Addis Ababa University

Addis Ababa Institute of Technology

School of Electrical and Computer Engineering

Telecommunication Engineering Graduate Program

Bandwidth Optimization of IP Core Network Using MPLS Traffic Engineering and Quality of Service: the Case of Ethio Telecom Backbone Network

By

Samrawit Eshetu

Advisor

Dr. Yalemzewd Negash

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 2021

Addis Ababa, Ethiopia

Addis Ababa University
Addis Ababa Institute of Technology
School of Electrical and Computer Engineering
Telecommunication Engineering Graduate Program

Bandwidth Optimization of IP Core Network Using MPLS Traffic Engineering and Quality of Service: the Case of Ethio Telecom Backbone Network

By
Samrawit Eshetu

Approved by Board of Examiners

_____	_____	_____
Chairman / School Dean	Signature	Date
Dr. Yalemzewd Negash	_____	_____
Advisor	Signature	Date
Dr. Fitsum Assamenew	_____	_____
Examiner	Signature	Date
Dr. Sosina Mengistu	_____	_____
Examiner	Signature	Date
_____	_____	_____
Director, Postgraduate Program	Signature	Date

Declaration

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

Samrawit Eshetu _____

Name Signature

Addis Ababa, Ethiopia _____

Place Date of Submission

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

Dr. Yalemzewd Negash _____

Advisor's Name Signature

Abstract

The rapid growth of the number of different telecom service users, the significant inventions of services, and web-based applications make the service providers ~~expected to have~~ a huge number of subscribers. People also show their interest to use the newly emerging services and applications since these services and applications are making life easier in day-to-day activities. Consequently, this makes the service providers ~~have~~ an enormous number of users. Even though it is good to increase the number of subscribers for the providers, the traffic that is forwarded from these subscribers to the provider's network is also vast. As a result, this will make the service provider's network ~~become~~ congested. Providers should have to consider their backbone network capacity while offering the different types of services. The increase in the number of customers without the timely deployment of the network expansion project will make the network to be exposed to congestion. Network expansion or deployment of new projects takes high cost as well as is time-consuming. But before the implementation of new projects, network bandwidth optimization should be implemented to use the available network resources effectively and efficiently.

The ~~motivation~~ of this paper is to investigate and analyze the performance and link bandwidth utilization of the core network by implementing MPLS TE + QoS. The impact of QoS parameters is being analyzed by using two scenarios; MPLS LDP + BE and MPLS TE + QoS scenarios. Simulation tools such as GNS3, Ostinato, and PRTG are used to compare the performance of the two scenarios. The analysis result shows that in MPLS TE + QoS scenario packet loss is improved by 29%, throughput improved by 17.4%, and latency improved by 15.3%. From this result, it is highly recommended that service providers should have to deploy MPLS TE + QoS on their core (backbone) networks, which makes them more beneficiary.

Keywords—MPLS, IP, MPLS-TE, QoS

Acknowledgment

First of all, I would like to give a special thanks to the Almighty God for everything that happened in my life.

Next, I like to thank Dr. Yalemzewd Negash, who has been my supervisor during the thesis work period, for his continuous follow-up and guidance. His cooperation and advice were very useful and constructive.

Then, I want to express my special appreciation to AAiT in collaboration with Ethio Telecom for the motivation and sponsorship to make this program successful.

I am grateful to my family for their continuous support especially my mother.

Finally, I want to thank my work colleagues and classmates for their boundless support and advice.

Contents

List of Figures

List of Tables

List of Abbreviations

ACLs	Access Lists
AF	Assured Forwarding
ATM	Asynchronous Transfer Mode
bps	bits per second
BE	Best Effort
BW	Bandwidth
BGP	Border Gateway Protocol
CBQ	Class Based Queuing
CT	Class Type
CoS	Class of Service
CQ	Custom Queuing
DiffServ	Differentiated Service
EF	Expedited Forwarding
E-LER	Egress Label Edge Router
EXP	Experimental
ECN	Explicit Congestion Notification
FTP	File Transfer Protocol
FEC	Forward Equivalent Class
HTTP	Hypertext Transfer Protocol
HWQ	Hardware Queuing
ITUT	International Telecommunication Union Organization
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IP	Internet Protocol

IPTV	IP Television
IPP	IP Precedence
ISPs	Internet Service Providers
IP RIB	IP Route Information Base
IP FIB	IP Forward Information Base
ILER	Ingress Label Edge Router
IGP	Interior Gateway Protocol
IP	Internet Protocol
IETF	Internet Engineering Task Force
LDP	Label Distribution Protocol
LSP	Label Switching Path
LSR	Label Switching Router
LFIB	Label Forwarding Information Base
MP-BGP	Multiprotocol BGP
MPLS	Multiprotocol Label Switching
NMPs	Network Performance Metrics
PHB	Per Hop Behavior
QoE	Quality of Experience
QoS	Quality of Service
RI	Route Information
SIP	Session Initiation Protocol
SWQ	Software Queuing
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
TE	Traffic Engineering

TCP	Transport Control Protocol
ToS	Type of Service
TCP/IP	Transport Control Protocol/Internet Protocol
TTL	Time to Leave
UDP	User Datagram Protocol
VoIP	Voice over IP
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
WFQ	Waited Fair Queuing
WRED	Waited Random Early Detection

1. Introduction

1.1. Background

Nowadays the evolvement of different telecommunication technologies and web-based service applications in the communication aspect results to have a huge number of users for the service provider. For making life easier by finishing the process within a short period. The new emerging technologies in different interests in communication areas are continuing and users are attracted and showing their interest in those services and applications. Consequently, the telecom network number of users becomes huge from time to time. This is an indication for the Internet Service Providers (ISPs) to have a well-organized network and infrastructure. Which is to fulfill the mandate and Quality of Experience (QoE). Meanwhile, due to the invention of new devices, new applications, and services which are mainly dependent on the way of connectivity.

The emergence and innovation in the information and communication technology aspects provide a significant improvement as of our day to day activities. Even though the new and fast-emerging technologies, internet-based applications, and different types of services are more supportive for our day-to-day activities, they require more Bandwidth (BW). This leads to the demand for the usage of network services to grow significantly. The integrated services voice, video, and data, real-time and non-real-time service traffic should have transported in a converged core (backbone) network to guarantee the service quality [1].

These days, it is known that rapid growth in the invention of different services and web-based applications such as Voice over IP (VoIP), IP Television (IPTV), online gaming, real-time multimedia streaming, video conferencing, etc., leads to the requirement of more bandwidth. The service provider's backbone network should have the capability to

fast switching and forwarding of the traffic that comes from the users for efficient utilization of the network and requires the deployment of different techniques for network management.

Ethio telecom is a telecom service provider in Ethiopia and offering different types of services on the existing backbone network. Increasing the number of subscribers without capacity enhancement or better resource management leads to network congestion and consequently, bad Quality of Service (QoS) and QoE will be experienced. However, services quality should have taken into consideration in order to become a world-class service provider, and hence the provider should fulfill the predefined standards by concerned organizations. In the meantime, service providers prefer link upgrading (adding an extra link) where the bottleneck is happened instead of implementing bandwidth optimization techniques in the existing core network. Deployment of a new project and enhancement resources is quite challenging due to cost, time, and different resources consumption and hence, it requires intensive consideration.

Most service provider backbone network is based on Internet Protocol Multi-Protocol Label Switching (IP MPLS). Which is an emerging technology that is playing an important role in supporting the requirements of real-time applications [1] and can support different techniques of QoS provisioning and Traffic Engineering (TE) for making the backbone networks to become more scalable and improve the performance. The implementation of MPLS in an IP core network (backbone infrastructure) results in a faster forwarding and switching of packets. In most backbone networks, QoS was not implemented as service segregation, rather it follows the best effort (BE) scenario also known as First In First Out (FIFO) as the name indicates the first come first serve scenario. Even though there is a segregation of customers as (platinum, Gold, Silver, and Bronze) which is based on their service type and payment scheme only. In Ethio Telecom also the

backbone network was deployed using MPLS Label Distribution Protocol Best Effort (MPLS LDP + BE) due to ease of implementation. This means the traffic follows the predefined route by the Interior Gateway Protocol (IGP) rule which is always the shortest path and makes this link becomes congested by letting other links be underutilized. Therefore, the motivation of this thesis is to implement traffic classifications based on the demand using QoS for congestions management and applying MPLS TE at the backbone network for better utilization of link bandwidth by securing customer QoE.

1.2. Statement of the problem

Due to the rapid growth of the usage of BW intensive services, the traffic volume is increasing continuously. In line with the rapid growth of the services and number of customers, there must be a capable backbone network infrastructure that can carry all the traffic that comes from customers accordingly. Ethio telecom provides several telecom services by using different infrastructures to offer different types of services. Ethio Telecom deploys an IP + MPLS-based backbone (core) network. Since different services are offered on the existing infrastructure, the increase in the number of subscribers leads to a rise in the traffic volume significantly. Without the timely implementation of core network expansion or the deployment of the new project due to different reasons will create network congestion and this leads to dropping of packets, consequently, the company will experience the bad quality of experience and degradation of revenue.

As shown in figure 1.1 the general topology of the core network, which is having two different planes that are, plane A and plane B. The figure tries to show the traffic route selection which is shown as a red arrow. But other redundant links are not utilized in both planes. In most service providers, there is no implementation of QoS in their backbone network, rather it follows BE scenario. Using BE scenario in the core network

leads to network congestion as the traffic volume increases continuously which is comes from different access devices.

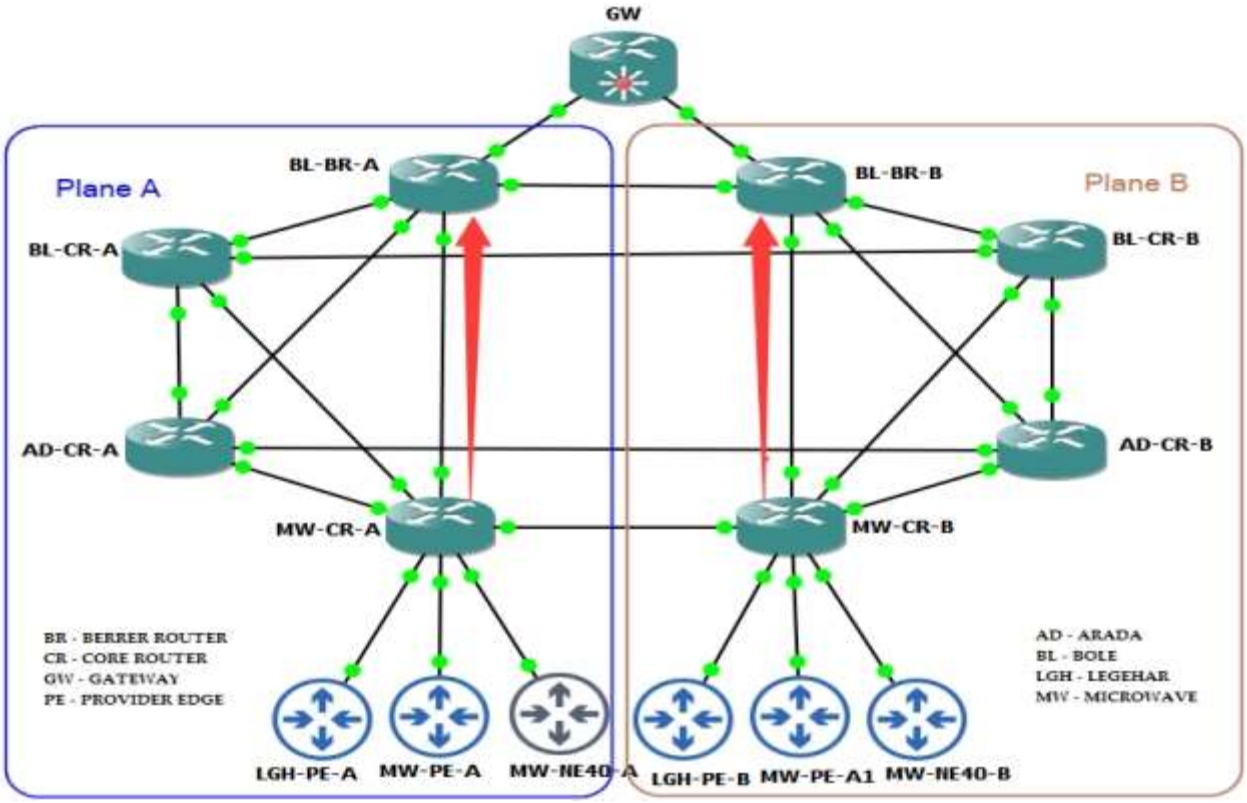

Figure 1.1: General topology of the core network

In Ethio telecom the existing core network is based on MPLS LDP + BE, and the traffic flow is mainly dependent on the predefined IGP rule or metric then all MPLS traffic follows the IGP rule only. Therefore, the above MPLS LDP + BE scenario is not capable to handle the traffic appropriately during congestions or at pick hour. In this case Figure 1.1, shows the traffic always selects the shortest path which is created by IGP (red arrowed path). In the monitoring report as shown in Figure 1.2, both shortest path links

were utilized near to the full capacity. Therefore, the technical team preferred to add an extra link instead of applying the bandwidth optimizations technique in the network.

