Addis Ababa University

Addis Ababa Institute of Technology

School of Electrical and Computer Engineering

Telecommunication Engineering Graduate Program

Software Defined Networks Based Seamless MPLS QoS

By:

Asheber Bekele GSR/2170/13

Advisor:

Dr. Sosina Mengistu

A Thesis Submitted to the School of Electrical and Computer Engineering in Partial Fulfillment of the Requirements for the Degree of Masters of Science in Telecommunication Engineering

October 12, 2023

Addis Ababa, Ethiopia

Addis Ababa Institute of Technology

School of Electrical and Computer Engineering

Telecommunication Engineering Graduate Program

Software Defined Networks Based Seamless MPLS QoS

By: Asheber Bekele

Approval by Board of Examiners

_____	_____	_____/_____/_____
School Dean	Signature	Date
Dr. Sosina Mengistu_____	_____	_____/_____/_____
Advisor	Signature	Date
Dr. Fitsum Assamnew____	_____	_____/_____/_____
Examiner	Signature	Date
Dr.Ephrem Teshale_____	_____	_____/_____/_____
Examiner	Signature	Date
_____	_____	_____/_____/_____
Examiner	Signature	Date

October 12, 2023

Addis Ababa, Ethiopia

Declaration

I, the undersigned, declare that this Master's thesis is my original work, has not been presented for a fulfilment degree in this or any other university, and all sources of materials used for the thesis have been fully acknowledged.

Name: Asheber Bekele Signature: _____

Place: Addis Ababa Date of Submission: _____

This thesis has been submitted for examination with my approval as a university advisor.

Advisor's Name: Dr. Sosina Mengistu Signature_____

ACKNOWLEDGEMENTS

First, I want to thank God for blessing me and helping me successfully complete my research work.

Next, I want to express my gratitude to Sosina Mengistu (PhD) for being my advisor throughout my thesis work. She has consistently supported and guided me. She watched carefully, gave straightforward advice, and helped me in a positive way. Ephrem Teshale (PhD) and Fitsum Assamnew (PhD) assessed my work and gave valuable suggestions and feedback while I was working on my thesis. I am grateful for their support.

I would like to thank ethio telecom and AAiT for their support and sponsorship in making this program successful.

I want to say a big thank you to all my friends at work, especially Workneh Berhanu and Medhin Worku.

Lastly, I would like to extend my sincere gratitude towards my family. First and foremost, I would like to express my gratitude to my loving and supportive wife, Kidist, and my two amazing children, Deborha and Yoseph, who continuously inspire me. I would like to give a special acknowledgment and gratitude to my grandmother, mother, as well as my sister's and brother's, for the numerous sacrifices you have selflessly made for my benefit. During my academic journey, they have consistently provided me with valuable support

Abstract

The Internet service provider (ISP) need more advanced MPLS networks for improved performance. The MPLS protocol tries its best to provide good service, but it does not guarantee traffic priority or quality. The Seamless MPLS (S-MPLS) technology improved performance by integrating both aggregate and core networks into one MPLS domain. However, there are some problems that make it hard to control the amount of data being used and the path that data takes when there is a lot of internet traffic. Implementing QoS in S-MPLS can also enhance ISP network performance. However, QoS in Seamless MPLS allows headend routers in an AS to optimize traffic routing without considering the needs of other AS routers. Using SDN-based Seamless MPLS QoS will be able to see the entire network topology of different domains, monitor of the status of the links, add or remove forward traffic information and guarantee end-to-end quality of service.

The inspiration of this proposal is to examine and analyze impacts of QoS actualizing in seamless MPLS with SDN based seamless MPLS. This study examines the effects on Quality of Service (QoS) parameters through the analysis of four distinct scenarios Seamless MPLS, QoS Seamless MPLS, SDN based Seamless MPLS and QoS SDN based Seamless MPLS with Several different domains are combined into one large MPLS domain. Simulation tools like GNS3, Ostinato, and Wire shark are used to compare how well the four scenarios perform.

The analysis results show that in QoS SDN based Seamless MPLS throughput is improved by 14.7%, latency is improved by 12.8%, and packet loss is improved by 18% compared to Best Effort Seamless MPLS. Based on the research findings, it is evident that the adoption and implementation of Quality of service (QoS) Software Define Network (SDN) based Seamless Multi-Protocol Label Switching (MPLS) can confer various benefits in service provider core network.

Keywords—Seamless MPLS, QoS, SDN, Performance, Analysis

Table of Content

List of Acronyms

2G	Second Generation
3G	Third Generation
4G	Fourth Generation
AAA	Authentication, Authorization and Accounting
ABR	Area Border Router
AN	Access Network
API	Application Programming Interface
AS	Autonomous System
ASBR	Autonomous system boundary router
ASG	Aggregation Service Gateway
ATM	Asynchronous Transport Mode
BGP	Boarder Gateway Protocol
BGP-LS	BGP-Link State
BGP-LU	BGP-Labeled Unicast
BNSF	Base Network Service Functions
BR	Backbone Router
CAPEX	Capital Expenditures
CCP	Centralized Control Plane
C-DPI	Controller-Data Plane Interfaces
CE	Customer Edge Router
CLI	Command Line Interface
DCP	Distributed Control Plane
Diffserv	Differentiated-Service
eBGP	Exterior BGP
EGP	Exterior Gateway Protocol
EIGRP	EIGRP Enhanced Interior Gateway Routing Protocol
ER	Edge Router
ERO	Explicit Route Object
FEC	Forwarding Equivalency Class
GE	Gigabit Ethernet
GNS3	Graphical Network Simulator-3
GUI	Graphical User Interface
HCP	Hierarchical Control Plane
HE	Head End

HTTP	Hypertext Transfer Protocol
iBGP	Interior BGP
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
IP	Internet Protocol
IS-IS	Intermediate System - Intermediate System
ISP	Internet Service Provider
JAR	Java ARchive
JSON	JavaScript Object Notation
JVM	Java Virtual Machine
L2	Layer 2
L3	Layer 3
LAN	Local Area Network
LDP	Label Distribution Protocol
LER	Label Edge Router
LFIB	Label Forwarding Information Base
LSP	Label Switch Path
LSR	Label Switch Routers
LTE	Long Term Evolution
MAC	Media Access Control
MD-SAL	Model-Driven SAL
MPLS	Multi-protocol label switch
MPLS-TE	MPLS Traffic Engineering
NAT	Network Address Translation
NB	Northbound
NBI	NB Interface
NetConf	Network Configuration protocol
NETCONF	Network Configuration Protocol
NH	Next Hop
NHS	Next Hop-Self
NLRI	Network Layer Reachability Information
NMS	Network Management System
NOS	Network Operating System
NQA	Network Quality Analyzer
OAM	Operation, Administration and Maintenance
ODL	OpenDaylight

OF	OpenFlow
OPEX	Operational Expenditures
OSI	Open Source Interconnection
OVS	OpenvSwtich
OVSB	Open vSwitch Database
OVSDB	OVS Database
P	Provider Router
P2P	Point-To-Point
PCC	Path Computation Client
PCE	Path Computation Element
PCEP	Path Computation Element Protocol
PCErr	Path Computation Error
PCNtf	Path Computation Notification
PCRep	Path Computation Reply
PCReq	Path Computation Request
PE	Provider Edge Router
PHP	Penultimate Hop Popping
PW	Pseudo Wire
QoS	Quality of Service
RAM	Random Access Memory
RAN	Radio Access Network
REST	Representational State Transfer
RESTCONF	REST Configuration Protocol
RFC	Request for Comment
RIB	Routing Information Base
RIP	Routing Information Protocol
RPC	Remote Procedure Call
RR	Route Reflector
RSVP	Resource Reservation Protocol
RSVP	Resource Reservation Protocol
SAL	Service Abstraction Layer
SB	Southbound
SBI	SB Interface
SDN	Software Defined Network
SDN	Software Defined Networking
SLA	Service-level agreements
S-MPLS	Seamless Multiprotocol label switching

SNMP	Simple Network Management Protocol
SP	Service Provider
SSH	Secure Shell
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TE	Traffic Egineering
TED	Traffic Engineering Database
TTL	Time to Live
VLAN	Virtual LAN
VPLS	Virtual Private LAN Service
VPN	Virtual Private Network
VPWS	Virtual Private Wire Service
VRF	Virtual Routing and Forwarding

List of Figures

List of Tables

1. Introduction

1.1. Background

The increasing popularity of web-based services like VoIP, IPTV, and video conferencing has led to a need for augmented bandwidth resources. To improve network efficeny, service providers must have a backbone network that can swiftly switch and forward customer traffic. Traditional network architectures have limitations, such as maximizing costs and having a longer time to market. The IETF created MPLS, which employs label technology for packet forwarding, to overcome the shortcomings of conventional IP networks. MPLS traffic engineering chooses the most effective channel for data packet forwarding, allowing for optimal use of network resources. IP/MPLS services are most commonly used for VPN services, with MPLS technology at the core [1]. Qualtiy of sevice is a different way to save money instead of using a tool that controls the amount of data being used on a specific network.

Quality of Service (QoS) refers to the capacity of a network to provide enhanced service to selected network traffic across a range of technologies. The overarching objective of QoS is to facilitate priority features, including dedicated bandwidth, controlled levels of jitter and latency, as well as improved loss characteristics. Quality of Service (QoS) mechanisms guarantee the provision of end-to-end performance assurances to users by leveraging a diverse range of technologies. These technologies encompass resource reservation, allocation, prioritized scheduling, queue management, and routing strategies, all of which can be effectively implemented through a network operating system. [2].

Most service provide as ethiotelcom backbone networks often use the best effort (BE), otherwise referred to as First in First out (FIFO), for service segregation. Customers categorized based on service type and payment scheme. The MPLS Label Distribution Protocol Best Effort (MPLS LDP + BE) was chosen for constructing the backbone network

due to its convenient installation process. This approach ensures traffic follows the shortest route, causing congested links and underutilizing other links [3].

SDN is a new internet architecture that provides flexibility and programmability by obtaining a comprehensive overview of the network and its utilization, including information about connection usage and network congestion. SDN separates the intelligence of the network from the devices that do the actual work, and puts it in a central controller. The controller communicates with the devices through the OpenFlow protocol. Packet forwarding elements in the data plane match incoming flows and perform defined actions, whereas the control plane handles routing choices. Because of its flexibility and reactivity, SDN is well suited for new technologies such as Core network, 5G and cloud data centers [2].

This paper motivation to investigation the Quality of Service Performance advantages by the comparison of Seamless MPLS with SDN based seamless MPLS. By four scenarios are simulated and graphically shown for comparison and study with regard to QoS Performance criteria.

1.2. Problem Statement

In order to supply a variety of telecom services, telecom service providers need many infrastructures. Real-time applications including phone, video, and data are being used Seamless MPLS is becoming more and more important. However, if a network expansion is not deployed in a timely manner, network congestion may lead to packet loss, which would harm the company's customer experience and revenue.

The majority of service providers operate their networks using the best-efforts (BE) service scenario. Using the BE scenario in a network causes network congestion since diverse access devices are contributing to the constant increase in traffic volume.

The seamless MPLS protocol tries its best to provide good service, but it doesn't guarantee traffic priority or quality of service. When the links are not optimized, it becomes hard to control how much bandwidth is used and maintain a steady flow of traffic during

congestion. This is the main problem or disadvantage of Seamless MPLS. It is challenging to give better QoS for users because of this constraint. Bandwidth reallocation and congestion management are required individually for each head end router in each Autonomous System (AS) when implementing QoS in a seamless MPLS network, without taking into account any other Autonomus System.

To address these challenges, SDN based seamless MPLS QoS for different network domains . By using the benefits of SDN controller, we can see the entire network structure, which helps improve the quality of service for network performance.

1.3. Objective

1.3.1. General Objective

The primary aim of this investigation is to conduct a comparative evaluation of the Quality of Service (QoS) performance between seamless Multiprotocol Label Switching (MPLS) and Software Defined Networking (SDN)-based seamless MPLS networks.

1.3.2. Specific Objectives

The specific objectives of this thesis are:

- To simulate and evaluate QoS parameter in Seamless-MPLS and SDN based Seamless MPLS
- Compare and analysis current QoS parameter in seamless MPLS with SDN based seamless MPLS
- To check the effect of usingSeamless MPLS with SDN based Seamless MPLS on QoS parameters Latency, Throughput and Packet loss.

1.4. Methodology

To attain the aims, the technique planned to be employed in the study is first state of the art, similar research projects, and problem statements are used as a baseline. The process starts with a look at the various technologies that provide SDN-based Seamless MPLS

QoS. The methodologies for modeling and assessing the architecture's performance are then used. This study undertook a comprehensive way theoretical analysis of the Seamless MPLS and SDN based Seamless MPLS with and without Quality of Service (QoS) discussed.

In the course of implementation, a practical environment is developed through the utilization of a network simulation tool like GNS3, SDN, and Wireshark etc. The subsequent graphic representations serve to compare and analyze the test results across four scenarios, specifically in relation to performance metrics.

- To Simulate and evaluate Seamless MPLS, QoS Seamless MPLS, SDN based Seamless MPLS with and without Quality of Service (QoS) using GNS3 and Open daylight
- To analysis performance of these four scenario by using Ostinato traffic generator
- To compare the analysis results of these four scenario by using Wireshark network analyzer.

1.5. Scope and Limitations

1.5.1. Research Scope

This thesis works on QoS Performance Evaluation of Software Define Network based Seamless MPLS. The present study employs simulation, measurement, and analysis techniques to investigate the latency, throughput, and packet loss characteristics of Seamless MPLS and SDN-based Seamless MPLS networks, both with and without Quality of Service (QoS) provisions.

1.5.2. Limitations of the Study

This research proposal focuses exclusively on a subset of service provider access, aggregator and core network domains which is Labeled BGP access with flat LDP core and aggregation network and also limited to measure the QoS performance of SDN

based Seamless MPLS with existing Seamless MPLS using performance measurement namely latency , throughput and packet lost.

1.6. Contributions

The service provider network has different types of services with different quality requirements. It is important to find ways to meet the needs of each service while making the best use of network resources that change over time. This is a major challenge for the network. We use an SDN controller and seamless MPLS to create a better quality of service for Differentiated-Service (DiffServ) traffic. The objective of this thesis is to enhance the quality of service (QoS) performance of end-to-end networks through the integration of emerging software-defined networking (SDN) technologies with the existing seamless multiprotocol label switching (MPLS) architecture. This enhances the flexibility and scalability of service delivery in the telecommunications industry's core IP/MPLS network, while reducing the constraints of conventional seamless MPLS design.

