Network Slicing System Supporting Ultra Reliable Low Latency Connectivity in 5G

Abraham Kwabena Afriyie

School of Science

Thesis submitted for examination for the degree of Master of Science in Technology.
Espoo November 23, 2018

Thesis supervisor:

Prof. Raimo Kantola

Thesis advisor:

Dr. Jose Costa-Requena
Author: Abraham Kwabena Afriyie
Title: Network Slicing System Supporting Ultra Reliable Low Latency Connectivity in 5G
Date: November 23, 2018
Language: English
Number of pages: 8+49
Department of Communication and Networking
Professorship: ELEC3029 - Communications Engineering
Supervisor: Prof. Raimo Kantola
Advisor: Dr. Jose Costa-Requena

Network slicing has been considered as a key feature for the 5G network segmentation. The network slicing concept aims to bring efficient utilization of network resources, flexibility in network deployment and support for fast growing applications and services. Current LTE mobile networks cannot deal with the growing amount of data traffic due to the insufficient capacity and lack of network flexibility.

The purpose of this project was to design, develop and implement a testbed that demonstrates how network physical resources can be sliced dynamically to support Ultra Reliable Low Latency connectivity in a 5G network. The design is for TAKE5 testbed (www.take-5g.org) which is built on top of X-Network LTE network located in Aalto campus for easy integration. The project concentrates only on Radio Access Network (RAN) and backhaul network slicing. EPC slicing is not considered for the thesis.

The project intends to make network slicing clear by first designing and further implementing the concept by making use of practical network devices that support virtualization to provide isolation between slices. Indoor base stations (eNBs) as well as multiple virtual Evolved Packet Cores (vEPCs) were also used in the implementation. The implementation was tested, and the results compared with already existing network slicing outcomes.

Keywords: Network Slicing, URLLC, SDN, Latency, Reliability, LTE
Preface

This master’s thesis work is part of a mobile network utilizing LTE technology called NetLeap built cooperatively by Nokia and Aalto University since 2014.

I would like to thank my supervisor, Prof. Raimo Kantola (Aalto University) for providing me the opportunity and great guidance during the writing of this master’s thesis. Sincere thanks and gratitude to my advisor, Dr. Jose Costa-Requena for his help and good guidance during the development and implementation of this thesis. I also want to give thanks to Aalto IT especially Niko Suominen for all the support during the implementation of this thesis.

Finally, I would like to present my deepest gratitude to my family whose love and continuous support made me capable to reach what i am today. Above all, thanks for always believing in me and helping me through difficult times.

Otaniemi, 23.11.2018

Abraham K. Afriyie
# Contents

## Abstract

## Preface

## Contents

## Abbreviations

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Introduction</td>
<td>1.1 Motivation</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>1.2 Objective and scope of thesis</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>1.3 Use cases</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>1.4 Methodology</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>1.5 Structure</td>
<td>5</td>
</tr>
<tr>
<td>2 Background</td>
<td>2.1 LTE Base station</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>2.1.1 Capabilities and limitations</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>2.2 Packet transport technologies</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>2.2.1 Ethernet</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>2.2.2 Carrier Grade Ethernet</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>2.2.3 Multiprotocol Label Switching (MPLS)</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>2.3 Network virtualization</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>2.3.1 Use cases</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>2.4 Redundancy in networks</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>2.5 Delay in networks</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>2.6 Network slicing as defined by 3GPP</td>
<td>13</td>
</tr>
<tr>
<td>3 Testbed transport slicing</td>
<td>3.1 Requirements</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>3.2 Testbed components</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>3.3 Testbed transport slicing design</td>
<td>22</td>
</tr>
<tr>
<td>4 Testbed implementation</td>
<td>4.1 Base station configuration</td>
<td>28</td>
</tr>
<tr>
<td></td>
<td>4.2 VLAN creation and node virtualization</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>4.3 vEPC setup</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td>4.4 Quality of Service</td>
<td>31</td>
</tr>
<tr>
<td></td>
<td>4.5 User Equipment (UE) configuration</td>
<td>34</td>
</tr>
<tr>
<td>5 Results and discussion</td>
<td>5.1 Abstraction and isolation</td>
<td>35</td>
</tr>
<tr>
<td></td>
<td>5.1.1 Abstraction</td>
<td>35</td>
</tr>
<tr>
<td></td>
<td>5.1.2 Isolation</td>
<td>36</td>
</tr>
<tr>
<td></td>
<td>5.2 Slice testing and measurements</td>
<td>37</td>
</tr>
</tbody>
</table>
5.2.1 Discussion of results ........................................... 40
5.3 Limitations ......................................................... 41
  5.3.1 Hardware .................................................... 41
  5.3.2 Broadband management protocol (BMP) .............. 41
5.4 Future Work (X-Network) ....................................... 42

6 Conclusion .......................................................... 43

References .................................................................. 44

A Appendix .................................................................. 49
List of Figures

Figure 1: Basic Network Virtualization components. Reprinted from [22]. 10
Figure 2: Network Delay Types. Reprinted from [27]. .................... 13
Figure 3: 3GPP Release 14 5G System Architecture, RAN only. Reprinted from [32]. ......................................................... 14
Figure 4: Non-Roaming 5G System Architecture. Reprinted from [34]. 14
Figure 5: 3GPP 5G Core Architecture, Non-Roaming Scenario. Reprinted from [32]. ......................................................... 15
Figure 6: Example of Network Slices. Reprinted from [28]. ............ 16
Figure 7: 8615 Smart Router front Panel. Reprinted from [38]. ....... 19
Figure 8: MX204 Front Panel Ports, LEDs, and Buttons. Reprinted from [39]. ......................................................... 20
Figure 9: Flexi Zone Indoor Pico module Interfaces. Reprinted from [40]. 21
Figure 10: 8000 INM uses IP addresses to connect to 8615 NEs over TCP/IP or UDP/IP. Reprinted from [41]. .............................. 22
Figure 11: Designed Transport Network overview. ....................... 24
Figure 12: Example Slice in Figure 11. .................................. 26
Figure 13: Deployment setup. ............................................. 27
Figure 14: Single hop data path virtualization. Reprinted from [45]. 30
Figure 15: Cumucore virtual EPC Setup: Reprinted from [46]. ...... 31
Figure 16: Virtual Network (slice) configuration. ....................... 38
Figure 17: Measured delay in virtual network with PLMN ID 24438. 39
Figure 18: Measured delay in virtual network with PLMN ID 24439. 39
Figure 19: Measured Throughput against different MTUs. ............ 40
Figure A1: Measured throughput for slice 1 with PLMN ID 24438 ...... 49
Figure A2: Measured throughput for slice 2 with PLMN ID 24439 ...... 49
Figure A3: E2E measured delay for slice 1 between UE and UPF. .... 50
Figure A4: E2E measured latency for slice 2 between UE and UPF. 50
Figure A5: Latency measured for first slice 1 between UPF and eNB. 51
Figure A6: Measured latency for slice 2 between UPF and eNB. .... 51
Figure A7: Throughput measured when MTU is 100 bytes ............ 52
Figure A8: Throughput measured when MTU is 200 bytes .......... 52
Figure A9: Throughput measured when MTU is 500 bytes .......... 53
Figure A10: Throughput measured when MTU is 1000 bytes ......... 53
Figure A11: Throughput measured when MTU is 1500 bytes ......... 54
List of Tables

Table 1: 8615 Smart Router Supported DiffServ PSCs/PHBs. Reprinted from [47]. .................................................. 32
Table 2: Coriant 8615 Routers Default QoS Mapping Table. Reprinted from [47]. .................................................. 33
Table 3: Measurements performed on each slice. .............................. 40
Abbreviations

(R)AN 5G RAN
3GPP 3rd Generation Partnership Project
5G Fifth Generation
5GC 5G Core network
AF Application Function
AMF Core Access Mobility Management
AN Access Network
AUSF Authentication Server Function
CCNF Common Control Network Function
CP Control Plane
CPF Control Plane Function
DN Data Network
E2E End-to-End
EPC Evolved Packet Core
Gb Gigabit
GTP GPRS Tunneling Protocol
IMSI International Mobile Subscriber Identity
INM Intelligent Network Manager
IP Internet Protocol
LTE Long-Term Evolution
MTC Machine Type Communication
NEF Network Exposure Function
NF Network Functions
NRF NF Repository Function
NSSF Network Slice Selection Function
PCF Policy Control Function
PLMN Public Land Mobile Network
QoS Quality of Service
RAN Radio Access Network
SCNF Specific Control Network Function
SDN Software Defined Networking
SLA Service Level Agreement
SMF Session Management Function
SNMP Simple Network Management Protocol
UDM Unified Data Management
UE User Equipment
UP User Plane
UPF User Plane Function
URLLC Ultra Reliable Low Latency Connectivity
VR Virtual Router
1 Introduction

This chapter presents the motivation for this thesis and the problems that it aims to resolve. The objective and scope for the thesis is then presented followed by some use cases. After that, the thesis methodology is presented, detailing how the thesis work will be carried out. The chapter then ends with the structure of the rest of the thesis, detailing how the rest of the thesis will be presented.

1.1 Motivation

Present LTE network provide mobile users with much resources, the 5G, currently being standardized is expected to provide improved network resources and support many services including critical communication services that require ultra reliable low latency connectivity (URLLC). Services such as industrial automation and control, real-time operation of smart electrical power grid, etc require the provision of an ultra-reliable communication network. Furthermore, URLLC services typically require reliable data transmission. These services have been identified in a variety of fields, however, the common requirement among them is low latency combined with high reliability [1]. Latency performance in the past generations of mobile networks have improved significantly but this improvement does not meet the requirements of URLLC services. Building a specific low latency network has still been a major problem. These problems come from the basic variety of network latency causes such as queuing which involves assigning packets to one of the several interface queues based on classification, packet processing, transmission, etc [2, 3].

Achieving high reliability and low latency at the same time may be challenging to accomplish in cellular network. The problem resides in the low layer protocols where the mechanisms of acknowledgements or lack of acknowledgement that trigger the packet resending are used to ensure delivery of a frame or packet. This adds jitter and delay to the network. Therefore, packets or frames that are delivered at the first attempt experience minimal latency while packets or frames that because of radio fading needed one or more resending experience a significantly higher latency.