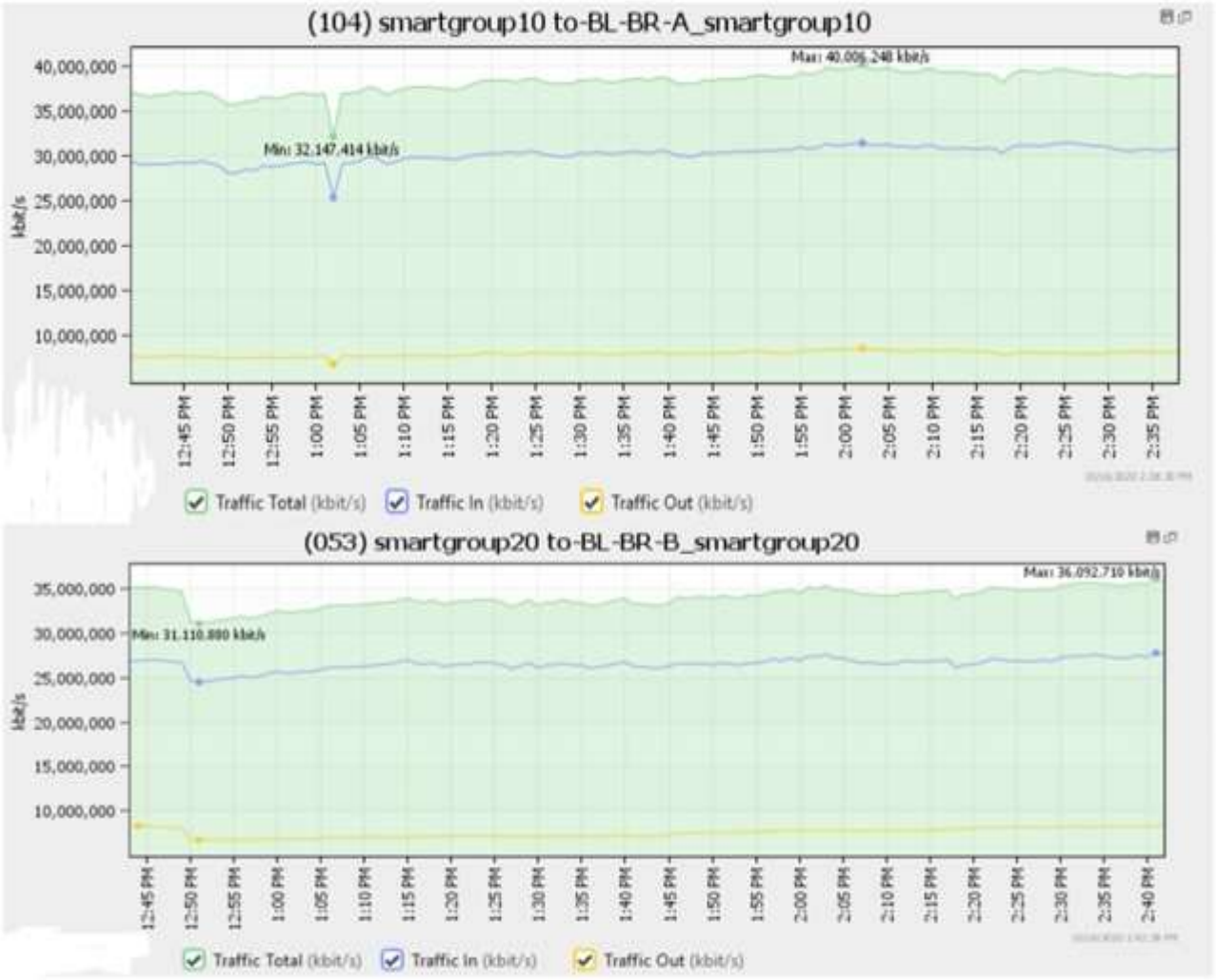

Figure 1.2: Monitoring result of Shortest paths

1.3. Objective

1.3.1. General Objective

The main objective of this thesis is to study the performance of the backbone (core) network in terms of QoS metrics and investigate how to optimize and utilize the links

efficiently by deploying MPLS TE + QoS, and compare the network performance between the existing MPLS LDP + BE and the proposed MPLS TE + QoS in the IP Backbone network of ethio telecom to achieve the general objective, the following specific objective will be followed.

1.3.2. Specific Objective

A specific objective of this thesis is to study the performance of the backbone (core) network and investigate how to optimize and utilize the links efficiently by deploying MPLS TE + QoS in the IP Backbone network by:

- Analyze the total traffic flow through each link
- Analyze the traffic demand
- Normalize the traffic and the links
- Apply QoS using with the help of Simulator
- Deploy the TE Label Switching Path (LSP) using a simulator in the IP backbone network.

1.4. Methodology

In this thesis, the following methodology ~~will be~~ performed. As shown in Figure 1.3 by studying the traffic flow pattern and the performance of the backbone network and implementing techniques for the effective BW utilization by using,

- Literature review of related works
- Data collection of each link utilization
- Identify each link capacity

- Analyze the traffic flowing through each link
- Specify and categorize the different types of services
- Identify and categorize services
- Using the GNS3 platform, to analyze the network before and after applying TE + QoS, and the aggregate traffic flowing via each link by creating congestions.
- PRTG tool will be used to monitor the links and Ostinato network traffic generator is used to generate the traffic.

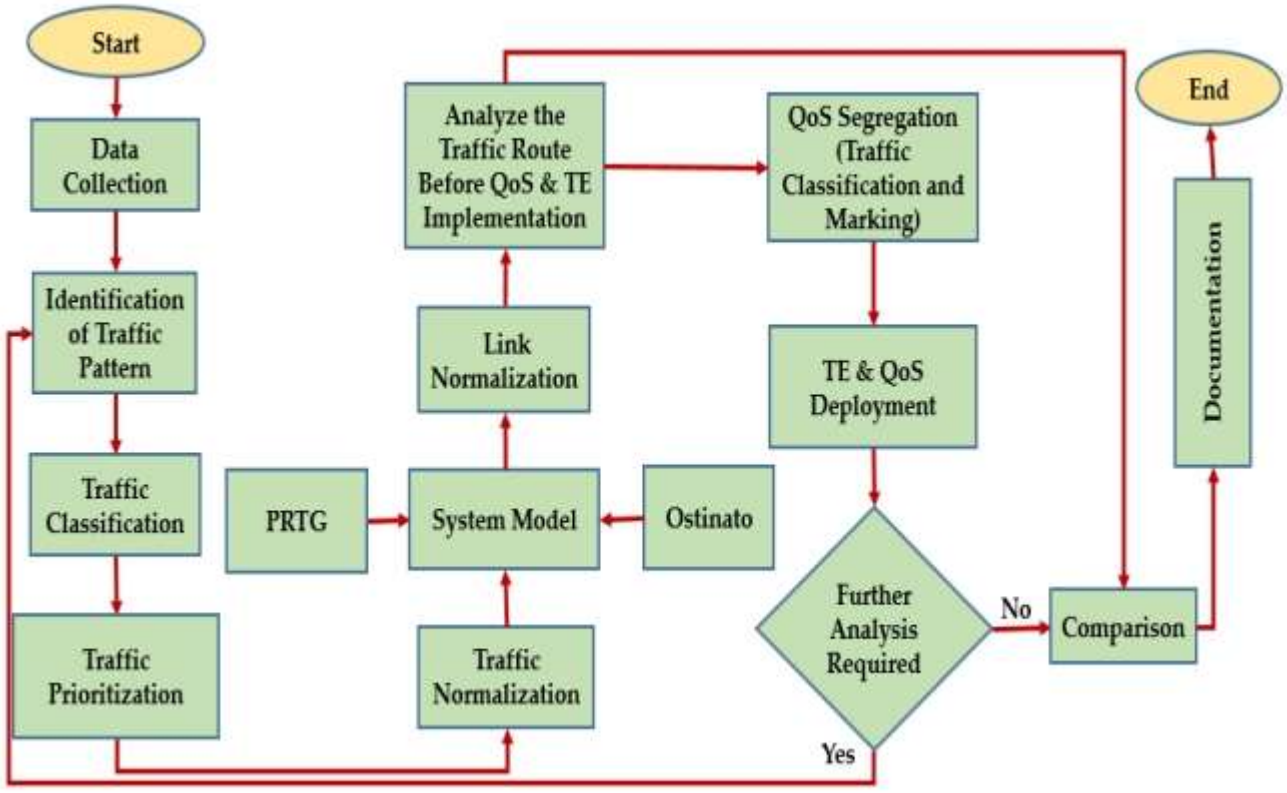

Figure 1.3: Methodology Flowchart

1.5. Scope and Limitations

1.5.1. Scope of the Thesis

This thesis mainly focuses on the selected routers and links in the core network by which congestion is the main problem, in the Addis Ababa region.

1.5.2. Limitations of the Thesis

Due to the process intensiveness of the simulation tools and the memory limitation of the personal computer, it is not possible to simulate all the connected access networks to the core network in the simulation environment. But it should be noted that reducing the number of access devices in the simulation environment will not change the overall result.

1.6. Contributions

This paper mainly focuses on how to fairly distribute the traffic through the core network. The dynamic growth in the traffic will affect the overall performance in the core network without implementing any controlling or management mechanism. After deploying the traffic (link) management techniques, the traffic will flow by the predefined path (route) rather than using only the default route. This link controlling or management mechanism will maximize the performance of the core network, easily decided the route of the new traffic consequently this will increase the degree of satisfaction of Ethio Telecom customers.

1.7. Literature Review

A lot of researches has been conducted their research ideas in the implementation of QoS in MPLS deployed networks and the diverse mechanisms of implementing QoS mechanisms in a service provider backbone network. Nowadays most service provider's backbone network is based on IP MPLS. In [1], experimented on MPLS in the core

network by using the Differentiated-Service (DiffServ) technique and QoS + TE to improve core network efficiency. TE modifies routing patterns to provide efficient mapping of traffic stream to network resources to reduce congestion by improving service quality in terms of latency, jitter, and packet loss. The experiment was performed in two scenarios or parts. The first part was MPLS with DiffServ and the second part was performed with MPLS TE. The simulation was based on a common topology consisting of four IP and 5 MPLS nodes and using Class-Based Queuing (CBQ) except the IP nodes and MPLS Label Switching Routers (LSRs) using drop-tail queuing links between IP nodes. The links data rate is 1Mbps except for the links between IP nodes and MPLS LSRs link capacity of 2Mbps. Under this condition, Transport Control Protocol (TCP) and User Datagram Protocol (UDP) traffic flow was measured and analyzed by attaching file transfer protocol (FTP) traffic to TCP, voice and video traffic to UDP flow. The demonstration was done in different scenarios as, no DiffServ, DiffServ without MPLS, DiffServ, and MPLS with single path finally DiffServ with MPLS multipath. The simulation was run in a series by sending rates of traffic at 60%, 80%, and 100% of network BW. The simulation results clearly show that a pure IP network only provides best-effort service, and the overall delay was optimized from 83.lms to 77.25ms.

In [2], the authors want to connect nine MPLS nodes by creating two paths, one for the Expedited Forwarding (EF) class and the other for the Assured Forwarding (AF) class. Reducing one of the links BW by half in the MPLS network and experimenting with two scenarios. This experiment shows that the throughput measured at the destination host was very much lower than compared to the source. So that packets were suffering to travel via a congested network, consequently decreases the throughput. Both types of traffic experience packet drop (loss) because both types of traffics are treated equally. This was a good experiment using the java network simulation tool and implementing

DiffServ, when the link becomes congested AF's traffic throughput decreases but, prioritized EF packets did not suffer any throughput loss.

The other interesting experiment was performed in [3] by prioritizing different types of services in a different category. By defining the QoS policy with the IP Precedence (IPP) and analyzing the result with and without the implementation of QoS. Before QoS implementation, the aggregate traffic throughput at the destination is full of its capacity. But after implementing QoS those predefined types of services occupied the maximum predefined QoS policy. The paper also suggested to the ISPs to implement QoS using IPP and type of service (ToS) to satisfy the needs.

In [4] the authors want to state the various and efficient mapping of ToS bits to the Differentiated Service Code Points (DSCP) bits, by manipulating QoS parameters with constraint-based TE LSP with Network Performance Parameters (NPMs) respectively. To show the variation of different QoS implementation mechanisms, DSCP parameters may vary depending on different NPMs. By assigning DSCP values for different types of packets that are entering the core network from the access networks in a Per-Hop-Behavior (PHB) environment. Mainly assigning a DSCP value for critical traffics such as delay and packet loss sensitive traffics and transmitting in a network is not quite efficient. Rather other factors should be considered such as defining the Class Type (CT) and an LSP that is DiffServ aware in a PHB environment. Finally, it concludes TE is the main tool to optimize the network performance as considering the main objective.

In [5] the authors tried to optimize the quality of the service by allocating a dedicated BW for the predefined traffic types. The simulation is done between two distinct places. By using the IPP in collaboration with CBQ and evaluating the effectiveness of QoS in the MPLS deployed network. Finally, the result was collected by creating and injecting

additional miscellaneous traffic to the network to create congestion. Before the implementation of QoS, IPP and BW allocation for each traffic type, the utilization of the services becomes degraded but after the implementation of QoS, IPP, and BW allocation for each traffic type, the traffic utilized the link by occupying nearly the predefined BW.

1.8. Thesis Layout

This thesis paper is composed of five chapters. Chapter one is about the overall introduction of the thesis and includes background, statement of the problem, the objective of the study, methodology how to achieve the stated objectives, the scope, and limitation of the thesis, contribution, and finally the related works of literature.

Chapter 2 introduces the basics of MPLS, the benefits and the most common terminologies that are used in MPLS are explained, and also the basic concept IP and IP network is discussed.

In Chapter 3, the basic concept of QoS its Models, and different QoS parameters are introduced, the chapter also talks about the MPLS DiffServ-aware-TE and the techniques of congestion management, the benefit of classification and marking of network traffic, and finally about SLA.

Chapter 4 discusses the simulation environment such as an overview of the used simulation tools, the simulation scenarios, and considerations in the analysis of QoS parameters. Lastly discussed link utilization and performance of the network.

The last chapter, chapter five discusses the conclusion drawn from the analysis part and about the future work. References are also included at the end of the paper.

2. Introduction to MPLS and IP Network

2.1. Overview and Benefits of MPLS

As the name implies as multi-protocol label switching, uses several labels that are tagged to the packet for packet forwarding and switching. It is a layer 2.5 protocol in the TCP/IP protocol stack or it lies in between the network layer and data link layer. It is adopted by combining the advantages from both IP and Asynchronous Transfer Mode (ATM) technologies, and it uses a packet forwarding technique by using labels to determine the path that is from source to destination (edges of MPLS network) in the backbone network to increase the forwarding rate by shortening packet processing time. A set of packets that travel from a particular node that follows the same path are called a stream [12]. As the packet enters the node, the stream in which the packet is encoded with a short fixed-length value is known as "label". Figure 2.1 shows the MPLS network architecture and the different terminologies that are used by MPLS. These different terminologies will be discussed briefly in the next sections.

The IP protocol establishes the neighbor relationship so that the neighbors will exchange the Route Information (RI) and generates an IP Route Information Base (IP RIB). Then LSP obtains routing information from IP RIB. After identifying the routing information, the label switching protocol will obtain the RI from IP RIB which is established between neighbors, so that the route prefix in the IP RIB is mapped to a Forward Equivalent Class (FEC). In the IP RIB, the active optimal route is used to generate forwarding entry in an IP Forward Information Base (IP FIB). FIB is also known as forwarding or Media Access Control (MAC) table and it is used as network bridging in the routing and updates the routing table dynamically.