1.7. Literature Review

Seamless MPLS consolidates multiple ISP networks' MPLS domains into a single domain. However, implementing Quality of Service in different network domains cannot guarantee end-to-end service quality. SDN-based with Seamless MPLS QoS is feasible solution, but performance is not yet analyzed.

Recently, researchers proposed several schemes for QoS seamless MPLS based IPBackbone .

The author in [4] have described the MPLS and Seamless MPLS are analyzed and compared using four quality of service performance measures: throughput, latency, packet loss, and jitter. First, the author set up two network situations called MPLS and Seamless MPLS using eNSP and their respective configuration files. Following that, network traffic is produced with Ostinato, simulation data is collected with Network Quality Analyzer (NQA), and the findings are presented with MATLAB. From comparisons result Seamless MPLS significantly enhances file transfer throughput by

36.87%, reduces end-to-end packet delay by 15.98%, and reduces packet loss and jitter by 12.5% compared to MPLS. The research paper has limited to Seamless MPLS and does not consider QoS Seamless MPLS.

The objective of research in [3] is to enhance the efficiency of link utilization in the IP core network of ethio telecom by implementing MPLS TE + QoS. She will compare the network performance of the current MPLS LDP + BE with the suggested MPLS TE + QoS. By applying Traffic Engineering (TE) and Quality of Service (QoS) techniques in the GNS3 platform, network analysis was conducted to evaluate its performance. The analysis involved comparing the network's conditions before and after TE + QoS implementation, focusing on the enhancement of throughput, reduction in packet loss, and improvement in latency. The results demonstrated a noteworthy 26% increase in throughput, a 6% decrease in packet loss, and a remarkable 21% decrease in latency. Using MPLS TE + QoS in the core network does not guarantee a consistent level of service across different domain network approaches.

The researchers in [5] presents an approach to improve the QoS in seamless MPLS Networks by implementing the Resource Reservation Protocol (RSVP). RSVP-TE helps bundle user data into an RSVP LSP that goes to a distant LDP destination, so it can take advantage of features like quick alternate route selection and efficient traffic management. It deviates from the IGP by independently assessing and making decisions regarding reserved traffic. The current investigation is using a tool called the Enterprise Network Simulation Platform (ENSP) to study the Seamless MPLS architecture along with an architecture called RSVP-TE Seamless MPLS. The findings indicate that there is a 19% enhancement in throughput. When the size of the file increases, there is a 12.5% reduction in Jitter and a 21.45% decrease in latency. RSVP-TE Seamless MPLS was found to be more dependable than seamless MPLS, according to the analyses and results.

In [6] the assessment of Quality of Service (QoS) implementation in MPLS networks was conducted in collaboration between the IP Precedence (IPP) and Class-Based Queuing (CBQ). In the absence of prioritized bandwidth allocation, the throughput for all types of network traffic experienced a considerable reduction from 2 megabits per second (Mbps)

to below 200 kilobits per second (kbps). However, if the traffic is given special bandwidth and prioritized treatment, it guarantees that all traffic near the Quality of Service (QoS) allocation for bandwidth will receive the specific amount of bandwidth required for particular applications. This is similar to how a virtual private network (VPN) network is set up. All of the cited contributions share a common characteristic - they address the concept of Quality of Service (QoS) on various MPLS networks. However, these contributions fail to take into account the broader perspective of other network domains and are unable to ensure end-to-end Quality of Service.

In [7] the proposed incremental deployed approach, SoIP, Improving the quality of service assurance in the Internet is achieved through the creation of a software-defined overlay network that is built on top of the existing IP network. This utilizes per-flow management in SDN to meet resource demands while maintaining differentiated services. A coupling mechanism is proposed for better resource utilization.

Minimize jitter in SDN by utilizing dynamic features, monitoring real-time network device status, and rerouting packets based on available bandwidth. [8] Proposed a The Quality of Service (QoS) management framework is responsible for the dynamic allocation of network resources to ensure desired levels of QoS. The researchers employed a route optimization algorithm in order to oversee the state of network devices and ascertain the optimal route for rerouting QoS traffic. The writers showed that if we can find when there is too much data being sent at once, we can send the important data on a different path with more space for it. This would help reduce the chances of losing any packets of data. This plan uses Dijkstra's algorithm to make congestion, throughput, packet loss, and jitter better. However, we have not yet analyzed how well SDN based seamless MPLS QoS performs.

1.8. Thesis Layout

This thesis consists of a total of six chapters. The first chapter provides comprehensive coverage of the study's introduction, problem statement, objectives, literature review, scope, and limitations. The second chapter provides an introduction to MPLS, Seamless

MPLS architecture, Quality of Service, and their respective features. The third chapter examines SDN and its associated protocols, including Path Computation Element and the OpenDaylight controller. In the fourth chapter of this thesis, explains the setup of the simulation network utilizing the Seamless MPLS simulation tools. Moving on to the fifth chapter, the simulation results for packet loss, latency, and throughput are presented along with their analysis. The final chapter encompasses the thesis' conclusion and outlines potential future directions.

.

2. Seamless MPLS

2.1. Multiprotocol Label Switching (MPLS)

MPLS is a way to send information quickly and efficiently in advanced communication networks by using short labels. This method can expand, offer full IP services, and is easy to install and manage. The packet is located between the headers of Layer 3 and Layer 2 protocols. MPLS is a type of networking protocol that sits between layers 2 and 3 of the OSI model. It helps with transferring data on a network.

MPLS is commonly used in phone and internet networks to make data transfer faster and better. MPLS works in the network layer of a computer network and uses labels to guide data packets along specific routes that have already been set up. This helps data move quicker by finding the fastest route. MPLS is very helpful in networks with lots of data and complicated routing needs. In simple terms, MPLS is a useful way to combine different communication protocols and transfer data efficiently in telecom networks. These protocols create rules and guidelines for communication, making sure interactions are smooth and the same for everyone. Some examples of network protocols are TCP, IP, and HTTP. These rules are really important for making different networks, like the internet, work well together. MPLS can help with many different ways to connect to the internet [1].

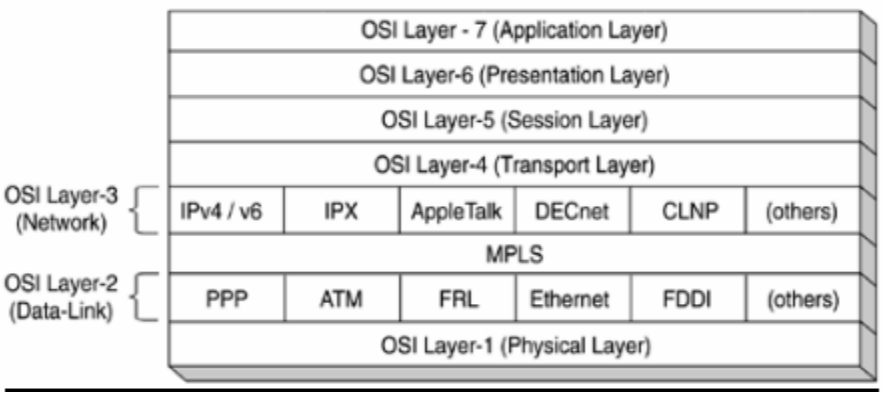

Figure 1:Position of MPLS in OSI Mode [1]

The label has 20 bits, the Class of Service has 3 bits, and the label stack has 1 bit [1]. Just like IP, it also has fields that tell us about the quality of service and how long the packet will exist. In backgrounds without ATM, there is only a code called virtual channel identifier (VCI) or virtual path identifier (VPI). This code helps routers find the next address to send a packet faster [9] [10].

2.1.1. MPLS Header

MPLS headers use a 20-bit label Use a 20-digit code to identify the Label Switched Path (LSP) in the packet, which is created using Forwarding Equivalency Class (FEC). The EXP field is a small part of data with 3 bits that helps with Quality of Service functions. The stack field indicates the bottom of the label stack. The 8-bit TTL field functions similarly to the TTL field in IP headers.

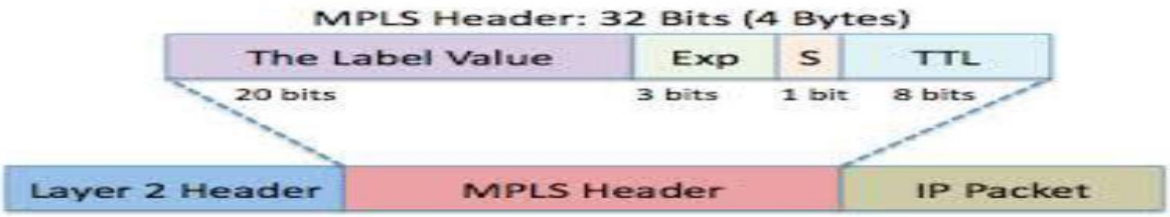

Figure 2: MPLS Header[11]

2.1.2. MPLS Architecture

The center part of MPLS is composed of Label Switch Routers (LSRs), while the outer part is composed of Label Edge Routers (LERs). Certainly, here are some key terminologies associated with MPLS (Multiprotocol Label Switching) technology [5][12][13]:

- **Label:** A short identifier given to each packet by a special MPLS router to help identify and manage the packets. It helps decide the route the packet should take in the network.
- **Label Switching Router (LSR):** it refers to any router that is located in the MPLS (Multiprotocol Label Switching) domain functions by utilizing label switching

mechanisms in order to forward packets. When a Label Switching Router (LSR) receives a packet, it proceeds to perform a lookup operation in its designated routing table in order to determine the appropriate next hop for the packet. The process involves the removal of the previous label affixed to the header, followed by its subsequent replacement prior to the packet's transmission to the subsequent hop. [14].

- **Label Forwarding Information Base (LFIB):** A table that is saved in a Label Switching Router (LSR). It matches labels that come in with the interfaces and labels that they should be sent out through.

- **Label Distribution Protocol (LDP):** A method for routers to share labels with each other in order to create paths for switching labels.

- **Label Edge Router (LER):** A router that serves as a starting or ending point to an MPLS network. It assigns labels to incoming packets and takes label off outgoing packets

- **Label Switched Path (LSP):** The path that a labeled packet follows through the network based on the labels assigned to it.

- **Forwarding Equivalence Class (FEC):** The data flow in question is regularly treated in the same manner during forwarding operations, and its identification is based on features such as address, tunnel, and a certain Class of Service (CoS) that the device typically assigns to the corresponding label of Forwarding Equivalence Classes (FECs). Subsequently, a packets assigned to a certain Forwarding Equivalency Class (FEC) will be routed through an appropriate label switched path (LSP). As soon as the router receives a packet, it begins evaluating whether or not it fits into one of the Forwarding Equivalency Classes (FEC) models that have previously been set up. Rather of being actual labels or packets, Forwarding Equivalency Classes (FECs) are notional entities created by routers [3].

- **Penultimate Hop Popping (PHP):** A method where the second-to-last router before the final destination removes the MPLS label to show the original packet's header.

2.1.2.1. MPLS Methodology of Operation

Multiprotocol Label Switching (MPLS) is a technology that makes sending and receiving data over the internet faster and more efficient by combining information from different layers of the network. By assigning packets to a specific FEC only once, the goal is to speed up how quickly the packets are delivered. IP packets are sorted into groups by Label Edge Routers (LSRs) using a small label. After the IP packets' MPLS headers have been assigned by the starting point LSRs, middle LSRs direct the packets through the chosen Label Switch Path (LSP). The substitution of the label on the outgoing packet occurs through the replacement with the label obtained from the incoming packet. This process is accomplished through the utilization of the Forwarding Equivalence Class (FEC) table within routers, and subsequently transmitted to the subsequent Label Switching Router (LSR). Upon reaching the Egress Label Switching Router (LSR), the label is removed and the packet is transmitted as an IP packet towards the designated destination address [1][11].

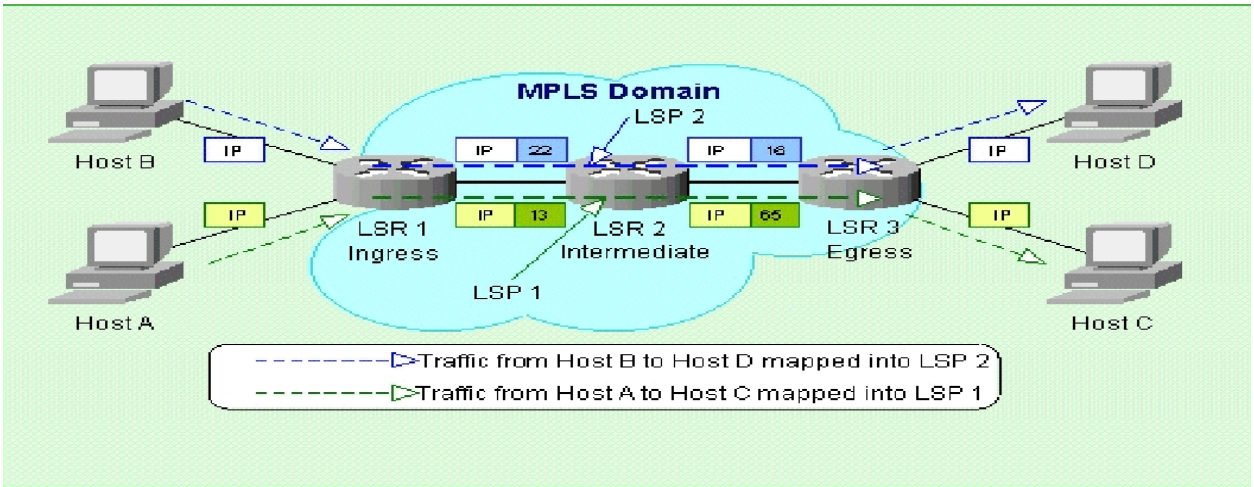

Figure 3: MPLS Operation [15]
(Source: http://www.slideshare.net/ameliakot/fyp-presentation-15100528)

Multiprotocol Label Switching (MPLS) encompasses a range of operational procedures, comprising the swap, push, and pop operations [1].

- In the swap operation, the assigned label is exchanged with a newly designated label, thereby facilitating the forwarding of the packet along the designated path of the newly assigned label.
- In the process of a push operation, the extra label is added to the existing label, creating another layer of Multi-Protocol Label Switching (MPLS) around the packet.
- During the execution of a pop operation, the removing of the outer label from the package subsequently unveils an inner label beneath. If the last label on the label stack is removed, the packet will leave the MPLS tunnel and usually the egress router will help with this. These actions do not examine the information inside the packet below the MPLS Label stack. This means that the packets can be forwarded without depending on a specific routing table for each protocol. At the point of egress routing, solely the payload persists subsequent to the elimination of the final label, necessitating the availability of routing particulars regarding the packet's payload.

