tables containing three columns: *rules, actions, and counters* (Figure 2-7). The *rules* column specifies the header fields that define the flow. Rules are matched against the headers of incoming packets.

If a *rule* matches, the actions from the *action* column are applied to the packet and the counters in the *counter* column are updated. If a packet matches multiple rules, the rule with the highest priority is applied.

Each rule specifies an exact match from header fields or a wild card i.e. *ANY*. The set of possible actions are: forward the packet to an output port, modify the packet in some fashion, or send the packet to the next table or to the group table. An OpenFlow switch supports three types of OpenFlow ports: *physical ports*, *logical ports* and *reserved ports* [34].

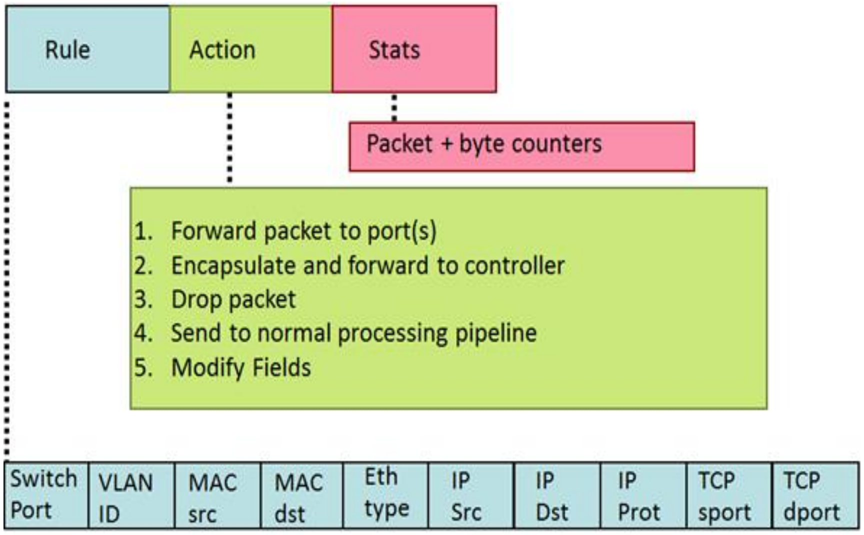


Figure 2-7: Flow Table [35]

The OpenFlow *physical* ports correspond to a hardware interface of the switch (i.e. on an Ethernet switch, physical ports map one-to-one to the Ethernet interfaces). The OpenFlow *logical* ports are switch defined ports that do not correspond directly to a hardware interface of the switch (i.e. packet encapsulation). The only difference between physical ports and logical ports is that a packet associated with a logical port may have an extra metadata field called *Tunnel-ID*. The *reserved* ports are defined in OpenFlow switch specification [34]. A switch is not required to support all reserved ports, just those marked as “required”.

2.6.4 SDN Benefits

The benefits that enterprises and carriers can achieve through an OpenFlow-based SDN architecture include:

Centralized control of multi-vendor environments: SDN control software can control any OpenFlow-enabled network device from any vendor, including switches, routers, and virtual switches. Rather than having to manage groups of devices from individual vendors, IT can use SDN-based orchestration and management tools to quickly deploy, configure, and update devices across the entire network.

Increased network reliability and security: SDN makes it possible for IT to define high-level configuration and policy statements, which are then translated down to the infrastructure via OpenFlow. An OpenFlow-based SDN architecture eliminates the need to individually configure network devices each time an end point, service, or application is added or moved, or a policy changes, which reduces the likelihood of network failures due to configuration or policy inconsistencies

More granular network control: Open Flow’s flow-based control model allows IT to apply policies at a very granular level, including the session, user, device, and application levels, in a highly abstracted, automated fashion. This control enables cloud operators to support multi-tenancy while maintaining traffic isolation, security, and elastic resource management when customers share the same infrastructure.

Better user experience: By centralizing network control and making state information available to higher-level applications, an SDN infrastructure can better adapt to dynamic user needs. For instance, a carrier could introduce a video service that offers premium subscribers the highest possible resolution in an automated and transparent manner. Today, users must explicitly select a resolution setting, which the network may or may not be able to support, resulting in delays and interruptions that degrade the user experience. With OpenFlow-based SDN, the video application would be able to detect the bandwidth available in the network in real time and automatically adjust the video resolution accordingly [31].

2.7 Ethernet over MPLS

Any Transport over MPLS (AToM) is a solution for transporting Layer 2 packets over an MPLS network, allowing service providers to use the MPLS network to provide connectivity between customer sites with existing Layer 2 networks. Instead of separate networks with network management environments, service providers can use the MPLS network to transport all types of traffic for different customers. The Each frame is transported as a single packet, and the PE routers connected to the backbone add and remove labels as appropriate for packet encapsulation:

- The ingress PE router receives an Ethernet frame and encapsulates the packet by removing the preamble, the start of frame delimiter (SFD), and the frame check sequence (FCS). The rest of the packet header is not changed.
- The ingress PE router adds a point-to-point virtual connection (VC) label and a label switched path (LSP) tunnel label for normal MPLS routing through the MPLS backbone.
- The network core routers use the LSP tunnel label to move the packet through the MPLS backbone and do not distinguish Ethernet traffic from any other types of packets in the MPLS backbone.

- At the other end of the MPLS backbone, the egress PE router receives the packet and de-encapsulates the packet by removing the LSP tunnel label if one is present. The PE router also removes the VC label from the packet.
- The PE router updates the header, if necessary, and sends the packet out the appropriate interface to the destination switch.
- The MPLS backbone uses the tunnel labels to transport the packet between the PE routers. The egress PE router uses the VC label to select the outgoing interface for the Ethernet packet. EoMPLS tunnels are unidirectional; for bidirectional EoMPLS, you need to configure one tunnel in each direction [56].

EoMPLS has two modes:

- VLAN mode—Transports Ethernet traffic from a source 802.1Q VLAN to a destination 802.1Q VLAN through a single VC over an MPLS network. VLAN mode uses VC type 5 as default (no dot1q tag) and VC type 4 (transport dot1 tag) if the remote PE does not support VC type 5 for subinterface (VLAN) based EoMPLS.
- Port mode—allows all traffic on a port to share a single VC across an MPLS network. Port mode uses VC type 5 [57].

2.7.1 Restrictions for EoMPLS

- Ensure that the maximum transmission unit (MTU) of all intermediate links between endpoints is sufficient to carry the largest Layer 2 packet received.
- EoMPLS supports VLAN packets that conform to the IEEE 802.1Q standard. The 802.1Q specification establishes a standard method for inserting VLAN membership information into Ethernet frames.

- Unique VLANs are required across interfaces. You cannot use the same VLAN ID on different interfaces.
- For a particular EoMPLS connection, both the ingress EoMPLS interface on the ingress PE and the egress EoMPLS interface on the egress PE have to be subinterfaces with dot1Q encapsulation or neither is a subinterface.
- 802.1Q in 802.1Q over EoMPLS is supported if the outgoing interface connecting to MPLS network is a port on a Layer 2 card.
- EoMPLS is not supported on Layer 3 VLAN interfaces [57].

2.7.2 QinQ for EoMPLS

The IEEE 802.1Q VLAN tag uses 12 bits for VLAN IDs, so a device supports a maximum of 4094 VLANs. This is far not enough for isolating users in actual networks, especially in metropolitan area networks (MANs). 802.1Q-in-802.1Q (QinQ) is a flexible, easy-to-implement Layer 2 VPN technology based on IEEE 802.1Q, and provides enough VLANs for isolating users in MANs. QinQ enables the edge device on a service provider network to insert a SVLAN tag into the Ethernet frames from customer networks, so that the Ethernet frames travel across the service provider network (public network) with double VLAN tags. QinQ enables a service provider to use a single SVLAN to serve customers who have multiple CVLANs.

QinQ delivers the following benefits:

- Releases the stress on the SVLAN resource.
- Enables customers to plan their CVLANs without conflicting with SVLANs.
- Provides an easy-to-implement Layer 2 VPN solution for users.

- Enables the customers to keep their VLAN assignment schemes unchanged when the service provider plans VLANs in the service provider network [58].

QinQ frame transmitted over the service provider network carries the following tags:

- CVLAN tag—The Customer VLAN Tag field. The CVLAN tag identifies the VLAN to which the QinQ frame belongs when it is transmitted in the customer network.
- SVLAN tag—The Service VLAN Tag field. The service provider has allocated this tag to the customer. The SVLAN tag identifies the VLAN to which the QinQ frame belongs when it is transmitted in the service provider network.

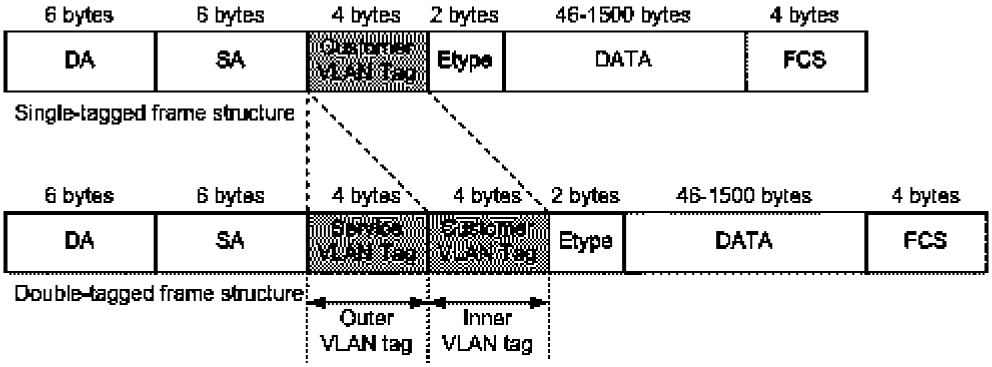


Figure 2-8: Single-tagged and double-tagged Ethernet frame header

2.7.3 Broadband Ethernet-based DSLAM

VLAN aggregation on a DSLAM will result in a lot of aggregate VLANs that at some point need to be terminated on the broadband remote access servers (BRAS). Although the model could connect the DSLAMs directly to the BRAS, a more common model uses the existing Ethernet-switched network where each DSLAM VLAN ID is tagged with a second tag (Q-in-Q) as it connects into the Ethernet-switched network.

The only model that is supported is PPPoE over Q-in-Q (PPPoEoQinQ). This can either be a PPP terminated session or as a L2TP LAC session. No IP over Q-in-Q is supported.

PPP over Q-in-Q encapsulation processing is an extension to 802.1q encapsulation processing. A Q-in-Q frame looks like a VLAN 802.1Q frame, only it has two 802.1Q tags instead of one [59].

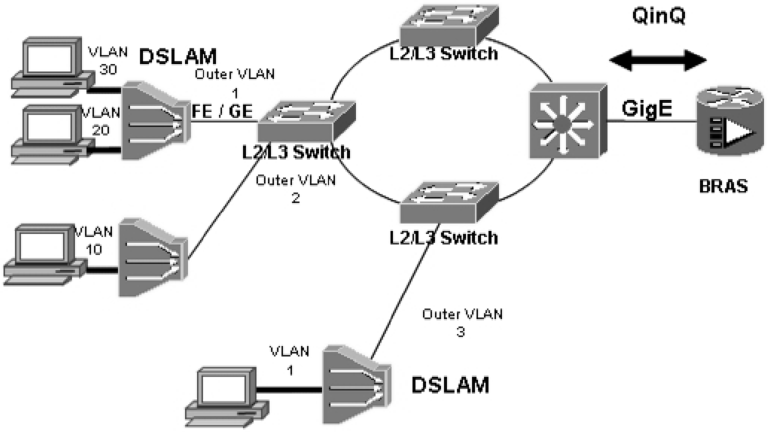


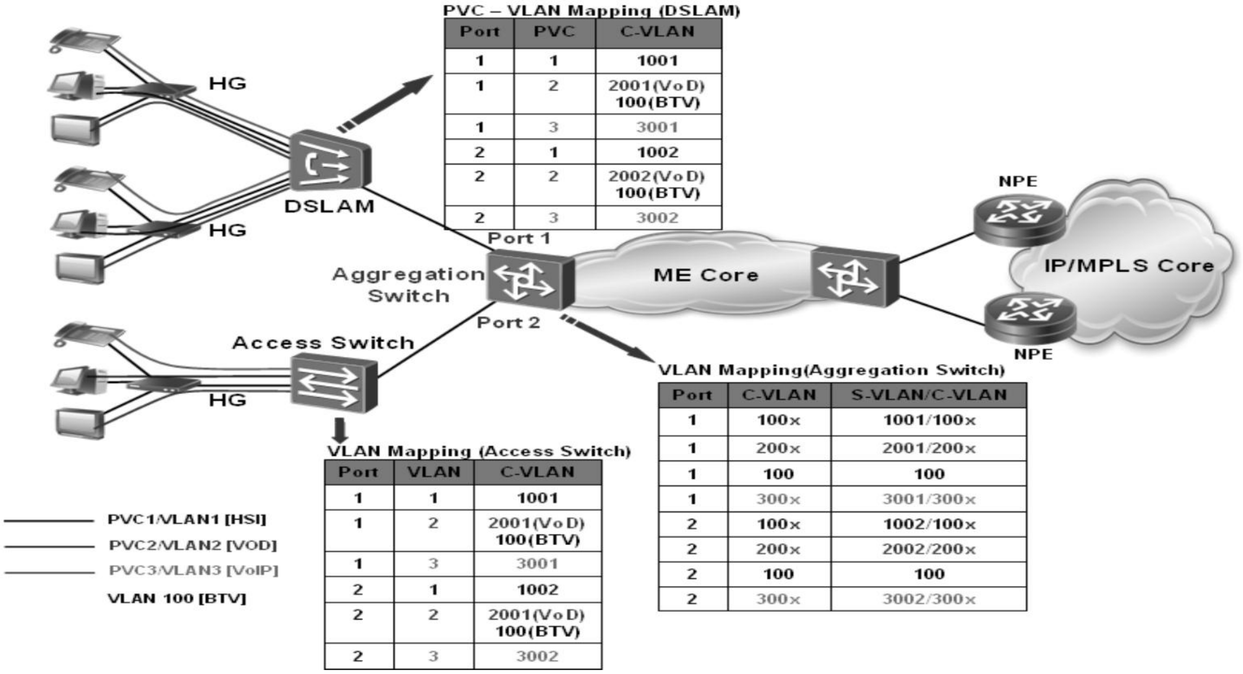
Figure 2-9: QinQ in NGN [59].

As shown in Figure (2-10), MANs use the QinQ technology. There are two access modes for broadband users: ADSL and LAN access. A user uses multiple services, such as HSI, VoIP, and IPTV.

In ADSL access, the digital subscriber line access multiplexer (DSLAM) supports multiple permanent virtual connections (PVCs) and uses different PVCs to carry different services. For example, PVC 1 is used to carry HSI service, PVC 2 carries IPTV service, and PVC 3 carries VoIP service. All home gateways (HGs) use the same configuration. The DSLAM maps the PVC to a VLAN according to the port number and PVC. Figure (2-10) shows the mapping relationship. For example, The VLAN IDs for Internet access of PCs range from 1001 to 2000. The VLAN IDs for the VoD service range from 2001 to 3000. The VLAN IDs of the VoIP service range from 3001 to 4000. For the BTV service, multicast VLAN 100 is used.

In LAN access, HGs use different VLANs for different services. For example, VLAN 1 carries the HSI service, VLAN 2 carries the IPTV service, and VLAN 3 carries the VoIP service. All HGs use the same configuration. The access switch maps VLANs as shown in Figure (2-10). Multicast VLAN 100 is also used for the BTV service.

The aggregation switch tags services with different outer VLAN tags based on VLAN IDs. For example, on port 1, the aggregation switch tags the Internet access service with the outer VLAN tag of VLAN 1001, the VoD service with the outer VLAN tag of VLAN 2001, and the VoIP service with the outer VLAN tag of VLAN 3001. The inner VLAN tags represent user information. The outer VLAN tags represent service information, and also location information of DSLAMs or access switches. Different DSLAMs or access switches are tagged with different outer VLAN tags. User data is forwarded to the NPE according to the outer VLAN tags and MAC addresses. The NPE performs QinQ termination and enters the IP forwarding procedure or relevant VPN [60].



PVC – VLAN Mapping (DSLAM)

Port	PVC	C-VLAN
1	1	1001

1	2	2001(VoD)
		100(BTV)

1	3	3001
2	1	1002

2	2	2002(VoD)
		100(BTV)

2	3	3002

VLAN Mapping(Aggregation Switch)

Port	C-VLAN	S-VLAN/C-VLAN
1	100x	1001/100x
1	200x	2001/200x
1	100	100
1	300x	3001/300x
2	100x	1002/100x
2	200x	2002/200x
2	100	100
2	300x	3002/300x

VLAN Mapping (Access Switch)

Port	VLAN	C-VLAN
1	1	1001

1	2	2001(VoD)
		100(BTV)

1	3	3001
2	1	1002

2	2	2001(VoD)
		100(BTV)

2	3	3002

Figure 2-10: VLAN Mapping and Selective QinQ in NGNs [60]

2.8 Related Work

A major concern for operators is how to integrate the SDN and NFV architecture into the legacy hardware. In the area of NFV, the recent ETSI NFV standardization body has defined several use cases for a virtualized CPE/PE in paper [36]. The proposals consist of both fully or partially edge devices deployments along with the coexistence of virtualized functions and the legacy elements. On the other hand, proposals to integrate the SDN architecture in the core have been carried under other sections. The load balancing and QoS routing mechanisms are carefully addressed by many researchers, starting from the data centers, where SDN is already a mature technology, to considerable solutions that might also be applied to IP/MPLS core. In [37] analyzes two issues: a) the impact of SDN on raw performance (in terms of throughput and latency) under various workloads, and b) whether there is an inherent performance penalty for a complex, more functional, SDN infrastructure.