Generally, high reliability is achieved using redundancy in time, in data or in hardware. An example of redundancy in time is resending a lost packet. An example of data redundancy is having a checksum in each frame or packet or using fountain coding. Data redundancy tends to add delay in the network. The most common hardware redundancy schema is duplication where some piece of hardware such as a processor, a power unit or a whole network node is duplicated. When targeting high reliability, we can rely on a well understood discipline called reliability engineering. It advises to identify the sources and locations of failures, choose the most risky places, apply some replication to eliminate the problem, check whether the target level has been reached, if not carry on adding more redundancy to address the next most risky spot etc.
Low latency in 5G is achieved due to the new 5G radio that by its design will deliver packets with low delay. In addition, the backhaul network from the base stations to the edge of the Internet must provide sufficient capacity. For example, by running fiber to each base station for example 10Gbit/s Ethernet and using high capacity switches and routers in the backhaul network, we can avoid introducing significant additional delay in the backhaul network to the packets. Delay in the backhaul network is a matter of providing sufficient capacity, i.e. engineering of the network. Low delay in the radio part is a matter of radio system and air interface protocol design. [4]

Network slicing and network virtualization have been some of the areas being investigated to provide a solution for URLLC services. The 5G network is expected to handle new services with different requirements, therefore developing a “one-size-fits-all” network architecture to handle all of these new services will not be possible. Network slices are required to provide private networks to accommodate these different services or use cases. [5]

Furthermore, network slices are logical isolated end-to-end (E2E) networks running on a common physical or virtual network being independently controlled and managed by an orchestrator. A network slice in [6] is made up of a collection of resources that are properly combined to meet the requirements of the service that such slice support. [7] The E2E slice can comprise of different segments that consists of slices in the access networks, transport and the core. A slice can be configured to meet the requirements such as bandwidth, latency, etc for a specific service or application [8]. Moreover, in a slice environment where a lot of different nodes are involved, a network orchestrator is required to coordinate network processes for creating, managing and delivering services or applications. This thesis will make use of a network orchestrator (Intelligent Network Manager) provided by Coriant to create and coordinate the network nodes to meet the required requirements of a particular service.

Virtualization has been successfully used in computing to achieve an unprecedented level of automation and ease of scaling and consequently reduce costs. Virtualisation related to computing is called cloud computing. In cloud computing all software is packaged and runs either in containers or virtual machines (VM). Both containers and VMs have an IP address and the orchestrator of the cloud can migrate them from one physical machine to another and even to a different data center. This creates a need to control the network layer in the network with software so that no manual configuration on the network is needed while the management of the cloud software is automated. One approach to achieve software control of the network is to use Software Defined Networking (SDN). In SDN the control and data planes are separated and a controller in the control plane can be used to manage the forwarding behaviour of many data plane nodes or switches. SDN is now about 10 years old and is being used in data centers and private networks. Its introduction into wide area is studied and proposed for 5G network. The goal is to reduce costs, the same as in cloud computing.
SDN allows to provision the use of link and node capacity in the network for different use cases and also for individual user flows. A candidate architecture for SDN is OpenFlow, however, it does not find uniform support in the mobile industry. In OpenFlow, data plane consists of Open Flow switches. OF switching is poorly available in hardware that would be suitable for a mobile network. Instead of OpenFlow there are many other protocols that can be used by an orchestrator/controller to manage hardware switches that are suitable for 5G networks and are available today. This is the reason why we have chosen a pragmatic approach in building the 5G test network in Otaniemi. We expect that by using commercial hardware switches we are able to build a stable slicing system while being able to control the network flexibly by software. SDN, however, is not the first time virtualisation is introduced into networking. For example, many types of IP routers support the concept of virtual routers (VR). A VR has its own routing table. An orchestrator is used to assign links or shares in links to each VR. The VR routing table can be formed either using normal dynamic IP routing protocols or also managed by the controller. [4]

This thesis will take advantage of this feature to create separate logical networks using network devices (routers or switches) that support virtualization. The logical separation of the slices will be done by running multiple VLANs in the radio part (eNB) of the network combined with multiple virtual routers (VR) on the network core devices. Each PLMN is mapped to VLAN on the backhaul. Each network core device will be running multiple VRs and the VRs connected by virtual links forming virtual networks. The transport in our case will be segmented into VLANs, therefore, traffic from the eNBs received at access device (Coriant switches) ports are VLAN tagged. The tagged traffic are then segmented using the appropriate VRs. The network controller (8000 Intelligent Network Manager) with user interface directly controls all the functionalities of the core devices. Therefore a network slice or logical network can easily be created. Hence, having multiple segmented networks (slices) each configured with different network service requirements is the proposed solution to provide URLLC.

1.2 Objective and scope of thesis

5G networks are expected to be able to fulfil the different users’ QoS requirements. Network slicing is a technology for 5G networks expected to address the diverse user specific service QoS demands. [8] The objective of this thesis is to design, develop and implement a testbed that demonstrates how network physical resources can be sliced dynamically to support Ultra Reliable Low Latency Connectivity (URLLC) in 5G network. The thesis work concentrates on both Radio Access Network (RAN) and backhaul network slicing. EPC slicing is not considered for the thesis. The proof of concept implementation should show the feasibility of providing a network slicing system using physical network devices that support network virtualization. The implementation is meant as an experimental system which will later be deployed in a real network which will serve as a 5G testbed for research purposes.
The validation of this network slicing system will be done with the deployment in real network located in Aalto Campus. The validation will be done with the upgrade of the current X-Network LTE network into a 5G network to provide URLLC for certain industrial Internet services and applications. The X-Network is a joint initiative between Nokia Networks and Aalto IT. The network is meant for research and development use in mobile environment where users get unlimited usage of network capacity and features for application developments and testing.

The network upgrade will involve the use of routers (8615 smart router) and an Intelligent Network Manager (orchestrator) provided by Coriant. The upgrade will also involve Juniper network devices. These routers support virtualization and therefore can be used to create the required slices. The slices will then be managed and controlled by the 8000 Intelligent Network Manager (INM) provided by Coriant.

Furthermore, the upgrade will include the increase of the number of current network (X-Network) users and coverage to the whole of Aalto University campus as well as opening the network to other research groups and partners. The project is expected to deliver very low latency on fast slices and 10ms latency on other slices for different kinds of services.

1.3 Use cases

The future 5G network is expected not only to support and expand mobile broadband performance but to address many new use cases. These new cases have varying requirements that need to be satisfied by the network while not interfering with each other. The creation of slices is particularly suitable for new machine type communication (MTC) services. These MTC services can be categorized into two different categories, massive MTC services and mission-critical MTC services. Factory automation is one example use case that falls under the mission-critical MTC. Factory automation can provide many possibilities for manufacturers and also help industries to achieve efficient production. Current factory automation is mainly based on wired connectivity. However, efficient and deterministic mobile or wireless connectivity can help provide location flexibility to a large number of factory machines. [9]

Furthermore, the Next Generation Mobile Networks (NGMN) alliance provides many varieties of emerging use cases varying from sensitive to low-latency applications, from best-effort to ultra-reliable applications which relates to health and safety, etc. The NGMN also categorizes these use cases into eight families. These families include broadband access in dense areas (e.g. pervasive video), broadband access everywhere (e.g. 50+ Megabits per second everywhere), higher user mobility (e.g. high-speed trains), massive Internet of Things (e.g. sensor networks), extreme real-time communications (e.g. tactile internet), life-line communications (e.g. natural disaster), ultra-reliable communications (e.g. o-health services) and broadcast-like services (broadcast services). [10]
Though these use cases form only a small part of the many 5G use cases, network slicing will make it possible for service providers to allocate sufficient network resources to meet the different requirements for each use case.

1.4 Methodology

The thesis work is carried out in three steps. First, a literature study is carried out on existing network slicing solutions. Current specification of network slicing is studied, and the definition of the network slicing concept is examined. A network slicing implementation using router/switch virtualization is designed based on the current active network infrastructure (X-Network network).

Secondly, we create a proof-of-concept implementation that demonstrates as many network resource virtualization features as possible to explore the potential of the network slicing concept. As said earlier, the SDN controller (8000 INM) for the transport layer is a Coriant proprietary controller with many features. The network is implemented using physical network devices, Juniper MX204 3D universal edge routers, Coriant 8615 smart routers and LTE supported eNBs, Nokia Flexi Zone Indoor BTS. The network devices (routers) are connected to each other using 10Gbit/s fiber cables as well as a 1Gbit/s copper connection to both the eNBs and the vEPCs. This setup forms the transport network for this thesis.

Thirdly, the system is tested, and some measurements are performed. The obtained measurements are analyzed and discussed. Furthermore, the system is examined and limitations with the solution are discussed. A conclusion is then drawn from the work that has been done.

1.5 Structure

The rest of the thesis work is structured as follows. Chapter 2 will present the background of the problem at hand and some technologies that will be used to execute the thesis. In Chapter 3, a detail information about the various aspects of the transport network that is the physical network infrastructure for the thesis is presented. In Chapter 4, the proof-of-concept implementation is presented in detail. In Chapter 5, the system is discussed, including some testing results and measurements. Some requirements and limitations are also presented in this chapter. Finally, in Chapter 6 a conclusion drawn from the work performed is presented and discussed.
2 Background

This chapter presents the different packet transport technologies and protocols that will be implemented in this thesis. It also presents some capabilities and limitations of the radio equipment that will be used. These technologies include Ethernet, carrier grade Ethernet, MPLS used in routers as well as some use cases. Redundancy and delay in network nodes are also presented in this chapter.

2.1 LTE Base station

A base transceiver station (BTS) is a radio transmitter/receiver including an antenna that facilitate wireless communication between the user equipment and a network. LTE (Long Term Evolution) as defined by the 3rd Generation Partnership Project (3GPP) defines the access network part of the Evolved Packet System (EPS). Some of the requirements for the new access network are high spectral efficiency, short round trip time, high peak data rates, flexibility in frequency and bandwidth, etc. An LTE base station is simply an LTE access network base station, evolved NodeB (eNB), capable of supporting all the LTE access network part requirements. [11]

2.1.1 Capabilities and limitations

One of many capabilities of an LTE base station is to support Radio Access Network (RAN) sharing. RAN sharing refers to the sharing of the radio access network assets and can be classified as either passive or active. In passive RAN sharing, only cell sites are shared by mobile network operators. Active RAN sharing on the other hand extends this to the sharing of the transport infrastructure, radio spectrum and baseband processing resources. [12] This sharing mechanism is used between several mobile network operators (MNO) to share the cost of building the radio infrastructure in particular in rarely populated areas. In densely populated areas building the network is driven by the need for high capacity, so RAN sharing is not really relevant. When a RAN is shared an eNB will announce several Public Land Mobile Network (PLMN) codes and typically a user is bound to exactly one PLMN. [4]

In UMTS/LTE, a base station can be shared in two ways, Multi-Operator Core Network (MOCN) and Mobile Operator Radio Access Network (MORAN). The difference between these two lies in the frequency allocation. In MORAN a dedicated frequency is required for each operator while in MOCN the entire spectrum and frequencies are shared. [13]

In MOCN, a base station is shared by broadcasting several public land mobile network (PLMN) IDs of different mobile network operators on the air interface in the system information block. A user equipment (UE) that will like to connect to a particular operator decodes the broadcast system information to determine the available core network operator and performs the PLMN ID selection process.
During radio resource control (RRC) procedure, the selected PLMN ID is specified and then used by the eNB to forward attachment request to a mobility management entity (MME) belonging to the correct operator core network. [14] The 5G testbed in Otaniemi contains 4G base stations that only support RAN sharing. For research purposes RAN sharing can be used emulate slicing that will be introduced in 5G base stations.