2.1.3. MPLS Layer 3 VPNs

MPLS Layer 3 VPNs enable private and secure networks over shared infrastructure. MPLS L3 VPNs connect multiple sites securely. This tech is often used in enterprise networks to securely connect dispersed offices or remote users to a central network. MPLS Layer 3 VPNs use labels to route traffic between sites, ensuring secure delivery of data. This network technology is gaining popularity for its scalability, flexibility, and cost-effectiveness. MPLS Layer 3 VPNs provide secure and efficient network communication.

RFC 2547bis allows service providers to use their internet network to offer secure connections for clients. RFC 2547bis VPNs, which are also called BGP/MPLS VPNs, use

BGP to share information about the routes for the VPN within the provider's main network. The goal of this strategy is to develop a service that is easy for users to navigate and can be implemented on a large scale. This service will allow for the establishment of Virtual Private Network (VPN) policies, either by the service provider alone or in partnership with the client.

2.1.3.1. MPLS Layer 3 VPNs Network Components

Allow service providers to provide an essential additional service that enhances customer commitment and satisfaction. In RFC 2547bis, a Virtual Private Network (VPN) is comprised of rules that regulate connections among numerous locations. These policies govern and oversee the connectivity between different VPN locations. A customer's location is connected to the network of the service provider through one or multiple ports. The service provider designates a VPN routing table for each port. According to RFC 2547bis, the VRF table is commonly known as the VPN routing table[16][3].

- Customer Edge (CE) Routers

CE routers allow customers to connect to the service provider network by using a data link connecting to PE routers. The CE device, which can serve as either a host or a Layer 2 switch, is commonly an IP router that establishes a connection with its directly connected PE routers. Once the adjacency is established, the CE router informs the PE router about the local VPN routes and also gains knowledge of remote VPN routes from it.

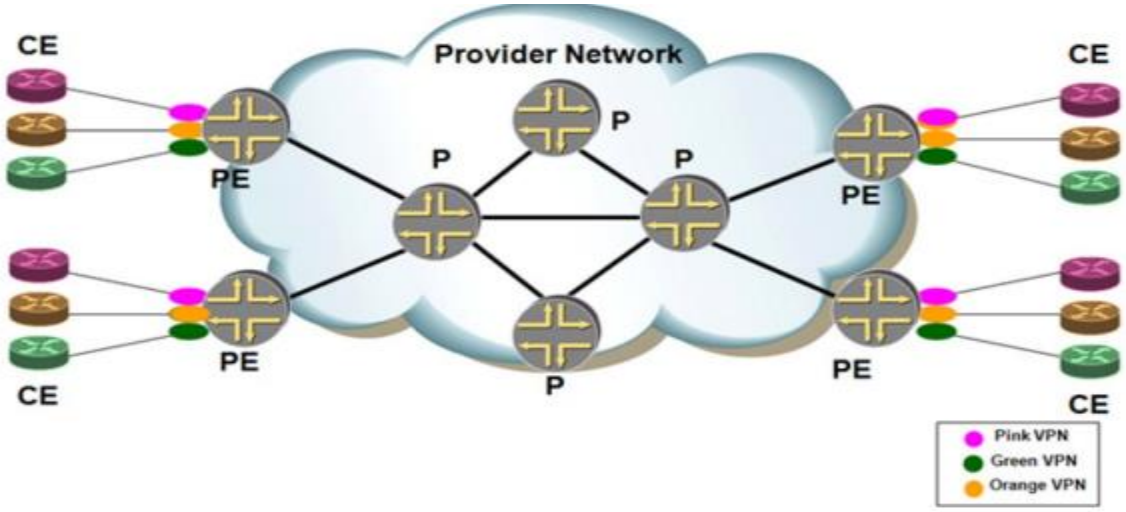

Figure 4: The fundamental building blocks of a BGP/MPLS VPN[16]

- Provider Edge (PE) Routers

The exchange of routing information between Provider Edge (PE) routers and Customer Edge (CE) routers is facilitated through a variety of routing protocols. A Provider Edge (PE) router is required to maintain only the Virtual Private Network (VPN) routes associated with the connected VPNs. The present design enhances the scalability of the RFC 2547bis model by negating the necessity for PE routers to uphold the VPN routes of the service provider. Each Provider Edge (PE) router has a Virtual Routing and Forwarding (VRF) instance created for every connected site. Every customer connection is assigned to a particular Virtual Routing and Forwarding (VRF) instance. The aforementioned is a network port situated on the Provider Edge (PE) router, which lacks any affiliation or linkage with a Virtual Routing and Forwarding (VRF) instance. It is possible for a single Virtual Routing and Forwarding (VRF) instance to be linked to multiple ports on a Provider Edge (PE) router. PE routers possess the capability to maintain multiple forwarding tables, thereby enabling per-VPN routing segregation. The initial step in local virtual private network (VPN) route discovery involves customer edge (CE) routers, followed by the exchange of VPN routing information between provider edge (PE) routers using internal Border Gateway Protocol (IBGP). PE routers are able to connect with route reflectors through IBGP sessions, which eliminates the requirement

for a full IBGP mesh setup. The RFC 2547bis model becomes more scalable with the use of multiple route reflectors, as it eliminates the requirement for a single network component to handle all VPN routes. In the realm of using MPLS for VPN data transportation, it is important to mention that the starting Provider Edge (PE) router acts as the initial Label Switching Router (LSR), while the ending PE router acts as the final LSR.

- Provider (P) Routers

Provider (P) routers are routers within the network of the service provider that are not linked to customer edge (CE) devices. P routers serve as Multi-Protocol Label Switching (MPLS) transit Label Switching Routers (LSRs) in order to facilitate the transmission of virtual private network (VPN) data traffic between Provider Edge (PE) routers. As traffic traverses the MPLS network utilizing a dual-layer label stack, the P routers solely necessitate the upkeep of routes to the provider's PE routers without the obligation to maintain individual VPN routing information for every customer site.

2.1.3.2. MPLS Layer 3 VPNs Operational Model

- **Control Flow**

In a Border Gateway Protocol/Multi-Protocol Label Switching Virtual Private Network, the control flow encompasses two distinct sub flows. The first sub flow involves the transmission of routing information between Customer Edge (CE) routers and Provider Edge (PE) routers situated at the edges of the provider's backbone network. Additionally, routing information is exchanged between PE routers within the provider's backbone network.

Second, sub flow creates LSPs connecting the PE routers. In Figure 4, the interface/subinterface is linked to VRF Green by PE1 for the purpose of route learning from CE1. CE1 promotes the prefix to PE1, which then creates a local route within the VRF Green. PE1 uses IBGP to advertise the prefix learned from CE1 to PE2. Before initiating the route promotion, PE1 engages in the selection of an MPLS label and assigns its loopback address as the BGP next hop. The RFC 2547bis protocol allows for the

allocation of overlapping address spaces, specifically the use of RFC 1918 private addressing, through the implementation of route distinguishers (RDs) and the VPN-IPv4 address family. RFC 2547bis enables regulated dissemination of routes amidst PE routers via the implementation of BGP extended community attributes referred to as route targets. When PE2 gets the route advertisement from PE1, it checks the BGP extended community attributes to decide if it should add the route to the prefix in VRF Green. If PE2 adds the path to VRF Green, it will let CE2 know about it. The way we do things for VRF Orange is still the same.

- **LSP Establishment**

To use MPLS for sending VPN traffic, you need MPLS LSPs between the PE router that knows the route and the advertising PE router. MPLS LSPs can be created and kept using LDP or RSVP. The provider uses RSVP to quickly reroute traffic in case there is a problem in the network. This helps prevent interruptions in the service for about 50 milliseconds. RSVP LSPs allow you to decide how much bandwidth to allocate or use Traffic Engineering to pick a route for the LSP. RSVP-based LSPs ensure good quality of service and help manage traffic efficiently. You can use LDP and RSVP LSPs for MPLS forwarding and Traffic Engineering, and also for Fast Reroute, based on how the network is set up. When there are both LDP and RSVP LSPs between PE routers, the starting LSR chooses the RSVP LSP instead of the LDP LSP. RSVP LSPs are preferred more than LDP counterparts. This model allows the provider's backbone to gradually set up RSVP-based LSPs.

- **Data Flow**

In a Virtual Private Network (VPN), the host located in Site2 transmits data to the default gateway in order to establish a connection with the Server situated in Site1. CE2 searches for the pathway and transmits the packet to PE2. PE2 receives the packet and searches for the appropriate path in VRF Green. Additionally, it locates data regarding the MPLS indicator, BGP subsequent destination, the subinterface responsible for transmitting the packet, and the original MPLS label. MPLS is used for traffic routing from PE2 to PE1

with the assistance of two labels. PE2 places the label at the bottom of the stack. The label stack contains the label for the LDP or RSVP-based LSP. The document is transmitted to the initial P router on the LSP. This router utilizes LDP/RSVP to switch the file depending on the primary label. The penultimate router eliminates the first label and transfers the packet to PE1. PE1 receives the package and removes the label, transforming it into an IPv4 package. The PE1 device employs a bottom label to determine the specific customer device connected directly to it and to determine the appropriate destination for the data transmission. Ultimately, PE1 forwards the IPv4 packet to CE and subsequently to the Server located at Site 1.

2.2. Quality of Service in MPLS Network

The main advantages of MPLS architecture are that it is not limited to any specific protocols, it can make use of quality of service features, and it has advanced traffic management capabilities at a larger network level. Despite the absence of QoS management tools in the MPLS specification, effective traffic flow management within the network can still guarantee satisfactory QoS..

MPLS does not create new ways to organize and prioritize network traffic. Right now, MPLS helps with Differentiated Services (DiffServ) and Integrated Services (IntServ) combination, This technology enables network operators to effectively arrange and distribute network resources for different types of data, emphasizing the priority of specific types of traffic. This implies that they can provide exceptional voice and video communication, unique data services, and service level agreements (SLAs). MPLS and DiffServ collaborate to simplify the control and management of service quality in the central portion of the network.

2.3. Seamless MPLS

The increased demand for a converged packet network accommodating fixed and mobile services, network operators encounter challenges in ensuring cost-effective and proficient service deliveryThe industry is focused on incorporating components into the network

that enable the utilization of MPLS technology in the access network. This enables the formation of networks with a single domain exclusively. Seamless MPLS provides a versatile solution for accessing MPLS, enhancing the advantages of traffic engineering, and ensuring reliable network performance through service-level agreements [17].

Seamless MPLS represents a progressive evolution of the MPLS architecture, conceived to effectively manage the increasing complexity and diversity of network demands. This solution integrates diverse interconnections and services to deliver a unified and coherent networking encounter, simplifying network setup and manageability and flexible end-to-end service delivery, while concurrently enhancing their adaptability and scalability. This approach simplifies the process of identifying and resolving issues, as well as recovering from faults, by decreasing the need for provisioning at intermediary locations within the entire network. This tool has the capability to separate networks into core and aggregation components in designs involving multiple areas within a single autonomous system or across different autonomous systems. The concept of smooth transportation focuses on breaking down the network into separate sections known as IGP/LDP domains. These domains consist of the core, aggregation, and access layers. This subdivision aids in minimizing the dimensions of routing and forwarding tables found within routers. The Label Distribution Protocol (LDP) is frequently employed for the dissemination of labels and the establishment of Label Switched Paths (LSPs). This facilitates communication between devices in various domains such as access, aggregation, or core, by means of intra-domain LDP LSPs [4], [12].

The protocols outlined in RFC 3107 aim to establish a hierarchical structure for Local Service Providers across multiple domains by utilizing BGP-labeled unicast (BGP-LU) as an inter-domain label distribution mechanism. This ensures the availability and accessibility of services across different domains. This feature allows the Interior Gateway Protocol (IGP) within separate domains to maintain a relatively small link state database, while transmitting external reachability information via the Border Gateway Protocol (BGP) that can encompass a large number of routes, potentially reaching millionsIn single-AS multi-area architectures, the iBGP is crucial for creating LSPs within

a domain. On the other hand, the application of the external Border Gateway Protocol (EBGP) is aimed at expanding Label Switched Paths (LSPs) from the autonomous system (AS) to reach destinations beyond its boundaries. Both methodologies achieve seamless transport of MPLS across domains via hierarchical LSPs. They do this by using a BGP-distributed label to navigate isolated domains and an LDP distributed label to reach the intra-domain Area Border Router (ABR) or autonomous system border router (ASBR) that corresponds to the labeled BGP next-hop within the autonomous system [12][16].

The consistent Seamless MPLS transport engineering system has been organized to consider both the type of access and the size of the network. This system offers five different models to choose from based on what the customer needs and what the operator prefers. These are different types of network equipment and configurations that use labeling and routing protocols to connect different parts of a network. These items are Labeled BGP core access and aggregation, Flat LDP core and aggregation, Labeled BGP core and aggregation, Labeled BGP access with flat LDP core and aggregation, and Labeled BGP core and aggregation with redistribution into access network IGP. They help in managing and directing network traffic efficiently. In this research paper, we are using a system called Labeled BGP Access with Flat LDP Core and Aggregation architecture.

2.3.1. Labeled BGP Access with Flat LDP Core and Aggregation

The BGP access with flat LDP core and aggregation architecture model, as shown in Figure 5, is designed for small geographic areas. This architectural design relies on an access network enabled with MPLS, where fiber and packet microwave links are combined in a smaller network setup.