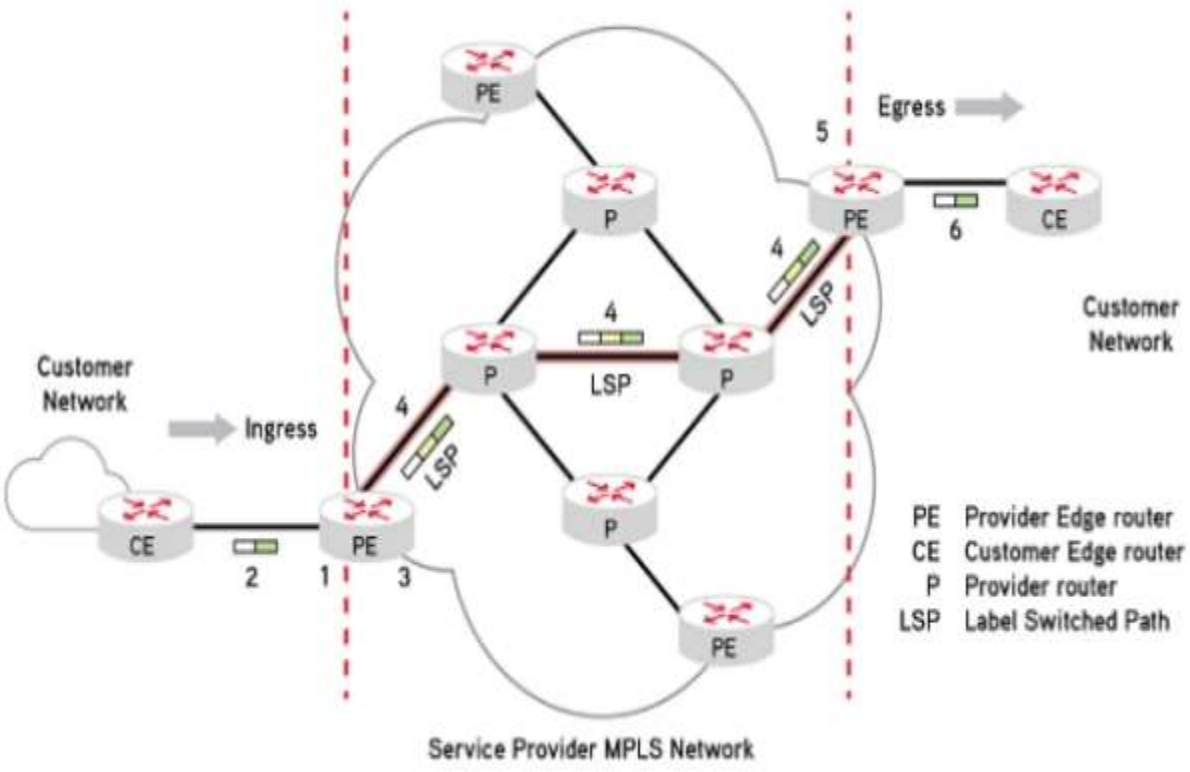

Figure 2.1: MPLS network [11]

LSP establishes a neighbor relationship, allocates a label for each FEC, and advertises a label to the upstream node. Besides, it obtains a label from downstream nodes and uses label information to generate a Label Forward Information Base (LFIB). After establishing the MPLS forwarding plane as shown in Figure 2.2, the node generates the IP FIB and LFIB to forward the data packet. As shown in Figure 2.1. Labels are assigned and distributed by downstream Label Switching Router (LSR) to an upstream LSR. Label Distribution Protocol (LDP) is a protocol used for label distribution and it defines messages in the label distribution process as well as procedures for processing these messages. The LSRs create a mapping of incoming labels, next-hop nodes, and outgoing labels from LFIBs for specific FECs, so this mapping is used for the establishment of the LSPs as shown in Figure 4. Since MPLS uses multiple labels in the packet forwarding

process, it makes the network scalable, utilizes the available BW by using different features such as LDP, RSVP-TE, MP-BGP extensions.

MPLS system architecture consists of two basic planes such as the control plane and the forwarding plane as shown in Figures 2.2 and 2.3 below.

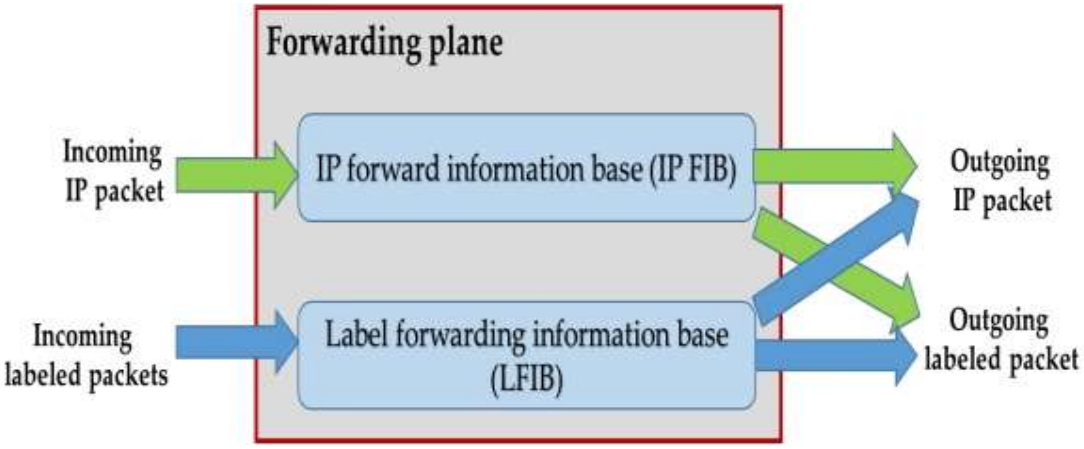

Figure 2.2: MPLS forwarding plane [17]

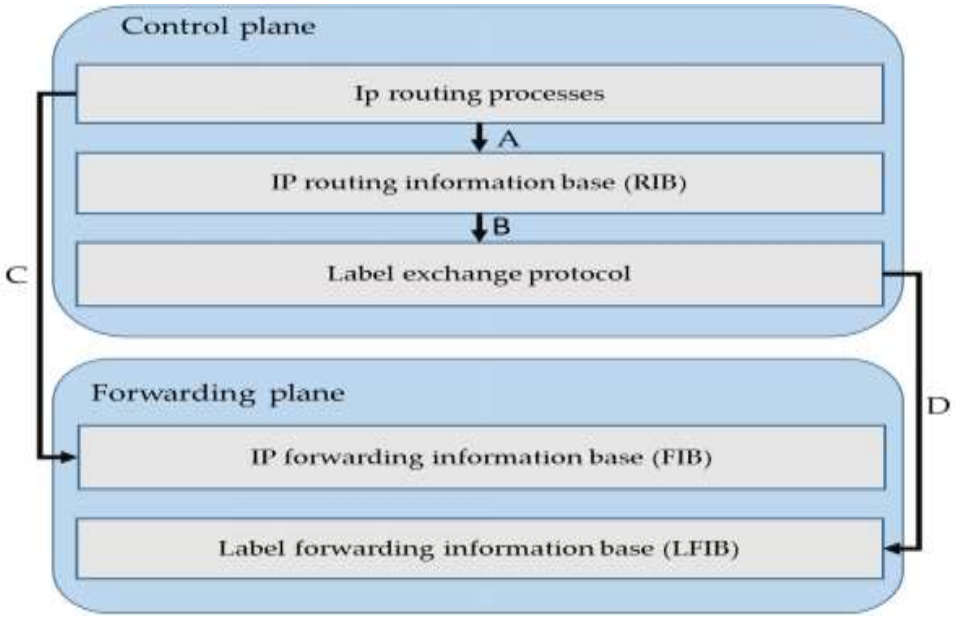

Figure 2.3: Workflow of MPLS System [17]

- The control plane: It is connectionless and it creates and distributes label forwarding information base and establishes or tears down LSPs.
- The forwarding plane: It is also called the data plane which is connection-oriented. The forwarding plane adds or deletes labels from IP packets and forwards the received packets based on LFIB and its connection can be created on layer 2 networks.

2.1.1. Forwarding Equivalent Class (FEC)

It is a data flow that is processed in the same mode during forwarding [19] and it can be identified by address, tunnel, and a Class of Service (CoS) typically assigned to the same label of FECs by the device. Traffic that is labeled as the same FEC can be forwarded by using the same manner in the same path.

2.1.2. Ingress/Egress Label Edge Router (I/E LER)

Once an IP packet enters the MPLS network from a non-MPLS network, the edge device that receives the IP packet is called Ingress Label Edge Router (I-LER). The I-LER creates an MPLS header in the packet and inserts a specific label to this field. This I-LER pushes a label (label adding operation) called label tagging to the packet before forwarding is done.

After the MPLS labeled packet traverses through, it reaches the edge of the end node in the MPLS network so that this node will pop the MPLS label and forward the pure IP packet to the non-MPLS network. This operation is performed by Egress Label Edge Router (E-LER). Penultimate Hop Popping (PHP) operation is also performed by penultimate LSR to decrease the number of labels in the label stack.

2.1.3. Label Switching Router (LSR)

In the MPLS network, the packet traverses through different nodes, so those nodes other than I-LER and E-LER are called Label Switching Routers (LSRs). These nodes receive a packet, perform label swapping or label replacement operations. This operation is carried out by transit nodes, to replace a label on the top of the label stack in an MPLS packet with another label. LSRs use the next entry label forwarding entry NHLEF to forward the packets. Since the incoming label maps each label to a set of NHLEF, it consists of the packet's next-hop and the operation to be performed on the packet's label and used for forwarding labeled packets [6] in collaboration with Interior Gateway Protocols (IGPs) such as IS-IS, OSPF, and/or other link-state interior protocols.

2.1.4. Label Switching Path (LSP)

LSP is a path or a route through which the packet travels that is predefined by the IGP protocols or from IGP routing information which is based on the predefined IGP metrics. Since LSPs are unidirectional, the returning traffic takes another LSP. MPLS assigns packets to FEC then distributes labels that identify the FEC and establishes the LSP. Downstream LSRs assign labels for the FEC to upstream LSRs via a label advertisement protocol, so that the downstream LSR informs its upstream LSR of the label. Then each upstream LSRs adds the label to the local LFIB, then through this process, LSP is established as shown in the below Figure 2.4.

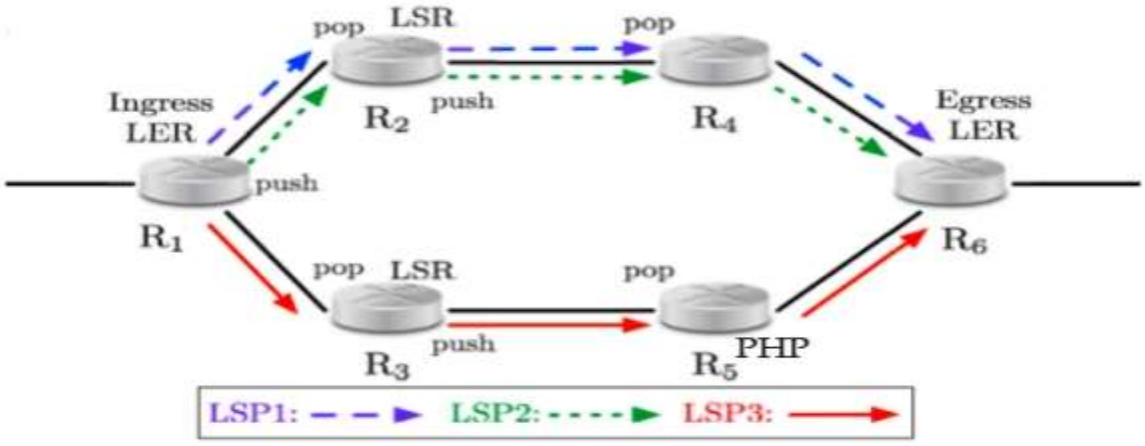

Figure 2.4: MPLS LSP formation

There are two types of LSPs, which are Dynamic LSP and Static LSP. A Static LSP is manually configured, while Dynamic LSP is dynamically established by interior routing protocols and LDP.

2.1.5. Label Distribution Protocol (LDP)

LDP is a label distribution protocol and it generates and exchanges labels for its prefixes between routers then advertises to their neighbors either by a dedicated LDP or by extending the existing protocols like Border Gateway Protocol (BGP). Like other protocols, LDP first establishes a neighbor adjacency before exchanging label information.

2.1.6. MPLS Header

Figure 2.5: MPLS header [11]

As shown in the above Figure 2.5 the MPLS header is a 32-bit length and from which a 20-bits is dedicated for the identifier which uniquely identifies FEC to which the packet belongs, and this 20-bit field identifies the label value. A Bottom of Stack (BoS) field that takes a 1-bit length which identifies the bottom of a label stack. Since MPLS supports multiple labels, and if the value of BoS is set to 1 the label is at the bottom of the label stack. An 8-bit length is set for the Time to Leave (TTL) field which indicates the value of the TTL and it has the same functionality as IP packets. The 3-bit Experimental (EXP) field in the MPLS header is reserved for experimental use. Most commonly this bit is for QoS purposes (RFC 3032).

2.1.7. MPLS Traffic Engineering (MPLS-TE)

The motivation of MPLS-TE is to create and decide the path or the route by defining different constraints in which for the selection of the path so that the flow of the traffic will be along this predefined route. There are different TE deployment mechanisms in the selection of the traffic to be routed. One of them is by manipulating the IGP metrics. To minimize the overall cost of operation by using the available BW in an efficient way and other resources effectively [7]. TE can mitigate the effect of congestion that happened in the network, through better utilization of all the available BW, then the network nodes will be in the optimized resource utilization and consequently, this will improve the performance of the network. TE has an important feature by rerouting the traffic in the case of link failure, building new services or for virtual leased line services, and as per the required capacity planning.

2.2. MPLS Virtual Private Network (VPN)

Besides the benefits of fast-forwarding and switching of a packet in the MPLS-enabled network, it also supports the provider to offer different kinds of services for different customers as per the requirement. For customers who have different offices and are

located in a different geographical area, the service offered is MPLS Virtual Private Networks (MPLS-VPN). MPLS-VPN can be used in the same router by using the virtualization technique. MPLS VPN is very important since traffic between sites is transmitted via label switched path. MPLS-VPN provides a low cost, high security, and provides advanced QoS. MPLS-VPN has the concept of Virtual Routing and Forwarding (VRF) technique which allows the router to have multiple routing tables (multiple VPNs) at the same time [19]. So that the different customers can use the same subnet of IP address that is connected to the same MPLS network by using VRF. Multi-protocol BGP (MP-BGP) is an extension of BGP enabling the BGP to carry the routing information for networks and address families. In [18] the authors mainly tried to show the detailed configuration of VRF using MPLS VPN. By creating MPLS tunneling from end to end in the provider's network which is from the source PE to the destination PE router within the MPLS domain. It supports the configuration of multiple customers using VRF and VPN by constructing multiple routing tables inside the same router.

2.3. IP Network

On the network, each of the devices is designated as a node with having a unique address. These addresses are a numeric quantity that is easy for computers (nodes) to communicate with each other. So this unique numeric figure is called IP address. The IP address is a 32-bit header in length, and from this 32 bit, 8 bit is dedicated for QoS called ToS bits. The Differentiated Service (DiffServ) model is based on redefining the meaning of the ToS field (the 8 dedicated bits) in the IP header. The corresponding most 6 significant bits are dedicated for Differentiated Service Code Points (DSCP) and the remaining 2 bits are used for Explicit Congestion Notification (ECN) as shown in Figure 2.6. DSCP is backward compatible with the IP Precedence (IPP) values. It has four Assured Forwarding (AF) classes by grouping three AFs and giving an order for the class

selector and drop probability respectively. There are also two additional classes such as Default class which is without the implementation of QoS or Best Effort (BE) scenario and the other is Expedited Forwarding which is dedicated for the delay and drop sensitive packets.

The information that is included in the IP packet is used to forward the packet to the desired destination by the router.