Several recent attempts on both control and user plane have been done to optimize the existing NGN architecture for the upcoming threats in terms of huge data increase and signaling storms. One line of research focuses on the development of a new architecture and further goes into the implementation details. Authors in [38] proposed a third generation approach, multiple layers of tags to achieve isolation and designate routes through the data center network. The tagging protocol can be either carrier Ethernet or MPLS, both of which support multiple layers of tags. Another publication [39] proposes a new encapsulation / decapsulation on top of the IP Layer referred to as vertical forwarding implemented in the Forwarding Element (FE) s and managed by a central controller. The tunneling process is attributed to a line card incorporated in the FE.

Many papers address the implementation of triple play services over MPLS aggregation networks. For instance, [40] describes the different methods of delivering an aggregation solution for these access technologies. It describes routing-based aggregation solutions were first used by operators to deliver triple play services and explores their limitations and the migration of the networks to an MPLS-based aggregation solution, the problems it solves and the benefits it delivers. In [41], propose a tunnel splicing mechanism for heterogeneous network with MPLS and OpenFlow routers. Two key mechanisms were suggested: first, abstract the underlying network devices into uniformed nodes in order to shield the details of various equipment, second, strip the manipulation of flow table and label switch table from controller and fulfill it in an independent module. This article [42] considers SDN for network carriers, facing operation of large-scale networks with millions of customers, multiple technologies, and high availability demands. With specific carrier-grade features such as scalability, reliability, flexibility, modularity, and virtualization in mind.

As a matter of fact, issues such as load balancing and congestion avoidance in the context of SDN have also drawn researchers' attention. There is meanwhile an extensive literature on load balancing mechanism using SDN technology. Author in [43] addresses the impact of colliding flows on effective Equal Cost Multipath (ECMP) cross sectional bandwidth in a fat-tree topology. As a consequence, a bottleneck for both uplink and downlink directions might occur. This paper analyses the performance of two dynamic scheduling algorithms (Global First Fit and Simulated and Simulated Annealing) in comparison to ECMP. Global First Fit scheduler linearly searches all possible paths to find one whose link components can accommodate the flow. The algorithm can be applied in normal network load conditions, otherwise the links become saturated and the number of available paths is substantially decreased. The particularity of Simulated Annealing scheduler consists of assigning a single core switch for each destination host rather than a core switch for each flow, which reduces the number of available choices. The complexity of this algorithm is higher than Global First Fit and aims to reach a converged minimum by reducing the searching space.

Plethora of researches have been done related to the implementation of virtualization technologies in access and aggregation part of communication service providers' networks. A list of those papers will be discussed from their main advantages and disadvantages and how additive the papers were.

Paper [44] describes the design of the virtualized routing protocol, enabling a simple management and avoiding signaling messages overhead in the control plane level, and the different scenarios considered to validate the virtualized function. The paper addresses the latency issues may be added by NFV related to the routing function, yet the authors didn’t mention the latency of implantation of an IGP routing protocol from the convergence, table lookup and standby route activation point of view. The paper also discussed an approach to reduce the number of flow entries in the controller. There are many approaches may deliver the same value yet more reliable such as route summarization.

Paper [45] introduces a lightweight NFV-based MPLS solution in access network - H-MPLS (Hybrid - Multiprotocol Label Switching), based on the technology of “separated control plane and forwarding plane” and “MPLS PON”, which can support fast service deployment and accelerate migration to MPLS in the access. The author extend the MPLS domain to include the access part of the network using pseudo wire concept. The system proposed by the authors may add more overhead per packet. With MTU limited network, this may reduce the amount of user data per packet which is not suitable for real time applications.

Paper [46] discusses Software-defined Access Networks (SDAN) as the next generation architecture for access networking. With its simplified access nodes, flexible and programmable line technologies, and cloud home gateway & services, SDAN helps operators construct a simple, agile, elastic, and value-added access network. The authors extend the NFV to include users’ gateways which requires the providers to manage them. This may be considered as a violation for end users’ privacy.

CHAPTER THREE

THE CLOUDIFIED MODEL

CHAPTER THREE

THE CLOUDIFIED MODEL

This Chapter discusses a novel approach to re-design the NGN infrastructure from the perspective of both control and data planes using new technologies such as SDN and Network Function Virtualization (NFV). First, the challenges of this new architecture are addressed and the proposed solutions are presented. Second, possible enhancements are investigated in terms of flexibility, complexity as well as the performances in order to shed the light on the possibility of implementing the proposed system and the challenges that may face the providers along different phases.

The current design of NGN infrastructure that delivers triple play service as in figure (3-1) structured by an access layer devices that aggregates traffic from end users and provide some lower layers functionalities such physical layer media access type and data-link layer including PVC-to-VLAN mapping. All access layer devices are connected to aggregation layer edge router located at central offices that aggregates the traffic of services and deliver it to the core of the network were all servers are located.

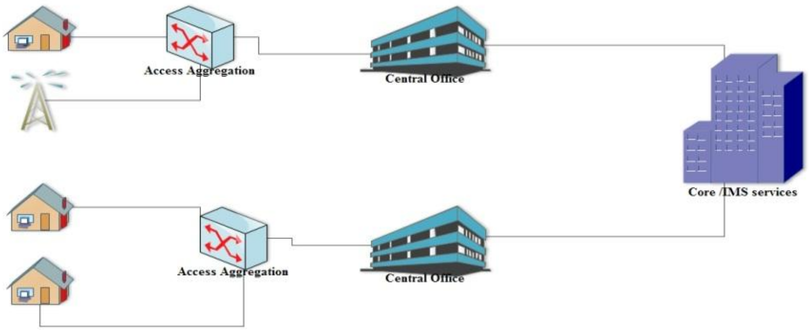


Figure 3-1: NGN traditional Architecture

The new cloudified model proposes to change the access layer of the NGN design to more intelligent devices. Access layer elements will be replaced by devices with SDN supported and all the intelligence of the network will be moved to the edges. The deeper layers of the network will the role of traffic switching and packet delivery only. Central office equipment will be replaced by server and storage in order to move network functions from hardware appliance to virtual machines using NFV technology as presented in figure (3-2).

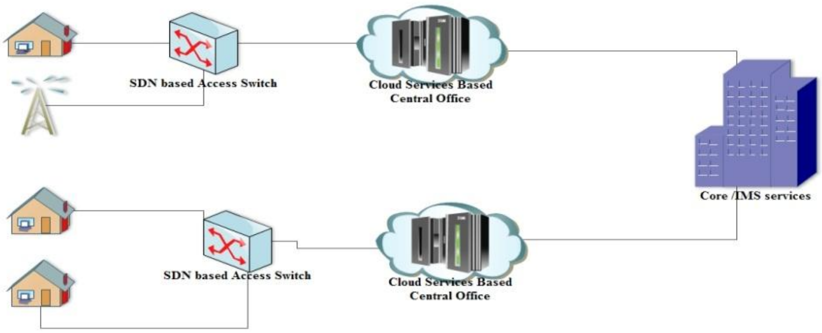

SDN based Access Switch
Cloud Services Based Central Office
Core /IMS services
SDN based Access Switch
Cloud Services Based Central Office

Figure 3-2: Cloudified Model

3.1 Architectural Design

The proposed architecture aims to change the existing architecture form relaying on hardware specific network appliance to be more virtualized. This model uses SDN and OpenFlow in the access part of the network while using NFV in the other part as shown in figure (3-3). The intelligence of the network will be moved from the edges of aggregation (wholesale) network to the access layer of the network. The roles of aggregation network include delivering packets and connecting access layer devices with core of IP services. All roles played by aggregation layer devices such as B-RAS will be moved to the access layer devices to be as close as possible to the end user. The devices of these layers (Aggregation and Core) will be virtualized as virtual network function “VNF” on general purpose servers rather than specific purpose network appliance. In this layer instead of using the traditional MPLS to connect devices, this protocol will be extended in this thesis to support the transmission of Ethernet packets over the prebuild MPLS architecture. The use of EoMPLS will allow the retailers to see their network devices as directly connected. The SDN based access layer devices will be the intelligent part of the network. All network operations such as QoS policies and rules, authentication and IP-related configurations will be moved to the access layers as discussed in the next section.

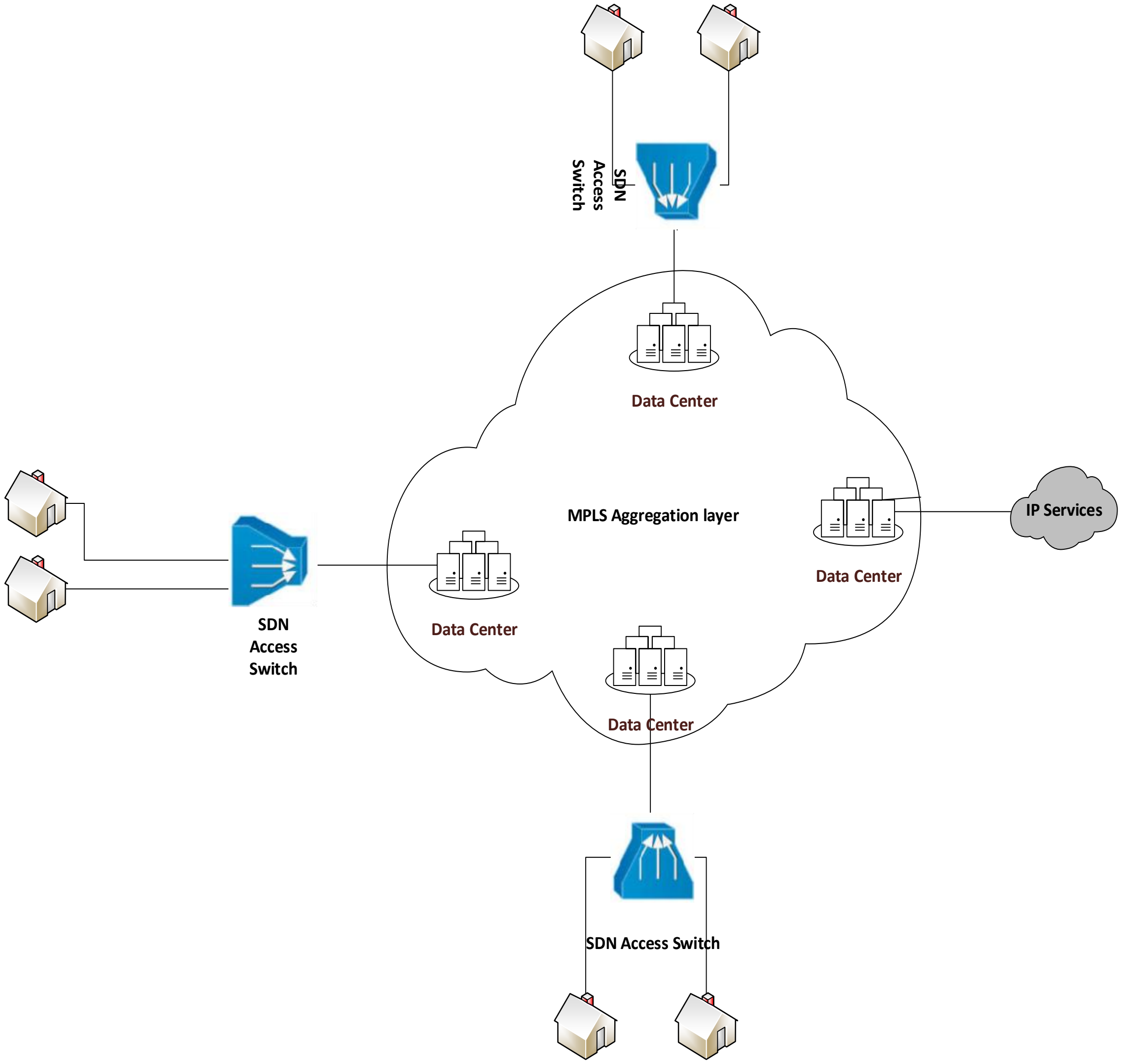


Figure 3-3: The Cloudified Model Design

3.2 Architectural Functionalities

The functionalities of main components are presented as follows:

- The ***SDN controller*** is the central entity of this architecture. It holds many responsibilities like the management of data plane and making routing decision for users' traffic between access layer switches and the edge router of aggregation layers (PE). Also include maintaining port statistics updated, balance the traffic and perform flow scheduling. The Controller via the *Northbound interface* (Representational State Transfer (REST) Application Programming Interface (API)) will be able send quires to control layer's servers to get user's line related control information such QoS policies, authentication and even IP configuration. (See Figure 3-4). The controller can install rules in the OpenFlow (OF) access switches in both reactive and proactive modes: during the connection establishment, the controller functions in proactive mode (it populates the flow entries in advance) whereas, for a service request it takes decisions based on the information contained in the packet header (reactive mode).
- The ***Virtual Provider Edge*** is the edge router in the aggregation layer of the network (wholesale). It is a virtual router function implemented on regular general purpose server. The roles of vPE include aggregate traffic from access layer and deliver it to core as services needed. The role of connecting control layer servers and SDN controller should be played by the vPE router also. The last role is to provide the service of connecting retailers and provide business connectivity services such l3VPN for end customers. All the functions B-RAS will be moved to the edge so this part of the network doesn't have to know much more

of the traffic. Therefore, latency added by this layer will be minimized since there is no need for deep packet inspection. S-VLAN also added by this device.

- The ***Middleboxes*** a middlebox or network appliance is a computer networking device that transforms, inspects, filters, or otherwise manipulates traffic for purposes other than forwarding [61]. Middleboxes are required between Access switches and Internet in order to add extra control on different types of traffic. Since the central offices of the services provider will based on cloud services, Middleboxes could be deployed on standalone hardware on virtual machines from multiple locations (Central offices) (i.e. firewalls, transcoders, Wide Area Network (WAN) optimizers, web proxy caches, intrusion detection systems, etc.).

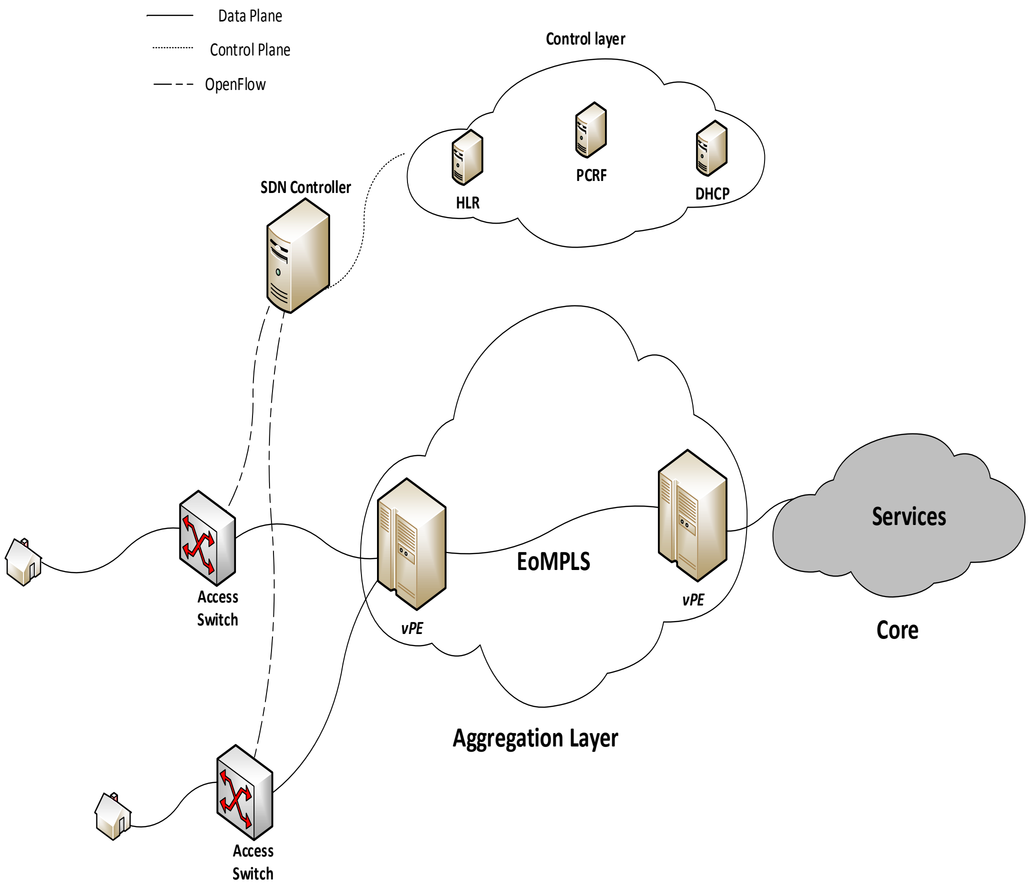


Figure 3-4: detailed proposed architecture

3.3 Cloudified Model Challenges

The proposed architecture brings extra challenges such as dynamic flow aggregation, policy paths and the ability to support multi-service. The following subsections present these issues along with the proposed solutions to each individual problem offered by the cloudified model.

3.3.1 Flow Aggregation

Typically, in a NGN network scenario, millions of users are attached to thousands of access switches (MSAN, DSLAM …etc.), which are connected to several gateways. Due to the fact that a NGN network has to serve millions of customers with different requests, this implies sophisticated policies on the service chain. In comparison to a data center where the traffic stays inside, in a NGN network the traffic goes back and forth from the user to the Internet. Another characteristic of NGN network is the fact that it has asymmetric edge (i.e. the access edge has lower bandwidth than the gateway edge). Most traffic is initiated from end users entering the access edge.