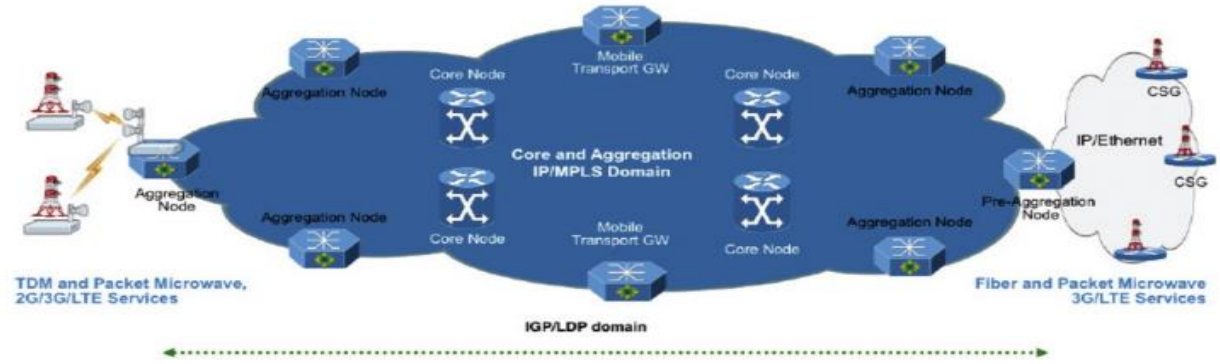

Figure 5: Labeled BGP Access with Flat LDP Core and Aggregation[16]

The proposed aggregation network for small-scale implementation consists of core and aggregation nodes integrated within a unified Interior Gateway Protocol and Label Distribution Protocol (IGP/LDP) domain, spanning up to 1000 nodes. The RAN access network has an independent IGP domain. Two methods for separation are proposed: incorporating the access network into a separate IGP area or implementing a different IGP process on pre-aggregation nodes. The Label Distribution Protocol (LDP) is used to construct intra-area Label Switched Paths (LSP) within individual domains. The integration of the aggregation, core and RAN access networks is achieved through labeled BGP LSPs, with pre-aggregation nodes acting as ABRs and performing the BGP next-hop-self operation to extend the hierarchical LSP of the iBGP across both domains.

The customer service gateways (CSGs) within the access, pre-aggregation, and aggregation nodes can facilitate the provision of mobile 2G/3G /LTE (and wireline) services. BGP community-based egress filtering is implemented at the pre-aggregation node ABRs to enable the controlled dissemination of remote destination information exclusively to the CSGs that necessitate it. In order to optimize the size of BGP labels and minimize the occurrence of superfluous updates, all superfluous prefixes are eliminated [16].

2.4. Quality of Service

In recent times, the increasing demand for multimedia services and the rapid growth of the Internet of Things (IoT) have presented a significant challenge in terms of ensuring provision of high-quality service (QoS) within next-generation networks. Internet Service Providers (ISPs) commonly employ a method known as link over provisioning to ensure the desired Quality of Service (QoS) is delivered. The quality of service play a crucial role in the assessment of service performance, administration of resource reservations, as well as granting precedence to specific applications, users, or data flows within computer networks. Differentiation methods encompass a range of performance metrics, such as throughput, bit error rate, jitter, delay, and packet loss. The transportation of traffic with specialized requirements or limited network capacity holds significant significance, notably for applications such as voice over IP, IPTV, and online gaming. These applications, necessitating a predetermined bit rate and being time-sensitive in nature, compels the prioritization of efficient transport mechanisms [18].

In [4], [19] the Quality of Service (QoS) feature enables network devices to handle diverse traffic types using distinct methods. Routers and switches examine incoming packets and categorize them into separate groups according to their data type. QoS behaviors function as guidelines for devices to manage the movement of traffic between different locations, allowing for the differentiation of traffic treatment based on its level of significance. This aids in attaining the intended standard of excellence for various forms of traffic.

This study aimed to implement quality of service (QoS) measures in the access network due to its proximity to the end-user, facilitating greater control over the overall user experience. The maintenance of low latency and consistent performance in real-time applications, such as video streaming or Voice over Internet Protocol (VoIP), is of paramount importance. Quality of Service (QoS) within the access network can also be customized in order to cater to the unique requirements of particular user groups or services, a practice known as localized traffic management. This approach allows for improved control of network congestion by implementing measures before data enters the core network, thus reducing the occurrence of bottlenecks. Additionally, the shaping

and prioritization of traffic aids in optimizing resource utilization within the network, resulting in greater efficiency. Moreover, the distribution of traffic management load across the network enhances its scalability. Ultimately, these measures ensure that end-users have a positive experience when utilizing the network.

QoS Implementation method commonly are [20] include:

- Classify traffic for the Class map.
- Define the QoS policy with Policy map.
- Apply service policy at the particular interface.

The core functions of Quality of Service (QoS) can be categorized as follows [21]:

- **Traffic classification:** The process of discerning and categorizing various forms of traffic, such as voice, video, and data, in order to implement suitable measures.
- **Traffic shaping:** A regulatory technique employed to effectively manage the flow of traffic by enforcing specified bandwidth limits for different types of traffic.
- **Traffic policing:** Involves the enforcement of traffic profiles and the discarding of network traffic that surpasses pre-established thresholds. This practice aims to mitigate network congestion.
- **Priority queuing:** A mechanism that grants elevated importance to critical traffic, thus ensuring its processing takes precedence over lower-priority traffic.
- **Resource reservation:** Involves the allocation of designated resources, such as bandwidth, to specific applications or users in order to guarantee the fulfillment of their performance needs.
- **Packet Marking:** Marking packets with specific values to indicate their priority or class of service.

- **Congestion management:** Implementing the utilization of algorithms to effectively manage network congestion while safeguarding against service degradation.

By implementing these mechanisms, service providers can optimize their core network's performance, ensure a consistent user experience, and allocate resources in a way that aligns with the needs of various applications and use.

2.4.1. QoS Model

2.4.1.1. Integrated Services (IntServ) architectures

Integrated Services (IntServ) architectures provide stringent quality of service (QoS) assurances by employing resource reservation techniques for bandwidth allocation and buffering. The initiation of data transmission occurs subsequent to the establishment of an end-to-end connection, employing a technique akin to circuit switched networks, for instance, Asynchronous Transfer Mode (ATM). Reservations are made for each individual flow through the utilization of the Resource Reservation Protocol (RSVP), effectively ensuring adherence to set specifications for bandwidth, latency, and jitter. However, the utilization of IntServ-based architectures presents a prominent concern due to the requisite extensive alterations within the network core [22][23].

2.4.1.2. Differentiated Services (DiffServ) architectures

The DiffServ model is an approach wherein traffic is categorized into various classes, with each class being allocated a distinct level of service. The mechanism relies on packet marking and enables users to indicate the desired treatment for each packet through the use of the Differentiated Services Code Point (DSCP) located in the IP header. This particular tactic adopts a traffic class-centric approach, thus facilitating a more streamlined network management process as opposed to focusing on individual flows. In the realm of networking, it is crucial for core routers to effectively forward packets by prioritizing them subsequent to the successful implementation of packet categorization functionality by edge routers [23].

In order to achieve effective classification, this research study investigates the integration of DiffServ Quality of Service model designs in access, aggregator and core network nodes using NBAR (Network-Based Application Recognition). A classification engine called NBAR can identify and categorize a wide range of protocols and applications. It may then instruct the internal application-specific integrated circuits (ASICs) to manage this flow correctly when combined with other features. In order to establish QoS, access lists w utilized to categorize incoming traffic in access networks. These access lists mapped to class-maps. The categorised traffic was then marked, remarked, and queue management was used in the service policy-map. Ultimately, it is imperative to execute the aforementioned service policies on both the inbounded and outbounded interfaces.

2.4.2. QoS Parameters

Traditionally, Telecom Service Providers offered the same service quality to all customers, with differentiation based on connectivity type or subscription fee. Ethio Telecom now classifies customers by their subscribed bandwidth, but not in QoS prioritization. With increasing connectivity demand due to emerging services and web-based applications, Telecom Service Providers should implement new service differentiation and QoS methods to improve revenues and customer service quality. Merging DSCP and MPLS features can provide a better strategy for QoS implementation in the backbone network [3].

Quality of Service (QoS) is a network traffic management methodology that facilitates the allocation of network resources in accordance with the specific characteristics exhibited by the traffic. In order to attain the necessary quality of service (QoS) for the traffic, it is imperative to regulate and manage the traffic characteristics on an individual hop-by-hop basis. The principal Quality of Service (QoS) characteristics that affect traffic within an IP network are throughput, latency, jitter, and packet loss [24].

2.4.2.1. Packet Loss

Packet loss is a term used to describe the loss of individual datagrams in a unidirectional flow of traffic between nodes. Although buffer space can provide some assistance, it cannot be entirely eliminated. The presence of congestion, imposition of traffic rate limitation, occurrence of physical layer defects, and incidence of network element failures are all influential factors that contribute to the loss of datagrams. Queue overflows can arise due to congestion, however, the implementation of rate-limiting ensures that client traffic adheres to Service Level Agreements (SLAs). Network element failures can potentially lead to the loss of datagrams until the connection is reestablished. Conversely, physical layer issues have the potential to generate bit errors [25], [26]. Equation 1 demonstrates the prescribed method for calculating the packet loss percentage value. [source: Telkom Polytechnic].

$$\text{Packet Loss} = \frac{\text{Packet Sent} - \text{Packet Received}}{\text{Packet sent}} X\ 100 \qquad \text{Equation 1}$$

Table 1: Quality Standards Tip hone TR 101 329 for Packet Loss[26]

	Category	Packet Loss
Packet Loss standard	Excellent	0%
	Good	3%
	Medium	15%
	Poor	25%

When network components become overwhelmed with data beyond their capacity, congestion ensues, leading to the rejection of packets. For instance, in the event that a packet is received by a router at a rate exceeding its processing capacity, the router has the capability to either store or forward the packet, yet certain packets may be discarded.

2.4.2.2. Latency(Delay)

Latency in TCP/IP networks is the time delay caused by transmission from one point to another. It can be classified into packetization, queuing, propagation, transmission, and processing delays. Packetization delay occurs once, while queueing delay occurs when routers process packets. Propagation delay occurs during information travel, while

transmission delay is determined by media speed and data packet size. Processing delay involves network device route changes and task switching [27].[source: Telkom Polytechnic].

$$\text{Delay} = \frac{Packet\ Length\ (bit)}{\text{Link bandwidth (bit/s)}} \text{Second} \qquad \text{Equation 3}$$

Table 2: Quality Standards ITU-T G.114 for Delay[27]

	Category	Delay
Latency(Delay) standard	Good	0 – 150ms
	Medium	150ms – 400ms
	Poor	>400ms

Diverse factors, such as the attributes of network components (including cable, router, and switch), serialization delay, routing and switching latencies, as well as queuing and buffer management, collectively contribute to variations in latency. The extent of propagation latency is influenced by the caliber of network components. The propagation delay denotes the temporal interval required for information or data to traverse a communication medium at the velocity of light, spanning from the from the source to the destination.

2.4.2.3. Throughput

Throughput represents a quantitative measurement denoting the capacity of data that a system or device is capable of processing within a designated time period. The phenomenon under consideration is influenced by multiple factors, encompassing variables such as network users, topology, and devices. The present article offers a systematic approach for the computation of throughput values. The accurate assessment of hard drive, RAM, and network and Internet connectivity serves to optimize data transmission proficiency [28][27]. [source: Telkom Polytechnic].

$$\text{Throughput} = \frac{\sum \text{Sent Data(bit)}}{\text{Time Data Delivery (s)}} [\text{bps}] \qquad \text{Equation 2}$$

Table 3: Telkom Polytechnic Quality Standards for throughput[26]

	Category	Throughput/Bandwidth
Throughput standard	Excellent	100%
	Good	75%
	Medium	50%
	Poor	< 25%

Although there exists a mathematical formula common to both throughput and bandwidth, it is important to distinguish between the two concepts. Throughput specifically pertains to the immediate actual capacity of data transmission at a given point in time, within specific conditions, and within the context of the internet network employed for the purpose of downloading a designated quantity of content.

2.4.2.4. Jitter

Jitter refers to the variation observed in latency intervals due to the occurrence of packet collisions and fluctuations in network traffic volume. When considering network performance, it is imperative to consider the influence of both latency and delay. The adjustment of network performance can be achieved by implementing a minimal delay measure in cases where a substantial delay in signal fluctuations, known as jitter, is encountered. However, it is important to note that the network's performance is adversely affected by elevated levels of jitter and excessive delay [27][24]. [source: Telkom Polytechnic].

$$\text{Jitter} = \frac{\sum \text{variation delay}}{\sum Packet\ Received)} \text{Second} \qquad \text{Equation 4}$$

Table 4: Quality Standards ITU-T G.114 for Jitter[27]

	Category	Jitter
Jitter standard	Good	0 s/d 20 ms
	Medium	20 s/d 50 ms
	Poor	>50ms

Congestion within the Internet Protocol (IP) network, occurring at the interfaces of routers or network operators, is a commonplace challenge frequently resulting in the occurrence of jitter. Congestion may give rise to various adverse consequences such as data packet loss, delayed queuing, and sluggish response times. The congestion present in densely networked environments not only decreases throughput but also leads to extended reaction times. The network's quality is influenced by the presence of jitter, which induces delays in packet transmission within the circuit, leading to variable latency.

3. Software Defined Network (SDN)

The extensive expansion of IP networks has become more complex and increased challenges regarding their management. Traditional networks are constructed using various components such as switches, routers, and other devices. These networks have employed distributed protocols and closed, proprietary interfaces, which have presented challenges for network operators, third parties, and vendors to innovation. Traditional control and data planes have historically been regarded as advantageous for network resilience. However, it should be noted that making alterations to the decentralized control plane necessitates the implementation of manual adjustments across all network devices. The absence of automation in contemporary networks renders them inflexible and incapable of promptly adapting to real-time requirements. To overcome these restrictions, Software Defined Networking (SDN) has emerged as an alternative method for establishing networks. The software-defined networking (SDN) framework comprises an SDN controller that serves as a central controlling unit with comprehensive knowledge of the network it manages. Low-level devices are transformed into purely forwarding entities devoid of any control functionality, as they solely receive instructions via specialized interfaces. SDN aims to provide a more efficient and adaptable solution for managing complex networks [29][12].

3.1. SDN Reference Architecture

An SDN is made up of three layers: the application layer, the control layer, and the data plane layer[30], [31][32]. The following is a full explanation of the essential layers:

- **Data (forwarding) Plane:** This encompasses network devices such as routers, switches, access points, and similar equipment, which aid in the functioning of networks. SDN controllers are able to utilize Controller-Data Plane Interfaces (C-DPIs) to access and manage these devices effectively. The network components and controller(s) have the capability to establish secure connections, such as Transport Layer Security (TLS), in order to interact with each other. The OpenFlow

protocol is commonly utilized as the primary standard for the interface between controllers and data plane devices, known as the Controller-Data Plane Interface (C-DPI), facilitating effective communication.