An LTE supported base station (eNB) should also be able to support backhaul traffic isolation. Traffic isolation in the backhaul starts from the eNB through the transport network to the operator’s core network. This can be achieved by partitioning the transport network into multiple virtual domains for traffic separation while efficiently sharing the backhaul bandwidth. The eNB can be assigned with multiple IP addresses or configured with multiple VLANs to identify and manage each mobile operator’s traffic in the backhaul network. A mobile operator’s traffic can be mapped to one or multiple VLANs in the eNB. QoS control can also be enabled per each VLAN. [12]

As explained above, RAN and transport sharing is a to reduce CAPEX and OPEX, however, there are potential limitations. RAN sharing may have a negative impact on the QoS due to reduction in signal strength when antennas are combined. Also, in MOCN, all elements are shared including radio spectrum hence this feature may not be viable if existing spectrum regulations do not allow it. Lack of service differentiation in terms of availability and network quality may also be a potential drawback. [15]

2.2 Packet transport technologies

Packet transport enables transport networks to switch packet connections at a client port and across the transport network. The switching operates at packet level and identifies connections based on the information present in the packet header. The packet header can carry information about the service the packet needs (Class of Service (CoS)) thereby allowing the packet to be treated differently on the same connection. The connection format and the class of service identifiers depend on the packet technology being used. Packet switching brought some distinct dimensions to transport networks as compared to previous technologies. This includes connection bandwidth flexibility, ability to provide differentiated services for packets carried over the same connection and across connections, sharing of a physical client packet port (Ethernet), etc. [16]

2.2.1 Ethernet

For the past years, Ethernet has gained popularity for interconnecting carrier routers and switches. The change from synchronous bit stream oriented transmission to Ethernet was highly driven by three factors, support for high speed links, lower cost per Mbps and flexibility in connection rates. Ethernet defines two transmission
units, packet and frame. The frame includes not only the payload of the data being transmitted but also includes the physical media access control (MAC) addresses of both sender and receiver, VLAN tagging and quality of service information as well as error correction information to detect transmission problems.

The IEEE 802.1Q, a networking standard that support virtual local area network (VLAN) on an IEEE 802.3 Ethernet network defines a system of VLAN tagging for Ethernet frames as well as procedures to be used by bridges and switches in handing such frames. A point to point Ethernet virtual connection (EVC) can be established across a transport network to extend a point to point EVC or create a point to point tunnel between two transport network devices. In Ethernet frame format, an EVC is identified by a 12-bit VLAN ID tag in the Ethernet frame header. Furthermore, the 16-bit VLAN tag contain in addition to the 12-bit VLAN ID, a 3-bit field often known as priority code point (PCP) as well as a drop eligibility indicator (DEI) bit. For Class of Service (CoS) indication, the PCP is used. [16]

2.2.2 Carrier Grade Ethernet

The high demand in IP based services such as Internet Protocol Television (IPTV), voice over IP, etc. in recent years has increased the need for affordable bandwidth while respecting the more demanding service level agreement (SLA) as well as ensuring acceptable end-to-end quality of service (QoS). Carrier grade Ethernet (CGE) services have emerged as a technology to provide solution to this demand. [17]

Carrier Ethernet is the use of high bandwidth Ethernet technology for Internet access and communication among academic, government and business local area networks (LANs). It addresses the limitations of legacy technologies by providing flexible bandwidth increments and the ability to add new services using a single technology. [18]

Unlike in normal corporate Ethernet, in CGE no MAC learning, no broadcast to unknown MAC or spanning tree protocols are used. Instead, the Forwarding tables are populated by a management system. This way broadcast storms that can destroy QoS in large corporate Ethernets can not occur and the network behaves in a much more predictable manner. [4] With this technology, once an Ethernet service is deployed, bandwidth can be added through remote provisioning to the Ethernet port speed. This enables service providers to sell the amount of bandwidth a subscriber needs.

Applications enabled by a Carrier Ethernet network infrastructure include Ethernet layer 2 networking and Ethernet access to IP (layer 3) services. Example of these applications include site-to-site layer 2 virtual private networks (VPNs), 3G/4G cell site mobile backhaul interconnection, that is interconnecting 3G/4G base stations at cell sites to their base station controllers at a mobile switching center, Ethernet
access to IP services such as IP VPNs, dedicated Internet access, access to cloud services, etc. [18]

2.2.3 Multiprotocol Label Switching (MPLS)

As explained above, the number of IP services continues to increase, and telecommunications carriers have been willing to efficiently accommodate their client traffic. Many packet network technologies including MPLS and Ethernet were introduced in response to such demand. MPLS is essentially a technology for traffic engineering and for IP network optimization. It is considered “multiprotocol” because it is designed to accommodate multiple protocols. Routers that support MPLS protocol suite are known as label switching routers (LSRs). These routers take forwarding decisions based on a label added between the link layer and network layer headers. They also participate in control plane information exchange to set up label switched paths.

Packet forwarding in an MPLS network is slightly different compared to IP network packet forwarding. In IP networks, packets are forward hop by hop from one router to the next that is, each router in the network independently makes forwarding decisions for each packet about which next hop to use to forward that specific packet. The decision to forward a particular packet is based on the information in the packet header combined with data from a forwarding table which the router creates as it runs a network layer routing algorithm.

However, the approach in MPLS network is slightly different, a router’s (LSR’s) decision about packets have the same forwarding criteria is called a forwarding equivalence class (FEC). This decision occurs as the packet enters the network. In this case, the ingress LSR assigns a label for each FEC and sends that label with the packet. A router that receives a labeled packet does not need to analyze the packet header instead it uses the label to directly find the next hop in the label information base table. The router before forwarding the packet swaps the old label for one that indicates the FEC for the next hop router. [19]

2.3 Network virtualization

With virtualization, virtual rather than physical version of resources is provided to consumers. [20] The Internet and various computer networking technologies are the key enablers for virtualization. There are many reasons why we need to virtualize. Sharing of resources, isolation, easy management, etc are some of the reason’s virtualization is required. Network virtualization is defined by the ability to create logical isolated network partitions on top of the underlying physical network resources. This technology helps address many problems including security, scalability, high availability, flexibility, etc. There are many ways to implement virtual networks. One way to implement a virtual network is to use virtual routers connected by virtual links. [21]
One important strength of network virtualization is the capability to handle multiple network provider scenarios and hide the specifications of the network infrastructure, including the existence of multiple administrative domains. Network virtualization involves two main components, link virtualization and node virtualization. Link virtualization permits the transport of multiple separate virtual links over a shared physical link. Virtual links are often identified explicitly by tags but can also for example be identified implicitly by a time slot or a wavelength. There are many varieties of standard link virtualization techniques available in the current Internet. Some of these techniques include ATM, Ethernet 802.1q, 802.1ad, 802.1ah, MPLS, etc.

The virtual node is another important element in the virtual network architecture. Node virtualization is based on isolation and partitioning of physical resources of the substrate node. Resources such as CPU, memory, storage capacity, link bandwidth, etc. are partitioned into slices and each slice allocated to a virtual node according to a set of requirements. “Virtualization of substrate nodes, in combination with virtualization of links interconnecting those substrate nodes, enables the creation of virtual networks, functionally equivalent to a physical network”. Figure 1 depicts the basic components of network virtualization. [22]

![Diagram](image)

Figure 1: Basic Network Virtualization components. Reprinted from [22].

2.3.1 Use cases

In the telecommunication industry, there are many use cases for virtualization. One use case for this technology is supporting for the future 5G network. The fundamental concept of 5G is to make it possible to deliver services anywhere. To make this possible, networks must first become virtualized, that is making them software driven so that one physical network can contain multiple slices to support this concept. Network slicing is very important to 5G because it allows network resources to be shared in an elastic way and for services to be created with resources aligned to their specific requirements.
Another use case of virtualization in the telecom industry is its ability to reduce both CAPEX and OPEX of network operators. To prepare for future service demand in the telecommunication industry requires that operators have to install more hardware or capacity than they need at first. This approach is no longer sustainable by network operators given the complexity, scale and the rapid evolving nature of next generation networks and the services they deliver. Virtualization provides operators the opportunity to efficiently leverage the multi-purpose, flexible processing power of network devices in an elastic way. This means that if the compute power is already installed and capacity available, addressing the growing demand becomes an incremental change. Using virtualization to reduce OPEX and CAPEX, network operators also have the advantage of increasing their profit indirectly through lower expenditures. [23]

2.4 Redundancy in networks

The basic definition of redundancy is the use of additional or alternate components to take over for the active component when the active component fails. Network level redundancy means implementing a network with redundant links and network devices as well as the use of protocol techniques. This ensures network availability in the case of a network device or path failure. Redundant links refers to the use of multiple links between two devices in the network so that when one link fails, the other can take over. Device level redundancy involves the use of additional nodes within the network to provide an alternative path between two communicating end nodes. [24] There are various concepts that can be used to implement network redundancy. Some of these concepts are as follows

Disjoint path: In graph theory, a network is described as an interconnection of nodes by links. Practically, the nodes represent e.g., routers in a communication network. Links on the other hand represent the connectors that bind the nodes together, e.g., cables in a communication network. One aspect of graph theory that has been extensively studied is the shortest path problem. The problem of finding the shortest path between two nodes in a network such that the sum weights of its constituent links is minimized. Examples of shortest path algorithms are the Bellman-Ford and the Dijkstra algorithm. When the shortest paths are used in a communication network, signals can be exchanged with minimal delay between two routers.

The disjoint path problem could be viewed as an extension of the shortest path problem where instead of having a single path, several paths that do not share any nodes or links are computed. Having disjoint paths to a network traffic increases the reliability of network connections as well as the network survivability. Disjoint paths have a wide range of applications, e.g., having multiple disjoint paths for traffic in a communication network would improve its transmission reliability. Also, by sending traffic simultaneously on multiple disjoint paths, the failure of a path would not affect the performance of the other path. [25]
Load sharing: This concept works by statistically distributing network traffic types across multiple links to reduce network load fluctuations. The load is shared based on the network resources available. Load sharing relies on the forwarding table of the router to share the traffic, if routing table has multiple paths to a destination. If there are equal cost paths to a destination, forwarding process and forwarding of packets will be decided based on the load sharing algorithm used.

For example, in MPLS the introduction of traffic forwarding equivalence classes (FECs) gives network operators the flexibility to partition their traffic according to their proposed service model. To establish label switched paths (LSPs) between ingress and egress label switched routers (LSRs), MPLS control plane and associated signaling protocols are used. This enables operators to optimize the use of network resources and offers certain QoS services by assigning different routes to different traffic classes. Load sharing is an extension where a single FEC may be forwarded over a well-defined set of label switched paths (LSPs). This set of LSPs is known as LSP group. [26]

2.5 Delay in networks

Delay in a telecommunication network can be defined as the time needed for a bit of data to travel from a source to destination. There are four types of delay that contribute to the overall E2E delay. These are processing delay, queueing delay, propagation delay as well as transmission delay. Mathematically, this can be represented as follows

\[ D_{E2E} = D_{PROCESSING} + D_{QUEUEING} + D_{PROPAGATION} + D_{TRANSMISSION} \]  

(1)

Processing delay is the time it takes to handle a packet on the network system. A network node (router) needs to examine the received packet header to determine the output link. It also checks for bit errors to determine if a packet is corrupt, packet processing e.g. encryption, firewalling, etc. All these functions performed by the router form part of the processing delay and normally many features are used on the edge router while intermediate routers use a minimum set of features.