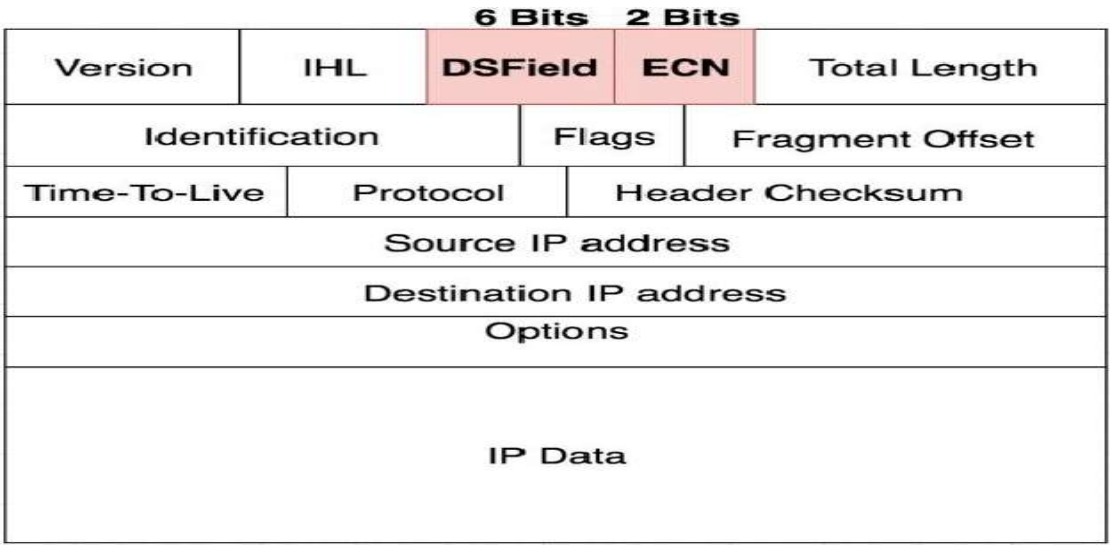

Figure 2.6: IP Packet Structure [21]

3. QoS, MPLS DiffServ-aware-TE, Congestion Management, and SLA

3.1. QoS in IP/MPLS Network

Traditionally most Telecom Service Providers (TSPs) offered the same level of quality of service performance to all of their customers [6]. Most differentiation among customers has been done only by their connectivity type or BW subscription fee. In Ethio Telecom, customers are classified by the BW they subscribed to. Though customers are classified as Silver, Bronze, and Gold, this customer prioritization was not implemented in the QoS prioritization technique in the core network. Recently, the connectivity demand becomes increasingly because of the newly emerging services and web-based applications, which require more BW or network quality. Thus SPs should have new ways of service differentiation and implementation of QoS in their core network to improve the revenues as well as to assure the customer's service quality by applying different mechanisms and techniques. There are different techniques and approaches in deploying QoS. A packet can be treated in different steps in the OSI model. In layer three treatment, an IP packet can be treated by using the DSCP field to prioritize the packet referring to the tagged DSCP value. By merging the different features of DSCP and MPLS, it will give a better strategy for the implementation of QoS in the backbone network. The mechanism is to ensure that excessive congestion does not occur for the packets within the assured or guaranteed QoS [7].

QoS is a technology used to manage data traffic in the network in which to reduce the occasions such as, packet loss, jitter, and latency. It also provides control of network resources for better network management. Besides, it sets boundaries and priorities for different traffic categories that traverse across a network. The volume of application usage, an increase in the number of devices connecting to the network, a significant rise in social media usage, a significant increase in the usage of IoT devices means the network

will frequently be flooded. This network overload can lead to discrepancies in the performance of the network, as a result, significant degradation in the quality of service will be experienced. Defining QoS policies is essential for the traffic management of the packets that are traveling across the network.

QoS can mitigate these issues by defining a certain number of traffic classes depending on the granularity of different traffics, and it offers the following benefits:

- Delay Reduction

Delay is the amount of time taken by a packet to traverse from the source to the destination. The Delay/Latency of the packet should be as close to zero as possible. Classification and prioritization of packets are very essential.

- Packet Loss Prevention

Packet loss occurs because of network congestion. The network device (node) disregards inbound data packets due to overload. With QoS effectively in place, the steady stream of traffic is supported, which means packets won't be drop out completely, prioritization dictates the traffic type pipelined accordingly.

- Jitter Reduction

It is another effect of network congestion and results in degradation of the quality of services. The irregular signal pulses result in unreliable distribution and speed of data packets, consequently flickering effects, and out-of-sequence of packet delivery will occur.

- Improved Security

QoS can block unwanted or suspicious traffics in its path, acting as a firewall to make it a key component of a more secure network infrastructure. QoS can be viewed from the customer side and provider side. From the service provider's point of view, QoS is the possibility to make more revenue by offering a wider range of services and guarantee the quality of those services as well as keeping the network performance good. From the user's point of view, it is the possibility to get a better service from the network and be able to use different applications that require different resource requirements. To satisfy the service user demands that fulfill the user's need and this may not be always easy because different users may have different degrees of expectations on quality [7], [8].

3.2. QoS models

Internet Engineering Task Force (IETF) has proposed different QoS models and mechanisms to meet the demand of QoS such as DiffServ and Integrated Services (IntServ) models [7].

3.2.1. Integrated Services (IntServ) Model

This QoS model works by allocating and preserving the BW for a specific route on a network by implementing a resource allocation using Resource Reservation Protocol (RSVP). The main problem of IntServ architecture is its scalability issue since it requires huge storage and processing overhead on the routers for data forwarding and buffer management. The reservations are made on a per-flow basis [8]. The setting of state in all routers along the path is non-scalable and non-workable administratively.

3.2.2. Differentiated Service (DiffServ) Model

It is designed by IETF (RFC 2474) to meet the differing levels of QoS requirements for different traffic flows. Which makes the stateless network to be scalable and robust. By marking the DiffServ field of the packets and treating them differently, the different

traffics can be categorized into different classes [9]. Traffic classification, marking, rate shaping, policing is done by the edge routers either in a PHB manner or using end-to-end serviced techniques [11]. The core functions of DiffServ which are performed by the network devices are classifying, policing, shaping, queuing, scheduling, and remarking. The packet that is received by the edge network device by the ingress interfaces will be classified into the appropriate classes. There is also additional policier and rate-limit assignment configuration for the different classes. The traffic scheduler takes the packet and rearranges them by using the predefined rules and queuing to make them in order which is configured for the scheduler. Then if there is shaping to shape the rate, finally the device remarks the DS field value and forwards it to the packet for the next PHB.

3.2.3. Best Effort Scenario (BE)

This model doesn't use any of the QoS prioritization, which means all packets are treated equally. BE model is mostly used as a default model whereby networks have not yet configured for any QoS policies.

3.3. MPLS DiffServ-aware-TE

It is a very useful provider's tool when the network links running close to full capacity. Traffic Engineering (TE) is the process of controlling how the traffic flows through the network to that optimize the available resource utilization and improve the performance of the network. The aim here is to reduce the overall cost of operation and using the BW resources more efficiently. Using MPLS-TE can assist and utilize the available bandwidth in the non-shortest path. In the MPLS deployed core network, traffic engineering is one of its features. TE modifies the traffic routing pattern to provide an efficient mapping of the traffic stream to the available network resources [1]. So the efficient mapping can reduce the occurrence of congestion and improve service quality in terms of latency, packet loss, and jitter, as well as reduces the impact of network failure to sustain service

availability. MPLS-TE can bring explicit routing paths in the MPLS domain by creating LSP from the originating LSR to the terminating LSR also intermediate LSR through an explicitly defined LSP. MPLS-TE also supports constraint-based traffic routing. Since IGP computes the routing information by using typically a single metric (constraint), rather constraint-based routing approach to meet some requirements by taking more detailed information of the network that allows the LSR to compute the path that fulfills the predefined requirements. MPLS allows [7] the originator of the LSP to do the path computation and map the packets to that LSP, and once the packet is mapped to that LSP forwarding is done based on the label.

3.4. Congestion Management

Queuing is one of the temporary congestion management mechanisms on an interface of network devices by storing excess packets in buffers until BW becomes available. By determining the order of the identified packet to control the congestion in the interface based on priorities assigned to the packets [12]. Congestion management entails certain queues, assigning packets to those queues based on the classification of the packet, and scheduling the packets in a queue for transmission in some queue support routers to meet the varying BW, jitter, and delay requirements for different applications. Queuing consists of two parts: HardWare Queuing (HWQ) and SoftWare Queuing (SWQ).

- HW queuing

The HW queuing is sometimes referred to as transmit queue and it uses a First-In-First-Out (FIFO) strategy which is necessary for the interface drivers to transmit packets one by one Scheduling packets into an HW queue based on QoS requirements.

- SW queuing

It is one way of handling an overflow of the arriving traffic to use queuing mechanism and algorithms to sort the traffic and to determine some method of prioritizing on to an output link, and the most popular queuing tools from the simplest to the complex are (FIFO), Priority Queuing (PQ), Custom Queuing (CQ), Flow-Based Waited Fair Queuing (FBWFQ), Class-Based Waited Fair Queuing (CBWFQ).

3.5. Classification and Marking Network Traffic

Implementing the different mechanisms of QoS especially in the core network is very useful for the mitigation of congested and slow channels. To minimize congestion situations and to allow some critical traffic types to be transported by using a special treatment without delay and packet drop if possible or within the minimum acceptable range. The following listed three steps summarize the steps to follow on the configuration of QoS for different traffic flows,

- Construct a class map: In this step identify the traffic types that need special treatment. This step defines a group of network traffics using various classification tools such as Access Lists (ACLs), IP address, IPP, IP Differentiated Service Code Points (IP DSCP), MPLS Experimental bit, etc...
- Policy map: This step clarifies what will happen to the classified traffic which is defined in step one as a class map. A policy map chooses the group of traffic (class-maps) on which to perform QoS functions such as Queuing, dropping, policing, shaping, and marking. Traffic policy-map associating the traffic class with one or more QoS features.
- Service policy: In this step, it clarifies where the predefined policy will be applied appropriately to the desired interfaces, sub-interfaces, or any other interfaces in the router.

3.6. QoS Parameters

QoS is a traffic management strategy that allows network resources to be used based on traffic characteristics. To achieve the QoS as per the requirements, by controlling and managing the traffic characteristics hop by hop basis which is called PHB. In the core network, the QoS parameters that have a great impact on the performance of the network by influencing the traffic are Throughput, Delay, Packet Loss and, Jitter.

3.6.1. Throughput

Throughput is defined as the amount of traffic that is passing through in the particular physical or virtual link measured in a typical unit time between two devices in bits per second (bps). One of the different factors that affect the system's throughput is the dynamic nature of traffic flow across the network. The different network resources become a bottleneck at different times. Some of the factors that affect the throughput and bandwidth are network devices, network topology, and the number of users [11]. Table 1 shows the grade percentage ranging of the throughput from poor to excellent. Equation (1) shows the formula to calculate throughput.

$$Throughput = \frac{\sum sent\ data\ (bit)}{time\ delivery\ (sec)}\ [bps] \quad \ldots . \text{eq (1)}$$

Table 3.1: Quality standards for throughput [11]

Throughput Analysis	
Category	Throughput
Excellent	100%
Good	75%
Medium	50%
Poor	<25%

3.6.2. Packet Loss

Packet loss is the drop of the datagram along its way from source to destination in the network due to different reasons that occurred in the network. One of the reasons is congestion in the network when a node disregards inbound data packets due to overload. A node uses a buffer to temporarily queue the packets and that helps to reduce the loss. The different factors that increase the packet loss are:

- Network hardware problem: Outdated hardware (such as Routers, Switches, and Firewalls) and failure of one of these network elements can be the reason for losing a packet.
- Network congestion: When the number of the packet sent to the network exceeds the threshold value (some predefined limit) or the total capacity of the network because the bursty nature of the traffic can be the cause to lose a packet.
- Over utilized links (devices): these links (devices) may transmit packets to their destination by making the network extremely sluggish or inefficient. This also happens when there is a link that is a bottleneck. In table 2, it shows the standards that are predefined by the ITUT.

Table 3.2: Quality standard for packet loss [11]

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

Packet loss can be calculated by using the formula shown in Equation (2).

$$Packet\ loss = \frac{Packet\ sent - Packet\ received}{Packet\ sent} * 100\% \quad \ldots . \text{eq (2)}$$

3.6.3. Delay

One of the QoS metrics, defined in RFC 7679, measures the time taken by the datagram to travel between two network nodes and is commonly referred to as delay or latency. Delay in ISPs is defined as the difference between the time at which the packet enters the network and the time it leaves the network. In this process every element in which the traffic passes through increases the delay. Delay can be calculated using the formula shown in Equation (3).

$$Delay = \frac{Packet\ length\ (bit\ )}{Link\ BW\ (\text{bps})}\ [sec] \quad \ldots . \text{eq (3)}$$

Table 3.3 shows the standards of end-to-end delay that are predefined by ITUT.

Table 3.3: Quality standard for delay

Delay Standard	
Category	Delay (ms)
Good	0-150
Medium	150-400
Poor	>400

3.6.4. Jitter

Jitter is the variation of delay when the packet traverses through the network. It measures the delay variation between two consecutive datagrams which belong to the same traffic stream. To mitigate the jitter problem a buffer space is available in the network node and datagrams are queued. But lengthy queue also creates an additional processing delay. The formula to calculate the jitter is shown below in Equation (4).

$$Jitter = \frac{\sum Varistion\ delay}{\sum Packet\ received}\ [sec] \quad \ldots\ldots \text{eq (4)}$$

3.7. Benefits of Implementing QoS with MPLS TE

- Improved Network Performance

Traffic marking allows to fine-tune the attributes for traffic on the network. This increased granularity helps single out traffic that requires special handling and, thus, helps to achieve optimal performance. Traffic marking determines how traffic will be treated [12]. Based on the predefined attributes based on QoS for the network traffic set and segment network traffic into multiple priority levels or classes of service based on those attributes. Traffic marking is often used to set the IP precedence or IP DSCP values for traffic entering a network.

Table 3.4: DSCP values and AF classes

Class Name	Binary	Class Selector	Drop Probability
Default	000 000	0	BE
AF11	001 010	1	Low
AF12	001 100		Medium
AF13	001 110		High
AF21	010 010	2	Low
AF22	010 100		Medium
AF23	010 110		High
AF31	011 010	3	Low
AF32	011 100		Medium
AF33	011 110		High
AF41	100 010	4	Low
AF42	100 100		Medium
AF43	100 110		High
EF	101 110	5	Critical

As shown in Table 3.4, there are four DSCP classes called Assured Forwarding Classes (AF), default class, and EF class to put more prioritization on the IP packet as low, medium, or high drop probabilities.

Networking devices within the network can then use the newly marked IP precedence values to determine how traffic should be treated. For example, voice traffic can be marked with particular IP precedence or DSCP value, and a queueing mechanism can be configured to put all packets of that mark into a priority queue. Traffic marking can be used to identify traffic for any class-based QoS feature, for any feature that is available in the policy-map class configuration mode, and although some restrictions exist. It also allows assigning traffic to a specific QoS group within a device.

- Well organized backbone network

From the service provider perspective, implementing MPLS TE + QoS makes them beneficiary because providers already managed the core (backbone) network by fairly prioritizing and distributing the traffic type to all the available network resources. So it will be easy for the rerouting of the new requested traffic in the case of new service requirements.