- **The Controller Plan:** A computer program that controls the way data is sent through a network using C-DPI. It helps controllers talk to network devices and decide how to send traffic based on what applications the end users want to use. The controller functions as a network operating system (NOS) and transmits network regulations to the data plane. It transforms application requirements like QoS, traffic prioritization, and bandwidth management into forwarding rules for data plane network forwarding devices. The controller consists of functional constituents and control logic, which regulate controller behavior and allocate and manage network element resources. [30], [32].
- **Application Layer:** it includes network applications that aid in decision-making, security, and data visualization. It implements network management policies like firewalls and routing mechanisms. These apps talk to controllers through a open communication protocol called the REST API. The controller manages network parameters like throughput, latency, and availability, adjusting configurations for optimal traffic forwarding. Centralized network element management allows administrators to optimize service quality.

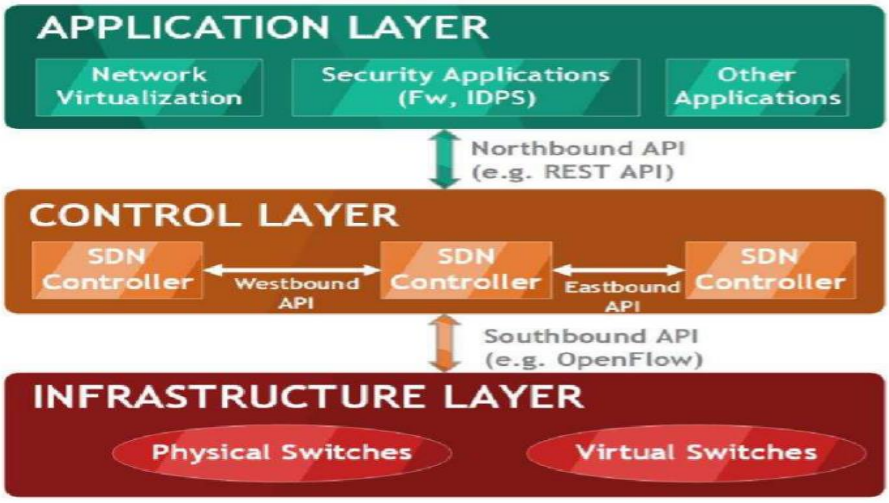

Figure 6: SDN architecture[33]

3.2. Northbound Interface (NBI) Protocol

Northbound APIs are connected to higher layer apps via the ODL Controller, using the OSGi framework or bidirectional REST APIs. These APIs, based on technologies like HTML, JSON, and XML, enable local or remote programs to interact with top-level apps. The ODL Controller generates network rules based on data sent through REST APIs, allowing higher-level business decisions, algorithms, and analytics [29]. The controller can make a connection that meets the agreement for how well the application should perform. It does this by using the North interface, which helps the application work well with other programs and be used on different devices. Different northbound APIs with specific definitions, programming languages, controller operations abstractions, and data plane behavior are available for proposal by controllers[12].

3.3. Southbound Interfaces (SBI) Protocols

The southern interface assists in the transmission of commands from the control layer to the data layer, as well as the transmission of network statistics from the data layer to the control layer. OpenFlow (OF)[34], Border Gateway Protocol-Link State/Path Computation Element Protocol BGP-LS/PCEP[35], Network Configuration protocol (NetConf)[36], Open vSwitch Database 100 (OVSDB)[37], and Simple Network Management Protocol (SNMP)[38] are just a few of the protocols that may be utilized in this interface. In the scenario of a hybrid network comprising both new Software-Defined Networking (SDN) nodes and legacy nodes, the merging of multiple protocols, such as OpenFlow and NetConf, becomes a plausible undertaking [12] [32].

3.3.1. BGP-Link State (BGP-LS)

The BGP Link-State (BGP-LS) is an rising address family inside the Border Portal Convention (BGP) that serves to empower the recovery of link-state data beginning from the neighborhood Activity Building Database (TED).The BGP routing protocol facilitates the transmission of data to external components subsequent to its acquisition from the inner gateway protocol (IGP). TED entries are transformed into paths by the TED on

behalf of the suitable Internet Gateway Protocol (IGP) using the innovative Border Gateway Protocol (BGP) Network Layer Reachability Information (NLRI) encoding framework. Following the transmission of all necessary data, BGP-speakers or Route Reflectors initiate a BGP-peer session with an external entity [12][35].

3.3.2. Path Computation Element Protocol (PCEP)

The Path Computation Element Protocol (PCEP) is a protocol that helps in using path computation elements (PCEs). It uses TCP to work. It provides network topology information to the Traffic Engineering Database (TED) and facilitates communication between PCEs and PCCs. PCE is essential in the Software-Defined Networking (SDN) controller to determine optimal pathways, while PCCs implement these pathways. PCEP messages enable initiation, preservation, and termination of sessions, enabling reciprocal engagement. The setup process includes Open and Keep Alive messages, as well as two PCEP messages: Path Computation Request (PCReq) and Path Computation Reply (PCRep). The PCE uses the TED to determine optimal routing paths, create new Label Switched Paths (LSPs), and perform load balancing operations [35], [39].

3.3.3. Network Configuration protocol (NetConf)

The NETCONF protocol enables a client to establish communication with a server, typically deployed for network management purposes. The controllers serve as intermediaries, possessing the authority to oversee specific domains, while the server functions as a regulated network device. The process of monitoring the operational status of a device and modifying its configuration is explicated in the NETCONF protocol. Moreover, it provides server implementers with a means to define supplemental operations, actions, and alerts. Network administrators have the ability to initiate management procedures and enroll in device notifications. The YANG data model encompasses the description of all data necessary for the purpose of accessing or modifying device monitoring or setup operations [12][36].

3.4. Open Daylight (ODL) Controller

OpenDaylight, an open source initiative by the Linux Foundation, aims to accelerate Software Delivery Networks (SDN) implementation by offering a universally accessible platform for businesses. It aims to reduce costs and prevent proprietary applications from hindering market growth. OpenDaylight allows corporations to use equipment from multiple manufacturers without requiring allegiance to a single brand. The platform's architectural design allows applications to access essential features and diverse collaborators contribute to the project. This strategy allows companies to use technology from multiple vendors without forming exclusive partnerships[40].

By emphasizing SDN, this approach facilitates customization and innovation of novel functionalities through the integration of protocols and network services. This software enables engineers and developers to create their own network design and management applications by segregating functions. The main responsibility of the ODL controller is to centrally manage and control physical and virtual network devices by following standard protocols and principles based on open source. This technology has the capability to operate with various communication protocols and guidelines. There are multiple protocols utilized in computer networks such as Open Flow, SNMP, RESTCONF, NETCONF, OVSDB, BGP-LS, and PCEP [41]. ODL has three main parts: network apps and services, controller platform, and SB interfaces and protocols. Layers are like managers of a network. They handle and control how everything works in the network.

3.4.1. The Controller Platform

The ODL is a customizable controller that simplifies SDN design, managing network devices without direct access to the underlying infrastructure. It includes Basic Network Services Functions (BNSFs), Service Abstraction Layer (SAL), and Platform Network Service Functions. BNSFs aggregate data and provide NB APIs, while Platform Service Functions offer tools and features for better SDN execution. The Service Abstraction Layer (SAL) is the core of ODL, supporting SB protocols and offering services to other modules and applications.

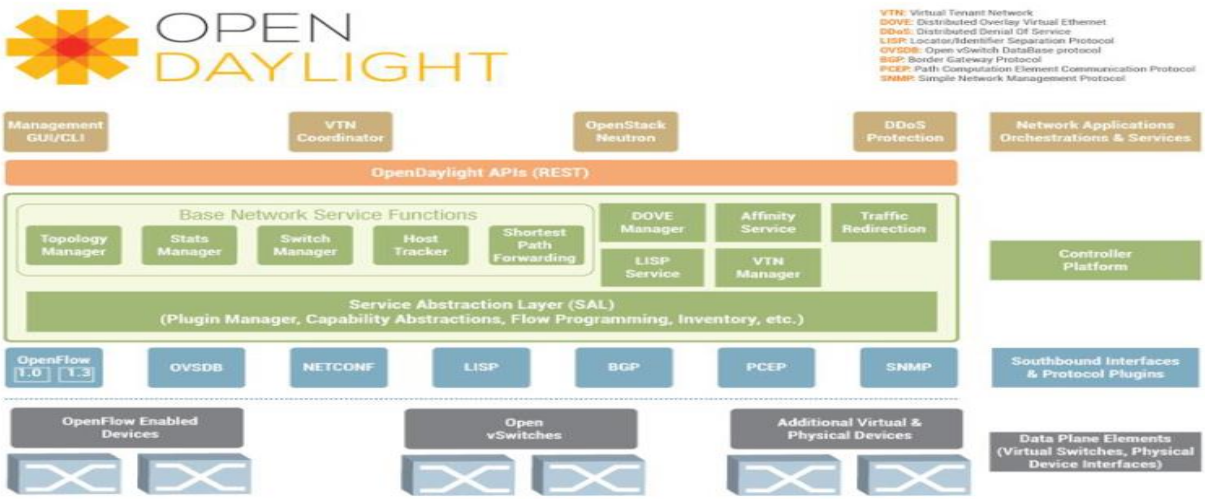

Figure 7: Open Daylight Architecture[41][42]

3.4.2. The Southbound Interface and Protocols Plugins

SB protocols are used for secure controller-network communication, allowing network elements to be managed and monitored. ODL supports multiple SB protocols through plugins, ensuring interoperability with other technologies and vendors. Supported plugins include OpenFlow Plugin, OVSDB Plugin, SNMP Plugin, BGP-LS/PCEP Plugins, and NETCONF Plugin. These plugins implement OF protocol specifications, manage open vswitches, manage off-the-shelf Ethernet switches, implement Java-based BGP and PCEP, and provide NETCONF protocol functionalities.

3.4.3. The Network Applications and Services

The systems and tools responsible for overseeing and coordinating all operations within a network. This section consists of services that manage and direct network traffic to meet the demands of Network Function Virtualization (NVF) and cloud computing [36]. The intermediate platform layer provides access to open NB APIs that can be utilized by applications. The ODL system enables the OSGi framework and two-way REST APIs for the NB APIs. The distinction between OSGi and REST API lies in their application scope. OSGi is designed for applications running within the same address space as ODL, whereas REST API caters to applications outside this address space.

4. Simulation Network Setup

The objective of this chapter is to create a network setup that imitates the configuration of a Seamless MPLS and SDN-based Seamless MPLS network in order to examine and analyze the Quality of Service (QoS) performance. The thesis's simulation network consists of three types of networks: access, aggregation, and core networks. GNS-3 serves as an emulation tool for simulating Quality of Service (QoS) in both Seamless MPLS and SDN connected Seamless MPLS networks. A simulation is carried out using an HP ELITEBOOK laptop that has 16GB RAM and 500GB storage capacity. Each simulation network setup consists of four distinct network domains, each with its own autonomous system (AS).

The initial access network router, named R11, operates with an AS number of 65011. This field consists of one access R11 router linked to a single ostinato traffic generator and connected to the access router. The access emulation is carried out using Cisco IOS C7200 routers. The access router is linked to the Cisco IOS XRV provider edge router (R1) in the core domain. The routers within this domain and with the core domain have established connections using Gigabit Ethernet (GE) interfaces. The Wireshark network Analyzer is utilized on the wire connecting the Access router (R11) and the Provider edge router (R1) to evaluate the performance of both simulations.

Second domain made up of one autonomous boarder router (R5), one route reflector router (R4), three provider edge routers (R1, R2, and R3), and one with an AS number of 100. SDN-capable Cisco IOS XRv 6.0.1 is utilized for one Provider edge router (R1), and Cisco IOS C7200 routers are used for Provider edge routers R2 and R3. Route Reflector and Autonomous Boarder routers are also use cisco IOS C7200 routers. All connection among routers in this core domain is based on Gigabit Ethernet (GE) interfaces.

Third domain composed of three Provider edge Router(R8, R9 and R10), one Route Reflector Router (R7) and one Autonomous boarder router (R6) with an AS number of 200. SDN capable Cisco IOS XRv 6.0.1 used for one of Provider edge router R10. Route Reflector and Autonomous Boarder routers are use cisco IOS C7200 routers. All

connection among routers in this core domain is based on Gigabit Ethernet (GE) interfaces.

The AS number 65012 belongs to the fourth access network router, identified as R12. Cisco IOS C7200 routers are employed in access emulation scenarios. The access router is linked to the provider edge router (R10) in the core domain using Cisco IOS XRV. The routers within this network domain and the central domain are interconnected using Gigabit Ethernet (GE) interfaces.

For the SDN part of the simulation, the OpenDaylight (ODL) controller, installed as Boron Stable Release distribution-karaf-0.5.4-Boron-SR4, is utilized. The controller is housed in a GNS-3 Ubuntu Docker/container and linked to the R1 and R10 edge routers of the Seamless MPLS provider by a hub. The Ubuntu Docker/container and Cloud-1 for the simulation network configuration are connected to the internet via the NAT cloud.

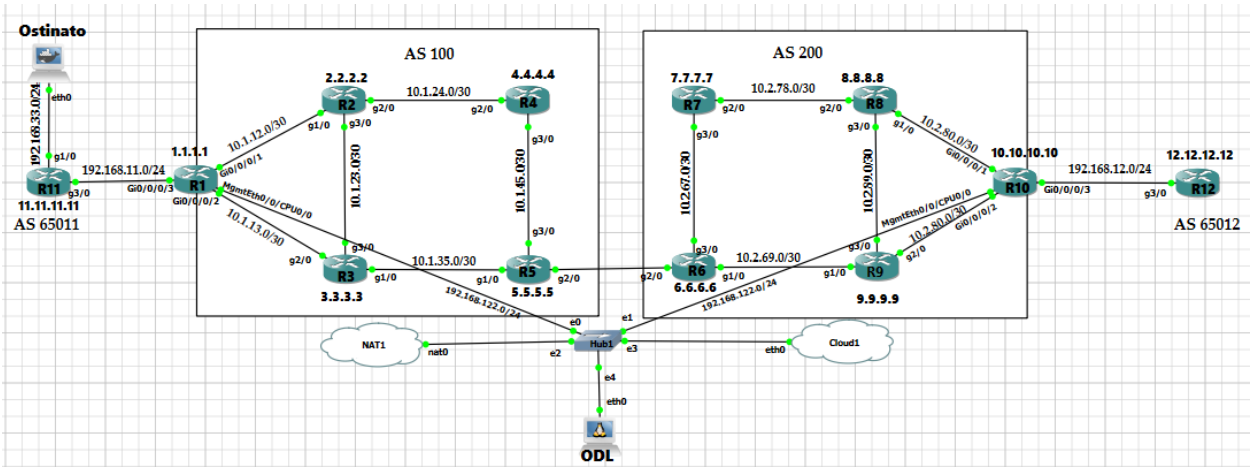

Figure 8: Simulation Network Setup

4.1. Simulation Tools Over view

4.1.1. Graphical Network Simulator-3 (GNS-3)

GNS-3 is an open-source program that permits clients to run distinctive arrange topologies on diverse working frameworks such as Windows, Linux, and Mac. It is made

up of organize gadgets and associations that mirror physical components. GNS3 was made to form a user-friendly graphical interface for organize imitating, arrangement, testing, and investigating.