Transmission delay is the time it takes to transmit the packet onto the link (wire). In other words, it is the amount of time needed by a router to transmit the entire packet onto the link. This is represented as

\[ D_{TRANSMISSION}[\text{sec}] = \frac{L[\text{bit}]}{R[\text{bps}]} \]  

(2)

where L is the length of the packet (packet size) and R is the link transmission rate.
Propagation delay is the time it takes to transmit one bit over a link. In other words, it is the time for one bit to propagate from a source to destination at propagation speed of the link. This means that the delay depends on the physical medium of the link. Propagation delay is represented mathematically as

\[ D_{\text{PROPAGATION}} = \frac{d[m]}{\eta c[m/sec]} \]  

where \( d \) is the distance, \( c \) the speed of light and \( \eta \leq 1 \). For fiber \( \eta \approx \frac{2}{3} \)

Queueing delay on the other hand is the time the packet is buffered before it can be sent. That is the time spent by the packet sitting in a queue waiting to be transmitted onto the link. The amount of time a packet needs to wait depends on the queue size. If a router queue is empty, a received packet is transmitted immediately but if not, then the packet has to wait behind other packets. This means that, queueing delay is proportional to the buffer size and the amount of cross-traffic entering the router. Figure 2 depicts the types of network delays. [27]

![Network Delay Types](image)

Figure 2: Network Delay Types. Reprinted from [27].

### 2.6 Network slicing as defined by 3GPP

The 3GPP considers network slicing as a key mechanism for the fifth generation (5G) network segmentation. It defines a network slice in the 5G architecture as a complete end-to-end (E2E) logical network which can be created dynamically and is capable of providing network specific capabilities and characteristics. It is also defined within a Public Land Mobile Network (PLMN) including the 5G Access Network (AN) as well as the core network control and user plane network functions. Based on this definition, a given user equipment (UE) may have access to multiple network slices over the same radio interface or access network where each slice may provide a particular type of service with an agreed Service Level Agreement (SLA). [28]
The network slicing concept is viewed by network infrastructure providers as an important aspect to increase their revenue. The concept allows the operators to virtualize their physical infrastructure to provide multiple network slices to various industries such as the automotive, e-health, etc. [29]

The architectural design and definition of network slicing for 5G systems has emerged due to the high expectations and limitations of the 4G system. The definition of the overall 5G architecture was based on the 3GPP "NextGen" ([30]) and "New Radio Access Technology" ([31]) release 14 technical reports. The overall architecture includes a 5G Core network (5GC) and a 5G RAN ((R)AN). The 5GC and the (R)AN are interconnected via the N2 and N3 interfaces for control plane (CP) and user plane (UP) respectively. Connection between (R)ANs can be done via the Xn interface, that is Xn-CP for control plane and Xn-UP for user plane. The 5GC is then connected to an external data network (DN) using the N6 interface. Figure 3 show the 5G system architecture for RAN only.

![Figure 3: 3GPP Release 14 5G System Architecture, RAN only. Reprinted from [32].](image)

Furthermore, the 3GPP was motivated to introduce the new 5G system architecture due to the need for more flexibility, elasticity and scalability in the mobile core network. In the new architecture, some network functions (NF) are similar to NFs in the LTE while other new functions have been introduced. Figure 4 denotes the 5GC architecture presented by 3GPP. [33]

![Figure 4: Non-Roaming 5G System Architecture. Reprinted from [34].](image)
One of the most important NF defined in the 5GC is the Access and mobility function (AMF) which handles access control and mobility as well as the integration of network slice selection functionality. [33] Also defined are the session management function (SMF) which is set up according to the network policy to handle user sessions, the Policy Control Function (PCF) same as the PCRF in LTE, its function is to integrate a policy framework for network slicing, the User Plane Function (UPF) which is the anchor point for intra or inter Radio Access Technology (RAT) mobility, packet routing and forwarding, user plane QoS handling, packet inspection and policy rule enforcement, etc. [32]

The NF Repository Function (NRF) is another important new function defined in the 5GC. This function is for providing registration and discovery functionalities allowing NFs to discover each other and communicate using open APIs. [33]

Another important NF defined is the Unified Data Management (UDM) similar to HSS in LTE. However, this function is designed to support authentication credential repository and processing function, storing long term security credentials as well as subscriber information.

To ensure network slice architectures can be applied to the various 5G use cases, allow third parties to modify network slices, enable flexibility in network deployment and reconfiguration by taking advantage of network function virtualization (NFV), Multi-access Edge Computing (MEC) and cloud computing technologies, the 5GC have been split into a set of Network Functions (NFs). As shown in Figure 5, a set of NFs are defined for both control plane functions (CPFs) and user plane functions (UPFs). The control plane NFs have been classified as the common control network functions (CCNFs) and slice specific control network functions (SCNFs) to differentiate between NFs which might be shared among multiple network slices and that of slice specific NFs. Among the CCNFs is a NF which is dedicated to slice selection and is denoted as the network slice selection function (NSSF). [32]

![Figure 5: 3GPP 5G Core Architecture, Non-Roaming Scenario. Reprinted from [32].](image_url)

The Service and System Aspects working group which specifies the service re-
quirements and the overall architecture of the 3GPP system developed a high-level architecture for network slicing.

The NextGen network will provide customized 5G network services by selecting the control plane and user plane needed for a specific service. The CCNF also include functions such as the AMF which should be commonly supported for all the sessions of a specific UE. A UE can be connected and served by a single CCNF at a time though multiple PDU sessions of the UE may be served by different network slice instances. Commonly requested functionalities such as UE level mobility management, authentication, network slice instance selection, etc can be provided by the CCNF. [35] Figure 6 shows an example of network slicing architecture in the NextGen.

The NextGen network will provide a customized 5G network services by selecting the control plane and user plane needed for a specific service. The CCNF also include functions such as the AMF which should be commonly supported for all the sessions of a specific UE. A UE can be connected and served by a single CCNF at a time though multiple PDU sessions of the UE may be served by different network slices instances. Commonly requested functionalities such as UE level mobility management, authentication, network slice instance selection, etc can be provided by the CCNF. [35] Figure 6 shows an example of network slicing architecture in the NextGen.

![Network Slicing Architecture](image)

Figure 6: Example of Network Slices. Reprinted from [28].

A brief introduction of the various components and their functions in Figure 5 above is given below:

**Access and Mobility Management function (AMF):** The AMF supports termination of non-access stratum (NAS) signalling, NAS ciphering and integrity protection, connection management, mobility management, registration management, access authentication and authorization, security context management.

**Session Management function (SMF):** The SMF node supports session management (session establishment, modification, release), UE IP address allocation and management, DL data notification, dynamic host configuration protocol (DHCP) functions, termination NAS signalling related to session management and traffic steering configuration for user plane function (UPF) for proper traffic routing.

**Application Function (AF):** Supports application influence on traffic routing, accessing network exposure function (NEF) and interaction with policy framework
for policy control.

**Policy Control Function (PCF):** Supports unified policy framework to govern network behaviours as well as providing policy rules to control plane function(s) to enforce them.

**Authentication Server Function (AUSF):** The AUSF acts as an authentication server.

**Network Slice Selection Function (NSF):** The NSF supports selecting of the Network Slice instances to serve the UE, determining the AMF set to be used to serve the UE as well as determining the allowed network slice selection assistance information (NSSAI).

**User plane function (UPF) supports:** packet routing and forwarding, packet inspection, QoS handling, acts as external protocol data unit (PDU) session point of interconnect to Data Network (DN) and an anchor point for intra and inter-RAT mobility.

**Unified Data Management (UDM):** Supports generation of Authentication and Key Agreement (AKA) credentials, access authorization, user identification handling and subscription management.

**Network Exposure function (NEF):** Supports exposure of capabilities and events, secure provision of information from external application to 3GPP network and translation of internal/external information.

**NF Repository function (NRF):** Supports service discovery function, maintains network function (NF) profile and available NF instances.
3 Testbed transport slicing

Network slicing as defined in 3GPP TS 22.261 gives network operators the flexibility to provide customized networks based on functionality requirements such as security, charging and policy control, differences in performance requirements, i.e. data rates, latency, mobility or even to serve specific users only such as public safety users, corporate customers, etc. Furthermore, a network slice is capable of providing the functionalities of a complete network including the RAN functions and core network functions. [36]

The definition of network slicing and deployment starts from the radio access network (RAN) as well as the packet core, however in order to guarantee end to end service level agreement (SLA) and key performance indicators (KPIs) for specific services that require strict bandwidth and latency guarantee, the transport network which also plays an important role needs to be sliced so that different services can be bound to the different transport slices. This means that service providers need to define logically isolated networks (virtual networks) to be offered as services to different customers. These logical networks are defined based on the customer requirements. From high level point of view, some of the key factors and requirements for the transport slicing include, the ability for a customer to define and convey their virtual network without having any knowledge about the transport network details, providers ability to map and translate their customers network models (e.g. layer 2/3 VPN) against traffic engineering constrained path, provisioning and managing of end to end paths to meet a given virtual network constraints, the ability to monitor virtual networks at different levels for example at customer level, orchestrations level and domain level, etc. [37]

3.1 Requirements

The purpose of the transport slicing is to allow the creation of slices over many core networks. The testbed implements a complete E2E slicing of both RAN and the transport network. The testbed should meet some of 3GPP requirements such as

- The testbed should follow 3GPP network slicing requirements
- The testbed should be able to create/modify/delete network slices
- The testbed should provide isolation among slices
- The testbed should allow appropriate bandwidth allocation to each slice based on its requirements

3.2 Testbed components

A brief explanation of the testbed component that is part of the slicing system includes the following:
**Transport slice Orchestration:** In order to create, manage and monitor slices, the Coriant 8000 Intelligent Network Manager (INM) will be used as our transport orchestrator or controller. The orchestrator will be used for controlling the transport nodes for this project. The 8000 INM provides a customized graphical user interface (GUI) for easy and quick service provisioning and management. It also enables the integration with other operational support systems (OSS) systems and processes through its various North Bound Interfaces (NBIs). The Coriant 8615 NEs can be reached for management and configuration using the Broadband Management Protocol (BMP), CLI, FTP, RADIUS, SNMP, SSH and TELNET.

**Transport routers:** The transport routers are responsible for routing the traffic between the eNBs and the vEPCs on both layer 2 and layer 3. For this project, two different SDN supported routers from different vendors will be used, the Coriant 8615 Smart Router and the Juniper MX204 3D Universal Edge Router. The 8615 router is a 44Gbps full duplex IP/MPLS router targeted for packet networks. It provides high 1GE Ethernet interface density for mobile or fixed access networks. In addition, the 8615 smart router provides the flexibility and capabilities needed to serve all-IP mobile and fixed networks including applications ranging from traditional consumer, enterprise and machine-to-machine connectivity to cloud networking needs. [38] Figure 7 shows an overview of the 8615 smart router front panel.

![8615 Smart Router front Panel](image)

Figure 7: 8615 Smart Router front Panel. Reprinted from [38].

The 8615 network element provides the following types of interfaces.