If we employ the proposed architecture, in order to save resources and Central Processing Unit (CPU) power, flow granularity can be used as a way to aggregate flows. Instead of processing and route each flow individually, a bundle of flows that flows the same pattern could be processed as group and then rerouted. Therefore, one of the options is to perform flow aggregation at the access edge and then apply rules at the same switch in order to implement policy paths towards the Internet. The packet classification is performed when traffic enters the network at the access edge and encode classification results in the header. Then, when traffic returns from the Internet, the access edge only needs to forward, as classification results are implicitly existed in the packet header.

3.3.2 QoS Policies

Due to the increase of real-time applications and the variation of services offered by CSP, the QoS in NGN networks has become an important requirement. An end-to-end QoS mechanism should ensure a special traffic treatment for different user profiles and different session types. This can be achieved by applying appropriate policies on the path along with traffic shaping.

Instead of apply QoS at the of aggregation layer by B-RAS, the SDN controller will query the PCRF server for users profiles and traffic treatment policy for each type of traffic. These policies can be applied not only to individual flows, but also to application / service specific bundles, in this way tailoring the circuit to have characteristics beneficial for the application or service (i.e. the path over which the bundle is routed). For instance, VoIP traffic must benefit from low latency paths. In the case of a VoIP bundle, a circuit can be dynamically created between source-and-destination packet switches, where the circuit path is the one with the smallest propagation-delay. In the same manner, all HTTP traffic can be redirected through a firewall on the path to the Internet. Another example is video traffic, where the low-latency for video is not as important as low-jitter.

Moreover, the video session can be routed over the non-shortest-propagation path in the employed topology.

The QoS has the responsibilities of storing classes of services along with their associated DSCP values, applying policies that either take advantage of the service class or apply a type queuing technique on the queues attached to ports on a switch. The approach starts by providing a ”module” inside the SDN controller that will perform the matching, classification, flow insertion, flow deletion, and policy handling for QoS. The module is capable of two functions within the OpenFlow: “Enqueue” and modify the “Network ToS” bits. Furthermore, the module itself allows the definition of two types of policies: “Queuing Policy” and ”ToS/ DSCP Policy”. A queuing policy utilizes the ”Enqueue” action in OF switch to Enqueue different types of flows in the network that match on certain criteria. The QoS module will send those flows to a queue on a switch port that has a predefined action of its own, such as rate limits, minimum bandwidth and/or bandwidth ceilings [62]. The actual configuration of the queues within a given switch is under the duties of the network administrator and it constitutes a Command Line Interface (CLI)-based configuration process.

Fortunately, there is a new protocol currently under development that tries to eliminate this process by providing a control and data-plane separation for the configuration of queues, ports, and other QoS based arrangements. This protocol is called OF-Config and this protocol allows one or more OpenFlow data planes to be instantiated and assign queues and ports to the OpenFlow data planes [63].

3.3.3 Multi-service Support

The QinQ technology is also called the Stacked VLAN or Double VLAN. This technology complies with the IEEE 802.1ad standard. It encapsulates the user private network VLAN Tag in the public network VLAN Tag to make messages traverse the backbone network (Public network) of carriers with two layers of VLAN Tags. In public networks, messages are transmitted only according to the external VLAN Tag (namely the public network VLAN Tag) and the private network VLAN Tag is shielded. This technology allows the provider to support multiservice over the same infrastructure with the feature of faster packet hop-to-hop delivery.

Scenarios such as the one mentioned in (section 2.7.3) cloud be easily implemented since SDN switches support real-time deep packet inspection. In the access layer each service cloud be assigned with different VLAN tag which represent the C-VLAN [66] added by switches. Based on the destination service port (VoIP, VoD ….etc.), the switch will assign the appropriate VLAN tag to each packet after inspect the packet. The S-VLAN [66] will be added by the vPE based on the access switch the packet originated by so routing across the aggregation layer can take place.

3.4 Proposed System Analysis

After a detailed explanations of the proposed architecture along with the foreseen challenges, this section aims to explore possible enhancements to the proposed design in terms of:

1. *Flexibility*: new services, software upgrades and traffic management;
2. *Deployment Complexity*: implementation, scalability and costs;
3. *Performances*: routing, latency and traffic monitoring.

3.4.1 Flexibility

• *Control Plane:*

The flexibility introduced by the virtualized functions eliminates the overprovisioning of services in the traditional architectures, is meant to bring extra automation and intelligence in the access layer of standardized environment. The orchestration management layer allows dynamic capacity allocation for the VMs based on the requirements (both horizontal and vertical scalability). This enhancement led to better traffic management and optimized routing all layer of the network. For instance, software upgrades can be maintained by the operator with no need for vendor implication.

Another advantage that virtualization might bring to operators, is the deployment of both production and test environments on the same platform.

• *User Plane:*

The user plane elasticity is mostly dictated by the Open vSwitch capabilities. Therefore, by sending periodic updates to the controller of the received / transmitted and dropped packets, the overall redundancy in the network increases, so the controller will be aware of the congested links. This characteristic is strongly related to the load balancing mechanism which is meant to equally distribute flows to less overloaded switches. The flow priority mechanism and aggregation can establish the QoS for any particular type of service (VoIP, video, etc.).

3.4.2 Deployment Complexity

• *Control Plane:*

The complexity of the employed solution can be analyzed in terms of implementation tools, scalability and costs. Even if the proposed solution preserves the control plane functionality, from the implementation point of view, it requires both hardware and software changes. For instance, the AAA, PE and PCRF functions can run as VMs in data centers and can be communicate with the central controller through the REST API. Since the controller and hypervisor can be implemented on virtualized server platform, it drastically decreases the complexity of exceeded hardware found in an operator network. For instance, one controller can attach to hundreds of switches and process millions of requests per second. The performance of testbed consisting of a 100 switches allocating 16 cores for process with 400-500 effective flows per second was analyzed in [63]. In this manner, the scalability grows proportional to the complexity decrease. The cost in Capital Expenditure (CAPEX) and Operating Expenditure (OPEX) is one of the major advantages of deploying SDN in telecom network. For instance [64] states that the EPC virtualization will increase CAPEX up to 30M Euro in the third year of deployment, whereas the decrease in OPEX is almost 100M Euro in the operations sector and up to 25M Euro lower budget allocated for maintenance purposes.

• *User Plane:* The innovative user plane consists of multiple OpenFlow hardware switches with integrated Open vSwitch (OVS). Open vSwitch [65] is a virtual switch that supports flows, Virtual LAN (VLAN)s, trunking, QoS, port aggregation even Layer 3 forwarding. The employment of SDN solution simplifies the user plane forwarding and flow aggregation based on variety of parameters such as ToS. The end user's IP address aggregates flows coming from the same residential gateway and access switch in a single tag and differentiates between user sessions based on the destination ports. Nevertheless, in a large production environment it might guarantee the network scalability. For instance, one of the possible deployments can be a fat-tree topology with edge (access), aggregation and core switches, which is very common topology in data center. One of the advantages of this solution introduced by this thesis is the low cost of implementation, since the price of a single hardware OpenvSwitch is thousands of Euro in comparison to millions that operators pay for the deployment and configuration of each gateway.

3.4.3 Performance

• *Control Plane:*

The control plane performance in the Cloudified architecture is expected to increase in terms of routing reliability in comparison to the standardized NGN deployment. For instance, the current load balancing mechanism is proactive and does not take into account the instantaneous load or capacity due to lack of load parameters telemetry between network elements, which might lead to overload in one or more network nodes.

In paper [67] a dynamic flow scheduling system has been proposed in order to collect statistics from switches, compute non-conflicting paths for the flows and re-route the traffic accordingly. A network-wide scheduler should measure the utilization of all links in the network and move flows from highly-utilized links to less utilized links.

Based on the flow size detected at the access switches, the scheduler measures the bandwidth consumed by intensive flows, as well as the required capacity and uses placement algorithms to compute good paths which are further installed on the switches. Due to the fact that in the proposed architecture the SDN-controller can manage large number of switches, it implicitly introduces a single point of failure into the network. New techniques like DevoFlow have been proposed in order to mitigate the flow scheduling overheads while maintaining the same network performance [68]. The network redundancy can be increased by deploying two central controllers which can communicate to each other via HyperFlow application [69]. The second controller serves as a backup in case of failure of the primary controller.

• *User Plane:*

The OpenFlow protocol allows software controller running on a server to configure the hardware forwarding tables of switches. Whenever the switch receives a packet, it will first look up in its flow table for L2-L4 header matching and then perform variety of actions including forward the packet to a specific port, encapsulate the packet or drop it. If no match is found, a query will be sent to the controller. In the proposed deployment the latency of the controller is decreased by installing predefined rules in the switch proactively. In every PACKET_IN message sent to the controller, the switch includes port statistics with the number of received/transmitted and dropped packets. Hence, in case of congested links, the traffic anomalies can be easily determined by the SDN controller. Paper [70] addresses the challenges of implementing monitoring rules in the network in order to determine the load on each switch. This paper introduces an adaptive algorithm based on linear prediction has been proposed with the goal to mitigate the amount of processed data by the controller and the overhead in the network produced by the load information. Recent paper [71] proposes to use sFlow standard in combination with SDN architecture in order to detect large flows in real-time and send this information to the Load Balancing Application on the top of the controller. In this manner, the extra load information in the packet header can be eliminated as mentioned in [70].

Paper [71] presents the use case of the load balancing where the sFlow-RT collector communicates with the Load Balancing Application via Open API. At a first glance, one of the approaches used to isolate network parts is to employ VLAN tagging, but a more advanced solution could be Flow Visor, which attributes the packets coming from slice or cluster of switches to be processed by which particular controller. This solution might prevent a malfunctioning controller to saturate switch’s CPU [72].

CHAPTER FOUR

SIMULATION ENVIRONMENT, TOOLS AND TECHNOLOGIES

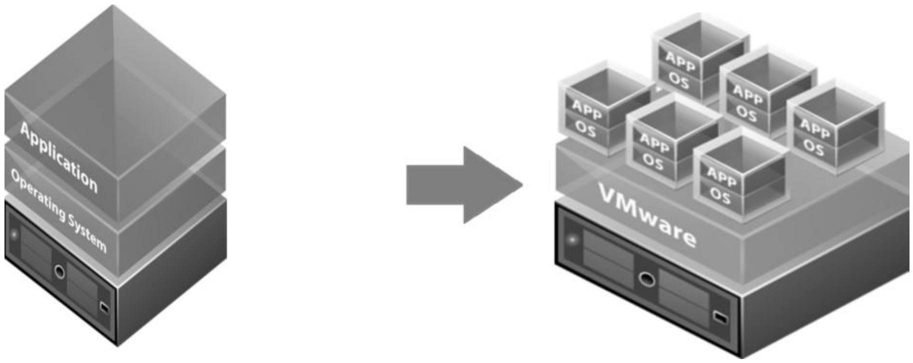
CHAPTER FOUR

SIMULATION ENVIRONMENT, TOOLS AND TECHNOLOGIES

This chapter describes the tools and technologies used in the simulation phase of the cloudified system. Both NFV and SDN tools were used and parts of the configuration of the test-bed are included along with explanation of the commands. The controller architecture is presented and different extensions of this controller are investigated. Also in this chapter, the cloudified system will be simulated using the standard NGN topology and a purpose defined scenario will applied on. The scenario will discussed in details also in this chapter.

4.1 Virtualization Environment

Today’s x86 computer hardware is designed with very high capacity and high ability to deliver multi-tasks in real-time. But most of computers run single operating system and limited number of applications, leaving most machines mostly underutilized. Virtualization technologies allow single platform to multiple virtual machine through resource sharing between these machines figure (4-1). Each of these virtual machines represents an independence fully functional machine able to run and deliver different services on the same physical machine. Resource management is done by a piece of software called hypervisor [47] among the several hosted virtual machines.



(a) Traditional Architecture (b) Virtual Architecture

Figure 4-1: virtualization environment [48]

Nowadays there are many well-known virtualization tools such as: VMware, VirtualBox, Kernel-based Virtual Machine (KVM), Proxmox, Virtual Machine Manager (VMM), etc. In this thesis, VMware is presented which was used to set up the simulation test environment presented in the cloudified system section.

4.1.1 VMware Workstation 10

VMware Workstation 10 is a Virtualized tool presented by VMware. This hypervisor allows the installation of several operating systems on single server or computer and run multiple applications in progress. The resource allocation is based on the intensity of operations.

This following Subsection aims to present the benefits of the current VMware software version necessary for the implemented testbed. More details about the supported features and configuration are provided in product documentation [49].

4.1.1.1 VMware Network Connections Configuration

The VMware Workstation 10 offers variety of network connections modes: *Bridged Networking, Network Address Translation*, *Host-Only* and *Custom* mode. The configuration mode used in the simulation presented in this thesis is *Custom*.

1. *Bridged Networking Configuration* - Bridged networking connects a VM to a network by using the network adapter on the host system. The host network adapter enables the VM to connect to the Local Area Network (LAN) that the host system uses. Bridged networking works with both wired and wireless host network adapters. By default, *VMnet0* is set to use auto-bridging mode and it is configured to bridge to all active network adapters on the host system. A VM must have its own identity on a bridged network. For example, on a Transmission Control Protocol (TCP) / Internet Protocol (IP) network, the virtual machine needs its own IP address.

2. *Network Address Translation (NAT) Configuration* - With NAT, a virtual machine does not have its own IP address on the external network. Instead, a separate private network is set up on the host system. In the default configuration, VMs are dynamically assign an address on the private network from the virtual Dynamic Host Configuration Protocol (DHCP) server. The host system has a virtual network adapter on the NAT network. The NAT device forwards network data between one or more VMs and the external network, identifies incoming data packets intended for each VM and sends them to the correct destination.

3. *Host-Only Networking Configuration* - In a host-only network, the VM and the host virtual network adapter are connected to a private Ethernet network. The network connection between the VM and the host system is provided by a virtual network adapter that is visible on the host operating system. The virtual DHCP server provides the IP addresses on the host-only network [49].

4. Custom Configuration: using pre-built virtual links, custom mode offers the ability to connect multiple virtual machines to build real network in a virtual environment.

4.1.1.2 Backup

A VMware snapshot is a copy of the Machine Disk File (VMDK) at a given point in time. Snapshots provide a change log for the virtual disk and are used to restore a VM to a particular point in time when a failure or system error occurs. This is a very important feature of the VMware, as it allows to go back to a previous machine states Figure (4-2).

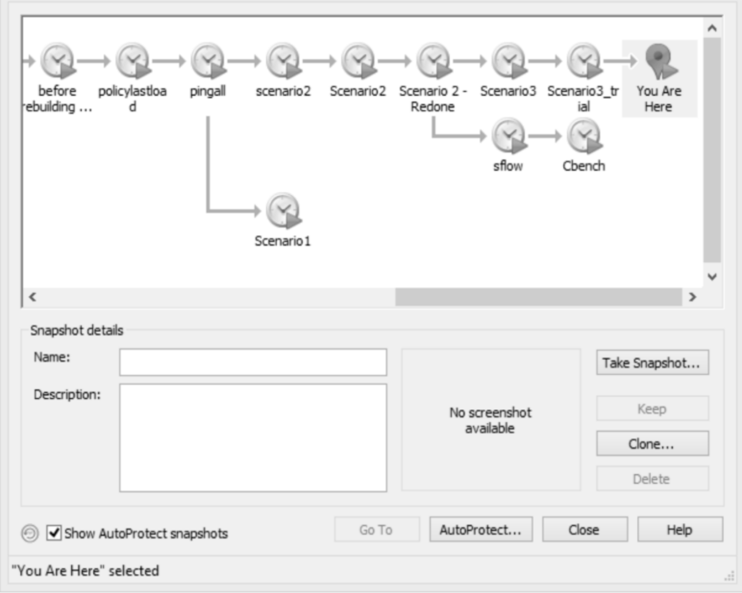


Figure 4-2: VMware snapshot [26]

Any data that was writable on a VM becomes read-only when the snapshot is taken. VMware administrators can take multiple snapshots of a VM to create multiple possible point-in-time restore points. When a VM reverts to a snapshot, current disk and memory states are deleted and the snapshot becomes the new parent snapshot for that VM. The snapshot file cannot exceed the size of the original disk file, but it requires overhead disk space.

3.1.2 Cisco CSR 1000V

The Cisco CSR 1000V Series Cloud Services Router provides a cloud-based router that is deployed on a virtual machine (VM) instance on x86 server hardware. The Cisco CSR 1000V provides selected Cisco IOS XE features on a virtualization platform.

When the Cisco CSR 1000V virtual IOS XE software is deployed on a VM, the Cisco IOS XE software functions just as if it were deployed on a traditional Cisco hardware platform. The Cisco CSR 1000V includes a virtual Route Processor and a virtual Forwarding Processor (FP) as part of its architecture. The Cisco CSR 1000V supports a subset of Cisco IOS XE software features and technologies [50].

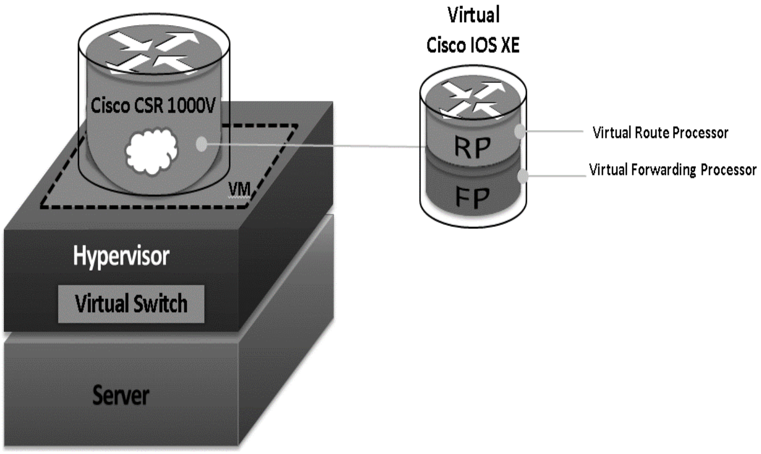


Figure 4-3: Cisco CSR 1000V [8]

3.1.2.1 Cisco CSR 1000V Benefits

The Cisco CSR 1000V Series uses the benefits of virtualization in the cloud to provide the following:

• Hardware independence

Because the Cisco CSR 1000V runs on a virtual machine, it can be supported on any x86 hardware that the virtualization platform supports.