The device can use the QoS groups to determine how to prioritize traffic for transmission. The assigned QoS value is usually used for one of the two of the following reasons as the first one is, to leverage a large range of traffic classes and the second is if changing the IPP or DSCP value is undesirable. Weighted Random Early Detection (WRED) uses precedence values or DSCP values to determine the probability that the traffic will be dropped. Therefore, the Precedence and DSCP can be used in conjunction with WRED.

3.8. Service Level Agreement (SLA)

A service-level agreement defines the level of service that is expected by the customer from the service provider by defining and putting threshold value for the metrics in which the service is measured and penalties should be there if the service levels could not be achieved. SLA is an agreement between providers and customers or within the company with different departments. SLA should include a description of services to be provided with customers expected levels, metrics by which the services are measured, duties and responsibilities of each party, penalties for breach, and a protocol for adding and removing metrics. In [7] the authors want to define SLA as the service quality experienced by the user in which the traffic experienced by traversing through the network and expressed in terms of latency, jitter, bandwidth guarantees, packet loss, resilience in the face of failure, and downtime.

4. Simulation Setup, Result, and Analysis

This chapter includes a brief introduction of simulation tools that are used for the analysis part. In addition, the Simulation setups with different scenarios are defined and elaborated, and finally, the analysis of QoS parameters will take place.

4.1. Overview of Simulation Tools

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

GNS-3 is an open-source platform (software) that allows users to run different network topologies by using different operating systems including Windows, Linux, and Mac operating systems. It consists of different network devices, such as routers, switches, firewalls, etc., and different types of cables such as fast Ethernet, gigabit Ethernet, and others to connect different devices by mimicking or emulating the hardware devices.

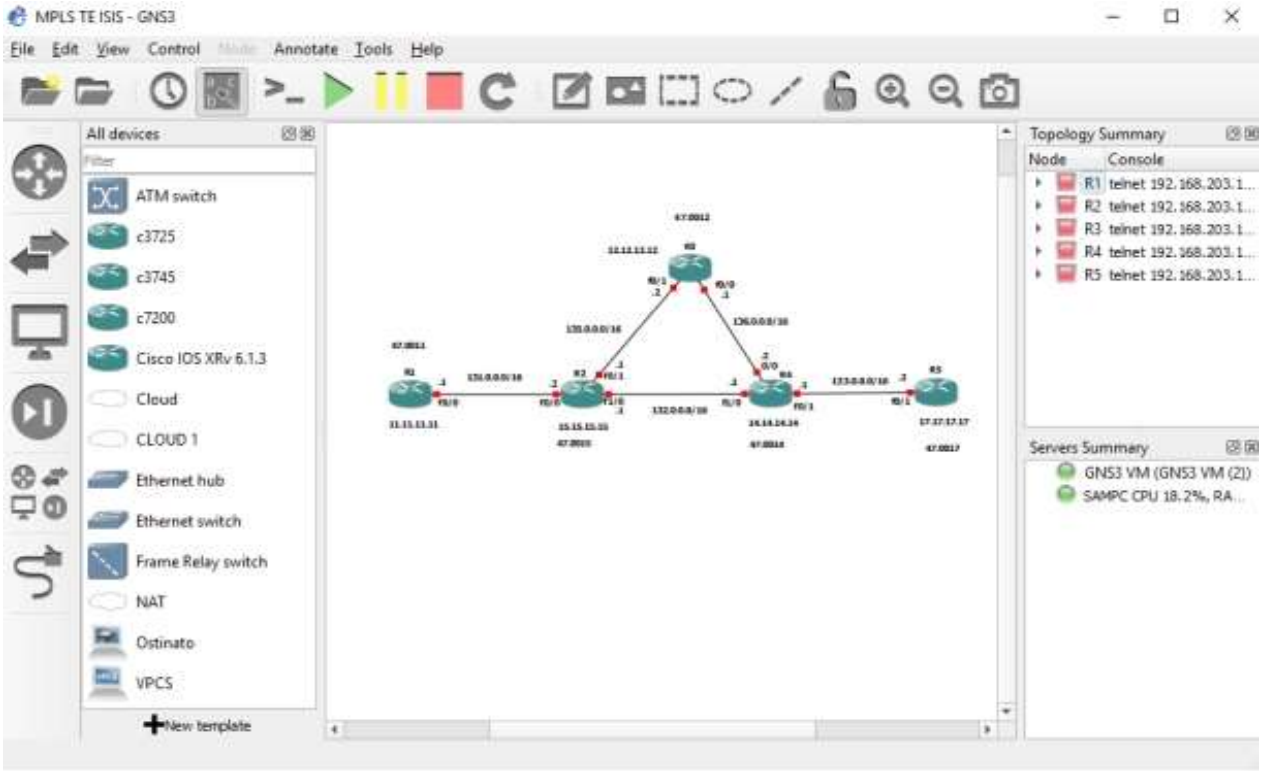

Figure 4.1: GNS3 Guide User Interface (GUI)

It is actively developed and giving support to the growing community. GNS3 is used to emulate, configure, test, and troubleshoot different networks by creating a more user-friendly graphical environment as shown in Figure 4.1.

Linking GNS3 to the pre-configured Virtual Machine (VM) can enable different features but, one can use GNS3 without VM. Even though this is a good way, this setup is limited and doesn't provide many choices. Vendors recommend to integrate GNS3 in a VM to enable the different images (devices) and features. GNS3 also allows the integration of different supportive tools in order to get well-manipulated outputs.

4.1.2. PRTG

PRTG stands for Paessler Router Traffic Grapher, and it is a unified network and monitoring tool of any objects having an IP address. It consists PRTG-Core server for data collection, management, and configuration. PRTG uses one or more probes that are used for data collection and monitoring purposes through sensors. By using different sensors of PRTG can monitor core network devices such as routers, switches, firewalls, etc.

By using standard protocols such as Simple Network Management Protocol (SNMP), Internet Message Access Protocol (IMAP), Simple Mail Transfer Protocol (SMTP), and so on to monitor the BW usage within the network, link availability, link downtime, etc. Beyond the monitoring capability, PRTG can track and charts the collected data as well as generates different types of network alarms. As shown in Figure 4.2, besides capturing the monitoring result for each added link, it can show the network down and uptime, the traffic in, the traffic out, and the total traffic that the link is carrying.

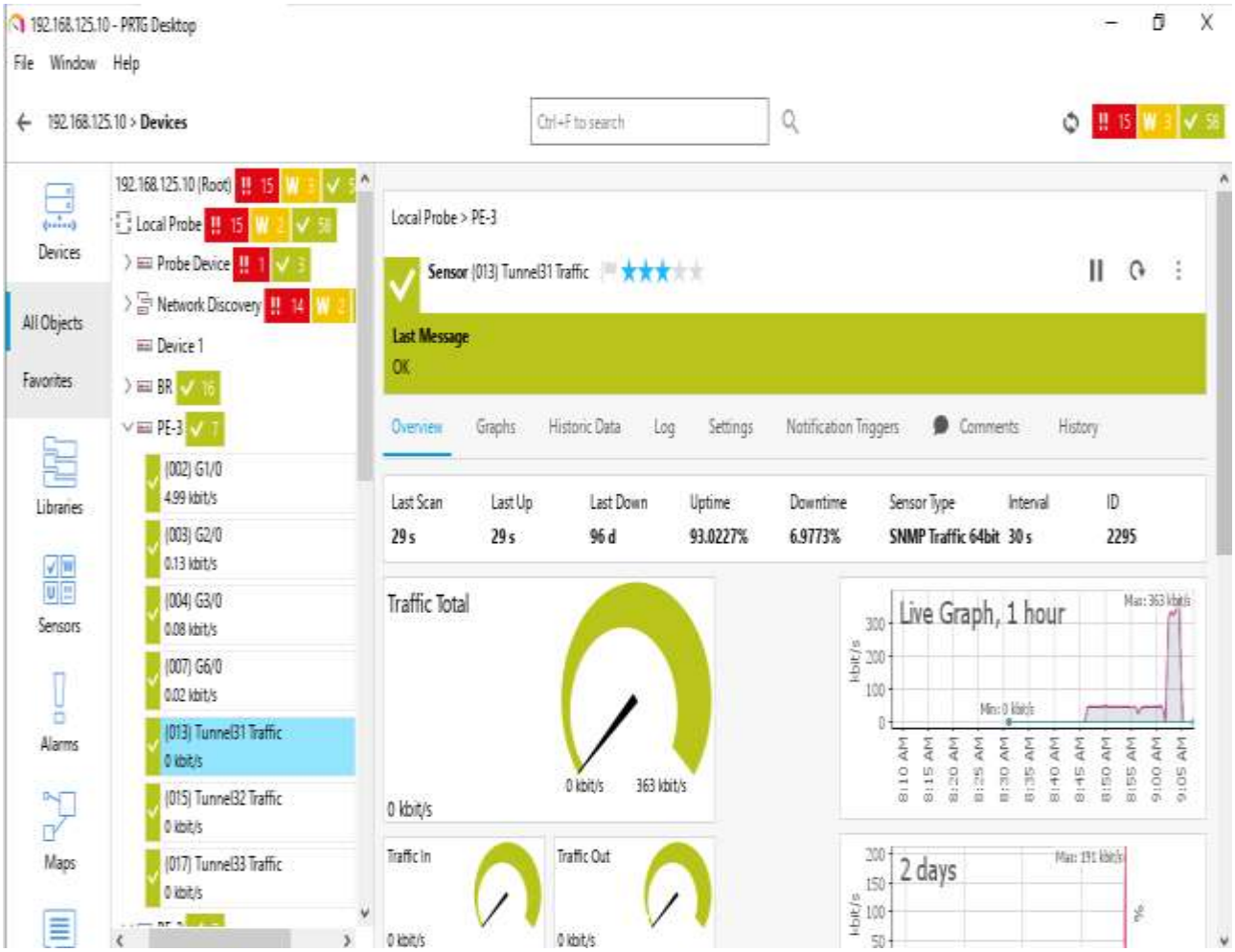

Figure 4.2 Sample PRTG GUI

4.1.3. Ostinato

Ostinato is an open-source network traffic generator platform with having an option of packet manipulation option with a very simple GUI for the manipulation of different operations [13]. It gives an option to generate traffic streams with different types of protocols at different data rates. Standard protocols that are supported by ostinato are IPV4, IPV6, IP Tunneling, and others; TCP, UDP, ICMP (v4 andv6), IGMP, and any text-based protocols such as, HTTP, SIP, NNTP, etc. It also has an option to integrate with

other platforms. In this test scenario, Ostinato is used to generate the required amount of traffic by using the traffic generator GUI as shown in Figure 4.3.

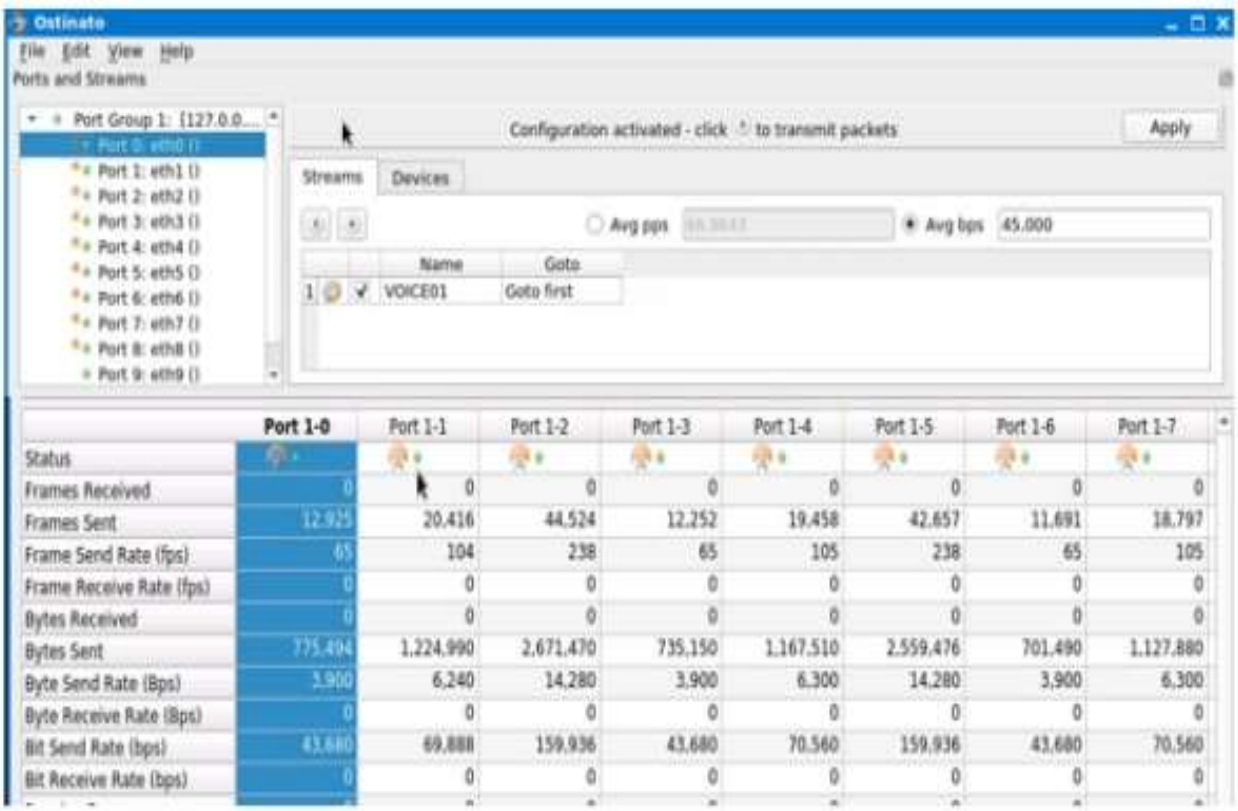

Figure 4.3: Ostinato GUI

4.2. Simulation Scenario and Network Topology

In the implementation part, the practical environment network topology is developed using the Guide Network Simulator-3 platform (GNS-3). The simulation is performed in two scenarios. To compare and contrast the performance of the network in terms of QoS parameters such as packet loss, delay, and throughput, with the BW utilization of the selected links for the two scenarios. The first scenario is MPLS-LDP + BE (scenario 1, which is the existing one), and the second is after the implementation of the MPLS-TE + QoS (scenario 2) scenario which is the proposed one. In order to compare the two results,

the same network topology is developed and implemented. In both cases, Ostinato and PRTG are used. PRTG is connected at the destination which is at the end node of the core network to monitor the connected links. Ostinato is used to simulate the traffic that is forwarded from different customers by generating the required amount of network traffic and feed it to the network. To create congestion by generating an excessive amount of packets and feed them to the network. Figure 4.4 and 4.5 shows the general architecture and simulation scenario topology. In both cases, three network domains (layers) are used such as, the access layer, the aggregation layer, and the core layer or domain is implemented which resembles the real network. Due to the memory limitation of the personal computer and the process intensiveness of the simulation tools, links are normalized. The traffic volume that is collected from the monitoring tool (from the real network) is used to simulate the percentage link utilization of the network.