- 2 ports 10GBASE-R small form-factor pluggable (SFP)+
- 16 ports 100/1000BASE-X small form-factor pluggable (SFP)
- 8 ports 100BASE-TX/1000BASE-T with PoE
- Station Clock Input and Output
- Pulse-per-Second Interface
- External Alarm Interface
- Stacking Interface

The Juniper Networks MX204 3D Universal Edge Router is an Ethernet-optimized edge router with 400Gbps capacity. It provides both switching and carrier-class Ethernet routing, enabling a wide range of business and residential applications and services, including high speed transport and virtual private network (VPN) services, high-volume Internet data center internetworking, etc. [39] Figure 8 shows the front panel of the MX204 router.
Figure 8: MX204 Front Panel Ports, LEDs, and Buttons. Reprinted from [39].

- Rate-selectable ports (can be configured as 100GE port or 40GE port or 10GE)
- Management (MGMT) port
- Building-integrated timing supply (BITS) port with light emitting diodes (LEDs)
- Universal Serial Bus (USB) port
- 1 pulse-per-second (PPS) and 10MHz GPS input and output ports
- ONLINE LED
- Solid-state drive (SSD)1 LED
- OFFLINE LED
- RESET button
- Solid-state drive (SSD)0 LED
- Alarm (ALM) LED
- OK/FAIL LED
- Time of day (ToD) port with LEDs
- Console (CON) port
- 10-Gigabit Ethernet small form-factor pluggable (SFP)+ ports
- Precision Time Protocol (PTP) grandmaster clock (GM/PTP) port

**LTE supported base station:** In order to test the E2E connectivity between the UEs and the vEPCs of the multiple slices, an access device is required. Due to the lack of 5G access point, an LTE support access point is used. The Nokia Flexi Zone Indoor Pico BTS is a small cell optimized for an indoor environment. It provides seamless mobility and enhanced user experience in enterprise and public indoor locations. The main application of the Flexi Zone Indoor Pico BTS is to
deliver an improved mobile broadband experience by offloading data traffic from macro networks. Specification in [40] provides more information about the Flexi Zone Indoor Pico BTS. Figure 9 shows an overview of the Flexi Zone Indoor Pico BTS.

![Figure 9: Flexi Zone Indoor Pico module Interfaces. Reprinted from [40].](image)

**Virtual Evolved Packet Core (vEPC):** The EPC is the latest evolution of the 3GPP core network architecture. It was first introduced by 3GPP in Release 8 of the standard. The EPC is based on an always-on connection. The Cummucore vEPC is a cloud-native solution that includes mobility, user management and traffic optimization. The vEPC is compatible with third party LTE base stations, subscriber management and billing management systems for E2E solution. It enables profitable services for network operators such as network slicing for IoT and media optimization. Furthermore, the Cummucore vEPC consists of 3GPP compliant Mobility Management Entity (MME), Serving/Packet Gateway (S/P-GW) network nodes. For this project, each slice will be connected to a vEPC to test slice connectivity requirements. Multiple user equipment (UE) with different PLMNs will then be connected to each vEPC to establish an E2E connectivity.

**Broadband Management Protocol (BMP):** The BMP defines a protocol for communication between the Coriant 8000 INM and the 8615 network elements. The BMP agent resides in the 8615 NE therefore communication between 8000 INM and the BMP agent is done over TCP/IP connection if the NE supports it. Alternatively, the communication can be done using the UDP/IP protocol. The communication can also be configured to use SHA-1 authentication.

It is possible to establish connection with other generic SNMP NEs as long as they support SNMP monitoring using MIB-II. For this project, BMP protocol is used between Coriant NEs while simple network management protocol (SNMP) is used between the INM and the Juniper devices. Figure 10 shows an overview of how the 8000 INM connect to Coriant 8615 NEs. [41]
Virtual Router Redundancy Protocol (VRRP): The virtual router redundancy protocol (VRRP) is a computer networking protocol designed to eliminate the single point of failure that might occur in the static default routed environment. It specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a local area network (LAN). The VRRP router controlling the IP address(es) associated with a virtual router is called the master, and forwards packets sent to those IP addresses. When the master becomes unavailable, a backup router takes the role of the master. The advantage gained from using VRRP is higher availability. This thesis work intends to provide high availability by implementing the VRRP mechanism between various virtual routers residing in the two Juniper MX204 routers. [42]

3.3 Testbed transport slicing design

In order to apply the concept of transport slicing in the X-Network network, it is very important that this concept is implemented and tested in a smaller network. The core network for the test network is made up of four (4) physical routers, two Coriant 8615 smart routers and two Juniper MX204 3D universal edge routers. These routers are connected and managed by a network controller, the Coriant 8000 INM. The 8000 INM is a powerful element, network and service management system that supports mobile backhaul, packet optical and business solutions [43]. These routers make up the network nodes which are connected to each other using fiber optic cables through their 10G physical interfaces. Due to the lack of 5G radio access nodes and 5GC, the test network will be setup using an LTE eNBs, the Nokia Flexi Zone Indoor BTS and the Cumucore vEPC respectively. The setup will also take advantage of the Nokia eNB RAN sharing feature in creating the transport slices. The eNBs are then connected to the network nodes through a 1G physical interfaces. Furthermore, two virtual vEPCs will be used in testing the network. These vEPC are installed and running on an AMD Accelerated Processing Unit (APU) and then connected to the Juniper MX204 3D routers through a switch. This physical network is called the transport network which can be sliced into multiple virtual networks.

The E2E slicing for this project will be implemented by creating logically isolated virtual networks which will provide the same services as a traditional dedicated network. The slicing implementation will be done at operator level, this means that
each slice will be implemented as a different mobile operator and assigned a specific PLMN identifier which will share the same RAN infrastructure. Furthermore, each eNB will be commissioned with two different PLMNs each having its own Virtual Local Area Network (VLAN) with a tag configured in the eNB. Traffic isolation in the core network would be done by virtualizing the network nodes (routers), that is creating virtual routers within the same physical router and then mapping these virtual routers to the different created VLAN interfaces to provide an E2E segmented connectivity. Therefore, the IP hierarchy for the transport slicing will be a combination of layer 3 and layer 2 domains where both domains will be virtualized, and the virtualized domains mapped to each other to keep traffic isolated. The end result will be a dedicated core network per transport slice as shown in Figure 11.

Practically, this can be achieved by virtualizing the network node or devices as well as virtualizing interconnections (data paths). Within each networking device, there are two planes that need to be virtualized, the control plane and the forwarding plane. Virtualizing the control plane involves virtualizing all the protocols, databases and tables needed to make forwarding decisions and also to ensure that the network is free from loops. Virtualizing the forwarding plane in this case will involve virtualizing all processes and table to be used for traffic forwarding. Furthermore, virtualizing a physical network device means that the device must have many control/forwarding instances, one for each network slice (VLAN). This can be implemented using the virtual routing (VR) technology. The VR technology allows a layer 3 network device to be virtualized by creating multiple VR instances in the same physical device. A VR instance consist of a forwarding table, an IP routing table, a set of interfaces that use the forwarding table and a set of rules and routing protocols that determines what goes into the forwarding table. Figure 11 shows an overview of the transport slicing for the test network.
Figure 11: Designed Transport Network overview.
Figure 11 describes the network design, which is a well designed and validated network architecture that is flexible and cost effective to support a wide range of wireless network services. The key features of this network design include high availability as well as layer 2 and layer 3 access. The functions of the Juniper MX204 routers in this design is to provide redundant paths as well as high availability needed in URLLC. In this scenario, additional links can be added through the MX204 routers to provide connection the various Cumucore vEPCs as well as the backup vEPC located in the data center. This prevents the case of single point of failure that may occur if one of the MX204 routers is unavailable. Having redundant paths to a specific slice vEPC will also provide high reliability as required in URLLC. A use case scenario is to provide two different paths from an eNB to the vEPC of a particular slice. This will create a situation where user’s traffic can be transmitted through multiple links to a specific operator vEPC. For high availability, an additional link between the two Juniper MX204 routers will be added and VRRP implemented between virtual routers as shown in Figure 11. An example application of such scenario to a specific transport slice is depicted in Figure 12.

Furthermore, the primary functions of the Coriant routers is to serve as access point for multiple eNB. These switches serve as the interface where multiple eNBs can be connected and provided with layer 2 and layer 3 access to the backhaul. At this point user traffic isolation to the backhaul is performed. Another important key feature of the Coriant routers being used as access point is the number of Ethernet ports. A single Coriant router provides 16 ports 100/1000BASE-X small form-factor pluggable (SFP) and 8 ports 100BASE-TX/1000BASE-T with power over Ethernet (PoE). This means that for future expansion of the network, these ports can be used to integrate new additional eNBs into the backhaul.
As shown in Figure 12, a slice consists of four (4) virtual routers. These virtual routers are software functions that duplicate in software the functionalities of layer 3 Internet Protocol (IP) routing which for many years has used dedicated hardware device. The VRs are virtually interconnected similar to the physical network to provide high reliability and high availability. Each slice will be configured to meet the requirements of a particular operator services.
4 Testbed implementation

Due to the lack of 5G radio, the tested is built using an LTE supported eNodeBs (eNBs), the Nokia Flexi Zone Indoor Pico BTS, taking advantage of its RAN and transport sharing features. The slicing of the transport network is done at operator level. This implies that each slice is physically implemented as a different mobile virtual operator and assigned with a specific PLMN ID that share the same RAN infrastructure. The deployment setup is depicted in Figure 13. The implementation considered only two slices with different bandwidth profiles and QoS settings. The implementation consists of the following components:

- Two virtualized Evolved Packet-Core (vEPC), the Cumucore vEPC (one per each slice)
- Two Nokia Flexi Zone Indoor Pico BTS
- Two LTE supported mobile phones each having a SIM (subscriber identity module) card with different PLMN information
- Two Coriant 8615 Smart Routers
- Two Juniper MX204 3D Universal Edge Routers
- One Juniper EX3300 switch

Figure 13: Deployment setup.
As shown in Figure 13 above, two indoor base stations (Nokia Flexi Zone Indoor Pico BTS) were used. Each of these base stations were connected to the Coriant 8615 device using their 1GE interface. Fiber cables are used to connect the transport nodes (routers) using their 10GE interfaces. The APU running the vEPCs are also connected to the nodes. Two LTE smart phones having SIM cards programmed with different PLMN IDs are used to test the slicing system. The rest of this chapter explains how each unit of this setup is configured.

4.1 Base station configuration

The LTE supported Nokia Flexi Zone Indoor Pico BTS provides a Local Maintenance Terminal (LMT) interface for management operations. The LMT allows us to adjust the physical network resources allocation of a specific PLMN, e.g., a specific network slice. The LMT is programmable by means of XML configuration files that are loaded and installed every time the network configuration changes. The PLMN ID is an identifier for a mobile network, particularly for its core. User equipment (UE) use the PLMN ID to select the network to connect. The Nokia Flexi Zone Indoor Pico BTS supports multiple PLMN ID configuration. Configuring the eNB to broadcast more than one PLMN IDs at the same time means RAN sharing. For this project the eNB is configured to broadcast five PLMN IDs even though only two were used.