• Sharing of resources

The resources used by the Cisco CSR 1000V are managed by the hypervisor, and resources can be shared among VMs. The amount of hardware resources that the VM server allocates to a specific VM can be reallocated to another VM on the server.

• Flexibility in deployment

You can easily move a VM from one server to another. Thus, you can move the Cisco CSR 1000V from a server in one physical location to a server in another physical location without moving any hardware resources [8].

3.1.2.2 CSR 1000V supported Features

The CSR 1000V supports the following Cisco IOS-XE feature depending on license purchased:

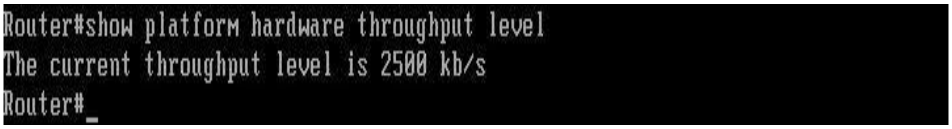
- Routing: BGP, OSPF, EIGRP, Policy-based Routing, IPv6, VRF-Lite, Multicast, LISP, GRE
- Addressing: DHCP, DNS, NAT, 802.1Q VLAN, EVC
- VPN: IPSec VPN, DMVPN, EasyVPN, FlexVPN
- MPLS: MPLS VPN, VRF, BFD
- Security: Cisco IOS Zone-Based Firewall, ACL, AAA, RADIUS, TACACS+
- High Availability: HSRP, VRRP, GLBP
- Traffic Redirection: AppNav (to vWAAS), WCCP
- Application Visibility, Performance Monitoring and Control: QoS, AVC, IP SLA
- Hybrid Cloud Connectivity: OTV, VPLS, EoMPLS
- Management: CLI, SSH, NetFlow, SNMP, Embedded Event Manager, RESTful APIs [41].

4.1.2.3 CSR 1000V Throughput

According to [42] CSR 1000V supports up to 10 Gbps depending on hardware specifications of the host machine and the license purchased. CSR

1000v comes with evaluation license that supports throughput up to 50Mbps for 60 days.

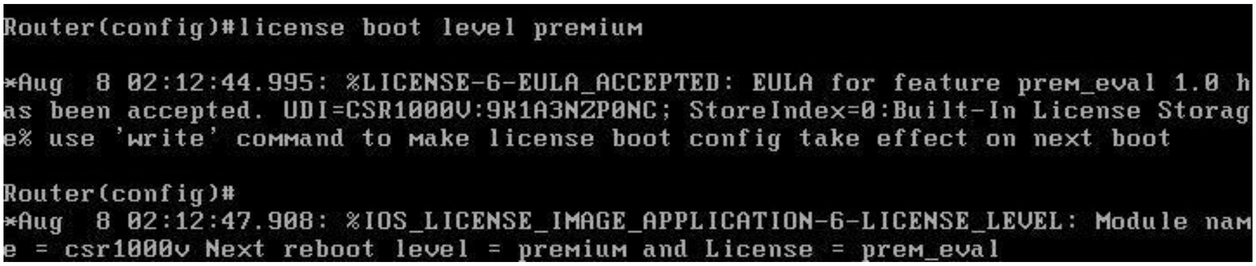
By default any version of this vrouter comes with preset throughput of 2.5Mbps as shown in figure [8].



```
Router#show platform hardware throughput level
The current throughput level is 2500 kb/s
Router#_
```

Figure 4-4: CSR 1000v default Throughput

The evaluation version supports variety of throughputs that could be activated as shown in figure (4-5, 4-6) once the trial period end the throughput will automatically drops to 2.5Mbps.

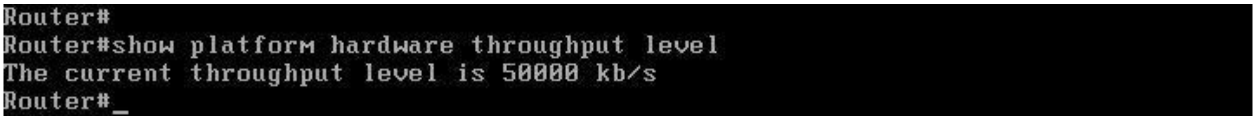


```
Router(config)#license boot level premium

*Aug  8 02:12:44.995: %LICENSE-6-EULA_ACCEPTED: EULA for feature prem_eval 1.0 h
as been accepted. UDI=CSR1000V:9K1A3NZP0NC; StoreIndex=0:Built-In License Storag
e% use 'write' command to make license boot config take effect on next boot

Router(config)#
*Aug  8 02:12:47.908: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Module nam
e = csr1000v Next reboot level = premium and License = prem_eval
```

Figure 4-5: trial license activation



```
Router#
Router#show platform hardware throughput level
The current throughput level is 50000 kb/s
Router#_
```

Figure 4-6: trial license Throughput

4.1.2.4 CSR 1000V Hardware Requirements

Hardware requirements of CSR 1000v varies as the implementation scenario and the version of vrouter’s software. The following are the minimum requirements for the Cisco IOS XE 3.8S and 3.9S releases.

- The Cisco CSR 1000V router VM: 4 virtual CPUs , 4 GB RAM , 8 GB Hard Drive , PC running the VMware vSphere Client 5.0 and Server running VMware ESXi 5.0

- For later software versions as follows: Memory: 16GB DDR3 or higher, Hard Drive: 100GB or higher, Network Cards: 1 Gbps (3 or higher), The minimum clock rate supported is 1.9 GHz and The Cisco CSR 1000V router supports a maximum of 10 vNICs [52].

4.2 Software Defined Network Tools

In this section, the tools offered by open project of SDN used in this thesis will be investigated. Tools such open vSwitch and OpenDaylight controller will be reviewed.

4.2.1 Open vSwitch

Open vSwitch is an open source software switch designed to be used as a virtual switch in virtualized server environment. A vSwitch forwards traffic between different Virtual Machine (VM)s on the same physical host and also forwards traffic between VMs and the physical network. Open vSwitch can currently run on any Linux-based virtualization platform (kernel 2.6.32 and newer), including: VMware, Kernel-based Virtual Machine (KVM), VirtualBox, Proxmox, etc.

Like a physical OpenFlow switch it supports standard management interfaces and protocols (e.g. NetFlow, sFlow, Switch Port Analyzer (SPAN), Remote SPAN (RSPAN), Command Line Interface (CLI), Local Control and Accountability Plan (LACP), Virtual LAN (VLAN) (802.1ag)) and multiple tunneling protocols (Generic Routing Encapsulation (GRE), Virtual Extensible LAN (VXLAN), IPsec, GRE and VXLAN over IPsec). In addition to that, the Open vSwitch is designed to support distribution across multiple physical servers. Open vSwitch configurations consists of bridges and ports. Ports represent connections to physical interfaces and patch cables [36].

Packets from any given port on a bridge are shared with all the other ports on that bridge.

Bridges can be connected through Open vSwitch virtual patch cables or using Linux virtual Ethernet cables (*veth*). Additionally, bridges appear as network interfaces to Linux, thus IP addresses can be assigned to them Figure (4-6).

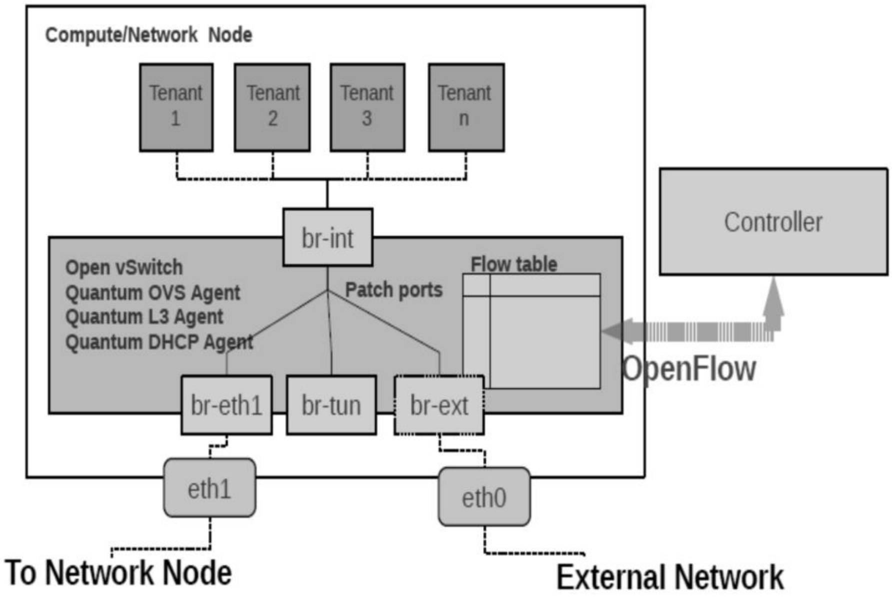


Figure 4-6: openvSwitch architecture [37]

4.2.1.1 Open vSwitch throughput

Open vSwitch delivers much higher throughput than vrouters [43]. There is no official document that gives clear number for the maximum throughput but many performance tests have been done by variety of network oriented researchers. The programmability feature offered by SDN gives the developers much more flexibility to develop approaches to increase the throughput.

Software accelerators is one of the innovative approaches to increase speed offered by many software vendors such as 6WIND.

Packet processing functions such as Layer 2 switching are performed in a fast path environment, running on dedicated processor cores outside the OVS kernel. This avoids the overheads and latencies associated with the OVS kernel. Unlike the standard OVS, the performance of 6WINDGate [53] scales linearly based on the number of cores configured to run the fast path, even if these cores are distributed across multiple processors.

4.2.2 Software Defined Networking Controllers

The SDN technology brings the development of multiple open-source controllers. A list of these projects along with a brief description of each has been summarized in [54]. Among them, one of the most popular and recent controllers is OpenDaylight. This Section presents an overview of the controller in terms of its architecture, Graphical User Interface (GUI) and its existing modules which were used in the simulation environment. Moreover, an extension of these modules and the algorithms behind it are thoroughly explained in the following Subsections.

4.2.2.1 OpenDaylight Controller

The OpenDaylight Project is a recent open-source project founded by some of the market leading vendors such as: Big Switch Networks, Brocade, Cisco, Citrix, Ericsson, HP, IBM, Juniper Networks, Microsoft, NEC, Red Hat and VMware. OpenDaylight is developed as a modular, pluggable, and flexible controller platform. This controller is completely programmed using Java and it is integrated within its own Java Virtual Machine (JVM). Hereby, it can be deployed on any operating system platform that has Java environment installed. From a high level approach, SDN is commonly described in layers:

1. *Network Apps & Orchestration:* The top layer consists of business and network logic applications that primarily control and monitor network behavior. In addition, it contains other complex orchestration

applications needed for cloud and NFV services in accordance with the requirements of those environments.

2. *Controller Platform:* The middle layer provides the framework in which the SDN abstractions can run and consists of a set of common APIs to the application layer (i.e. the northbound interface). Moreover, other protocols for configure and control of the physical hardware such as OpenFlow, Netconf, Open vSwitch Database Management Protocol (OVSDB), Locator / ID Separation Protocol (LISP), Border Gateway Protocol (BGP), etc. are implemented within the network (on the southbound interface).
3. *Physical & Virtual Network Devices:* The lowest layer consists of forwarding elements, which are basically physical and virtual devices, switches, routers, etc., that connect all endpoints within the network by forwarding the traffic between them.

The top layer applications access the controller via the Open API interface. Open-Daylight supports the Open Service Gateway initiative (OSGi) framework and bidirectional Representational State Transfer (REST) for the Northbound API. The OSGi framework is used for applications that are in the same network pool with the controller, while the REST (web based) API is used for applications that do not run in the same address space (they can even run on different VMs than the controller). The business logic and algorithms are part of the application layer. The applications use the controller to manage and monitor the network, run algorithms to perform analytics, and implement new rules in the network.

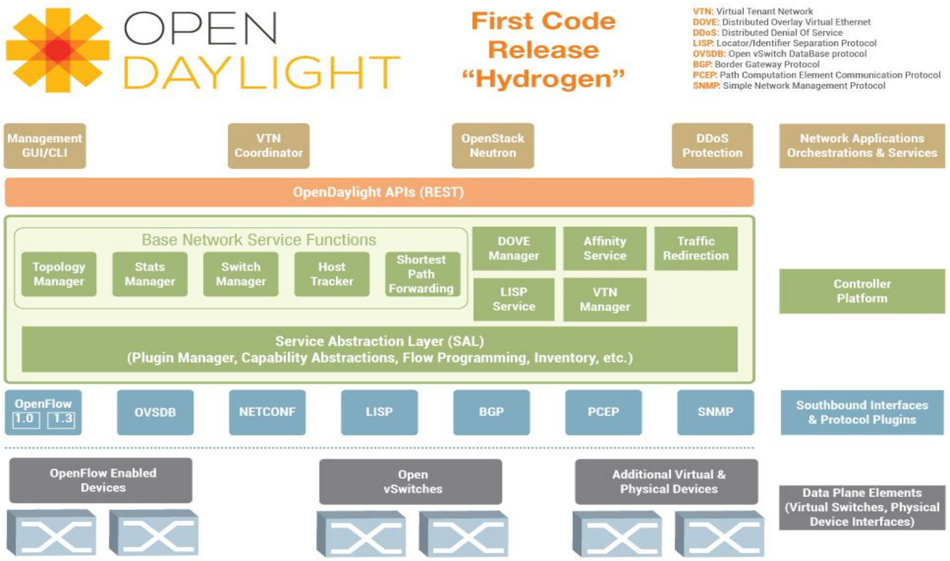

OPEN DAYLIGHT
First Code Release "Hydrogen"
VTN: Virtual Tenant Network
DOVE: Distributed Overlay Virtual Ethernet
DDoS: Distributed Denial Of Service
LISP: Locator/Identifier Separation Protocol
OVSDB: Open vSwitch DataBase protocol
BGP: Border Gateway Protocol
PCEP: Path Computation Element Communication Protocol
SNMP: Simple Network Management Protocol
Management GUI/CLI
VTN Coordinator
OpenStack Neutron
DDoS Protection
Network Applications Orchestrations & Services
OpenDaylight APIs (REST)
Base Network Service Functions
Topology Manager
Stats Manager
Switch Manager
Host Tracker
Shortest Path Forwarding
DOVE Manager
Affinity Service
Traffic Redirection
LISP Service
VTN Manager
Controller Platform
Service Abstraction Layer (SAL)
(Plugin Manager, Capability Abstractions, Flow Programming, Inventory, etc.)
OpenFlow 1.0 1.3
OVSDB
NETCONF
LISP
BGP
PCEP
SNMP
Southbound Interfaces & Protocol Plugins
OpenFlow Enabled Devices
Open vSwitches
Additional Virtual & Physical Devices
Data Plane Elements (Virtual Switches, Physical Device Interfaces)

Figure 4-7: OpenDaylight controller [55]

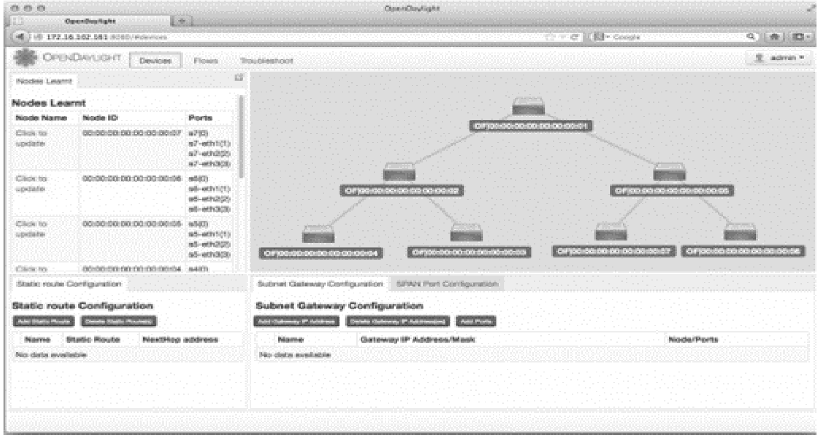
The Southbound interface is capable of supporting multiple protocols as separate plugins, i.e. OpenFlow 1.0, OpenFlow 1.3, BGP, etc. These modules are connected to a Service Abstraction Layer (SAL) which is the core of the modular design of the Controller and it allows to support multiple protocols on the southbound interface. The SAL determines how to map the requested service independent of the underlying protocol used between the controller and the network devices.

4.2.2.2 OpenDaylight Web Interface

The OpenDaylight Controller includes an application called *Simple Forwarding* which allows to use the basic services for making forwarding decisions and install flows across all devices on the OpenFlow network. This application discovers the presence of a host via the Address Resolution Protocol (ARP) message and installs destination-only (/ 32) entries across all switches in the network, with the corresponding output ports towards the host.

This can be seen when logging into the web interface with OpenDaylight Controller and with vSwitches running. A Fat-Tree topology is illustrated in

Figure (4-8). The port details along with the statistics can be seen in the “Flows” window. One of OpenDaylight main advantages in comparison to other existing controllers is that it provides the capability to install flow entries (L1-L4) in the switches using the Web Interface.