It may be connected to a pre-configured Virtual Machine (VM) to empower certain functionalities, in spite of the fact that this arrangement is confined and does not offer numerous choices. GNS3 integration in a VM is suggested by merchants to empower elective pictures and functionalities. GNS3 moreover empowers for the consolidation of assistant instruments for moved forward yield control [3].

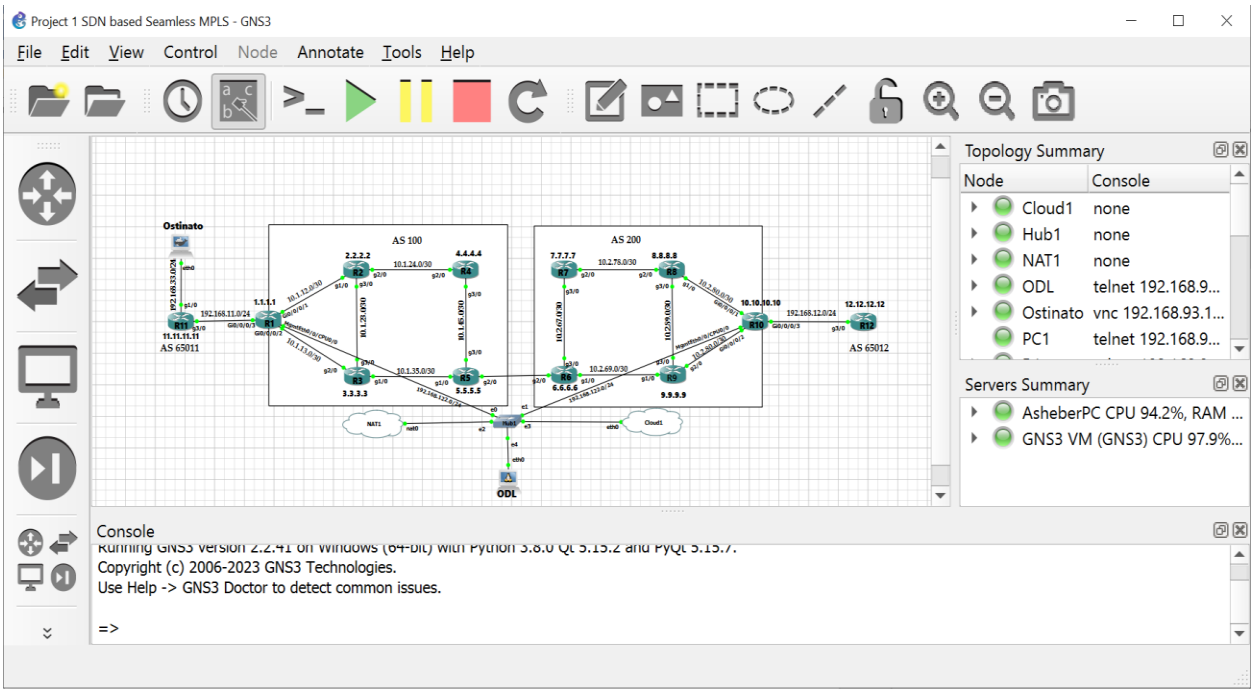

Figure 9: GNS3 Guide User Interface (GUI)

4.2. Ostinato

Ostinato is an open-source organize activity era apparatus with bundle adjustment highlights and an easy-to-use graphical client interface. IPV4, IPV6, IP Tunneling, TCP, UDP, ICMP (v4 and v6), IGMP, and text-based conventions such as HTTP, Taste, and NNTP are all bolstered. Ostinato can also connect to other platforms and produce traffic

streams with varying data rates. The activity generator GUI is utilized in a test situation to deliver the required amount of activity [43]. The goal is to create congestion in the network by generating an extremely large amount of packets and sending them. Due to the limited memory capacity of personal computers and the computational requirements of simulation tools, a normalization of links is introduced.

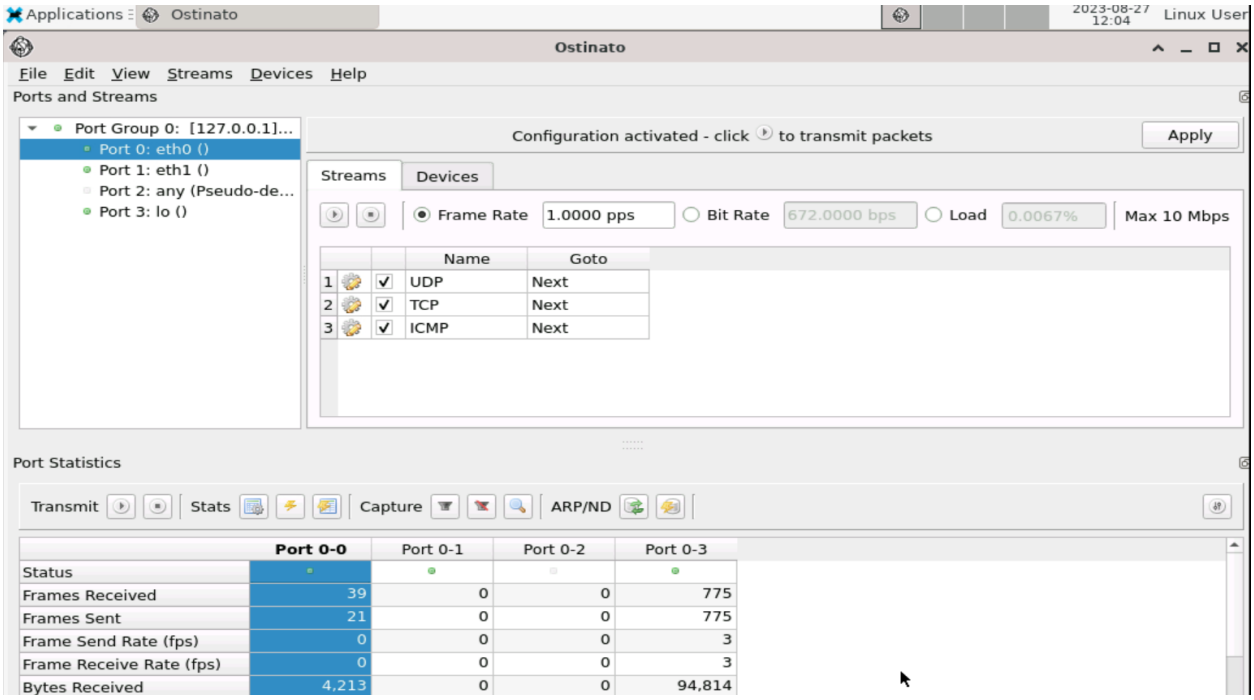

Figure 10: Ostinato GUI

4.3. Wireshark

Wireshark is a free and open-source network packet analyzer that used for network troubleshooting, analysis, software and communications protocol development. It has conventional protocol analyzer capabilities as well as a few unique ones. Its open source license allows networking specialists to improve it. Wireshark is available for common computing systems like as Unix, Linux, and Windows. It is used by network administrators, security engineers, developers, and students to troubleshoot network

difficulties, investigate security concerns, debug protocol implementations, and understand TCP/IP protocols [44].

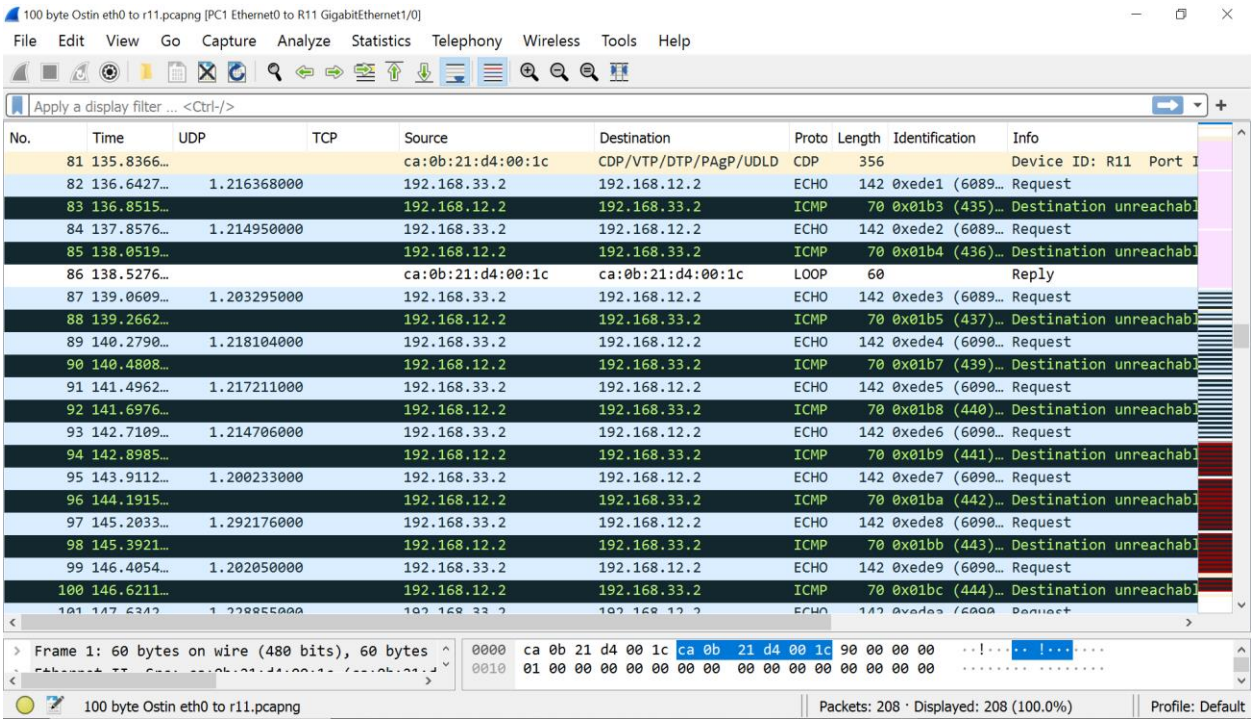

Figure 11: Wireshark GUI

4.4. Seamless MPLS Simulation

Seamless MPLS is being tested in a simulation that spans across four domains, consisting of two distinct aggregator and core networks and two separate access networks. AS 100 and AS 200 reside in the aggregator and core network domains, while AS 65011 and AS 651012 are located in the access network domains. This is accomplished by setting up loopback and link IP addresses, as well as implementing IGP (OSPF), MPLS/LDP, BGP-LU, and QoS on all routers within the network configuration. The IP address planning is as follows:

- In the access domain (AS-65011), the loopback addresses of router R11 were allocated point-to-point connection connectivity. Specifically, the addresses

11.11.11.11/32. Interface gi0/3 to connect VRF CUST-A with IPaddress 192.168.11.2/24.

- In aggregation and core domain (AS-100), the loopback addresses of provider routers R1, R2, R3, route reflector router R4, and ASBR router R5 are assigned point-to-point link connectivity. Specifically, the addresses 1.1.1.1/32, 2.2.2.2/32, 3.3.3.3/32, 4.4.4.4/32, and 5.5.5.5/32 correspond to these routers, respectively. Mangement interface MgmtEtho 0/0/CPU0/0 with IP address 192.168.122.102/24. In addition, create a cutomter VRF name as vrf CUST-A in gelobal and interface gi 0/0/0/3 with IP address 192.168.11.1/24
- In aggregation and core domain (AS-200), the loopback addresses of ASBR router R6, route reflector router R7 and provider routers R8, R9, R10 are assigned point-to-point link connectivity. Specifically, the addresses 6.6.6.6/32, 7.7.7.7/32, 8.8.8.8/32, 9.9.9.9/32, and 10.10.10.10/32 correspond to these routers, respectively. Mangement interface MgmtEtho 0/0/CPU0/0 with IP address 192.168.122.103/24. In addition, create a cutomter VRF name as vrf CUST-A in gelobal and interface gi 0/0/0/3 with IP address 192.168.12.1/24,
- In the access domain (AS-65012), the loopback addresses of router R11 were allocated point-to-point connection connectivity. Specifically, the addresses 12.12.12.12/32. Interface gi0/3 to connect VRF CUST-A with IPaddress 192.168.12.2/24. In addition, Apply Wireshark packet analyzer between R10 to Customer router (R12).
- Ostinato-1 traffic generator use the IP address of 192.168.33.2/24 that connect to customer router R11. In addition, Apply Wireshark packet analyzer between Ostin-1 to Customer router (R11).
- Ostinato-2 traffic generator use the IP address of 192.168.44.2/24 that connect to cutomer router R11 as to create congestion by generating random traffic and feed them to the network.

This architecture uses Option C connectivity for seamless MPLS setup, allowing network connectivity and extending MP-BGP neighbor relationships. It joins two aggregator and

core AS to a single MP-BGP domain and exchanges VPNv4 routers with the other network by route reflector this allow that segregate the Data Plane and Control Plane. Routers maintain their route target (RT) values across to the other side. Seamless MPLS implementation in the end-to-end aggregator and core network offers several advantages over access networks. It allows for efficient traffic aggregation, simplifies management, optimizes routing, ensures consistent service, reduces overhead, and optimizes traffic-engineering tasks. Core network routers have a better view of the network topology, allowing for more informed routing decisions. Centralizing the implementation in the core network reduces unnecessary overhead, especially when dealing with a large number of access points. It also helps maintain security and isolation between different access networks, which can be more effectively managed at the core level.

4.5. SDN based S-MPLS Simulation

The ODL controller is installed and running on an Ubuntu Docker/Container, and it is linked to the SDN-driven Seamless MPLS network. On GNS3, the ODL Boron Stable Release distribution-karaf-0.5.4-Boron-SR4 is downloaded and deployed using Ubuntu Docker. The ODL controller is linked to the SDN based Seamless MPLS network arrangement through the 192.168.122.0/24 IP address segment. The ODL controller is allocated the IP address 192.168.122.101/24 for Ubuntu. IP addresses are specified on the management interfaces of Head End(HE) routers R1 and R10.