Transport sharing means sharing the backhaul connection that link the eNB to the rest of the network. The Nokia Flexi Zone Indoor Pico BTS has only one physical Ethernet interface for backhaul connection, therefore connections to the different vEPC cores have to be multiplexed over the same physical link. The multiplexing is done through VLAN tagging (IDs), thus having multiple virtual LANs departing from the same Ethernet interface. The eNB can be configured with many VLANs, however only two user plane VLANs can be used for the testbed implementation. This is because there cannot be more than two user plane VLANs multiplexed over the same backhaul link. Therefore, two VLANs are configured in the eNBs and are assigned IP addresses.

Furthermore, to tell which IP address should be used by the base station as source IP address for packets towards the two different vEPCs, each eNB VLAN is mapped to a Transport Network ID, i.e., first VLAN associated with transport network ID 0 while second VLAN associated with transport network ID 1. This creates two different transport networks in the eNB. In addition, user plane, control plane, management plane, synchronization plane, etc are configured for each transport link (slice). Other requirements that need to be configured include defining the routing table for the eNB to route packets to the separate vEPCs, AMF/MME IP address configuration, etc. All of these configurations can be done using the BTS Site Manager, the software for managing the eNB. [44]
4.2 VLAN creation and node virtualization

Creating VLANs in both Coriant 8615 and Juniper MX204 routers is easy. However, both routers run on different operating systems (OS). Therefore, creating VLANs in 8615 routers is slightly different from that of the MX204 routers. In 8615 routers, VLANs to the router’s interfaces can be created using the following commands

```
router# configure terminal
router(config)# interface fe | ge if-module/interface [vlan]
router(config)# interface fe 3/0/1
```

An example of how to create a VLAN with ID 10 on interface fe 3/0/1 in 8615 routers

```
router# configure terminal
router(config)# interface fe 3/0/1.10
```

Also, to configure VLAN and assigned it to an interface (e.g xe-0/1/4) with unit 100 in Juniper MX204 for layer 3 routing, the following commands are used

```
set interface xe-0/1/4 vlan-tagging
set interface xe-0/1/4 unit 100 vlan-id 100
set interface xe-0/1/4 unit 100 family inet address 10.1.1.1/29
```

To virtualize the transport network nodes for this project, virtual routers technology is preferred. Virtual router instances are not strictly virtual routers because they do not have dedicated memory, processing, or Input/Output resources. However, they allow multiple instances of routing tables to exist on the same physical router. For this project creating a routing tables per slice helps isolate traffic on the same physical router. It achieves the virtualization of the networking device at the layer 3. When network devices are virtualized, the data paths between the virtual instances are also virtualized to provide logical interconnectivity between the virtual routing instances in this case virtual routers. This means that E2E path isolation is achieved by mapping each VLAN to its own dedicated virtual router instance.

Furthermore, the type of data path virtualization depends on the distance between the virtual routers. If the virtualized devices are directly connected to each other (single hop), then a link virtualization is necessary. If the virtualized devices are connected through multiple hops over an IP network, then a tunneling mechanism is necessary. This project adopts the single hop link virtualization since the network design involves directly connected virtualized devices. [45] Figure 14 shows an example single hop data path virtualization that is implemented in this project.
4.3 vEPC setup

The EPC used in this project is the Cumucore virtual Evolved Packet Core (vEPC). The Cumucore vEPC consist of 3GPP compliant Mobility Management Entity (MME), Serving/Packet Gateway (S/P-GW) network nodes. The functionality of the vEPC is implemented as macro-service designed to be extended with 5G network nodes and interfaces. The current Cumucore vEPC components include the Authentication and Mobility Function (AMF) module, the Session Management Function (SMF) as well as the User Plane Function (UPF) module.

The AMF is backward compatible and provides MME functionality with an S1-MME interface towards 4G RAN as well as N1/N3 interfaces. The S/P-GW functionality is run as UPF module and also includes 4G packet GW functionality in addition to the new 5G module. The UPF is designed and implemented as micro-service that includes backwards compactibility LTE GTP functionality complant with 4G S/P-GW as well as SDN functionality to provide flow-based tunneling for IP and non-IP transport technologies. In addition, the vEPC includes an SMF module as well as a custom Home Subscriber Server (HSS). The SMF is responsible for setting up and managing sessions while the HSS functionality is to manage subscriber data. These functionalities are implemented as virtual network functions (VNFs) that can be deployed on standard computing resources.

In this project, the vEPC is deployed in Linux operating system (OS). It also requires the following dependencies such as OpenSSL library for security and encryption functions, the Stream Control Transmission Protocol (SCTP) for S1-MME interface, and an SQL (Structured Query Language) database to emulate HSS and GTP module for S1-U interface. [46] The vEPC setup for this project is depicted in Figure 15.
4.4 Quality of Service

Generally, IP networks operate on a best-effort delivery basis. This means that all traffic has equal priority and equal chance of being delivered in a timely manner. When a network becomes congested, all traffic has an equal chance of being dropped. Quality of Service (QoS) architectures select network traffic, prioritize the traffic according to its relative importance and use congestion avoidance to provide priority indexed treatment. QoS can also limit the bandwidth used by a network as well as make network performance more predictable and bandwidth utilization more effective.

A slice in this project is implemented using both layer 2 (VLANs) and layer 3 (virtual routers) technologies. To specify different QoS configurations on the different VLANs on a given interface, a port level QoS classification configuration is required. A port level QoS offers differentiated QoS to individual VLANs on a specific port. In 8615 routers, a port level QoS classification configuration ensures all VLAN interfaces on a given port inherit the same settings, unless there is an explicit QoS classification configured at VLAN level. Port/node level QoS classification on the 8615 router is based on VLAN priority (PRI) field. This means that all tagged traffic is classified based on a VLAN PRI and untagged traffic classified as best effort (BE).

In order for each VLAN to be subjected to the correct forwarding treatment under
the network QoS policies, each packet entering the differentiated services (DiffServ) domain (e.g. Coriant routers) must first be classified into the appropriate DiffServ per-hop behavior (PHB) and or PHB scheduling class (PSC). [47] The standardized per-hop behaviors (PHBs) supported by the 8615 smart router is shown in table 1.

<table>
<thead>
<tr>
<th>CS7</th>
<th>Class Selector 7 PHB (for control and management plane traffic)</th>
</tr>
</thead>
<tbody>
<tr>
<td>EF</td>
<td>Expedited Forwarding</td>
</tr>
<tr>
<td>AF4</td>
<td>Assured Forwarding 4 PSC</td>
</tr>
<tr>
<td>AF3</td>
<td>Assured Forwarding 3 PSC</td>
</tr>
<tr>
<td>AF2</td>
<td>Assured Forwarding 2 PSC</td>
</tr>
<tr>
<td>AF1</td>
<td>Assured Forwarding 1 PSC</td>
</tr>
<tr>
<td>BE</td>
<td>Best Effort PHB (the default forwarding treatment)</td>
</tr>
</tbody>
</table>

Table 1: 8615 Smart Router Supported DiffServ PSCs/PHBs. Reprinted from [47].

Similar to resource reservation protocol (RSVP), a component of the integrated services model that provided a guaranteed bandwidth services, the IETF defines expedited forwarding (EF) behavior in [48]. The EF provides a robust service by providing low loss, low latency, low jitter and assured bandwidth services. These characteristics are suitable for video, voice and other realtime services.

Assured forwarding (AF) defined in [49], allows operators to provide assurance of delivery as long as the traffic does not exceed the subscribe rate. Traffic that exceed the subscription rate faces a higher probability of being dropped if congestion occurs. Four separate AF classes where all have the same priority has been defined by the AF behavior group. Within each class, packets are given a drop precedence such as high, medium or low where higher precedence means more dropping. Any traffic that does not meet any requirements of any other defined classes is placed in the default PHB which has best-effort forwarding characteristics.

The 8615 smart routers support the use of QoS mapping tables for translating between the class of service (CoS) markings used in different networking technologies, e.g., between IP differential service code points (DSCPs), MPLS experimental (EXP) bits and Ethernet VLAN user priority bits. Table 2 depict the default QoS mapping table used by the Coriant 8615 smart routers.
Table 2: Coriant 8615 Routers Default QoS Mapping Table. Reprinted from [47].

<table>
<thead>
<tr>
<th>QoS Class</th>
<th>Drop Probability</th>
<th>Ingress Classification</th>
<th>Egress Mapping</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>PRI</td>
<td>IP DSCP</td>
</tr>
<tr>
<td>CS7</td>
<td>—</td>
<td>7</td>
<td>56</td>
</tr>
<tr>
<td>EF</td>
<td>—</td>
<td>6</td>
<td>46</td>
</tr>
<tr>
<td>AF4</td>
<td>AF43</td>
<td>—</td>
<td>38</td>
</tr>
<tr>
<td></td>
<td>AF42</td>
<td>—</td>
<td>36</td>
</tr>
<tr>
<td></td>
<td>AF41</td>
<td>5</td>
<td>34</td>
</tr>
<tr>
<td>AF3</td>
<td>AF33</td>
<td>—</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td>AF32</td>
<td>—</td>
<td>28</td>
</tr>
<tr>
<td></td>
<td>AF31</td>
<td>4</td>
<td>26</td>
</tr>
<tr>
<td>AF2</td>
<td>AF23</td>
<td>—</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>AF22</td>
<td>—</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>AF21</td>
<td>3</td>
<td>18</td>
</tr>
<tr>
<td>AF1</td>
<td>AF13</td>
<td>—</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td>AF12</td>
<td>—</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>AF11</td>
<td>—</td>
<td>10</td>
</tr>
<tr>
<td>BE</td>
<td>—</td>
<td>2,1,0</td>
<td>0</td>
</tr>
</tbody>
</table>

In 8615 smart routers, ingress and egress QoS mapping can be defined on a node level and port levels with the command qos mapping ingress and qos mapping egress. Example of VLAN QoS mapping configured in the Coriant 8615 router is as follows:

```
gos mapping ingress vlan-pri 7 qos cs7
gos mapping ingress vlan-pri 6 qos ef
gos mapping ingress vlan-pri 5 qos af4 drop-precedence low
gos mapping ingress vlan-pri 4 qos af3 drop-precedence low
gos mapping ingress vlan-pri 3 qos af2 drop-precedence low
gos mapping ingress vlan-pri 2 qos be
gos mapping ingress vlan-pri 1 qos be
gos mapping ingress vlan-pri 0 qos be
```

```
!
```

```
gos mapping egress qos cs7 vlan-pri 7
gos mapping egress qos ef vlan-pri 6
gos mapping egress qos af4 drop-precedence high vlan-pri 5
gos mapping egress qos af4 drop-precedence medium vlan-pri 5
gos mapping egress qos af4 drop-precedence low vlan-pri 5
gos mapping egress qos af3 drop-precedence high vlan-pri 4
gos mapping egress qos af3 drop-precedence medium vlan-pri 4
gos mapping egress qos af3 drop-precedence low vlan-pri 4
```
gos mapping egress qos af2 drop-precedence high vlan-pri 3
gos mapping egress qos af2 drop-precedence medium vlan-pri 3
gos mapping egress qos af2 drop-precedence low vlan-pri 3
gos mapping egress qos af1 drop-precedence high vlan-pri 0
gos mapping egress qos af1 drop-precedence medium vlan-pri 0
gos mapping egress qos af1 drop-precedence low vlan-pri 0
gos mapping egress qos be vlan-pri 0

In the example QoS mapping configuration, ingress qos mapping applies to traffic that enters the 8615 router ports while egress qos mapping applied to traffic going out of the interfaces. For VLANs, the mapping is done based on the ingress and egress classification (VLAN priorities), drop probabilities as well as their QoS class. This means that all tagged packets coming from the eNB to the Coriant 8615 router interfaces will be treated by the Coriant 8615 router based on the VLAN priorities assigned to them. The same treatment also applies to packet going out of the Coriant 8615 routers interface towards the eNBs.