OpenDaylight
172.16.102.181:8080/#devices
OpenDaylight
Devices
Flows
Troubleshoot
admin
Nodes Learnt
OF|00:00:00:00:00:00:00:01
OF|00:00:00:00:00:00:00:02
OF|00:00:00:00:00:00:00:05
OF|00:00:00:00:00:00:00:04
OF|00:00:00:00:00:00:00:03
OF|00:00:00:00:00:00:00:07
OF|00:00:00:00:00:00:00:06
Static route Configuration
Subnet Gateway Configuration
SPAN Port Configuration
Add Static Route
Delete Static Route(s)
Add Gateway IP Address
Delete Gateway IP Address(es)
Add Ports

Nodes Learnt

Node Name	Node ID	Ports

Click to update	00:00:00:00:00:00:00:07	s7(0)
		s7-eth1(1)
		s7-eth2(2)
		s7-eth3(3)

Click to update	00:00:00:00:00:00:00:06	s6(0)
		s6-eth1(1)
		s6-eth2(2)
		s6-eth3(3)

Click to update	00:00:00:00:00:00:00:05	s5(0)
		s5-eth1(1)
		s5-eth2(2)
		s5-eth3(3)

Click to	00:00:00:00:00:00:00:04	s4(0)

Static route Configuration

Name	Static Route	NextHop address
No data available		

Subnet Gateway Configuration

Name	Gateway IP Address/Mask	Node/Ports
No data available		

Figure 4-8: OpenDaylight controller GUI

4.3 System Simulation

Tools mentioned in earlier sections have been used to deploy and simulate the cloudified infrastructure introduced by this thesis. Measurement tools used to results that will be discussed in next chapters. This section will cover the simulation environment in details. Properties of each device, link and application will be mentioned in next subsections.

4.3.1 Simulation Environment Topology

Since there are no standard topologies for each service, the majority of operators design their networks based on geographical and business requirements. Very similar to the data center model, NGN topologies are composed of three layers: access, aggregation and core. Paper [73] presents different topologies ranging from hub-spoke, ring, mesh or a combination of two or more topology.

The proposed topology presented in Figure (4-9) consists of three virtual routers to simulate aggregation network based on MPLS. OSPF has been used to provide end-to-end connectivity between provider edge routers (vPEs). IP addressing schemes have been declared in Figure (4-9). Port-Based EoMPLS pseudo wire tunnel has been established between both aggregation network's (Wholesale) edge interfaces. All routers are cisco CSR 1000v virtual machines presenting routing functions in the network. Vrouters properties are presented in Table (4-1). Each router's configuration is presented in Appendices (A, B and C). All links in the topology are 1Gbps speed links.

Table 4-1: Vrouter Properties

Type	Virtual Machine
Hypervisor	VMware
Software	Cisco CSR 1000v
Throughput	50 Mbps
RAM	3 GB
Processors	4
Interfaces	2 each bandwidth 1Gbps

Access layer has been simulated using two VSwitches to represent layer 2 connectivity between end users' and operator's network. Switches are controlled by OpenDaylight controller using totally separated management network. IP addressing schemes are presented in Figure (4-9). All switch are connected through 1Gbps links. All switches are virtual machines running openvSwitch software. Each router's configuration is presented in Appendices. SDN switches' properties are presented in Table (4-2).

Table 4-2: Switches' Properties

Type	Virtual Machine
Hypervisor	VMware
Software	OpenvSwitch
Throughput	Up to 1 Gbps
RAM	1 GB
Processors	4
Interfaces	2 each bandwidth 1Gbps

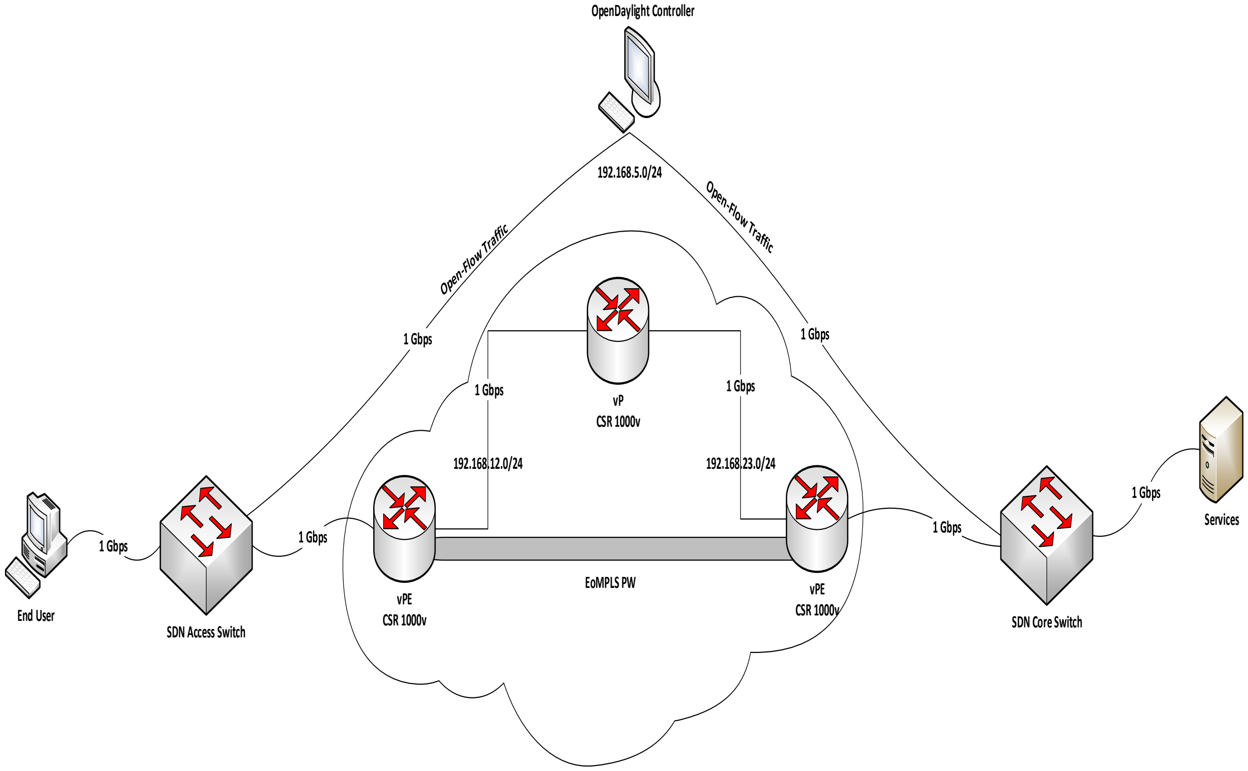


Figure 4-9: Proposed system Simulation topology

4.3.2 Simulation Scenario

Simulation scenario includes a subscriber with a 50Mbps profile applied to his link. The customer is connected to an access layer SDN based switch intended to aggregate traffic from customers towards the aggregation layer. The scenario support the multiservice through the use of QinQ feature. A server is connected to the network in order to deliver triple play services to the subscriber. For IPTV and VoIP, the service will be delivered using different codec schemes. Each Codec will be investigated against the requirement of ITU-T for each service. The results gathered using ixChariot application will be discussed in chapter Five.

CHAPTER FIVE

RESULTS AND DISCUSSION

CHAPTER FIVE

RESULTS AND DISCUSSION

This chapter presents different triple play services could be delivered using the testbed described in previous chapter and interprets the obtained results. Additionally, a brief insight of the expected results is given in order to estimate the possible outcome. The chapter is divided in three main parts corresponding to the three different services of triple play: Voice over IP, IPTV and Data services presented on a virtualized environment.

5.1 Quality of Experience and Quality of Service

In the past years Quality of Service (QoS) and Quality of Experience (QoE) of communication services have been the topic of various studies and research. As an example, the standardization sector of the International Telecommunication Union (ITU-T) has a dedicated study group (SG12) working on 'Performance, QoS and QoE'. Their purpose is to define clear and accurate measures for the quality perceived by end-users that are required to bridge the gap between the offered end-to-end service and the underlying technology.

5.1.1 QoS and QoE Definitions

Matching subjective opinions and experience with measurable objective parameters will in all cases be estimations of the technical reality.

The ITU defines Quality of Experience as 'The overall acceptability of an application or service, as perceived subjectively by the end-user' in ITU-T P.10/G.100 [74]. There are two notes with this definition:

1 – Quality of experience includes the complete end-to-end system effects (client, terminal, network, services infrastructure, etc.).

2 – Overall acceptability may be influenced by user expectations and context. .

In a different recommendation, ITU-T Rec. E 800,[75], the ITU defines Quality of Service as: Totality of characteristics of a telecommunications service that bear on its ability to satisfy stated and implied needs of the user of the service'. This definition allows for objective quantification of the quality of service as a set of service parameters.

Alcatel-Lucent Bell Labs in the Bell Labs Technical Journal 15, [75] illustrates the difference between QoE and QoS as follows: 'QoE focuses on user-perceived effects, such as degradation in voice or video quality, whereas QoS focuses on network effects such as end-to-end delays or jitter'.

5.2 Performances and Expectations of the Cloudified Model

The cloud based architecture envisions the flexibility of decoupling the user from the control plane for the access layer and the implementation of hardware independent network functions. The deployment complexity of the proposed topology was presented in the previous chapter. Furthermore, the implementation of Quality of Service (QoS) module and the routing algorithms of SDN switch were also presented. The QoS modules are integrated in the controller.

The performances of the network emulated testbed were analyzed based on the obtained results in terms of each services' KQI (Key Quality Indicator) such as throughput, loss and packet delay variation (jitter) for different types of traffic: Hypertext Transfer Protocol (HTTP), Voice over IP (VoIP) and video. It is expected to achieve a throughput close to the bandwidth limitation for the weakest link in the topology which is limited by the throughput of the virtual routers. All results has been gathered using Ixchariot.

5.3 Voice over IP (VoIP)

For VoIP QoS/QoE parameters the recommendations ITU-T P.863 and ITU-T P.563 are applicable in order to estimate speech quality. The voice quality of a telephone call depends on many factors including users' equipment, adopted codecs and network performance.

Here some of most important voice KQI and the performance of the proposed system related to it.

4.3.1 Throughput

Throughput requirements depend mostly on the codec. A codec (Coder/ DE-Coder) is an algorithm used encode audio or video content before sending it on the network. The effective bandwidth requirement for a particular codec is higher than the bit rate of the codec as the overhead of all network protocols (RTP, UDP, IP, Ethernet) should be taken into account. Table 5-1 show the bandwidth of each codec.

Table 5-1: VoIP Codec Bandwidth

Codec	**Data Rates /kbps**
G.711	64
G.722	48/56/64
G.723.1	5.3/6.3
G.726	16/24/32/40
G.729	8

As it was mentioned above, the client send VoIP traffic with different codec schemes to the server with the bandwidth limitation of each one. Figure 5-1 shows the bandwidth of each codec. The Cloudified model met the bandwidth requirements of all codecs.

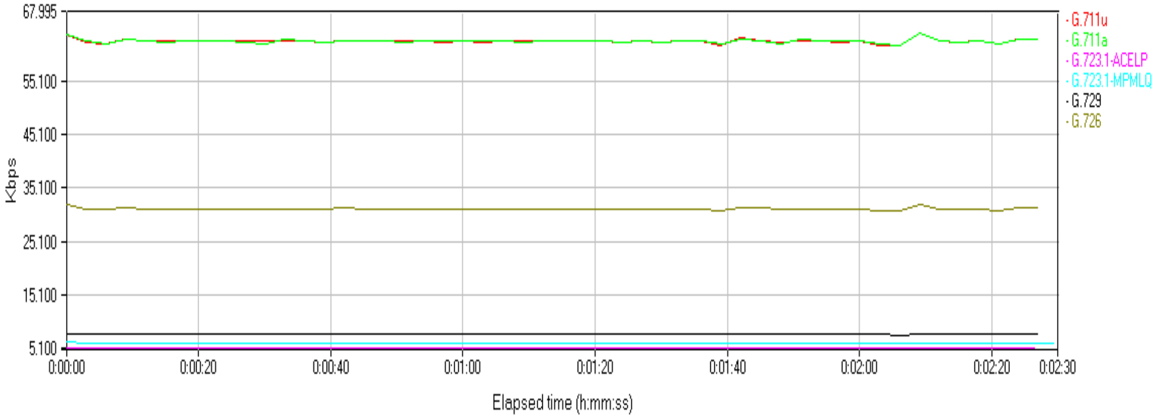


Figure 5-1: VoIP Throughput

5.3.2 Mean Opinion Score (MOS)

The Mean Opinion Score (MOS) is one of the most commonly used voice quality indicator. It provides a numerical indication of the perceived quality of received audio streams.

Several methods were introduced in order to derive the MOS value from objective measurement. Some measurement techniques are intrusive [76, 77] whereas others allows to compute the MOS in a totally passive way [78]. Table 5-2 shows the MOS comparison values and the satisfactory level that they provide.

Table 5-2: MOS comparison values

Very satisfied	4.3-5.0
Satisfied	4.0-4.3
Some users satisfied	3.6-4.0
Many users dissatisfied	3.1-3.6
Nearly all users dissatisfied	2.6-3.1
Not recommended	1.0-2.6

Each codec provides a certain quality of speech. The quality of transmitted speech is a subjective response of the listener. A common benchmark used to determine the quality of sound produced by specific codecs is the mean opinion score (MOS). Table 5-3 shows the relationship between codecs and MOS scores [80].

Table 5-3: Codec MOS values

Codec	Mean opinion score (MOS)
G.711 (ISDN)	4.1
G.729	3.92
G.723.1 r63	3.9
G.726 ADPCM	3.85
G.729a	3.7
G.723.1 r53	3.65

Figure 5-2 shows the MOS of each codec obtained by the proposed cloudified system. The cloudified model met the expectations of each codec related to MOS issues. The system shows average of 3.72 as mean MOS for all codecs. Individually, G.729 offered the highest MOS' average score (3.87) while both G.711 codec schemes offered the maximum MOS score (4.37). Also the minimum MOS score offered by G.711 codec scheme.

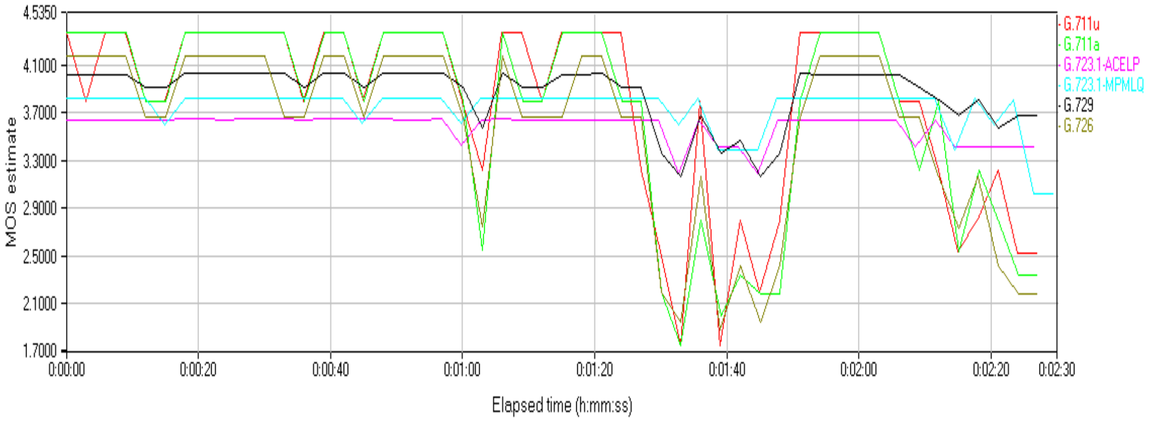


Figure 5-2: VoIP MOS

5.3.3 One-Way Delay

In real-time bidirectional communications keeping the end to end delay low is very important. Excessive end to end delay in voice communication have two side-effects:

• Echo: it is caused by the signal reflections of the speaker's voice from the far-end telephone equipment back into the speaker's ear.

• Talk overlap or Hello effect: it is the problem of one talker stepping on the other talker's speech.

The end to end delay is the sum of delays derived by multiple sources:

• Accumulation delay: it is caused by the need to collect a frame of voice samples to be processed by the voice codec. It is related to the type of codec used.

• Processing delay: is a function of both processing power and codec used. It is the time needed to encode and collect the encoded frames into a single network packet. Often multiple encoded frames are collected in a single packet to reduce the packet network overhead.

• Network delay: it is caused by the physical medium used to transport the voice data and by the protocols used. It is a function of link capacity and the processing that occurs as the packet transit the network.

• Jitter reduction delay: it is introduced by the procedure used to reduce the effect of jitter.

The International Telecommunication Union (ITU) considers network delay for voice applications in Recommendation G.114. This recommendation defines three ranges of one-way delay as shown in Table 5-4.

Table 5-4: one-way Delay Specifications

Range in Milliseconds	**Description**
0-150	Acceptable for most user applications.
150-400	Acceptable provided that administrators are aware of the transmission time and the impact it has on the transmission quality of user applications.
Above 400	Unacceptable for general network planning purposes. However, it is recognized that in some exceptional cases this limit is exceeded.

These recommendations are oriented for national telecom administrations. Therefore, these are more stringent than when normally applied in private voice networks. When the location and business needs of end users are well-known to the network designer, more delay can prove acceptable. For private networks 200 ms of delay is a reasonable goal and 250 ms a limit. All networks need to be engineered such that the maximum expected voice connection delay is known and minimized [81]. Figure 5-4 shows the one-way delay of each codec scheme on the Cloduified model. The system offer VoIP service with acceptable level of delay [Table (5-4)]. The average delay of the system is 7ms offered by all codec schemes. G.729 presented the highest delay (18 ms). On the other hand G.711 presented the lowest delay of all codecs (2 ms).