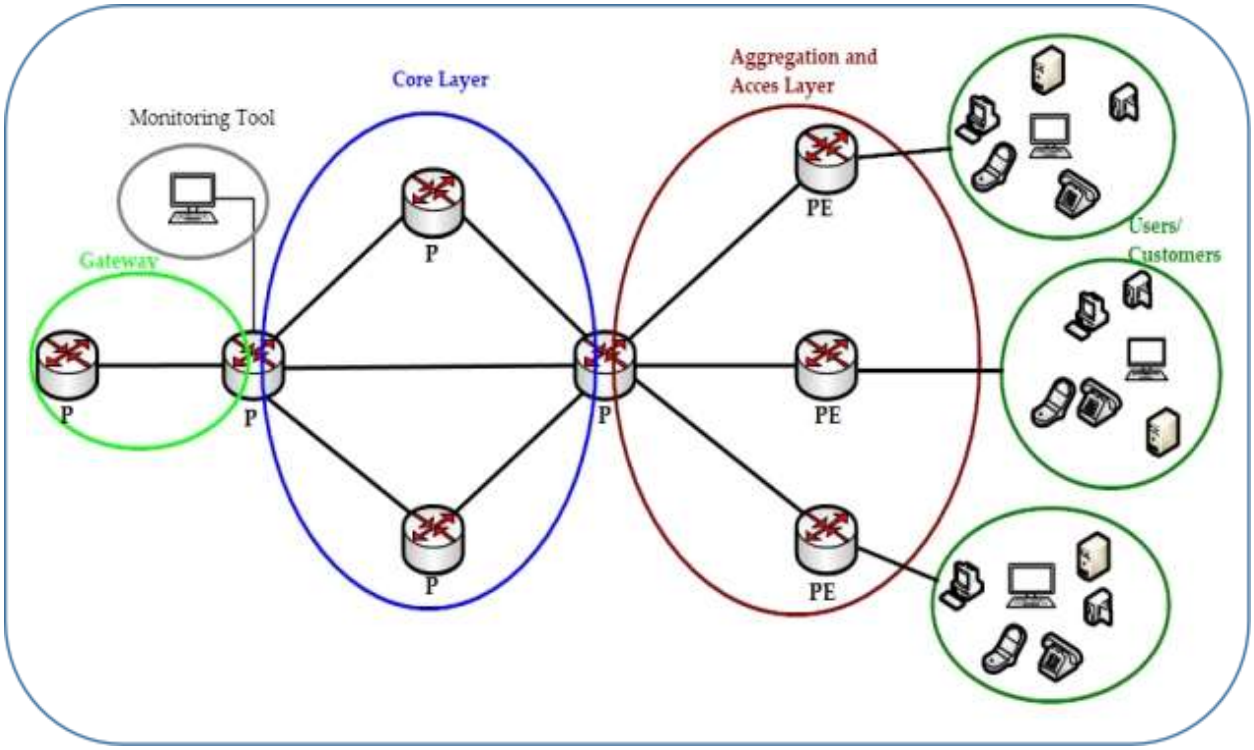

Figure 4.4: General network topology

Categorization of service traffics is done by using VRF such as VOICE (for voice traffic), DATA (for different local traffics, for instance, bank and insurance traffic), and BB (for internet traffic).

Besides the basic connectivity of IP configuration, MPLS, IGP which is IS-IS, DSCP to prioritize the categorized traffics, MPLS DS-aware TE, and different explicit paths are configured. MP-BGP is also configured to enables the BGP to carry the routing information for the user traffic.

From the data that is collected from the monitoring tool (from the real network), the VRFs traffic utilization is ordered in the ascending order as VOICE, DATA, and BB. Interfaces in the network should be monitored carefully not to be utilized in their full capacity, hence there has to be a defined threshold value, such as not to utilize more than 80% of the total link capacity.

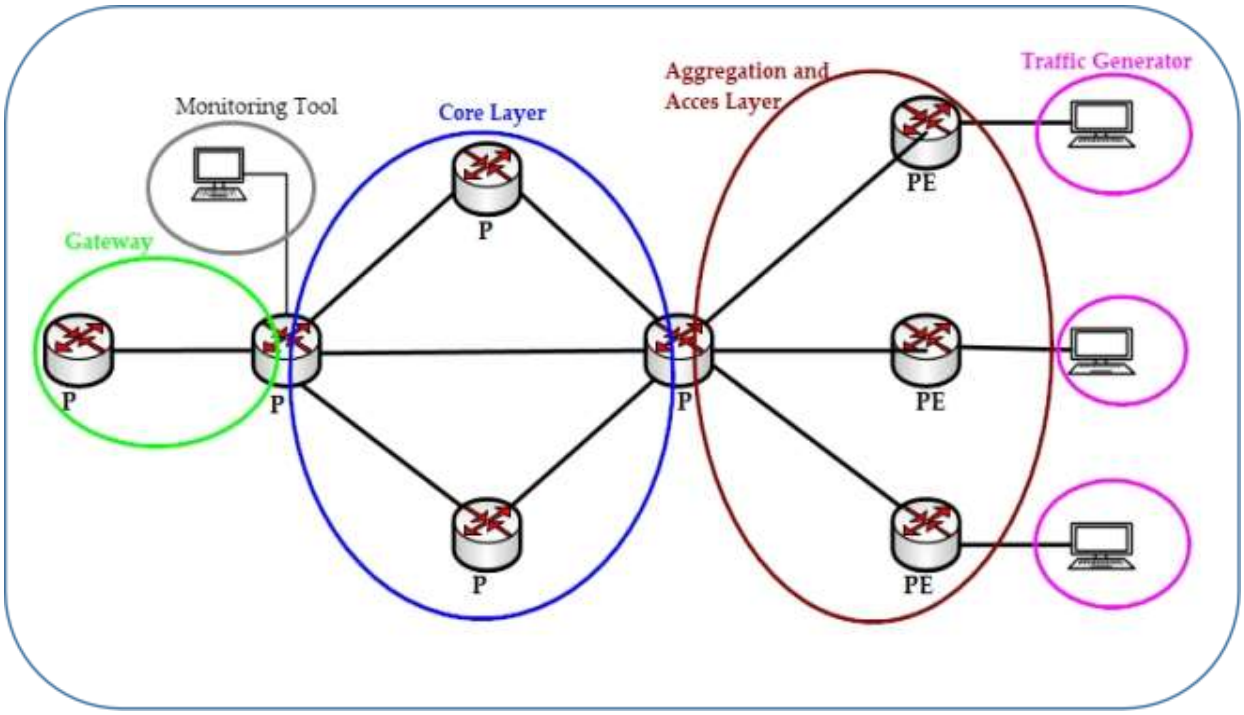

Figure 4.5: Simulation network architecture

Finally, the test results are collected from the simulator using PRTG technology which is integrated into the GNS-3 emulator platform, and from the ICMP echo request using CLI for both scenarios. In order to collect the results, the traffic generation takes place in three steps of data size. The first one is a data size lower than the threshold value, such as 65% of the BW and the second is a data size near to the threshold value which is 75% and the last is beyond 80% of the link BW. These three steps of data size generation are used for both scenarios and, the results are collected while generating each predefined data size.

4.3. Simulation Parameters Analysis

4.3.1. Packet Loss Analysis

As mentioned in section 3.6.2, there are different factors and reasons for the increment of packet loss. The major one is network congestion. Network congestion happened when the traffic that comes from the access devices or customers becomes greater than the link capacity. Physical errors such as inappropriate plugging of link interfaces, loose connections, etc. can be the reasons. For the packet loss analysis, congestion of the network is selected as a factor. By generating the excess amount of traffic and feed to the network using a network traffic generator. ICMP test type is used for the test purpose of the probes in three conditions i.e. data rate at 65%, 75%, and beyond 80% of the link BW. ITUT defines a standard recommendation for packet loss should not be greater than 3%. As shown in Figure 4.6 and tabulated from Table 4.1, there is no packet loss when the generated traffic was lower than the link BW.

Table 4.1: Output of Packet loss for scenario 1 & 2

Packet Sent (KByte)	0.1	0.5	1	2	3	4	5	6	7	8	9	10	10.5
Packet Loss % 1st Scenario	0.0	0.0	0.0	0.4	3.0	5.4	8.2	10.8	13.4	14.4	18.4	20.2	24.0
Packe Loss % 2nd Scenario	0.0	0.0	0.0	0.0	0.0	1.6	4.4	7.2	9.4	11.6	14.6	17.2	18.8

Hence the links are not congested for the first two data sizes. But the loss of packet in scenario 1 (MPLS LDP + BE) starts before scenario 2 (MPLS TE + QoS) when the traffic becomes near and beyond the threshold value, and the packet loss increases quickly as the network links become congested.

The performance of MPLS TE + QoS is much better than the MPLS LDP + BE scenario. For instance, with a data size of 10.5Kbytes, there is 6% less packet loss in MPLS TE + QoS scenario. Since MPLS advertises labels to select LSP, which establishes a large number of LSPs that may burden LSRs for the selecting of the best (shortest) path. In order to reduce this burden TE with an explicit path is configured to select the required LSP. On the other way, MPLS TE + QoS minimizes the effect of congestion and unavailability by rerouting the traffic in different LSPs in the case of link failure.

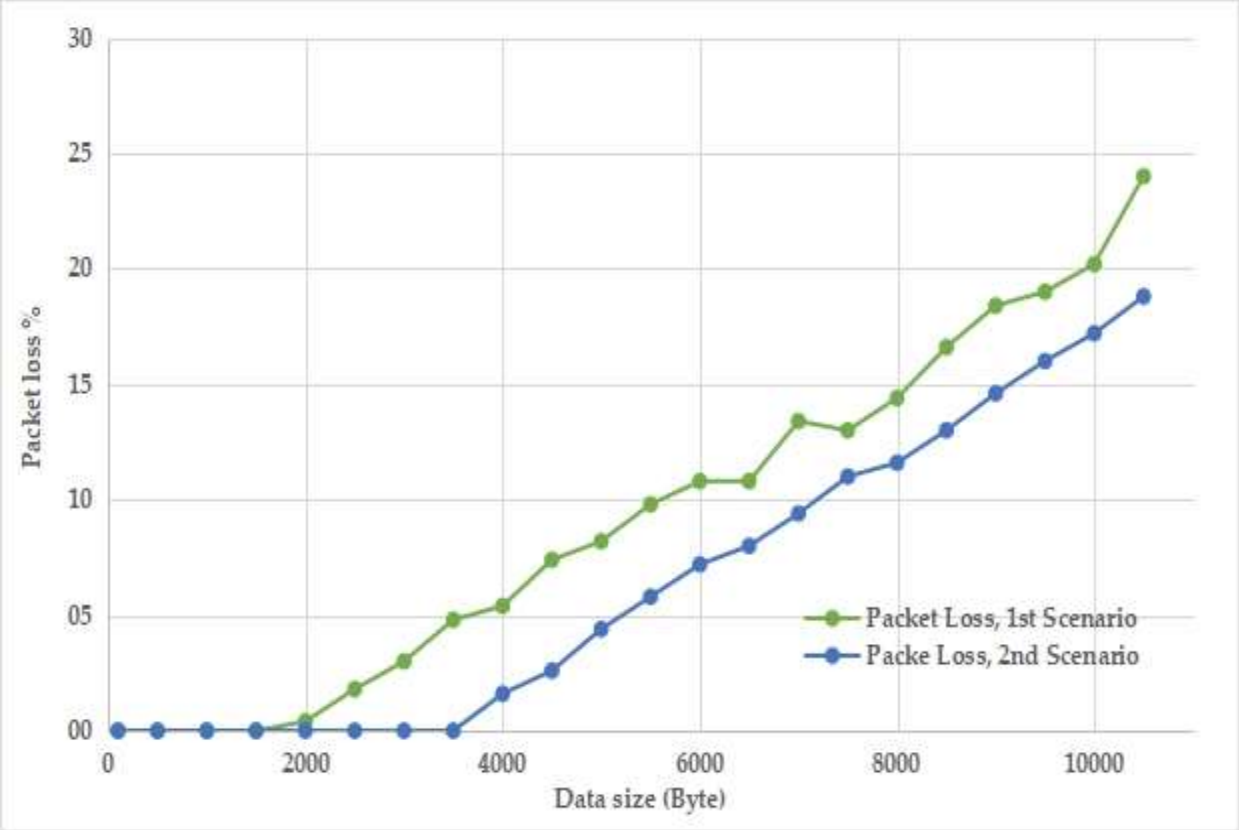

Figure 4.6: Graph of packet loss for scenarios 1 and 2

4.3.2. Throughput Analysis

Throughput is one of the important metrics of QoS in which is used to analyze the traffic passing through the link by measuring the amount of data rate transmitted successfully within a particular time. To compare the throughput, it is required to know the amount of data transferred and the time it takes to finish the transfer. As mentioned earlier in section 4.2 the data size is generated in three sizes such as 65%, 75%, and beyond 80% of the link BW. During the simulation, the ICMP echo request-response is collected while generating the predefined data sizes. Figure 4.7 shows the graph of the simulation result of throughput versus the data size. As shown in Figure 4.6 and shown in tabulated form in Table 4.2, there is no significant throughput difference between the two scenarios that

means when there is no congestion, which is generating the data size lower than the threshold value. But when the data size is increasing the throughput of MPLS TE + QoS is better than MPLS LDP + BE scenario. For instance, at a data size of 10.5Kbytes, the throughput difference is about 342.7Kbps which is 26% better than MPLS LDP + BE scenario. Hence, in this simulation the traffic uses TCP, hence it retransmits the packet due to packet drop or unacknowledged packets, this also limits the rate of the data transmission which directly affects the throughput.

Table 4.2: Throughput for different data sizes of scenarios 1 and 2

Packet Sent (Byte)	100	500	1000	2000	3000	4000	5000	6000	7000	8000	9000	10000	10500
Avg RTT (ms) for 1st Scenario	42.8	49.2	43.6	51.8	57.2	55.8	56.8	59.2	57	64.2	60.6	63.8	66
Avg RTT (ms) for 2nd Scenario	46.6	44.6	43.4	44.4	47.2	46.8	47.4	48	49	50.4	51.8	51.4	52
Throughput (Kbps) 1st Scenario	18.7	81.3	183.5	308.9	419.6	573.5	704.2	810.8	982.5	996.9	1188.1	1253.9	1272.7
Throughput (Kbps) 2nd Scenario	17.2	89.7	184.3	360.4	508.5	683.8	843.9	1000.0	1142.9	1269.8	1390.0	1556.4	1615.4

In MPLS TE, the packet is forwarded by using the MPLS TE tunnel (LSP). The packet that enters the MPLS domain uses different MPLS labels until it leaves this domain when the packet traverses through every LSR. Before configuring MPLS TE the traffic always selects the shortest path from the source to the destination which is predefined by IGP. Because the IGP uses 1/BW to calculate the traffic route, it always selects the shortest path. But after defining and configuring MPLS TE with an explicit path, the traffic can be

rerouted through the predefined LSP. Besides, tagging the selected DSCP valued for the prioritized traffics to give priority within the domain is also possible.