The ODL controller use as Path Computation Element (PCE) and Head End routers R1 and R10 use as Path Computation Clients (PCCs). The ODL controller collects traffic topology by forming BGP-LS neighborships with PCCs. A PCEP peer connection is necessary for the Seamless MPLS network configuration to create, edit, and remove traffic. Among the features of the ODL controller installed are odl-netconf, odl-bgpcep-bgp, odl-bgpcep-pcep, odl-mdsal, odl-yangtools and odl-restconf. The odl-bgpcep-pcep and odl-bgpcep-bgp features provide BGP-LS and PCEP plugin for ODL controller. The model driven service abstraction for the controller is enabled via the odl-mdsal feature. Yang data model-based abstraction on the controller is made possible by the odl-

yangtools feature. The controller can configure the PCCs using the southbound (SB) plugin provided by the odl-netconf feature.

The ODL controller is prepared by changing the settings in the karaf folder to connect with the PCCs and establish BGP-LS neighborship and PCEP peering. The 41-bgp-examplexml configuration file is made up of two parts: example-bgp-rib and example-bgp-peer. Example-bgp-rib sets the BGP Routing Information Base for the ODL controller, while example-bgp-peer connects the ODL controller to BGP-LS peers. The RIB ID and local AS number of the ODL controller are updated in the example-bgp-rib module. The BGP-LS speakers are S-MPLS Head End routers R1, configured as iBGP-LS peers and R10 configured as eBGP-LS peers with remote AS 100.

We need to make some extra settings for the PCCs to work together. These settings include BGP-LS, PCE, NETCONF, and SSH. To set up BGP-LS on both S-MPLS Head End routers, the ODL controller (192. 168.122.101) is added as a BGP neighbor to the global BGP configuration with Link-State address family. The BGP-LS connection between R1 and R10, as well as the connection between the ODL controller and the PCEs, is established by adding PCE configuration to the PCCs' traffic engineering configuration.

The ODL controller now connects with other devices using BGP-LS and PCEP protocols. However, the ODL controller needs to be capable of organizing the PCCs. To do this, start by allowing NETCONF and SSH on the PCC control planes. Then, the ODL controller (which stands for OpenDaylight Controller) connects to the PCCs (which stand for Path Computation Clients) by setting up NETCONF and SSH protocols. It also manages and controls the PCCs through the ODL controller.

5. Simulation Result

In order to examine the effectiveness of QoS in Seamless MPLS and SDN based Seamless MPLS technologies, the implementation portion of the study entails constructing a realistic environment utilizing an enterprise network simulation platform. Four different scenarios are created, the first of which uses a standard network with Seamless MPLS, the second QoS-based Seamless MPLS, the third SDN-based Seamless MPLS, and the fourth QoS SDN-based Seamless MPLS technologies. Besides the basic connectivity of IP configuration, Seamless MPLS, OSPF IGP, and DSCP are setup to prioritize the classified traffics. MP-BGP is also set up to allow BGP to carry routing information for user traffic.

To evaluate how well a system is working using three aspects of quality, Ostinato is used to generate network activity. To create a fair competition for resources among network traffics, two tools are made. One tool sends the required traffic for studying overall performance, while the other tool sends random traffic. The test results are gathered from the simulator using a technology called Wireshark. Wireshark is part of the GNS-3 emulator platform. The test results are also collected from the UDP echo request using a tool called Ostinato. Both scenarios use Ostinato to collect the test results. We use the average of 5 to 10 sample tests to make the data more accurate for each QoS parameter. To gather the findings, traffic is created in three stages with different amounts of data. The first situation is when the data size is smaller than a certain limit, like 65% of the BW. The second situation is when the data size is almost at the limit, around 75%. And the third situation is when the data size is greater than the limit. Because the simulation tools require a lot of memory and processing power, they only use a few extra nodes and links at the main areas.

Quality of Service (QoS) in a seamless MPLS network with Software-Defined Networking (SDN) improves user experience by ensuring appropriate service quality for different traffic types. It prioritizes critical applications, allows efficient resource utilization, and offers flexible policy-based control. Seamless MPLS integration with SDN allows for

efficient tunnel management, resulting in cost savings and compliance with Service Level Agreements.

5.1. Packet Loss Analysis

As mentioned in section 2.4.2.1, numerous factors and causes contribute to the rise of packet loss. Network congestion is a significant problem. Network congestion arises when the volume of incoming traffic from access devices or customers surpasses the capacity of the link. Physical mistakes such as incorrectly connecting interfaces, loose connections, etc. Potential causes Network congestion is taken into account when analyzing packet loss. Smartly generate additional traffic using a network traffic generator and deliver it to the network. The results of the experiment and the observations of packet loss are shown in Figure 17. For SDN based SeamlessMPLS traffic + QoS, the average packet loss is 5% compared to 23 % for conventional Seamless MPLS traffic. There is a noticeable difference between the Seamless MPLS and QoS SDN-based Seamless MPLS in this situation. Because packet loss is significantly impacted by the traffic that is passed at various packet sizes and delays. The recipient notices the sound of breaking or choppy streaming video pictures when a packet (in the form of voice data or video) is lost during delivery. In this section, Packet Loss of Best Effort seamless MPLS, QoS seamless MPLS, SDN based Seamless MPLS and SDN based Seamless MPLS + QoS presented in table 5.

Table 5: Packet Loss Measurement of Four Scenarios

Packet Size (Number of Packets)	600	800	1000	1200	1400
Seamless MPLS Packet Loss %	0%	3%	12%	19%	23%
QoS Seamless MPLS Packet Loss %	0%	0%	1%	9%	10%
SDN based Seamless MPLS Packet Loss %	0%	0%	8%	16%	18%
SDN based Seamless MPLS +QoS Packet Loss %	0%	0%	0%	2%	5%

There is no loss of data when the connections are not busy when the data sizes are between 100 and 600 Packets. This is shown in Table 5 and Figure 17. However, when there is a increase of data, the networks become crowded and there is a greater chance of losing packets. Compared to Seamless MPLS network design, the SDN-based Seamless

MPLS network architecture provides much better Quality of Service. For example, when there are 1400 Packets of data, using Seamless MPLS with QoS SDN based Seamless MPLS reduces packet loss by 18%.

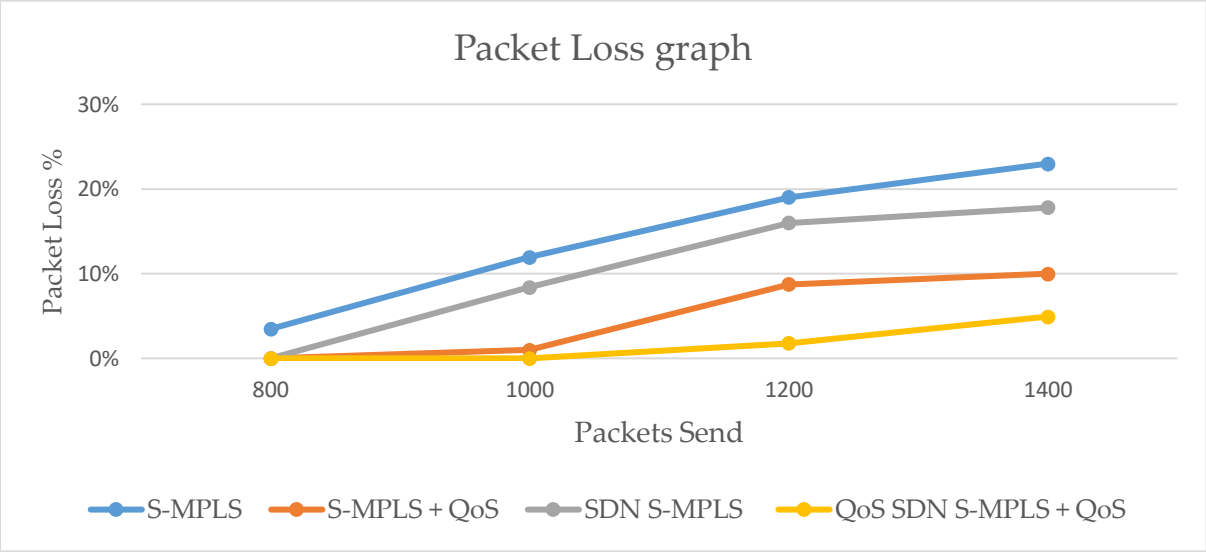

Figure 12: Packet Loss Result

5.2. Packet Latency Analysis

Latency is a quality of service (QoS) metric that quantifies the duration it takes for a packet to complete a round trip or one-way journey. It is a prominent concern for real-time traffic applications. The International Telecommunication Union (ITU) advises that the optimal latency for an end-to-end communication should not exceed 150 milliseconds. The consistent utilization of the same topology is observed across all cases pertaining to latency analysis. The UDP test type is utilized for the transmission of test probes, while varying data sizes are generated to collect the average completion time for each test probe. Table 6 exhibits the dataset that was generated and transmitted to the network.

Table 6: Packet Latency Measurement for four Scenarios

Packet Size (Byte)	200	400	600	800	1000	1200
BE S-MPLS Avg RTT(ms)	77	80	81	83	85	86
QoS S-MPLS Avg RTT(ms)	72	74	76	77	80	82
SDN S-MPLS Avg RTT(ms)	76	77	80	81	83	85
SDN S-MPLS + QoS Avg RTT(ms)	71	72	73	73	74	75

Figure 18 shows that the Seamless MPLS scenario has a larger latency than the QoS SDN-based Seamless MPLS scenario. The delay differences for the same data amount in the non-congestion environment are less than in the congestion situation. For example, at data sizes of 1200 bytes, QoS SDN-based Seamless MPLS improves latency by 11ms, or 12.8%, as compared to Seamless MPLS.

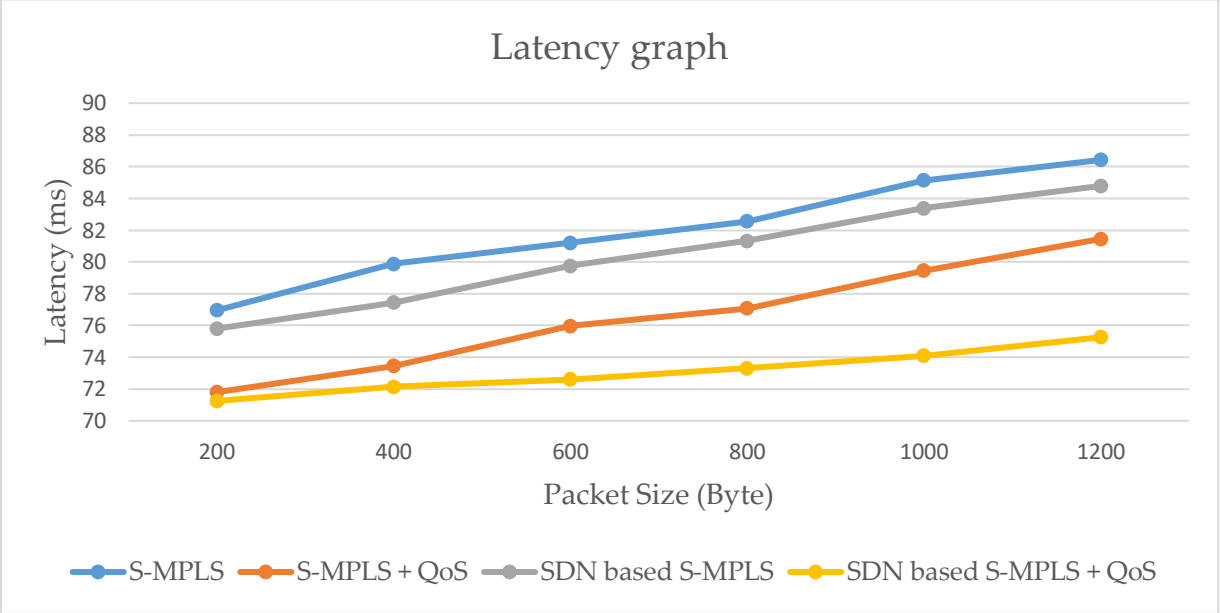

Figure 13: Packet Latency Result

5.3. Packet Throughput Analysis

Throughput is a QoS parameter that quantifies how many information units a system can handle in a given amount of time. In order to calculate the throughput, it is imperative to have knowledge of both the quantity of data transferred and the duration required to accomplish the UDP transfer. Ostinato traffic generator use to induce different network congestion in various contexts such as Best Effort S-MPLS, QoS S-MPLS, SDN coupled S-MPLS, and SDN based S-MPLS + QoS. In both scenarios, the Ostinato tool is employed to facilitate the transmission of a predetermined 100-packet User Datagram Protocol (UDP) protocol with a sequence of packet frames of byte size from the source router CE1 (R11) to the destination router CE2 (R12). Additionally, Wireshark network analysis is utilized to gather pertinent data, such as the average round trip time needed to accomplish the transfer for each packet size. The results pertaining to different byte sizes are presented in Table 7.

Table 7:Throughput Packet Measurement for four Scenarios

Packet Size (Byte)	200	400	600	800	1000	1200
S-MPLS Avg Avg RTT(ms)	77	80	81	83	85	86
S-MPLS Throughput (Kbps)	1247	2400	3556	4627	5647	6698
QoS S-MPLS Avg RTT(ms)	72	74	76	77	80	82
QoS S-MPLS Throughput (Kbps)	1333	2595	3789	4987	6000	7024
SDN S-MPLS Avg RTT(ms)	76	77	80	81	83	85
SDN S-MPLS Throughput (Kbps)	1263	2494	3600	4741	5783	6776
SDN S-MPLS + QoS Avg RTT(ms)	71	72	73	73	74	75
SDN S-MPLS + QoS Avg RTT(Kbps)	1352	2667	3945	5260	6487	7680

For example when 1200 byte packet frame size for BE S-MPLS Avg RTT(s) is 1.4333 sec. so the throughput is computed as the ration of the round trip time i.e. (1200 Byte * 8bits/byte)/1.4333 sec = 6,697.8 bps. Using the same procedure for SDN Coupled S-MPLS + QoS Avg RRT(s) is 1.25 second the throughput is (1200 Byte * 8bits/byte)/1.25 sec = 7,680 bps. Therefor at data sizes of 1200 bytes, QoS SDN-based Seamless MPLS improves throughput by 982 kbps , or 14.7%, as compared to Seamless MPLS. For different packet

size (byte) the result are tabulated for both scenarios as show in Table 6. And the throughput is computed and put in table 7.