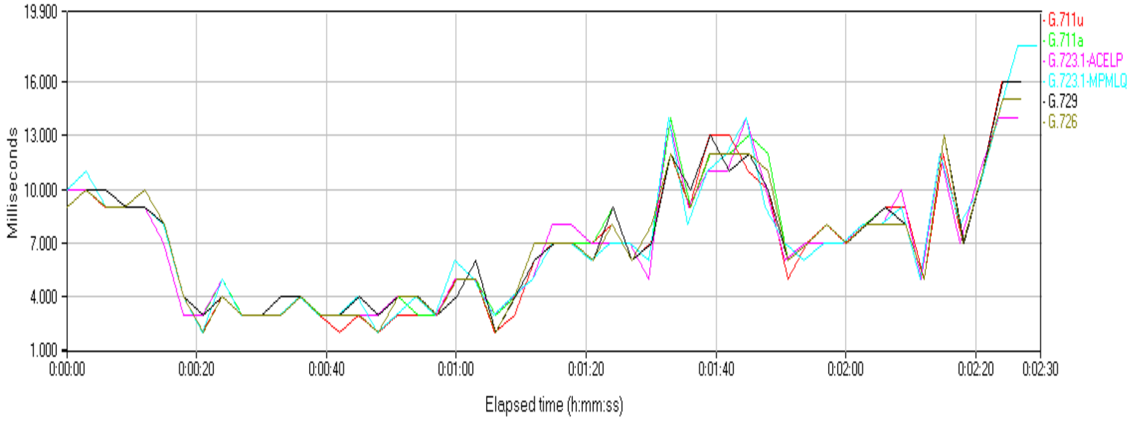


Figure 5-3: VoIP One-Way Delay

5.3.4 Packet loss

Another parameter that influences the quality of the communication is the packet loss percentage. Loss may be caused by discarding packets in IP networks (network loss) or by dropping the packets at the terminal due to late arrival as they do not fit inside the current jitter buffer hence need to be discarded. Network loss is normally caused by large buffers, network congestion, route instability such route change and link failure. Congestion is the most common cause of loss.

VoIP networks typically are designed for very close to 0 percent VoIP packet loss, with the only actual packet loss being due to L2 bit errors or network failures.

Figure 5-4 proved that the proposed system represents a good infrastructure to offer high quality loss free VoIP service. All codec schemes offer lossless data transfer with loss percentage of 0%.

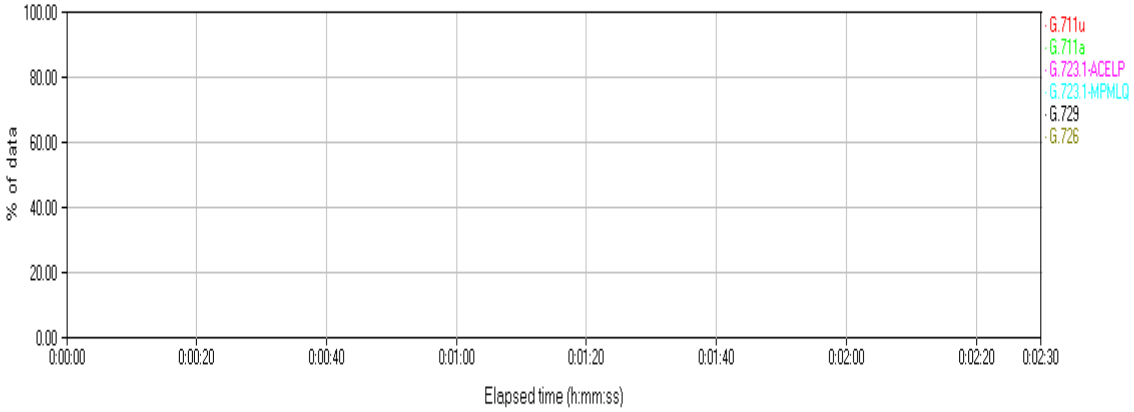


Figure 5-4: Packet loss

5.3.5 Jitter

Jitter is defined as the variance of the one-way delay. When jitter is high, packets arrive in chunks. A jitter buffer is usually used by the receiver to reduce delay variations. Call quality is not affected by jitter fluctuations as long as the jitter buffer can mask fluctuations. Latency constraints, which depend on the codec being used, impose a buffer flush at least 150 ms that usually corresponds to a few packets. Jitter can be controlled by network traffic engineering on routers and firewall, so that a preference path is reserved to voice packets. Nevertheless the de-jittering process, that also includes packet reordering, is usually performed on VoIP terminals.

Figure 5-5 states the jitter results of all codec schemes implemented on the proposed system. Jitter values are very acceptable to deliver a very high quality VoIP services to the end user. The average jitter of the system is 4.01 ms. Codec G.711 has the minimum average jitter with 3.81 ms. Minimum jitter for all codecs is 0 ms while the highest jitter value was 20 ms for codec G.723.1-MPMLQ .All results are based of RFC 1889 jitter.

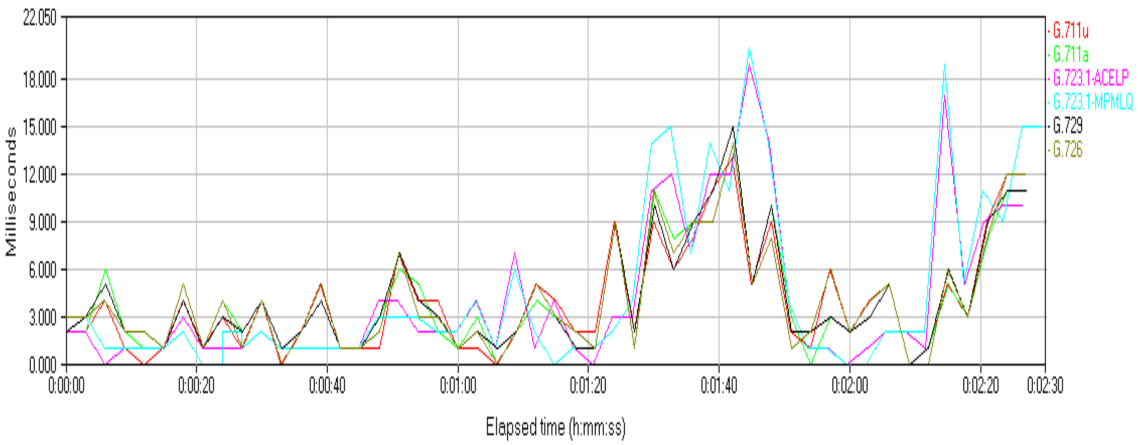


Figure 5-5: Jitter

5.3.6 Analysis

For VoIP, the requirements according to [83] are the following: an end-to-end latency of no more than 150 ms, an average jitter less than 30 ms and a loss smaller than 1 %.

The proposed system met all requirements of delivering a good VoIP service.

5.4 Internet Protocol television (IPTV)

QoS/QoE definitions for IPTV can be found in several sources. The Recommendation ITU-T G.1080 [80] defines user requirements for quality of experience (QoE) for Internet protocol television (IPTV) services. The QoE requirements are defined from an end user perspective and are agnostic to network deployment architectures and transport protocols. The QoE requirements are specified as end-to-end and information is provided on how they influence network transport and application layer behavior. In This testing environment we used MPEG-2 and encoding schemes and data-rates of 3.75 Mbps with different video compression standards.

5.4.1 Throughput

Throughput requirements of IPTV services depend upon encoding scheme used and quality as follows:

For MPEG-2 to deliver SD quality the data rate required is 3-4 Mbps and for HD is 16-20 Mbps. For HD quality the data rate required for SD quality is 2-3 Mbps and for HD is 8-10 Mbps.

Figure 5-6 shows the throughput testing results of MPEG-2 compression standards. All standards haves almost similar average throughput rate with 3.49 Mbps. Although, H263QCIF video compression standard has the highest throughput with 3.790 Mbps while H263CIF has the lowest throughput with 2.815 Mbps.

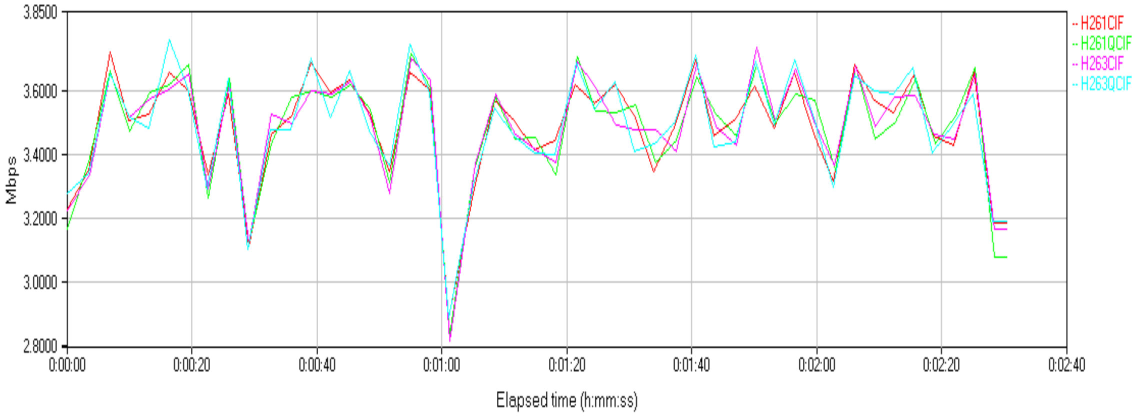


Figure 5-6: IPTV Throughput

5.4.2 One-Way Delay

For video streaming services, network delay can impact end-user “interactivity”, or the “finger-to-eye” delay.

For Broadcast Television services (such as IPTV or Cable TV), the impact that network delay has is on the time it takes for the end user to change from one TV channel to another.

For VOD services the network delay impacts the finger-to-eye delay, i.e. the response time it takes for user requests to be translated into actions visible to the end user.

For video-streaming applications, service providers typically target one-way network delays of less than 100 ms to achieve overall delays of 1 to 2 seconds [81].

Figure 5-7 shows the one-way delay for the standards. All results are below 100ms threshold. The system has average one-way delay of 12ms which is the one-way delay of all compression standards.H263QCIF compression standard has the highest delay among all standards while H263CIF has the lowest one.

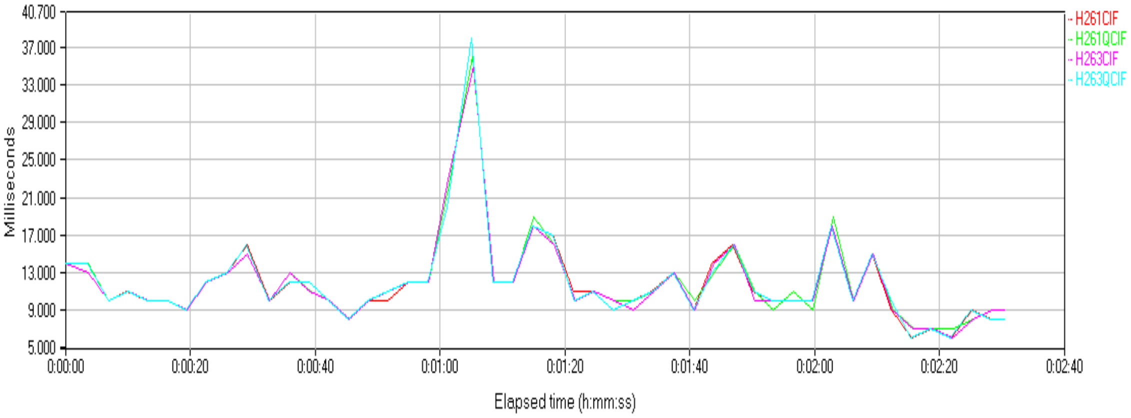


Figure 5-7: IPTV One-Way Delay

5.4.3 Packet loss

Any single unrecovered video packet loss may result in a visual impairment. With compressed video, the effect of even limited packet loss can be significant. Depending upon factors such as the specific encoding and compression scheme, losses of different packet types appear as different types and durations of visual impairment or artefact. With MPEG-4 encoding, impairments resulting from an equivalent duration of packet loss will generally be greater than for MPEG-2.

In practice, networks supporting video streaming services should typically be designed for very close to zero percent video packet loss [81].

Figure 5-8 Shows losses of IPTV packets in the test run on the proposed system. The system has total loss percentage of 6.68% of overall packets sent. H263CIF has the highest lost percentage 6.722 and H261QCIF has the lowest percentage 6.64%.

Figure 5-9 shows the consecutive packets loss. The system consecutive loss is 185 packets in a row.

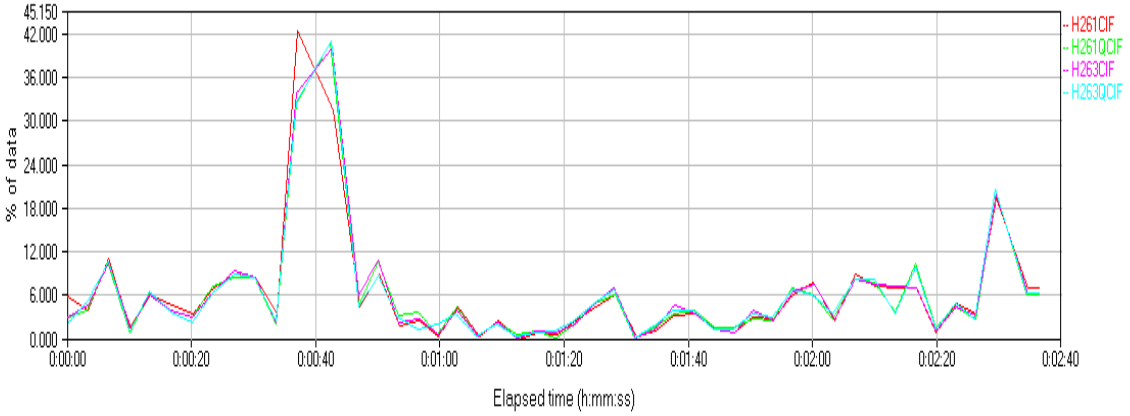


Figure 5-8: IPTV Data Loss

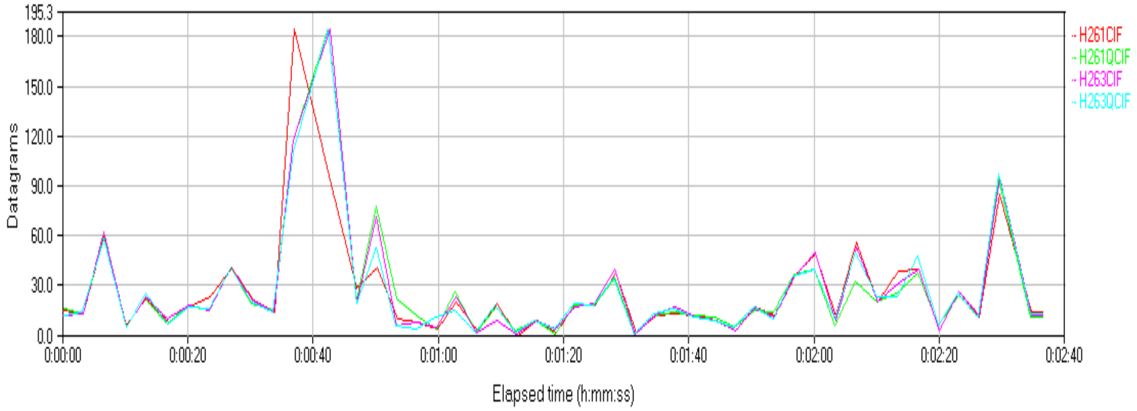


Figure 5-9: consecutive Datagram loss

5.4.4 Jitter

IPTV services are particularly sensitive to delays caused by overloaded servers, routing, network congestion and queuing as the IP video packets traverse the network. The quality of a video signal depends on the delivery of a lossless IP stream at a constant bit rate.

Typical IPTV STBs employ 250-ms jitter buffers so the jitter of the network depend on the buffer size of end user's equipment.

If excessive PCR jitter is present, the decoder cannot synchronize itself correctly to the data stream, resulting in visual impairments, such as pixelization, frame freezes, and loss of color.

Figure 5-10 shows the jitter of the compression standards. The system has overall average jitter of 2.3ms. The highest value of jitter obtained is 82 ms by H263QCIF compression standard.

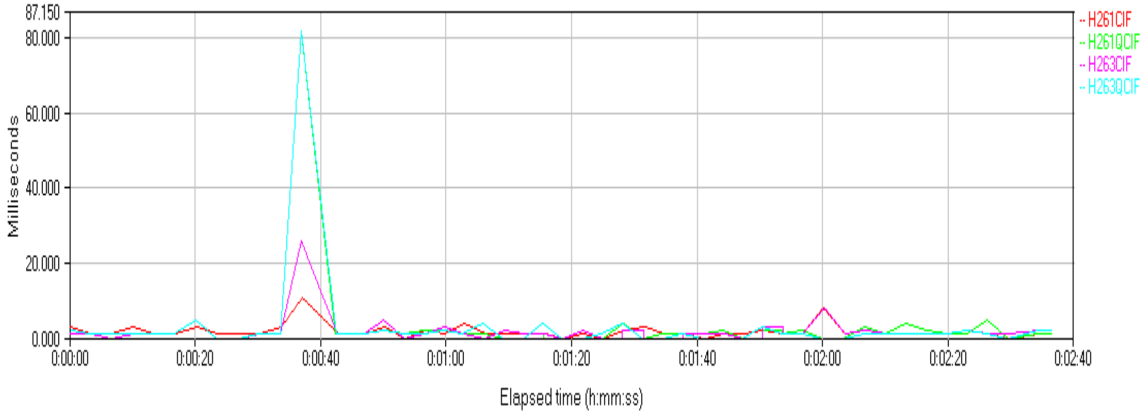


Figure 5-10: Jitter

5.4.5 Delay Factor

The DF is the time difference between the arrival and the drain of the media packets. It takes into account the amount of jitter present in the media stream and provides the necessary buffer required for error-free transmission at the next downstream point. Very large DF values indicate severe jitter in the network, which in turn indicates that the network requires more latency (larger buffers) to compensate for the time needed to fill the buffers before the packets can be sent to the receiver. Networks experiencing high DF and insufficient buffering will eventually experience packet loss due to buffer underflow or overflow conditions further exasperating the poor video quality [82]. In other words, it is a time value indicating how many milliseconds' worth of data the buffers must be able to contain in order to eliminate time distortions.