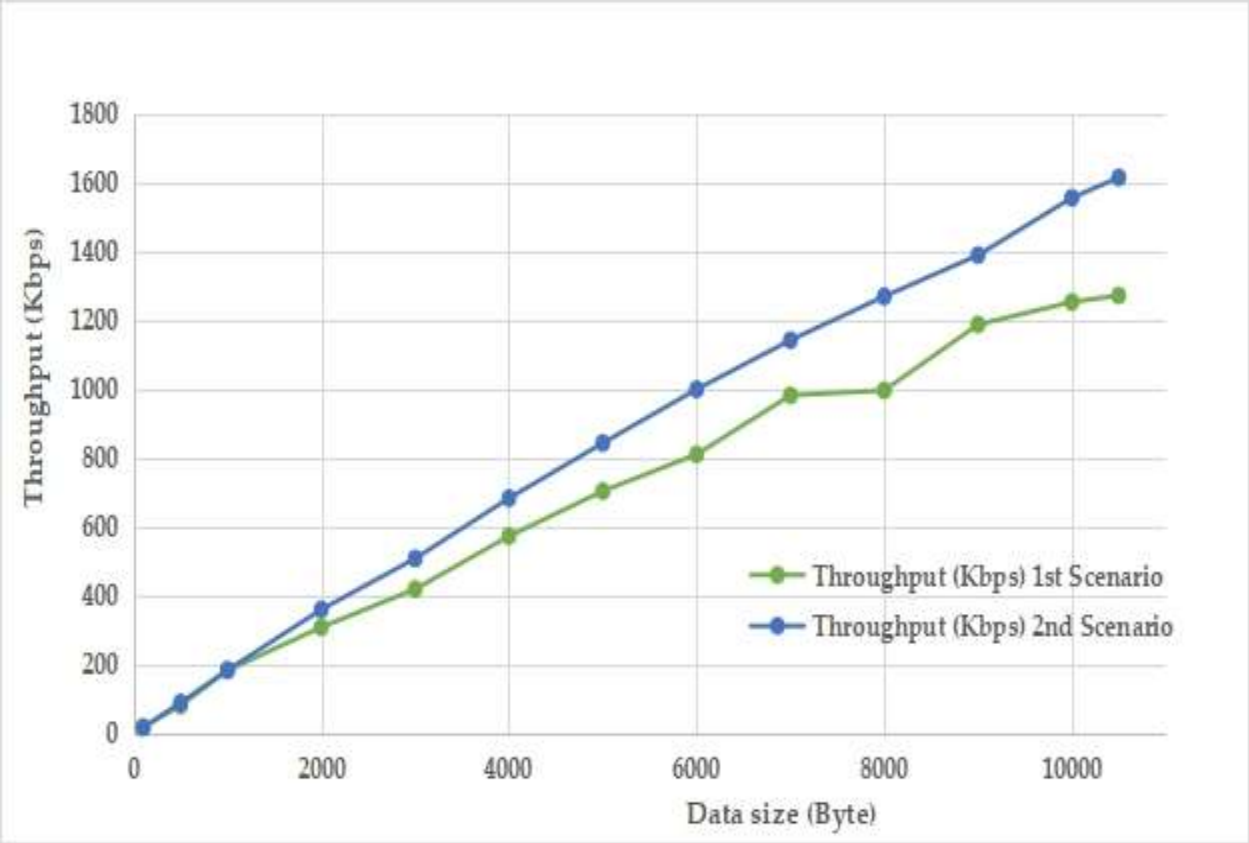

Figure 4.7: Throughput graph for scenarios 1 and 2

4.3.3. Latency Analysis

Latency is one of the QoS parameters to measure the time that the packet takes either in a round trip or one-way trip. In which the packet traverses from the source to the destination and goes back to the source or in a single trip that is from the source to the destination. Delay is the major problem for real-time traffics. ITUT recommends the maximum end-to-end latency should not be greater than 150ms. For the analysis of latency, the same topology setup is used for both scenarios. In the test instance

implemented, using ICMP ping test type is used to send the test probe. To collect the average completion time for each test probe different data sizes are generated and feed to the network as shown in Table 4.3. To increase the accuracy of the latency, an average of 5 test samples was used. For the latency analysis also, predefined data sizes are used.

Table 4.3: Result of latency for scenarios 1 and 2

Packet Sent (Kbyte)	0.1	0.5	1	2	3	4	5	6	7	8	9	10	10.5
Avg Completion Time (ms) 1st Scenario	42.8	49.2	43.6	51.8	57.2	55.8	56.8	59.2	57	64.2	60.6	63.8	66
Avg Completion Time (ms) 2nd Scenario	46.6	44.6	43.4	44.4	47.2	46.8	47.4	48	49	50.4	51.8	51.4	52

As shown in Figure 4.8, the MPLS LDP + BE scenario has higher latency than MPLS TE +QoS scenario. For the same data size in the non-congestion situation, the latency differences are smaller compared with the congestion situation. For instance, at data size 10.5Kbytes, the latency is improved by 14ms that is 21.2% compared with the first scenario.

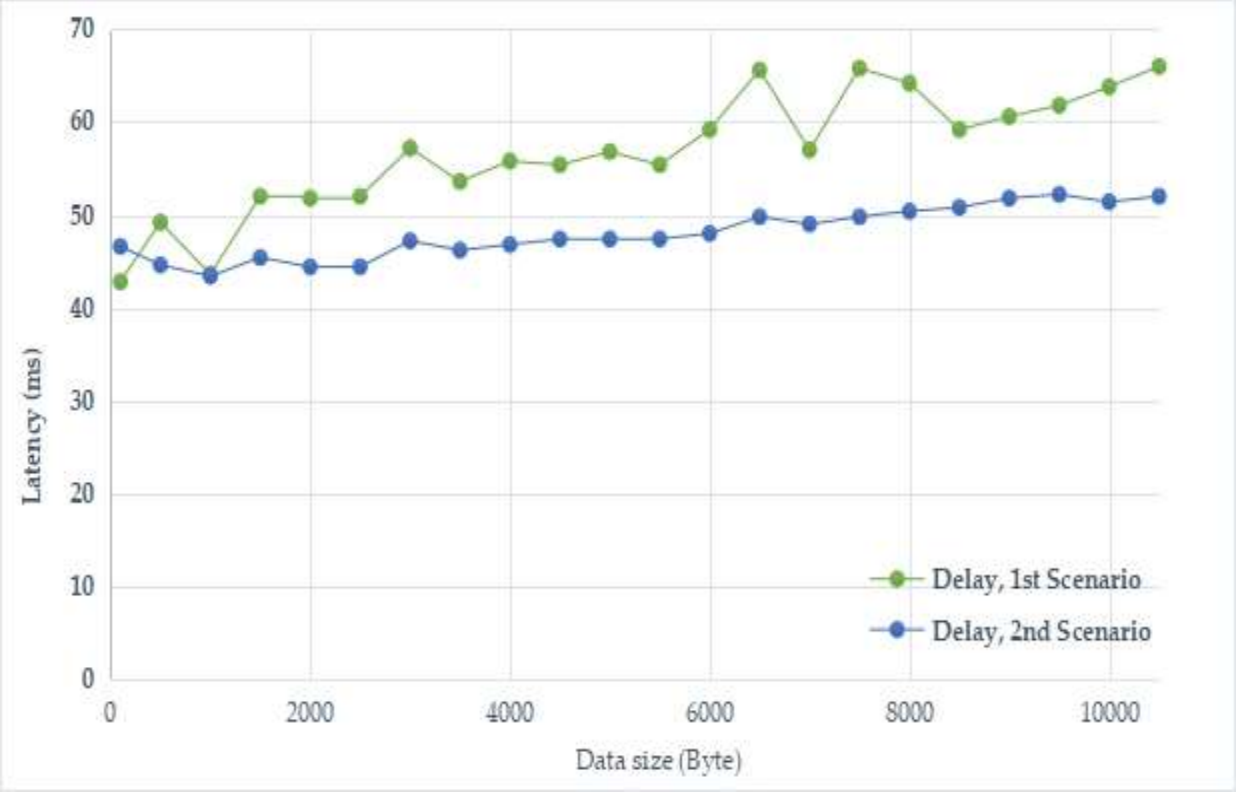

Figure 4.8: Latency graph for scenarios 1 and 2

4.4. Link Utilization and Performance of Network

Network link utilization is defined as the ratio of the current network traffic to the maximum traffic that the port (interface) can handle [15]. That is the indication of the usage of the bandwidth in the network. If the network utilization shows high, it indicates the network is busy otherwise low network utilization indicates the network is idle. If the network utilization as discussed in earlier sections is below the threshold value, then the network is utilizing the links below its capacity. But if the network utilization is very near or exceeds the threshold value this will cause network congestion and consequently, low transmission speed, network intermittency, or delay for any kind of request will happen.

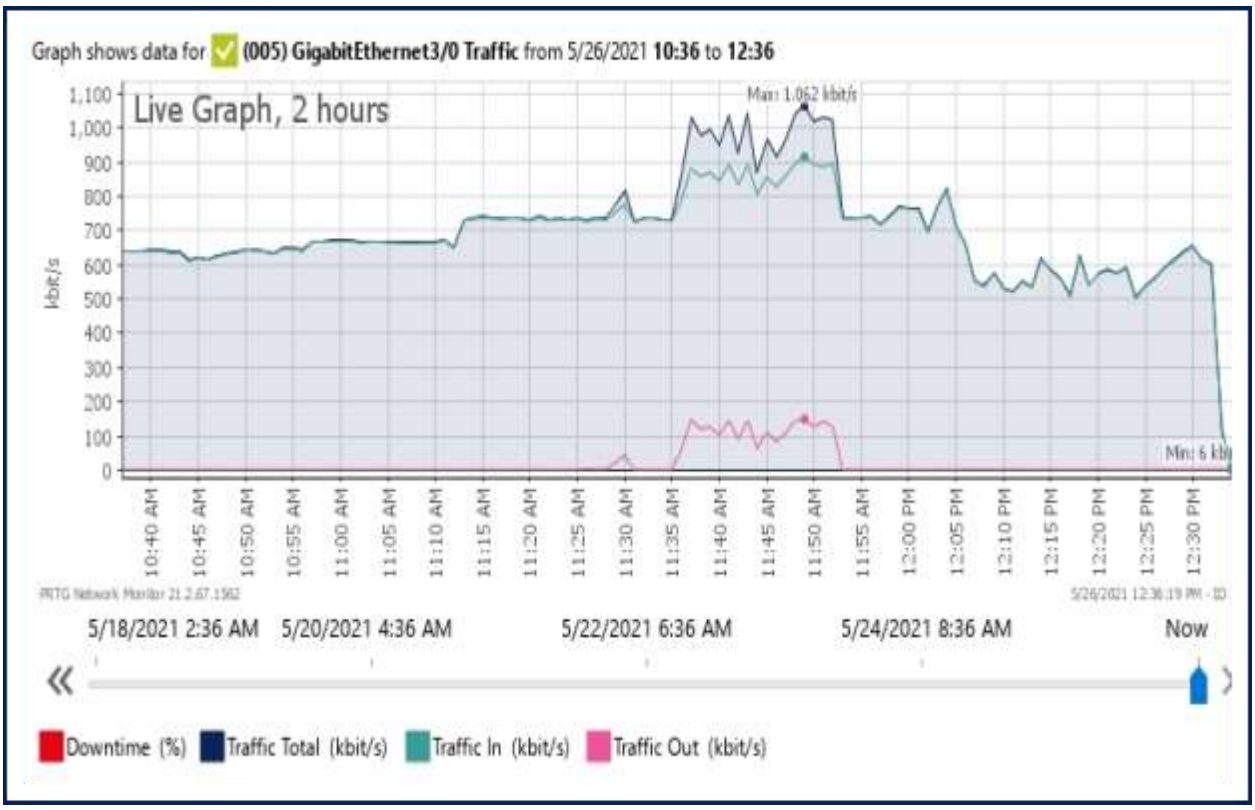

Figure 4.9: Shortest link utilization for scenario 1

As shown the monitoring result which is collected from PRTG network monitoring tool in Figure 4.9 for the shortest path link utilization, and Figure 4.10 (A & B) for non-shortest link utilization of the core network of scenario 1 while generation the traffic in different data size as defined in section 4.2. For the traffic which is generated below the predefined threshold value, near to the threshold value, and beyond the threshold value. Unless there is no traffic management or any implemented traffic controlling mechanism or any deployed traffic pattern rule, the traffic that comes from the source always selects the shortest path due to the IGP rule to reach the destination in scenario 1 i.e. only the shortest links are utilized. For the traffic generating below the threshold value, the network operates in a normal way since the traffic generated is lower than the threshold value.

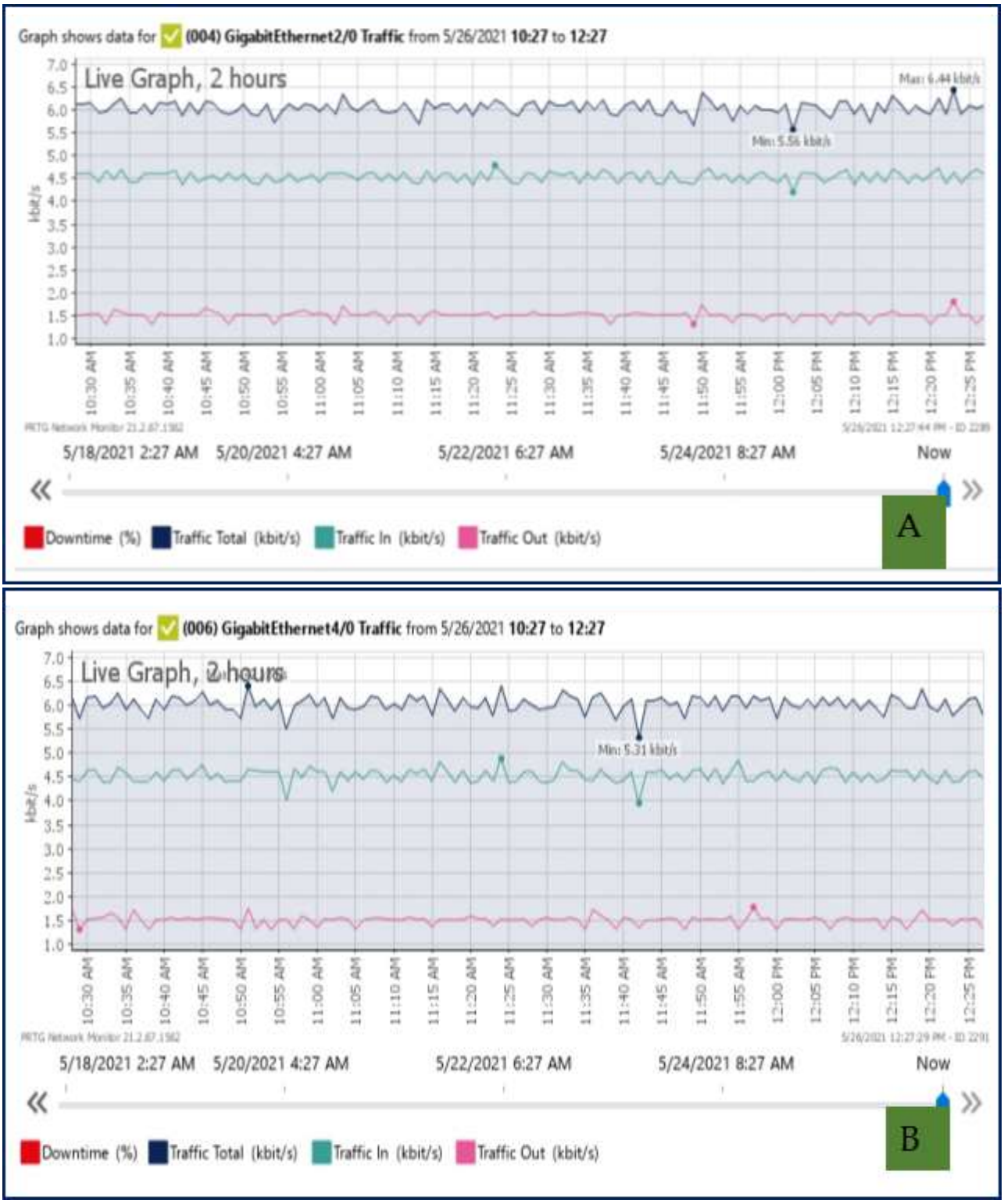

Figure 4.10: A & B Non-shortest link utilization for scenario 1

But after some time when the traffic is increasing, goes near to the threshold value, and exceeds the threshold value, these shortest links will be over-utilized and starts to operate abnormally, also the transmission rate and utilization of the links become degraded immediately. This will over-utilize the shortest path while letting the other non-shortest links underutilized.