Furthermore, other functionality such as QoS policing in the ingress interface as well as queue management, scheduling and shaping in the egress interface are configured to enable traffic management functionality of all VLANs configured in the transport network.

4.5 User Equipment (UE) configuration

The user equipment’s (UE) used in this project are LTE mobile phones. Since each UE will be used to connect to different vEPCs belonging to the different operator slices, a SIM card programmed with different IMSI (MCC+MNC+MSIN) is required. The IMSI reflects the PLMN IDs of the different operators. Two SIM cards are programmed with the PLMN IDs 24438 and 24439. Each of these SIM cards belong to a specific slice. The programmed SIM cards are then inserted into the UEs and their setting changed such that they only connect to the LTE network.
5 Results and discussion

The testbed developed for this thesis provides a basic concept of network slicing and show that it is possible to implement a slicing system using virtual routers. This chapter discusses the slicing concept as well as some limitations. The slicing concept is implemented and tested on real hardware, therefore some measurements are performed, presented and discussed. Finally, some limitations of the slicing system are presented.

5.1 Abstraction and isolation

In order to virtualize a network, we need to know what resources we are trying to slice. The network slicing system implemented for this thesis is validated against some attributes in terms of abstraction and isolation.

5.1.1 Abstraction

Abstraction is expected to provide a simplified representation of the physical network. This project takes in consideration three types of abstraction topology abstraction, node resource abstraction and link resources abstraction. Topology abstraction means abstracting the links and nodes of the physical network. Network links can be abstracted by virtualizing multiple chained links to form a single virtual link. Similarly, physical network nodes can be abstracted into a single node. The level of abstraction can range from lowest to maximum. The lower level abstraction is when there is one to one mapping where the virtual topology is similar to the physical network. [5]

The slicing system implementation for this thesis supports abstraction of links. The basic level form of abstraction is implemented for the slicing concept in this thesis. To create a single slice, virtual links are created by specifying the end nodes between which the virtual link is established. In addition, the intermediate nodes are also virtualized in the virtual link to create a single topology similar to the physical network.

Node resource abstraction on the other hand refers to the abstraction of the physical node resources such as CPU and other resources available at the physical device. For example, device CPU resources can be abstracted as a certain percentage of the full CPU core capacity at the device or a number of dedicated CPU cores. The slicing implementation for this thesis uses node resources in the virtual routers as well as the transport router resources. The transport router needs to classify each received packet and forward it to the correct virtual router. The virtual router then processes the packet again according to its routing table entries and then forwards the packet to the transport router where it is processed again. The transport routers used in this experiment do not provide the means to limit node resources (e.g. CPU resources) to each virtual router. Limitation of node resources to the various virtual routers might be very difficult to implement in this project.
Link resource abstraction relates to the abstraction of the physical bandwidth available at each link. Link bandwidth can be virtualized as a percentage of the available bandwidth of the physical link. The slicing implementation in this thesis supports bandwidth limiting using the QoS features provided by the transport device (Coriant 8615 and Juniper MX204). The QoS features of these devices allow configuration of maximum bandwidth rate for each virtual link, thereby effectively virtualizing the available bandwidth of the physical links.

5.1.2 Isolation

The implementation demands that the network designed should provide isolation between slices. This ensures that the operation of a particular slice is not affected by the activities in another slice. We demonstrate the ability of the network designed to provide radio access network (RAN) and transport network isolation. In the demonstration, two slices were created and allocated different PLMN IDs. The two eNBs were configured to broadcast each slice (operator) PLMN IDs on the air interface. Furthermore, traffic separation is done using VLANs to allow easy fulfillment of one of the requirements of the two slices. This will enable each operator to be able to route their traffic through their respective backhaul network. The two physical UEs (one per slice) were connected to their respective vEPCs and throughput measurement performed using the iperf tool. As shown in Figures 19 and 20 in Appendix A, the system guarantees both radio and transport resource isolation so that each slice can obtain only half of the available resources leading to an equal throughput for the UEs.

In the demonstration, we define three isolation attributes that are used for comparison. The first attribute is the control plane. The control plane attribute refers to the control plane of each slice. The LTE control plane is responsible for control operations such as security control, authentication, network attach, setting up of bearers and mobility management. This means a slice control operation should not interfere with the control operation of another slice. At the same time, the control operation of a particular slice should not be interfered by the operation of other slices. In the demonstration, each slice has full control of a set of virtual routers that are not shared with other slices. Only the transport network devices are able to process traffic from multiple slices.

The second isolation attribute for comparison is the user plane. The user plane isolation refers in this case to the network resources at the user plane such as forwarding table and queues. A slice should be allocated enough network resources for its operation without having effect on the other slice data plane. In the demonstration, each slice has its own virtual router but shares the resources of the physical router and links. However, the transport router needs to limit resources to each virtual router, but as the resources are not controlled by the virtual router, limiting the resources available can be done using the transport controller. Therefore, the implementation includes a mechanism for limiting the bandwidth resources for each virtual link by
taking advantage of the QoS features provided by the physical routers. Limiting the bandwidth prevents a slice from starving other slices of bandwidth resources over the transport network. The maximum of the physical link in this slicing setup is 1Gbps, hence each link belonging to the first slice is configured with a bandwidth limit of 700Mbps while the links belonging to the second slice are configured with 150Mbps bandwidth limit.

Note: If nodes can handle packets of wire speed, even shorter packets, then no isolation is needed.

The final isolation attribute for comparison is the address isolation. This isolation attribute refers to the flow space (subset of traffic) available to each slice. To determine which slice a given packet belongs to, a portion of the flow space can be reserved to identify a particular slice. There are many methods that can be used to provide flow space limitation. This implementation uses the VLAN field to identify virtual links between the virtual routers. Portions of the transport network which are VLAN aware include VLAN tags. As frames enter the VLAN aware portion of the transport network, tags are added to indicate VLAN membership. The transport network knows when a tag is related to a virtual link. By this scenario, the entire virtual network becomes available to a particular slice.

5.2 Slice testing and measurements

During the demonstration, we run various tests to determine the throughput and delay of each slice. The setup consists of two UEs (Samsung LTE smart phones), two Nokia LTE Flexi Zone Indoor Pico BTS, four routers (Coriant 8615 and Juniper MX204) connected to each other using fiber cables and two vEPCs deployed on PC engines APU systems. The IP addresses of the two vEPC (AMFs/MMEs) that are successfully connected to the eNBs are 172.16.0.1 and 172.28.0.1 respectively while the IP addresses of the first eNBs (eNB36) are 10.22.196.142 and 10.0.1.138 respectively. The second eNB (eNB37) is also configured with IP address 10.22.196.146 and 10.0.1.58 for both slices. The UE IP address is always assigned by the UPF, in this case the IP address of the UE is 10.200.1.151. Figure 16 shows the configuration parameters of the two different virtual networks (slices).
Next, we need to test if the first eNB (eNB36) configured with two PLMN IDs can properly connect the UEs through their respective slices to the different vEPCs. In order to test this, we deploy two LTE UEs with each having a programmed SIM (subscriber identity module) card. The PLMN IDs configured in the two SIM cards are 24438 and 24439. Each PLMN ID is mapped to a particular slice (virtual network) belonging to a particular mobile operator. As said earlier, the SIM cards were programmed with the IMSI (MCC+MNC+MSIN) of each slice. The IMSI
of the first slice (Red) is 244381000000001 while that of the second slice (Blue) is 244391000000001. The SIM cards were inserted into the respective UEs and their settings changed to detect and connect to only LTE network. The UEs within a few minutes detect the nearby eNB36, initiate an Attach request and connect to their separate vEPCs. The UEs belonging to the different slices were able to access their respective PDNs (Internet). The UEs were then moved to the second eNB (eNB37) to determine if they can still maintain the connection to their respective PDNs. This was successful due to the X2 interface configured between the two eNBs to allow UE handover.

Furthermore, to test the performance of each slice, the throughput of each virtual network (slice) was tested using the iperf tool. The throughput test was done between the UEs and their respective vEPC (UPFs). Both slices produce an average throughput of about 20Mbps as shown in Figure 19 and 20 respectively in Appendix A. To determine the E2E delay of each slice, we perform a ping test between each UE and their respective vEPC (UPF). The average E2E delay measured on the first slice is about 40ms while that of the second slice is 42ms. Figures 21 and 22 in Appendix A show the respective E2E delay measured on the two slices. It is also important to measure the latency between the eNB (slice VLANs) and vEPCs (UPF) of each slice. This is to determine in which virtual network where the delay is. The average latency test measured between the eNBs and the UPFs of the two slices shows a delay less than 0.6ms. These are also shown in Figures 23 and 24 in Appendix A. The overall summary of the delay measured per each slice is shown in Figures 17 and 18 respectively.

Figure 17: Measured delay in virtual network with PLMN ID 24438.

Figure 18: Measured delay in virtual network with PLMN ID 24439.

As shown in Figures 17 and 18, most delay is experienced at the eNB. Low delay or latency could be achieved if a new radio by its interface design can deliver packets with low delay. The 5G network is expected to feature a new radio that has this capability. The testbed could produce low latency if a new radio with minimal delay
is used instead of the LTE radio used in this demonstration. A summary of the measurements performed on the slicing system is shown in the table 3.

Table 3: Measurements performed on each slice.

<table>
<thead>
<tr>
<th>Slice</th>
<th>Maximum Throughput</th>
<th>Average RTT between UE and UPF</th>
<th>Average RTT between eNB and UPF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slice 1 (red)</td>
<td>19.3Mbps</td>
<td>39.957ms</td>
<td>0.486ms</td>
</tr>
<tr>
<td>Slice 2 (blue)</td>
<td>19.1 Mbps</td>
<td>42.11ms</td>
<td>0.538ms</td>
</tr>
</tbody>
</table>

Figure 19 shows a chart of the throughput against maximum transmission unit (MTU) measurement on each slice. The results obtained from both slices are similar therefore a single chart showing the approximate throughput obtained as the MTU (TCP packet size) is varied is presented in Figure 19. The result indicates that increasing packet size increase is proportional to the throughput. In other words as the packet size increases, the throughput also increases. All measured results obtained can be found in Appendix A Figures 26, 27, 28, 29 and 30.

![Figure 19: Measured Throughput against different MTUs.](image)

5.2.1 Discussion of results

Based on the various measurements performed on the slicing system implementation, the results show that the slicing system works practically well even though there is high E2E delay. Most of the delay experienced is likely due to the inability of
the LTE base station to deliver packet with very low delay. The backhaul network does not have this problem. The slice measurement in backhaul show that very low latency or delay can be achieved by having a base station that by its interface design can deliver packets with low delay. The 5G base station is expected to deliver packets with low delay, therefore very low E2E delay could be achieved if used in this project.