Figure 5-11 shows the Delay factor of the proposed system. The figure states that the system has DF of 109 ms.

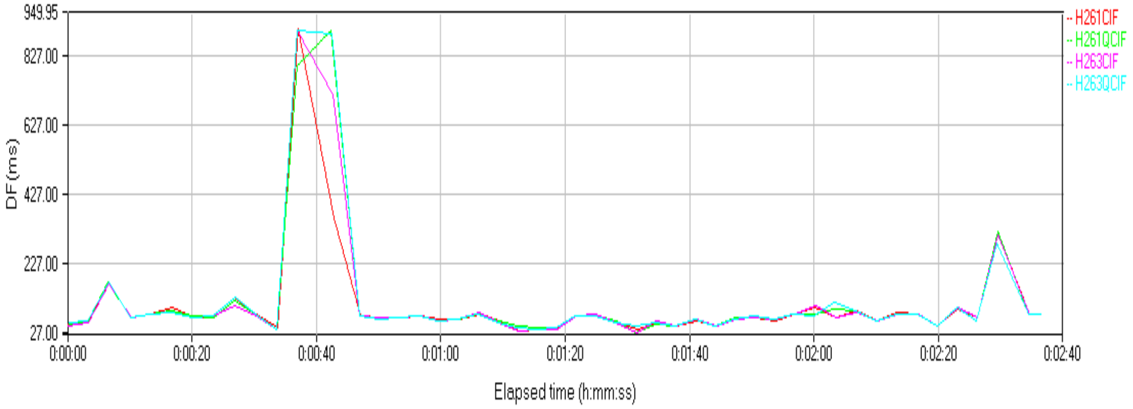


Figure 5-11: Delay factor

5.4.6 Media Loss Rate

The MLR is the number of lost or out-of-order flow packets counted over a period of time. It is important to include out-of-order packets in the MLR metric, as many stream consumer-type devices do not rearrange the order of packets received out of order. Therefore, any lost or out-of-order packets will introduce errors and visible distortions to the media stream, which may be perceptible to the end viewer. This fact makes the MLR component of MDI (Media Delivery Index) a popular measure for service level agreements (SLAs), as it is a much better indicator of network and video quality issues than a simple mean opinion score (MOS) [82].

Figure 5-12 shows the MLR of the proposed system. The results indicates that is the system has MLR of 139.6 (frame/sec)

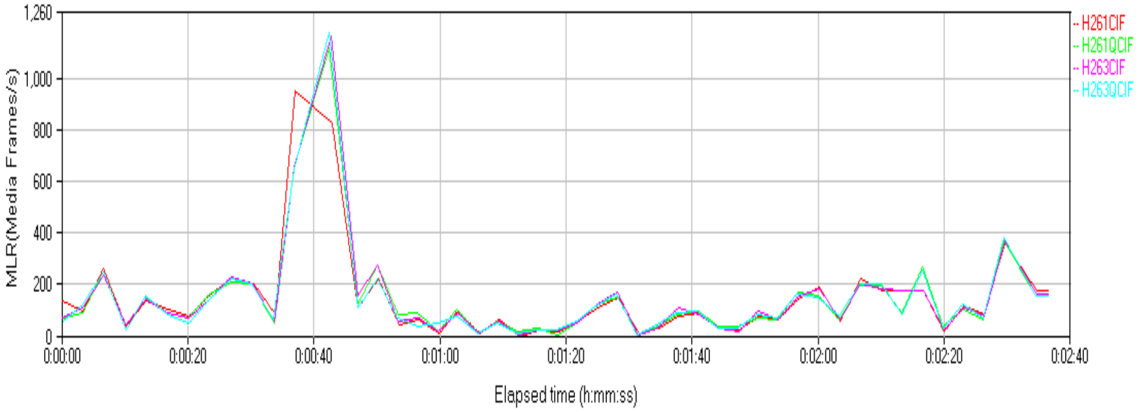


Figure 5-12: Media Loss Rate

5.4.7 Analysis

For streaming video, the loss must not exceed 5% and latency should be no greater than 4-5 seconds (depending on the video application buffering capabilities) [83].

The proposed system met the expectations of IPTV service except for losses related requirement. This problem could be solved using different video codec or other error tolerant application layer coding mechanisms such as Erasure Coding. Also adopting QoS policies related to queuing could help reducing the affection of packet loss.

5.5 Internet Access

According to the ITU: ‘Recommendations ITU-T Y.1540 and Y .15412together provide the parameters needed to capture the performance of IP networks, and specify a set of "network QoS" classes with end-to-end objectives specified. It is widely accepted (i.e., beyond the ITU-T) that the network QoS classes of Recommendation ITU-T Y.1541 should be supported by next generation networks, and thus by networks evolving into NGNs.

ITU-T G.1030 provides a model for estimating the performance of data applications over Internet Protocol (IP) networks. ‘This model consists of three steps: 1) network performance assessment, 2) application performance assessment, and 3) perceptual performance assessment. The third step is the one that introduces the idea of user experience (perception). This can be viewed as an “opinion model” which maps end user experience from the network layer up to the application layer. The recommendation includes a model for Web browsing, but other applications are left for further study. On the topic of web browsing, currently the ITU has Quality of Experience for further study in Study Group ITU-T SG 12 with provisional name: G.QoE-Web.

4.5.1 Network Performance

The network performance for internet access services depends on the user profile applied on access layer port. It defines the maximum throughput that user can get.

Figure 5-13 shows the download and upload speeds of the proposed system. The graph state that the maximum download speed is 35.65 Mbps and upload speed is 19.4 Mbps. the user profile applied is 45 Mbps for the download and 20 Mbps for the upload.

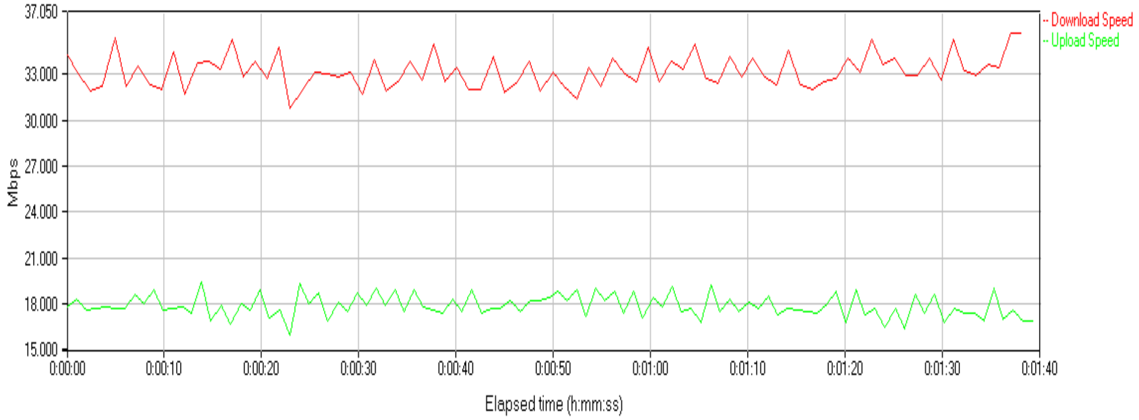


Figure 5-13: Upload and Download Speeds

5.5.2 Application Performance

Application performance could be measured by the response time of the application. The response time could be defined as the length of the time between an indication of the end of an inquiry and the display of the first character of the response at a user terminal.

Figure 5-14 shows the response time for variety of application that cloud be used in web serving. The system has average response time of 0.054 seconds. Secure HTTPs transactions have the highest response time .202 seconds while DNS queries has the lowest response time .0001 seconds.

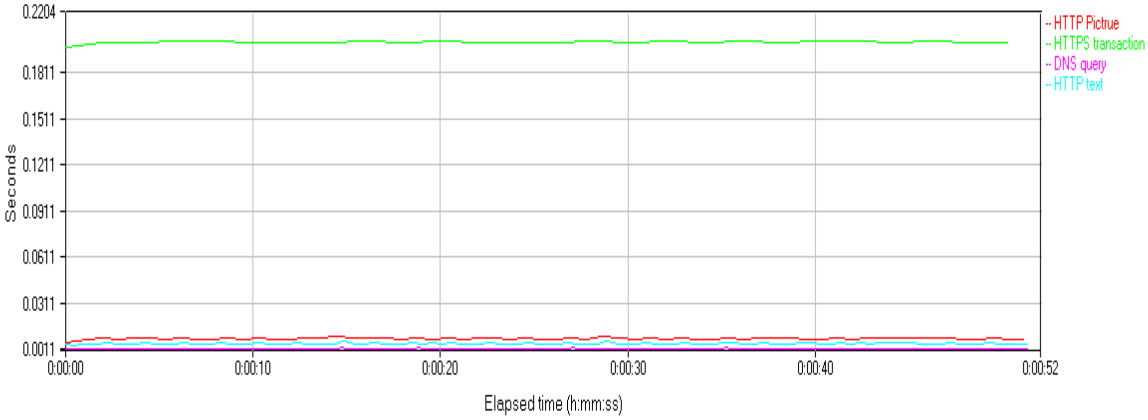


Figure 5-14: Response Time

CHAPTER SIX

CONCLUSIONS AND FUTURE WORK

CHAPTER SIX

CONCLUSIONS AND FUTURE WORK

6.1 Conclusion

Software Defined Networking (SDN) and Network Function Virtualization (NFV) are foreseen as revolutionary technologies in the standardized mobile network architecture. The CSPs' concerns regarding the issues related to cost, network overprovisioning, and complexity and limited performances. On the other hand, SDN and NFV could bring flexibility in controlling architecture components, smart usage of the network resources and intelligent traffic steering, while decreasing the Capital Expenditure (CAPEX) and Operating Expenditure (OPEX) costs. One of the main questions addressed by this work was to investigate which parts of the NGN network can be virtualized and how can SDN technology be smoothly integrated into the access layer of the NGN network. Due to the high increase in IP transit traffic that might lead to inefficient load distribution, and because of its flat Internet Protocol (IP) architecture, the NGN emerged as a suitable candidate for the deployment of NFV and SDN technologies.

In this new NFV / SDN context, the NGN access network can be transformed by employing a more flexible separation between control and user plane. This can be achieved throughout network virtualization of the control functions in the current NGN access layer devices using SDN based access switches. As a result, the user plane can be replaced by OpenFlow switches which are managed by a central entity, called the SDN controller. The main SDN controller could be responsible to proactively install flows in the switches and take routing decisions based on session type, as well as to equally distribute the load in the network. This controller is in charge of aggregating flows aggregation of different users.

Apart from the cost reduction, the most attractive advantages of NFV and SDN technologies are the flexibility in traffic management and congestion mechanisms, which current NGN architecture is lacking of, or require very long standardization process. In the proposed architecture, the traffic can be handled at two levels in the network: at the level of the access layer for groups of access SDN based switches, or it can be performed by the virtualized routers at aggregation layer. Moreover, the traffic steering on the service chaining might be easier done by employing policies dependent on the session type (e.g. Hypertext Transfer Protocol (HTTP), Voice over IP (VoIP) and video) with different bandwidth requirements.

The presented work also involved the validation of triple play services over the cloudified infrastructure. The control functions of NGN network were implemented on the top of the main SDN controller as a control layer that communicates with the controller through the *northbound* interface. The performance of triple play services was validated and presented in Chapter 5. The obtained results revealed that parameters such as loss, packet delay variation and throughput are within the requirements corresponding to the employed session types. Nevertheless, the latency in the controller message processing introduced by the simulation tool (OpenDaylight) might affect the network performance. This can be eliminated by repeating the experiment on physical switches according to the proposed topology. Additionally, the SDN controller and Cisco CSR 1000v features were investigated (OpenDaylight presented in Chapter 4) by comparing their performances as use case in the proposed topology.

6.2 Future Work

This project aimed to focus, apart from the design of a new architecture, on the validation of the triple play services. Nevertheless, the performance can be improved / optimized, for example, by configuring a defined queueing mechanisms on the switch ports. This can be translated in a weighted-fair-queuing scheduler which dynamically adjusts the weights based on the flow size. Moreover, the shortest path module in the controller should be changed to dynamically assign weights on the links based on the load information that it constantly receives from the switches. This would lead to a predefined path with proper bandwidth adjustment for each flow according to its size. A similar approach to this proposal is the Global First Fit scheduler presented in paper [84].

Another important requirement for this architecture is to deploy the full control functionality into the cloud or in the case of standalone elements to build the Open Application Programming Interface (API)s on *Northbound* interface. For instance, running standalone MGC would involve to actually build the *Representational State Transfer (REST) API* interface between MGC and the SDN controller.

Therefore, the benefits of a new control plane with all the network elements running on the top of the controller could be investigated in a further work.

A more careful assessment of how to integrate NFV in the SDN architecture could also be investigated. One of the exploring directions might be the Hypervisors integration with SDN controllers. This can be either deployed in an external cloud, or running on standalone platforms in operators' data centers. Other upcoming technologies such as Internet Protocol version 6 (IPv6), which will definitively challenge operators' deploying strategies can be better supported and more easily configured in the SDN framework.

In this manner, each flow has a certain *flow ID* assigned that simplifies the forwarding process at the switch level. In this manner, we could identify that particular flow in the network, or aggregate multiple flows in a single bundle. This can constitute as well the premises of a future work in this domain. Virtualization deployments often introduce I/O bottlenecks at various levels of your physical infrastructure and undercut the gains of virtual servers. This may affect real-time applications. So a queuing mechanisms should implemented on hypervisors to avoid these issues. This a new direction of research related to NFV that should be fulfilled.

In order to gather a better insight of the marketing aspects that come along with these new technologies, a product survey must be conducted. This should imply careful assessment of different vendor's products (OpenFlow switches) or software solutions. A useful conclusion to be reached should be, whether it is more cost-effective for operators to buy full solutions, accommodate only some features to their needs, or choose to invest in the OpenFlow hardware.

This would imply to implement their own SDN controllers on specific servers and adopt the cloud virtualization. This survey is meant to be carried out in a different project.

In order to have a complete solution which might actually be adopted by operators, it is very important to consider all the aforementioned aspects. Nevertheless, this thesis primary goal was to envision a first approach on the way to NFV / SDN upcoming technologies.

REFERNCES

[1]Cisco, 'The Zettabyte Era—Trends and Analysis'. [Online]. Available: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/VNI_Hyperconnectivity_WP.html. [Accessed: 24-Nov- 2014].

[2] Cisco; "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2013 –2018", 2014.

[3] "ETSI GS NFV 001 v1.1.1," October, 2013.

[4] White Paper, "Network Functions Virtualization, an Introduction, Benefits, Enablers,Challenges and Call for Action." 2012.

[5] Calvin Lo , " DSL and POTS – mixing it up in DLC" 2002 .

[6] C. Hellberg, D. Greene and T. Boyes, Broadband network architectures. Upper Saddle River, NJ: Prentice Hall, 2007.

[7] Himanshu Pandey, Lokesh Gyanchandani ,Santosh Kumar Singh " Channel Zapping Time Reduction Technique For Iptv " , International Technology Research Letters, Volume-1, Issue-1 2012.

[8] Djarallah, N.B. ;Pouyllau, H. ; Le Sauze, N. ; Douville, R. 'Business-driven PCE for inter-carrier QoS connectivity services ' ; Future Network & Mobile Summit (FutureNetw), 2011 .

[9] Maachaoui, M. ; El Kalam, A.A. ; Fraboul, C. ; Ouahman, A.A. Maachaoui, M.; El Kalam, A.A. ; Fraboul, C. ; Ouahman, A.A. "Virtual walled-garden model for IMS services provisioning "; National Security Days (JNS3), 2013.

[10] J. M. Arco, A. García, J. A. Carral, A. Paricio "LAYER 2 VPN ARCHITECTURES AND OPERATION"; Departamento de Automática Universidad de Alcalá .

[11] Lan jun ; Lin bi ying ; "Research for service deployment based on MPLS L3 VPN technology " ; International Conference on Mechatronic Science, Electric Engineering and Computer (MEC), 2011.

[12] FPL FIberNet, LLC ; Alcatel lucent ;"Dedicated Internet Access" ; 2010.

[13] Sylwester Kaczmarek, Magdalena Młynarczuk, Marcin Narloch, and Maciej Sac "The Realization of NGN Architecture for ASON/GMPLS Network" ;2011.

[14] Agilent Technologies;" Understanding DSLAM and BRAS Access Devices"; 2006.

[15] Brett Handley, "Multi-Service Access Nodes (MSANs): Gateways to Next-Generation Network (NGN)"; 2006.

[16] Ed Shrum, David Allan, David Thorne; "Broadband Remote Access Server (BRAS) Requirements Document"; 2004.

[17] W. Wanwu and H. Meizhen, 'Softswitch for the next generation network (NGN)', 2009 Global Mobile Congress, 2009.

[18] Wang, L. ; Agarwal, A. ; Atwood, J.W.;" Description and validation of the media gateway control protocol (MGCP) using SDL/MSC " ; Canadian Conference on Electrical and Computer Engineering, 2001.