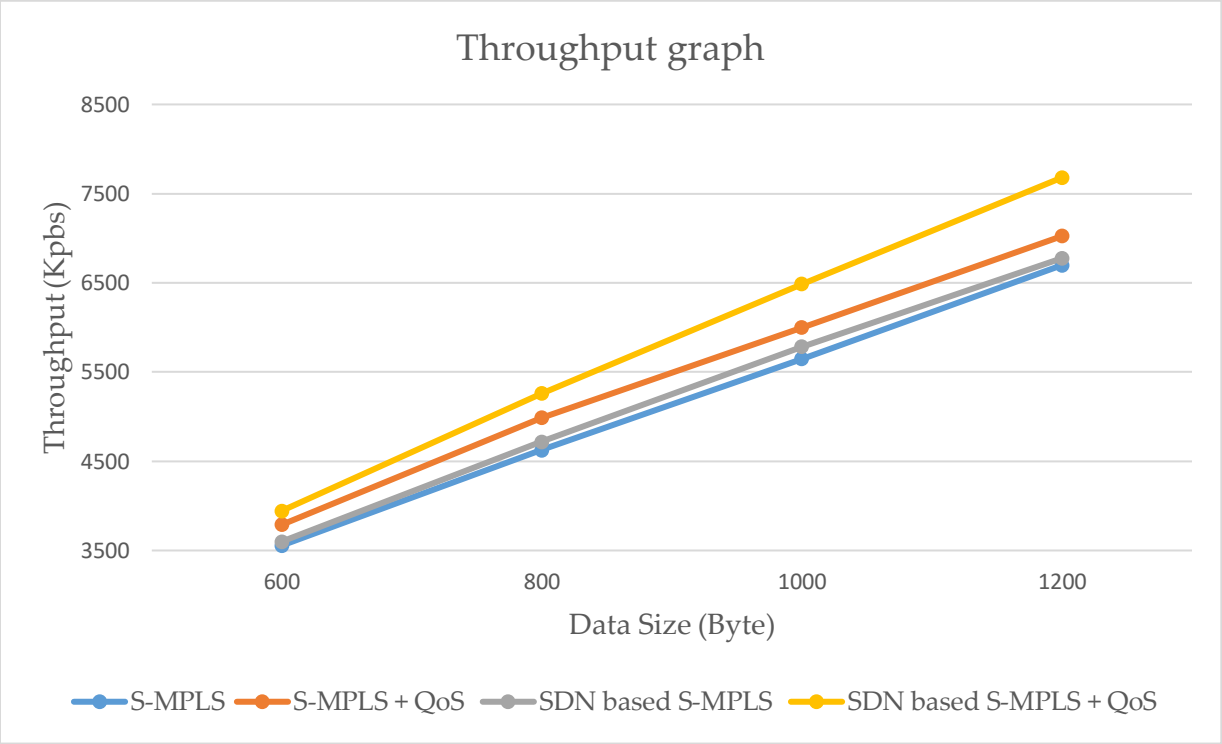

Figure 14: Packet Throughput Result

6. Conclusion and Future Works

6.1. Conclusion

The SDN methodology is now seen as the conventional networks' future. Flexibility, adaptability, and notably the capacity to accommodate new technologies are all positive aspects of this strategy. A controller entity must be employed to make a network programmable and controllable.

This thesis compares a QoS SDN-based Seamless MPLS architecture against classic QoS Seamless MPLS utilizing three QoS parameters: throughput, latency, and packet loss. Using a Cisco ISP router and GNS3 emulator, four scenarios (S-MPLS, QoS S-MPLS, SDN-based S-MPLS, and QoS SDN-based S-MPLS) are set up on the same network topology. Ostinato technologies are used to generate network traffic, while wireshark technology is used to collect simulation data. In Excel 2016, the results are graphed.

Seamless MPLS can improve how a network runs and make it less complicated, but it does not guarantee that the quality of service will be consistent from start to finish. Simply using QoS in a seamless MPLS network does not ensure end-to-end QoS. However, the SDN-based Seamless MPLS QoS network ensures that the quality of service is guaranteed from the start of a process to its completion. The SDN controller will be able to see the entire network structure. SDN-based Seamless MPLS + QoS routing efficiently utilizes network bandwidth and offers lower latency. The proposed methodology improves throughput by 14.7%. Regarding latency, it achieves a 12.8% reduction in packet delay. The proposed methodology reduces packet loss by 18% with similar congestion levels.

6.2. Future Works

Validating the suggested technique in a real-world IP Core network environment may be the main goal of future study. Future work directions might be viewed from this angle as:

- Research the effects of implementing the performance of QoS in Seamless MPLS Traffic Engineering with SDN based Seamless MPLS Traffic Engineering evaluation.
- Research the effects of implementing SDN based RSVP-TE vs. SDN based QoS Seamless MPLS Traffic Engineering on network resource usage.
- Research the effects of implementing SDN-based QoS Seamless MPLS with a high level of quality of service on IPV6 performance.

References

[1] J. Bhalla, "Multiprotocol Label Switching," *International Journal of Advanced Research in Management*, vol. 1, 2015, [Online]. Available: www.ijarmate.com

[2] N. Thazin, "QoS-BASED TRAFFIC ENGINEERING IN SOFTWARE DEFINED NETWORKING," 2019.

[3] B. Samrawit Eshetu Advisor Yalemzewd Negash, "Bandwidth Optimization of IP Core Network Using MPLS Traffic Engineering and Quality of Service: the Case of Ethio Telecom Backbone Network," Addis Ababa, 2021.

[4] Y. N. Habtamu Kumera and A. Ababa, "Analysing Impact of Seamless MPLS on QoS," 2018.

[5] G. Daba and A. Mulatu, "Quality of Service Comparison of Seamless Multi-Protocol Level Switching and Multi-Protocol Level Switching Networks," Addis Ababa, 2022.

[6] R. A. R. Anuar Zamani Othman, Md Mahfudz Md Zan, and Mat Ikram Yusof, *The Effect of QoS Implementation in MPLS Network*. Bandung: IEEE, 2012.

[7] C. Hu, Q. Wang, and X. Dai, "SDN over IP: Enabling Internet to Provide Better QoS Guarantee," in *Proceedings - 2015 9th International Conference on Frontier of Computer Science and Technology, FCST 2015*, Institute of Electrical and Electronics Engineers Inc., Oct. 2015, pp. 46–51. doi: 10.1109/FCST.2015.17.

[8] C. Xu, B. Chen, and H. Qian, "Quality of service guaranteed resource management dynamically in software defined network," *Journal of Communications*, vol. 10, no. 11, pp. 843–850, 2015, doi: 10.12720/jcm.10.11.843-850.

[9] M. Jeffrey and E. Cole, "Modeling Multi-Protocol Label Switching Networks in the Laboratory Modeling Multi-Protocol Label Switching works in the Laboratory," Georgia, 2015.

[10] Jitendra Joshi, Sonali Gupta, Priti Gupta, Nisha Singh, and Manjari Kumari, "Multi Protocol Label Switching with Quality of service in High speed Computer network 2013," *International Journal of Engineering Science and Innovative Technology (IJESIT)*, vol. 2, no. 2, pp. 83–87, Mar. 2013.

[11] S. Gurung, "IMPLEMENTATION OF MPLS VPN," 2015. Accessed: Aug. 24, 2023. [Online]. Available: https://www.theseus.fi/bitstream/handle/10024/103442/Sanjib%20Gurungthesis.pdf?sequence=1

[12] M. Worku and Y. Negash, “SDN Coupled Seamless MPLS Traffic Engineering Performance Analysis,” Addis Ababa, 2021.

[13] K. Jannu and R. Deekonda, “OPNET simulation of voice over MPLS With Considering Traffic Engineering,” 2010. [Online]. Available: www.bth.se/com

[14] K. Jannu and R. Deekonda, “OPNET simulation of voice over MPLS With Considering Traffic Engineering,” 2010. [Online]. Available: www.bth.se/com

[15] SITI AMELIABINTI AHMAD, “Simulation of ip traffic engineering improvement using MPLS.” Accessed: Aug. 24, 2023. [Online]. Available: https://www.slideshare.net/ameliakot/fyp-presentation-15100528

[16] Vinod. Joseph and Srinivas. Mulugu, *Network convergence : Ethernet applications and next generation packet transport architectures*. Morgan Kaufmann is an imprint of Elsevier, 2014.

[17] J. Networks, “BUILDING MULTI-GENERATION SCALABLE NETWORKS WITH END-TO-END MPLS,” 2012. Accessed: Aug. 24, 2023. [Online]. Available: https://www.juniper.net/content/dam/www/assets/white-papers/us/en/building-multi-generation-scalable-networks-with-end-to-end.pdf

[18] Z. Car and Mario. Kušek, *QoS Design Issues and Traffic Engineering in Next Generation IP/MPLS network*. Zagreb, Croatia: IEEE Xplore,Proceedings of the 9th International Conference on Telecommunications : ConTEL 2007 : Zagreb, Croatia, June 13-15, 2007, 2007.

[19] Evans John and Filsfils Clarence, “Nu~~rotocofLa6e~Switching (NPU) amffizerentiutedSmices (D3) as Quafity of Service (Qo3) Sofutions,” London.

[20] V. H. Shukla, “Implementing QOS Policy in MPLS Network,” 2015.

[21] Juniper Network, “Learn About Quality of Service (QoS),” 2015.

[22] Evans John and Filsfils Clarence, “Deploying IP and MPLS QOS for Multiservice Networks,” London, UK. [Online]. Available: http://www.mkp.com.

[23] H. E. Egilmez, S. Tahsin Dane, K. T. Bagci, and A. Murat Tekalp, “OpenQoS: An OpenFlow Controller Design for Multimedia Delivery with End-to-End Quality of Service over Software-Defined Networks,” 2012.

[24] B. Kibrab Alemayehu Advisor Yalemzewd Negash and A. Ababa, “Analyzing Impact of Segment Routing MPLS on QoS,” 2019.

[25] M. Hasib, "Analysis of Packet Loss Probing in Packet Networks," 2006.

[26] W. Sugeng, J. Eko Istiyanto, K. Mustofa, and A. Ashari, "The Impact of QoS Changes towards Network Performance," 2015. [Online]. Available: www.ijcncs.org

[27] W. Sugeng, J. Eko Istiyanto, K. Mustofa, and A. Ashari, "The Impact of QoS Changes towards Network Performance," 2015. [Online]. Available: www.ijcncs.org

[28] Halefom Gebremedhin, "Qos Performance Evaluation of SRTE," pp. 1–65, Dec. 2021.

[29] S. Mohammad Javad Yasini Supervisor, M. Guido Alberto, and S. Mohammad Javad Yasini Master Thesis, "IMPLEMENTATION OF SEGMENT ROUTING AND MPLS TRAFFIC ENGINEERING IN SOFTWARE-DEFINED NETWORK BASED ON GNS3 NETWORK EMULATOR AND OPENDAYLIGHT SDN CONTROLLER," POLITECNICO DI MILANO, 2015. Accessed: Aug. 25, 2023. [Online]. Available: https://www.politesi.polimi.it/bitstream/10589/141815/3/final%20thesis%20report-%20yasini.pdf

[30] M. Karakus and A. Durresi, "Quality of Service (QoS) in Software Defined Networking (SDN): A survey," *Journal of Network and Computer Applications*, vol. 80. Academic Press, pp. 200–218, Feb. 15, 2017. doi: 10.1016/j.jnca.2016.12.019.

[31] S. J. Vaughan-Nichols, "TECHNOLOGY NE WS OpenFlow: The Next Generation of the Network?," 2011.

[32] N. Thazin, "QoS-BASED TRAFFIC ENGINEERING IN SOFTWARE DEFINED NETWORKING," 2019.

[33] M. I. S.ZAVRAK, *(A Feature-Based Comparison of SDN Emulation and Simulation Tools)*. 2017.

[34] N. Mckeown *et al.*, "OpenFlow: Enabling Innovation in Campus Networks," California, Berkeley, Mar. 2008. Accessed: Aug. 25, 2023. [Online]. Available: https://doi.org/10.1145/1355734.1355746

[35] I. Šeremet and S. Čaušević, "An analysis of reconvergence delay when using BGP-LS/PCEP as southbound protocols," Bosnia and Herzegovina, May 2019.

[36] M. Dallaglio, N. Sambo, J. Akhtar, F. Cugini, and P. Castoldi, "YANG Model and NETCONF Protocol for Control and Management of Elastic Optical Networks," pisa, Italy, 2016. [Online]. Available: http://sssup.it/modulation-formats

[37] B. D. Ed. B. Pfaff, "The Open vSwitch Database Management Protocol, RFC 7047," RFC 7047. Accessed: Aug. 25, 2023. [Online]. Available: https://www.ietf.org/rfc/rfc7047.txt

[38] D. P. J. S. W. T. M. MacFaden, "Configuring Networks and Devices with Simple Network Management Protocol (SNMP)," RFC 3512. Accessed: Aug. 26, 2023. [Online]. Available: https://www.ietf.org/rfc/rfc3512.txt

[39] Thomas D. Nadeau and Ken Gray, "SDN: Software Defined Networks," 2013. [Online]. Available: www.finebook.ir

[40] A. Hemid, "Facilitation of The OpenDaylight Architecture," Sankt Augustin, Germany, 2017.

[41] P. Aragonès, S. Joan, N. Rosa, and M. Alsina, "Software Defined Networks (SDN) In Data Center Networks Alumne Professors Ponents," La Salle, Barcelona, 2018.

[42] F. Paolucci, F. Cugini, A. Giorgetti, N. Sambo, and P. Castoldi, "A survey on the path computation element (pce) architecture," *IEEE Communications Surveys and Tutorials*, vol. 15, no. 4, pp. 1819–1841, 2013, doi: 10.1109/SURV.2013.011413.00087.

[43] S. Srivastava, S. Anmulwar, A. M. Sapkal, T. Batra, A. K. Gupta, and V. Kumar, "Ostinato - A powerful traffic generator," in *2014 Recent Advances in Engineering and Computational Sciences, RAECS 2014*, R. 2014 2014 Recent Advances in Engineering and Computational Sciences, Ed., IEEE Computer Society, 2017, pp. 1–4. doi: 10.1109/RAECS.2014.6799557.

[44] Shaoqiang Wang, DongSheng Xu, and ShiLiang Yan, *Analysis and Application of Wireshark in TCP/IP Protocol Teaching*. Shenzhen: IEEE, 2010.