5.3 Limitations

Even though the implementation of the designed network slicing system was successful, there are some limitations that need to be considered if one is to develop larger slicing system based on this idea.

5.3.1 Hardware

Maybe the difference between the slicing solution implemented in this thesis and other solutions is the hardware used. Although the implementation was done using real network devices, there is a limitation as to the number of network slices that can be created. Slicing the backhaul network in this system is not a big problem since this is just a matter of creating more VLANs and virtual routers. The limitation is about the number of slices the base station can support. The Nokia LTE Flexi Zone Indoor Pico base station used in this experiment supports only two transport area control (TAC) configuration. This means that transport sharing (number of user plane VLANs) in the base station is limited to two even though more VLANs can be configured in the base station. This limitation becomes a problem if the slicing system is to be adopted in a production network to support the numerous 5G use cases where multiple slices (more than 2) are required. Another limitation is the allocation of node resources such as CPU resources to each virtual router. There is a possibility that that some virtual routers consume more CPU resources, starving other virtual routers (e.g. CPU over provisioning). This might be more difficult to implement and is beyond the scope of this project.

5.3.2 Broadband management protocol (BMP)

Another limitation encountered during the slicing system implementation is about the protocol used between the transport controller (Coriant 8000 INM) and the network devices, the broadband management protocol (BMP). As stated earlier, the slicing system is implemented using two different kinds of network devices from different vendors. The 8615 smart router from Coriant and Juniper MX204 from Juniper Networks. The BMP is a Coriant proprietary protocol and can be used between Coriant devices, thus between the 8000 INM and the 8615 routers. This means that a license is required in order to use this protocol. Also, to enable the transport controller to communicate with the Juniper devices, a standard protocol (SNMP) has to be used. The use of two different protocols between the transport controller and the network nodes in a slicing system might have an effect in managing and controlling the transport network.
5.4 Future Work (X-Network)

Considering this thesis work as the basis to upgrade the current X-Network LTE mobile network, there is a lot to be explored as part of the future work and improvements. The name X-Network refers to an LTE mobile network that was built cooperatively by Nokia and Aalto University. One of the future works could be to add more use case scenarios along with multiple RAN slicing. This means a base station that can support multiple RAN sharing and transport sharing would be needed. Another future work could be to add a simple slice orchestrator on top of the transport controller taking advantage of its Northbound Interface features. A simple slice orchestrator could have the function that could create, modify and delete a slice in the network slicing system within a few seconds. Also, to ensure that the X-Network provides a wider coverage to the Otaniemi campus, a lower frequency (e.g. 700Mhz) will be needed.
6 Conclusion

This thesis report discusses the concept of network slicing as an important aspect of the 5G architecture by first explaining some of the key enablers of this concept. RAN sharing and transport sharing are identified as an integral part of this concept. In addition, some background information about the various technologies and how they can be used to implement the concept were explained as well as some use cases. The goal of this thesis was to design and implement a network slicing system that supports Ultra Reliable Low Latency Connectivity (URLLC). This implementation is part of a larger project known as the WIVE project. To achieve this goal, network virtualization concept was adopted, and two aspects of the mobile network were considered, the RAN and the backhaul network. Slicing the RAN network was achieved by configuring the eNB to broadcast multiple PLMN IDs while the transport (backhaul) slicing was done using a combination of both layer 2 and layer 3 virtualization technologies. For reliability and high availability, redundant paths were created and VRRP mechanism was used between virtual routers. The slicing does not extend to the EPC, meaning that EPC virtualization is not part of thesis project.

The system implementation is able to meet the goal of this thesis even though there are some limitations. Successful implementation of the slicing system implies that network slicing is feasible to implement. A slice is a virtual network created by virtualizing the underlying physical network. The slicing system is also evaluated for performance by measuring the E2E delay of each slice as well as the delay in the backhaul network. The result shows high E2E delay in each slice due to the eNB used for this project. To meet the 5G latency requirement for an URLLC, a 5G radio is needed. Overall the network slicing system implemented in this thesis meets the design requirements and can be adopted and implemented in the Otaniemi 5G test network (X-Network).
References


[36] 3GPP TS 22.261 V0.1.1, Technical Specification Group Services and System Aspects; 'Service requirements for next generation new services and markets,' (Rel. 15), August 2016


[46] Cumucore, Cumucore vEPC Installation, Espoo, Finland

[47] Coriant, 'USER INSTRUCTIONS,' 8000 Intelligent Network Manager Online Documentation, 2018


A Appendix

Figure A1: Measured throughput for slice 1 with PLMN ID 24438

Figure A2: Measured throughput for slice 2 with PLMN ID 24439
Figure A3: E2E measured delay for slice 1 between UE and UPF.

Figure A4: E2E measured latency for slice 2 between UE and UPF.
Figure A5: Latency measured for first slice 1 between UPF and eNB.

Figure A6: Measured latency for slice 2 between UPF and eNB.
<table>
<thead>
<tr>
<th>Interval</th>
<th>Transfer</th>
<th>Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.00-1.00 sec</td>
<td>640 KBytes</td>
<td>1.20 MBytes/sec</td>
</tr>
<tr>
<td>1.00-2.00 sec</td>
<td>1.16 MBytes</td>
<td>9.76 MBytes/sec</td>
</tr>
<tr>
<td>2.00-3.00 sec</td>
<td>1.19 MBytes</td>
<td>10.0 MBytes/sec</td>
</tr>
<tr>
<td>3.00-4.00 sec</td>
<td>1.19 MBytes</td>
<td>9.99 MBytes/sec</td>
</tr>
<tr>
<td>4.00-5.00 sec</td>
<td>1.17 MBytes</td>
<td>9.82 MBytes/sec</td>
</tr>
<tr>
<td>5.00-6.00 sec</td>
<td>1.17 MBytes</td>
<td>9.82 MBytes/sec</td>
</tr>
<tr>
<td>6.00-7.00 sec</td>
<td>1.21 MBytes</td>
<td>10.2 MBytes/sec</td>
</tr>
<tr>
<td>7.00-8.00 sec</td>
<td>1.21 MBytes</td>
<td>10.1 MBytes/sec</td>
</tr>
<tr>
<td>8.00-9.00 sec</td>
<td>1.23 MBytes</td>
<td>10.4 MBytes/sec</td>
</tr>
<tr>
<td>9.00-10.00 sec</td>
<td>1.23 MBytes</td>
<td>10.4 MBytes/sec</td>
</tr>
<tr>
<td>10.00-10.12 sec</td>
<td>1.64 KBytes</td>
<td>10.8 MBytes/sec</td>
</tr>
</tbody>
</table>

Figure A7: Throughput measured when MTU is 100 bytes

<table>
<thead>
<tr>
<th>Interval</th>
<th>Transfer</th>
<th>Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.00-1.00 sec</td>
<td>11.6 MBytes</td>
<td>9.58 MBytes/sec</td>
</tr>
<tr>
<td>0.00-1.12 sec</td>
<td>11.6 MBytes</td>
<td>9.58 MBytes/sec</td>
</tr>
</tbody>
</table>

Figure A8: Throughput measured when MTU is 200 bytes
Figure A9: Throughput measured when MTU is 500 bytes

<table>
<thead>
<tr>
<th>ID</th>
<th>Interval</th>
<th>Transfer</th>
<th>Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>0.00-1.00 sec</td>
<td>1.26 MBytes</td>
<td>10.6 Mbits/sec</td>
</tr>
<tr>
<td>5</td>
<td>1.00-2.00 sec</td>
<td>1.53 MBytes</td>
<td>12.9 Mbits/sec</td>
</tr>
<tr>
<td>5</td>
<td>2.00-3.00 sec</td>
<td>1.51 MBytes</td>
<td>12.7 Mbits/sec</td>
</tr>
<tr>
<td>5</td>
<td>3.00-4.00 sec</td>
<td>1.58 MBytes</td>
<td>13.2 Mbits/sec</td>
</tr>
<tr>
<td>5</td>
<td>4.00-5.00 sec</td>
<td>1.55 MBytes</td>
<td>13.0 Mbits/sec</td>
</tr>
<tr>
<td>5</td>
<td>5.00-6.00 sec</td>
<td>1.56 MBytes</td>
<td>13.1 Mbits/sec</td>
</tr>
<tr>
<td>5</td>
<td>6.00-7.00 sec</td>
<td>1.58 MBytes</td>
<td>13.2 Mbits/sec</td>
</tr>
<tr>
<td>5</td>
<td>7.00-8.00 sec</td>
<td>1.53 MBytes</td>
<td>12.9 Mbits/sec</td>
</tr>
<tr>
<td>5</td>
<td>8.00-9.00 sec</td>
<td>1.52 MBytes</td>
<td>12.8 Mbits/sec</td>
</tr>
<tr>
<td>5</td>
<td>9.00-10.00 sec</td>
<td>1.57 MBytes</td>
<td>13.2 Mbits/sec</td>
</tr>
<tr>
<td>5</td>
<td>10.00-10.26 sec</td>
<td>411 KBytes</td>
<td>13.1 Mbits/sec</td>
</tr>
</tbody>
</table>

Figure A10: Throughput measured when MTU is 1000 bytes

<table>
<thead>
<tr>
<th>ID</th>
<th>Interval</th>
<th>Transfer</th>
<th>Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>0.00-1.00 sec</td>
<td>15.6 MBytes</td>
<td>12.8 Mbits/sec</td>
</tr>
<tr>
<td>5</td>
<td>0.00-10.26 sec</td>
<td>15.6 MBytes</td>
<td>12.8 Mbits/sec</td>
</tr>
<tr>
<td>5</td>
<td>10.00-10.26 sec</td>
<td>343 KBytes</td>
<td>13.1 Mbits/sec</td>
</tr>
<tr>
<td>ID</td>
<td>Interval</td>
<td>Transfer</td>
<td>Bandwidth</td>
</tr>
<tr>
<td>----</td>
<td>------------</td>
<td>----------</td>
<td>-----------</td>
</tr>
<tr>
<td>5</td>
<td>0.00-1.00</td>
<td>sec 2.14 MBytes 17.9 Mbits/sec</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>1.00-2.00</td>
<td>sec 2.37 MBytes 19.9 Mbits/sec</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>2.00-3.00</td>
<td>sec 2.40 MBytes 20.1 Mbits/sec</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>3.00-4.00</td>
<td>sec 2.40 MBytes 20.1 Mbits/sec</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>4.00-5.00</td>
<td>sec 2.40 MBytes 20.1 Mbits/sec</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>5.00-6.00</td>
<td>sec 2.40 MBytes 20.1 Mbits/sec</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>6.00-7.00</td>
<td>sec 2.40 MBytes 20.1 Mbits/sec</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>7.00-8.00</td>
<td>sec 2.40 MBytes 20.1 Mbits/sec</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>8.00-9.00</td>
<td>sec 2.40 MBytes 20.1 Mbits/sec</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>9.00-10.00</td>
<td>sec 2.40 MBytes 20.1 Mbits/sec</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>10.00-10.20</td>
<td>sec 482 KBytes 20.1 Mbits/sec</td>
<td></td>
</tr>
</tbody>
</table>

**Figure A11:** Throughput measured when MTU is 1500 bytes