[19] Ghazel, C. ; Saidane, L. "Dimensioning of Next Generation Networks Signaling Gateway for Improving a Quality of Service Target "; Second

International Conference on Future Generation Communication and Networking, 2008.

[20]Interexc.com, 'Softswitch - How it works | IXC - VoIP Software developer'. [Online]. Available: http://interexc.com/softswitch-how-it-works. [Accessed: 24- Oct- 2014].

[21] P. Mell and T. Grance, The NIST Definition of Cloud Computing (Draft), Special Publication 800-145 (Draft), National Institute of Standards and Technology, Gaithersburg, Maryland, 2011.

[22] M. L. Badger, T. Grance, R. Patt-Corner, and J. M. Voas, "Cloud Computing Synopsis and Recommendations," NIST Computer Security Division, Tech. Rep., 2012.

[23]R. Moreno-Vozmediano, Montero and I. Llorente, 'IaaS Cloud Architecture: From Virtualized Datacenters to Federated Cloud Infrastructures', Computer, vol. 45, no. 12, pp. 65-72, 2012.

[24] Rake-Revelant, J. ; Holschke, O. ; Offermann, P. ; Bub, U.; “Platform-as-a-Service for business customers ”; 14th International Conference on Intelligence in Next Generation Networks (ICIN), 2010 .

[25] Feng Liu ; Weiping Guo ; Zhi Qiang Zhao ; Wu Chou; “SaaS Integration for Software Cloud ” ; IEEE 3rd International Conference on Cloud Computing (CLOUD), 2010 .

[26] O. Ungureanu, 'Flexible and Programmable Evolved Packet Core: A New SDN-based Model', M.Sc., Delft University of Technology, 2014.

[27] G. Ragoonanan, "Network Virtualization opportunities for CSPS begin in the core of Next-generation networks," http://www.analysysmason.com/About-Us/News/Insight/Network-virtualisation-CSPs-Oct2013-RMA16/, Oct. 2013, [Online; accessed 13 Nov-2014].

[28] NFV White Paper, "Network Functions Virtualization: an Introduction, Benefits, Challenges and Call for Action," 2012.

[29] ETSI GS NFV 001, "Network Functions Virtualization (NFV); Use Cases," 2013.

[30] ONF, "OpenFlow-enabled SDN and Network Function Virtualization (NFV)," 2014.

[31] ONF White Paper, "Software-Defined Networking: The New Norm for Networks," 2012.

[32] ONF, "OpenFlow-enabled Software Defined Networking (SDN) and Network Functions Virtualization," 2014.

[33] B. Salisbury, "OpenFlow: Proactive vs Recative Flows," http://networkstatic.net/ openflow-proactive-vs-reactive-flows/, 2013, [Online; accessed 24-Nov-2014].

[34] Open Networking Foundation (ONF), "OpenFlow Switch Specification, version v.1.4.0," https://www.opennetworking.org/images/stories/downloads/sdn-resources/ onf specifications/openflow/openflow-spec-v1.4.0.pdf, 2013, [Online; accessed 24-Nov 2014].

[35] N. McKeown, “OpenFlow (Or: “Why can’t I innovate in my wiring closet?”),” http://cleanslate.stanford.edu, [Online; accessed 4-Dec-2014].

[36] ETSI GS NFV 001, “Network Functions Virtualisation (NFV); Use Cases,” 2013.

[37] Gelberger, A.; Yemini, N. ; Giladi, R. ;” Performance Analysis of Software Defined Networking (SDN) ” IEEE 21st International Symposium on Modeling, Analysis & Simulation of Computer and Telecommunication Systems (MASCOTS), 2013.

[38] Kempf, J. ; Ying Zhang ; Mishra, R. ; Beheshti, N.;” Zeppelin - A third generation data center network virtualization technology based on SDN and MPLS ”; IEEE 2nd International Conference on Cloud Networking (CloudNet), 2013 .

[39] M. S. G. Hampel and T.Bu, “Applying Software-Defined Networking to Telecom Domain.”Computer Communications Workshops (INFOCOM WKSHPS), April, 2013.

[40] Lahat, A. “The role of MPLS in delivering triple-play services”; Optical Fiber Communication Conference, 2006 and the 2006 National Fiber Optic Engineers Conference; OFC 2006.

[41] Xiaogang Tu ; Xin Li ; Jiangang Zhou ; Shanzhi Chen; “Splicing MPLS and OpenFlow Tunnels Based on SDN Paradigm ” ; IEEE International Conference on Cloud Engineering (IC2E), 2014.

[42] John, W. ;Kern, A. ; Kind, M. ; Skoldstrom, P. ; Staessens, D. ; Woesner, H.; “Splitarchitecture: SDN for the carrier domain ”; Communications Magazine, IEEE (Volume:52 , Issue: 10) ;2014.

[43] M. Al-Fares, S. Radhakrishnan, B. Raghavan, N. Huang, and A. Vahdat, “Hedera: DynamicFlow Scheduling for Data Center Networks,” in *NSDI*, vol. 10, 2010, pp. 19–19.

[44] Josep Batall´e, Jordi Ferrer Riera, Eduard Escalona and Joan A. Garc´ıa-Esp´ın ; “On the implementation of NFV over an OpenFlow infrastructure: Routing Function Virtualization” IEEE SDN for Future Networks and Services (SDN4FNS), 2013.

[45] Ruobin Zheng ; Wenle Yang “H-MPLS: A lightweight NFV-based MPLS solution in access network ”; IEEE 11th Consumer Communications and Networking Conference (CCNC), 2014.

[46] Ruobin Zheng; Wenle Yang ; Jun Zhou; “Future access architecture: Software-defined accesss networking ”; IEEE 11th Consumer Communications and Networking Conference (CCNC), 2014 .

[47] DON REVELLE ,“Hypervisors And Virtual Machines Implementation Insights On The X86 Architecture”, USENIX, Volume 36, Number 5, 2011.

[48] S. Chu, “vSphere Product Marketing,” 2013.

[49] VMware, “VMware workstation 10 documentation center,” http:// pubs.vmware.com/workstation-10/index.jsp#com.vmware.ws.using.doc/ GUID-BAFA66C3-81F0-4FCA-84C4-D9F7D258A60A.html, 2013, [Online; accessed 2-DEC-2014].

[50]Cisco, 'Cisco CSR 1000V Series Cloud Services Router Software Configuration Guide'. [Online]. Available: http://www.cisco.com/c/en/us/td/docs/routers/csr1000/software/configuration/csr1000Vswcfg.html. [Accessed: 02- Dec- 2014].

[51] Cisco Cloud Services Router 1000V with Cisco IOS-XE® Software Release3.10,“http://www.cisco.com/c/en/us/products/collateral/routers/cloud-services-router-1000v-series/qa_c67-729558.html “, [Online; accessed: 2-DEC-2014].

[52]Cisco, 'Cisco CSR 1000V Series Cloud Services Router Release Notes'. [Online]. Available: http://www.cisco.com/c/en/us/td/docs/routers/csr1000/release/notes/csr1000v_3Srn.html. [Accessed: 17- Sep- 2014].

[53]Opencloudblog.com, 'Switching Performance – Connecting Linux Network Namespaces | Open Cloud Blog', 2013. [Online]. Available: http://www.opencloudblog.com/?p=96,2013. [Accessed: 03- Dec- 2014].

[54]6WIND, '6WIND Press Release November 5', 2014. [Online]. Available: http://www.6wind.com/news-events/press-releases-2014/6wind-press-release-november-5. [Accessed: 28- Dec- 2014].

[55]Yuba.stanford.edu, 'List of OpenFlow Software Projects'. [Online]. Available: http://yuba.stanford.edu/~casado/of-sw.html. [Accessed: 03-Dec- 2014].

[56]Opendaylight.org, 'Technical Overview | OpenDaylight'. [Online]. Available: http://www.opendaylight.org/project/technical-overview. [Accessed: 05- Dec- 2014].

[57]Cisco, 'Catalyst 3750 Metro Switch Software Configuration Guide, 12.2(58)SE'. [Online]. Available: http://www.cisco.com/c/en/us/td/docs/switches/metro/catalyst3750m/softwa

re/release/12-2_58_se/configuration/guide/3750metro_scg.html. [Accessed: 04- Dec- 2014].

[58] Cisco, Cisco IOS Software Configuration Guide, [Online]. Available:

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SY/configuration/guide/sy_swcg/eompls.pdf; [Online; accessed 4-Dec-2014].

[59]H3c.com, 'H3C - Technical Support - Layer 2 - LAN Switching Configuration Guide'. [Online]. Available: http://www.h3c.com/portal/Technical_Support___Documents/Technical_Documents/Switches/H3C_5820X_Series_Switches/Configuration/Operation_Manual/H3C_S5820X%5BS5800%5D_CG-Release_1110-6W103/03/. [Accessed: 07- Nov- 2014].

[60] cisco, IEEE 802.1Q-in-Q VLAN Tag Termination, 2008.

[61] Huawei, “VLAN and QinQ Technology White Paper”, 2012.

[62] Carpenter, B "Middleboxes: Taxonomy and Issues". *RFC 3234;* (2002).

[63] R. Wallner and R. Cannistra, “An SDN Approach: Quality of Service using Big Switch’s Floodlight Open-source Controller,” *Proceedings of the Asia-Pacific Advanced Network*, vol. 35, pp. 14–19, 2013.

[64] ONF, “OpenFlow Configuration and Management Protocol,” https://www. opennetworking.org/standards/of-config, 2013, [Online; accessed 24-Nov-2014].

[65] M. Weldon, “Alcatel-Lucent Cloud: NFV, the New Virtual Reality,” http://fr.slideshare.net/Alcatel-Lucent/alcatel-lucentcloudcloud-bandnfvmarcusweldon, 2013, [Online; accessed24-Nov-2014].

[66] Open vSwitch, “Open Virtual Switch,” http://openvswitch.org/, 2013, [Online; accessed 24-Nov-2014].

[67] Reza Vaez-Ghaemi; “Next-Generation Packet-Based Transport Networks (PTN)”; 2010.

[68] M. Al-Fares, S. Radhakrishnan, B. Raghavan, N. Huang, and A. Vahdat, “Hedera: Dynamic Flow Scheduling for Data Center Networks.” in *NSDI*, vol. 10, 2010, pp. 19-19.

[69] A. R. Curtis, J. C. Mogul, J. Tourrilhes, P. Yalagandula, P. Sharma, and S. Banerjee, “DevoFlow: scaling flow management for high-performance networks,” in *ACM SIGCOMM Computer Communication Review*, vol. 41, no. 4. ACM, 2011, pp. 254–265.

[70] A. Tootoonchian and Y. Ganjali, “Hyperflow: a distributed control plane for openflow,”in *Proceedings of the 2010 internet network management conference on Research on enterprise networking*. USENIX Association, 2010, pp. 3–3.

[71] Y. Zhang, “An adaptive flow counting method for anomaly detection in SDN,” in Proceedings of the ninth ACM conference on Emerging networking experiments and technologies. ACM, 2013, pp. 25–30.

[72] “sFlow,” http://blog.sflow.com/2013/01/load-balancing-lagecmp-groups.html/, [Online; accessed 4-Dec-2014].

[73] R. Sherwood, G. Gibb, K.-K. Yap, G. Appenzeller, M. Casado, N. McKeown, and G. Parulkar, “Flowvisor: A network virtualization layer,” 2009.

[73] ITU-T Recommendation P.10/G.100 (2006) Amendment 2: ‘Vocabulary for performance and quality of service’, International Telecommunications Union, 2008.

[74]H. Batteram, G. Damm, A. Mukhopadhyay, L. Philippart, R. Odysseos and C. Urrutia-Valdés, 'Delivering quality of experience in multimedia networks', Bell Labs Tech. J., vol. 15, no. 1, pp. 175-193, 2010.

[75]L. Malfait, J. Berger and M. Kastner, 'P.563;The ITU-T Standard for Single-Ended Speech Quality Assessment', IEEE Transactions on Audio, Speech and Language Processing, vol. 14, no. 6, pp. 1924-1934, 2006.

[76] ITU-T Recommendation P.861, “Objective quality measurement of telephone-band (300-3400 hz) speech codecs”. ITU International Telecommunication Union, 1998.

[77] ITU-T Recommendation P.862. Perceptual evaluation of speech quality (pesq): An objective method for end-to-end speech quality assessment of narrow-band telephone networks and speech codecs. ITU International Telecommunication Union, 2001.

[78]Cisco, 'Understanding Codecs: Complexity, Hardware Support, MOS, and Negotiation'. [Online]. Available: http://www.cisco.com/en/US/tech/tk1077/technologies_tech_note09186a00800b6710.shtml#mos. [Accessed: 18- Dec- 2014].

[79]Cisco, 'Understanding Delay in Packet Voice Networks'. [Online]. Available: http://www.cisco.com/c/en/us/support/docs/voice/voice-quality/5125-delay-details.html. [Accessed: 17- Dec- 2014].

[80] ITU-T Recommendation G.1080: ‘Quality of experience requirements for IPTV services’, International Telecommunications Union, 2008.

[81]Cisco, 'IP/MPLS Networks: Optimize Video Transport for Service Providers'. [Online]. Available: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-next-generation-network-ngn-video-optimized-transport/white_paper_c11-637031.html. [Accessed: 12- Dec- 2014].

[82] Reza Vaez-Ghaemi; “IP Video Test in Transport Networks”,2008.

[83]T. Szigeti, End-to-end QoS network design. Indianapolis, IN: Cisco Press, 2013.

[84] ONF, “OpenFlow-enabled SDN and Network Function Virtualization (NFV),” 2014.

[85]Cisco, 'Carrier Ethernet'. [Online]. Available: http://www.cisco.com/web/IN/solutions/sp/network_infrastructure/carrier_ethernet.html. [Accessed: 17- Dec- 2014].

[86]Ngnlab.eu, 'NGN Layers'. [Online]. Available: http://ngnlab.eu/index.php/ngn-knowledgebase/ngn-architecture/layers-ngn. [Accessed: 13- Dec- 2015].

[87]Theregister.co.uk, 'NFV: All your basestations are belong to us'. [Online]. Available: http://www.theregister.co.uk/2013/12/09/feature_network_function_virtualisation. [Accessed: 17- Dec- 2014].

APPENDIX A –vPE1 Configuration

```
Current configuration : 1406 bytes
!
! Last configuration change at 18:56:37 UTC Sun Dec 28 2014
!
version 15.3
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
platform console virtual
platform hardware throughput level 50000
!
hostname vPE1
!
boot-start-marker
boot-end-marker
!
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
enable password cisco
!
no aaa new-model
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
multilink bundle-name authenticated
password encryption aes
!
!
!
!
!
!
!
spanning-tree extend system-id
!
!
redundancy
 mode none
!
!
!
!
!
!
ip tftp source-interface GigabitEthernet0
!
!
!
!
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.0
!
interface GigabitEthernet1
 ip address 192.168.12.1 255.255.255.0
 negotiation auto
 mpls ip
!
interface GigabitEthernet2
 no ip address
 negotiation auto
 no keepalive
 xconnect 3.3.3.3 200
encapsulation mpls
!
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
!
router ospf 1
 router-id 1.1.1.1
 network 1.1.1.0 0.0.0.255 area 0
 network 192.168.12.0 0.0.0.255 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
control-plane
!
line con 0
 logging synchronous
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 password cisco
 login
!
end
```

APPENDIX B–vP Configuration

```
Current configuration : 1406 bytes
!
! Last configuration change at 18:56:37 UTC Sun Dec 28 2014
!
version 15.3
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
platform console virtual
platform hardware throughput level 50000
!
hostname vP
!
boot-start-marker
boot-end-marker
!
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
enable password cisco
!
no aaa new-model
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
multilink bundle-name authenticated
password encryption aes
!
!
!
!
!
!
!
spanning-tree extend system-id
!
!
redundancy
 mode none
!
!
!
!
!
!
ip tftp source-interface GigabitEthernet0
!
!
!
!
!
interface Loopback0
 ip address 2.2.2.2 255.255.255.0
!
interface GigabitEthernet1
 ip address 192.168.12.2 255.255.255.0
 negotiation auto
 mpls ip
!
interface GigabitEthernet2
ip address 192.168. 23.2 255.255.255.0
 negotiation auto
 mpls ip
!
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
!
router ospf 1
 router-id 3.3.3.3
 network 3.3.3.0 0.0.0.255 area 0
 network 192.168.0.0 0.0.255.255 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
control-plane
!
line con 0
 logging synchronous
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 password cisco
 login
!
end
```

APPENDIX C–vPE2 Configuration

```
Current configuration : 1406 bytes
!
! Last configuration change at 18:56:37 UTC Sun Dec 28 2014
!
version 15.3
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
platform console virtual
platform hardware throughput level 50000
!
hostname vP
!
boot-start-marker
boot-end-marker
!
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
enable password cisco
!
no aaa new-model
!
!
!
!
!

!
!
!
!
!
!
!
!
!
!
!
multilink bundle-name authenticated
password encryption aes
!
!
!
!
!
!
!
spanning-tree extend system-id
!
!
redundancy
 mode none
!
!
!
!
!
!
ip tftp source-interface GigabitEthernet0
!
!
!
!
!
interface Loopback0
 ip address 3.3.3.3 255.255.255.0
!
interface GigabitEthernet1
 ip address 192.168.23.3 255.255.255.0
 negotiation auto
 mpls ip
!
interface GigabitEthernet2
no ip address
 negotiation auto
 no keepalive
 xconnect 1.1.1.1 200 encapsulation mpls
!
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
!
router ospf 1
 router-id 2.2.2.2
 network 2.2.2.0 0.0.0.255 area 0
 network 192.168.0.0 0.0.255.255 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
control-plane
!
line con 0
 logging synchronous
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 password cisco
 login
!
end
```