After the implementation of MPLS TE + QoS (scenario 2) and collecting the monitoring results while generating the same amount of traffic pattern as scenario 1 in the core network will be discussed next. As the result shows network link utilization of this scenario 2 is fairly distributed to all the available links as shown in the link monitoring result of Figures 4.11 and 4.12 for generating the same traffic pattern as scenario 1.

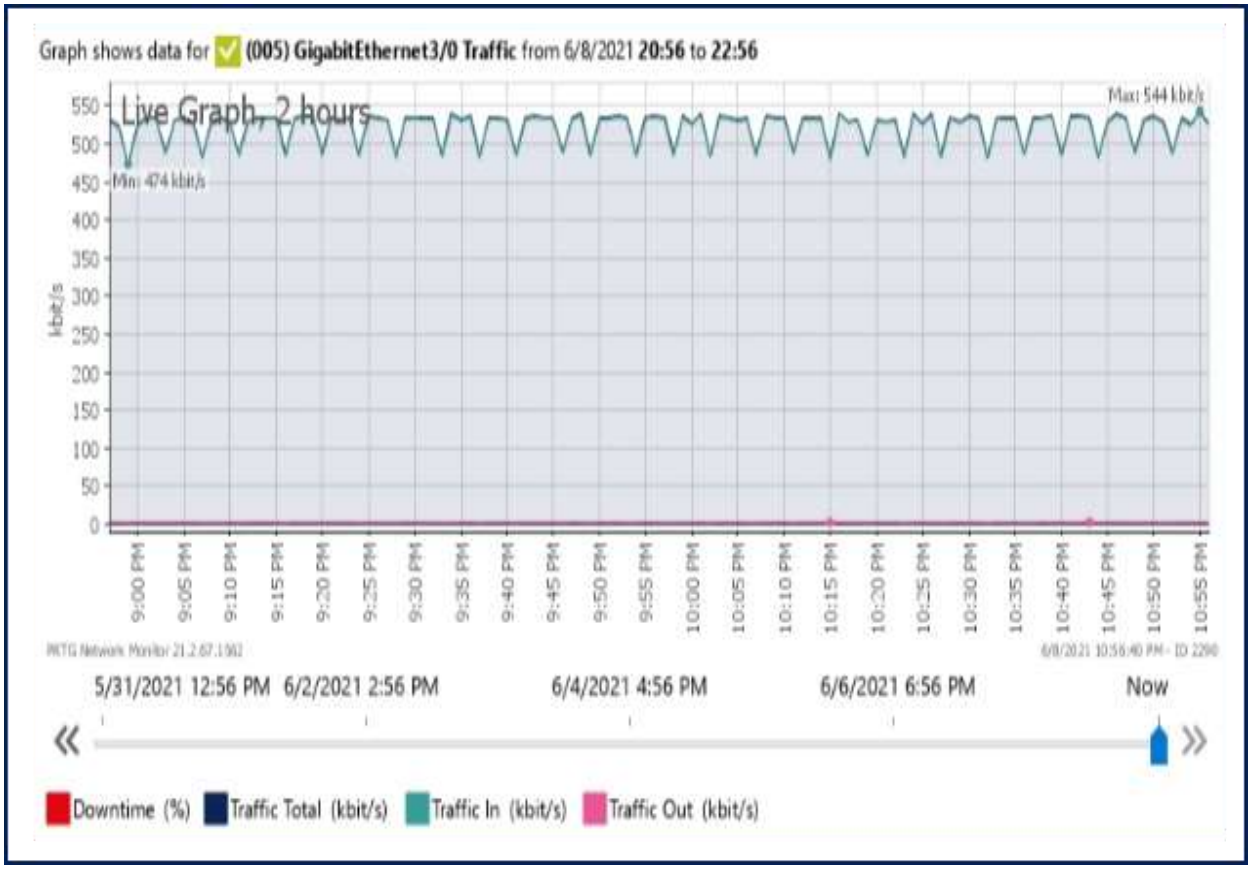

Figure 4.11: Shortest link utilization for scenario 2

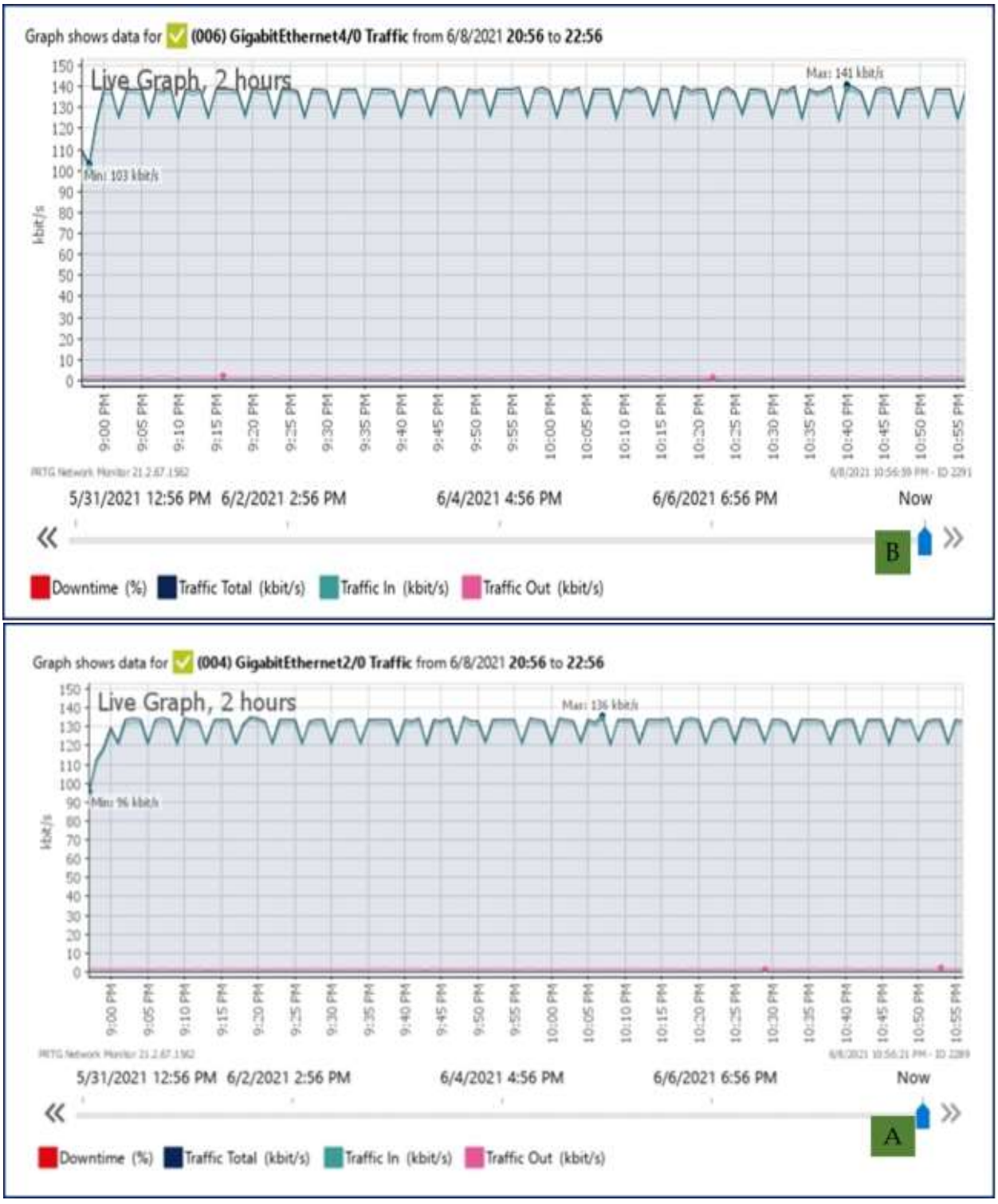

Figure 4.12 A & B: Non-shortest link utilization for scenario 2

Traffic prioritization can be done by collecting the different telecom company services and carefully arranging them by their important order. Then, after careful prioritization, marking those prioritized traffics will take place in layer three or layer two in the TCP/IP protocol stack. Finally configuring those stated and predefined specifications accordingly to the selected routers in the specified network domain.

The traffic that comes from customers is prioritized, classified, and marked according to the predefined requirements. In a PHB process, packet treatment is done in every router that the packet traverses through within the specified domain. And then according to the QoS classification and configuration in each router, the traffic will be treated accordingly.

In TE, hence there are several methods and techniques to deploy traffic engineering within the selected network domain. One of them is by manipulating the IGP metrics for the easiest selection of the traffic route. But in MPLS deployed network by using MPLS-TE can create different LSPs and manipulate them according to the required need for the traffic path. TE can creates static or dynamic LSPs according to the configuration from the source to the destination for the traffic to be routed. In this case, the transit routers (LSRs) can't manipulate the LSPs rather the LSP will be configured at the source (ILER) and the destination (ELER) of the LSP.

In a PHB QoS implementation scenario, as discussed earlier, every QoS specifications are configured in every router in the selected domain. Every router should have expected to process the configured QoS specifications whenever the packet arrives at the router which is an intensive process and may take quite a lot of processing time for the router. Consequently, the processing time will increase. But when using the MPLS-TE scenario only the I/E-LERs are responsible for the process of all the configured QoS specifications. This will play an important role in minimizing the overall processing time.

For the same topology as used earlier and for the same packet generating such as 100,000 packets, by sending rate of 450Kbps will take 180 seconds for the MPLS-TE + QoS deployed network. But for the PHB scenario implemented network for the same topology and packet generation as stated above it takes 240 seconds to transfer the generated packet. This is because in PHB the packet is processed such as checking the packet DSCP value, the source, and the destination addresses, packet size, etc. in every router that the packet traverses through. So this will increase the staying time of the packet at the router. Consequently, this will increase the overall delay of the packet.

5. Conclusion and Future Work

5.1. Conclusion

The analysis of this thesis work is about the optimization of link bandwidth and analyzing the performance of the network before and after the implementation of MPLS TE + QoS in the same network architecture. This work has investigated the drawbacks of the MPLS LDP + BE network scenario. To do the comparison and analysis of the two scenarios, three QoS performance parameters such as throughput, packet loss, and latency are used. Network setup is done using GNS3 with the necessary and required configurations as primarily. Then, network traffic is generated using the Ostinato network traffic generator and finally, the simulation results are collected using PRTG and CLI. This work is to show the effect of network link utilization that is mainly caused by network congestion due to different reasons. The links of devices that are mounted in the network should be monitored and controlled to identify whether the network is idle, normal, or busy. The network traffic should be kept to be lower than the predefined threshold values under different conditions. Otherwise, if the link utilization exceeds the maximum predefined threshold value, network elements will operate abnormally and the quality of different services will be affected as well as management of the network elements also becomes difficult.

From the simulation results the following conclusions are drawn:

- By implementing MPLS TE + QoS can improve the network performance by using enabler technologies such as DiffServ aware TE, QoS MP-BGP, etc.
- Compared to MPLS LDP + BE scenario, MPLS TE + QoS scenario improves the throughput by 26% within the mentioned data size in the simulation.

- And for the same congestion level MPLS TE + QoS scenario reduces the packet loss by 6% and improves the latency by 21%.
- The implementation of MPLS TE + QoS in the core network does not guarantee the end-to-end QoS.
- Service providers including Ethio Telecom should implement MPLS TE + QoS in their backbone network to manage the traffic easily and to secure SLA traffics to enhance QoS hence improving QoE.

5.2. Future Work

In the future work and recommendation part, this paper is done only by using manual manipulation of different network QoS parameters. It is recommended to

- Implement and analyze MPLS TE + QoS in the SDN implemented environment in collaboration with higher-level data manipulation tools such as machine learning tools for traffic pattern prediction
- Implementing MPLS TE + QoS in a seamless MPLS deployed environment to analyze the result.
- Using different congestion avoidance algorithms
- By applying different packet treatment techniques for instance per customer traffic classification for independent treatment.

References

[1]. J. Barakovic, H. Bajric, and A. Husic, "QoS design issues and traffic engineering in next generation IP/MPLS Network," *2007 9th International Conference on Telecommunications*, 2007.

[2]. M. R. Rahimi, H. Hashim, and R. A. Rahman, "Implementation of quality of Service (QoS) in multi-protocol label Switching (MPLS) networks," *2009 5th International Colloquium on Signal Processing & Its Applications*, 2009.

[3]. S. Karamchati, S. Rawat, S. Yarram, and G. P. Ramaguru, "Mapping mechanism to Enhance QoS in IP networks," *2018 International Conference on Information Networking (ICOIN)*, 2018.

[4]. X. Li, X. Lv, L. Liu, and W. Mei, "DiffServ-aware MPLS traffic engineering," *The 3rd International Conference on Information Sciences and Interaction Sciences*, 2010.

[5]. A. Z. Othman, R. A. Rahman, M. M. Md Zan, and M. I. Yusof, "The effect of QOS implementation in MPLS network," *2012 IEEE Symposium on Wireless Technology and Applications (ISWTA)*, 2012.

[6]. Hongyun Man, Linying Xu, Zijian Li, and Lianfang Zhang, "End-to-end QoS implement BY diffserv and MPLS," *Canadian Conference on Electrical and Computer Engineering 2004 (IEEE Cat. No.04CH37513)*.

[7]. D. Zhang and D. Ionescu, "QoS performance analysis in deployment of DiffServ-aware MPLS traffic engineering," *Eighth ACIS International Conference on Software*

Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD 2007), 2007.

[8]. S. Barakovic and J. Barakovic, "Traffic performances improvement using diffserv and MPLS NETWORKS," *2009 XXII International Symposium on Information, Communication and Automation Technologies*, 2009.

[9]. A. Saika, R. E. Kouch, B. Raouyane, M. Bellafkih, and M. M. Himmi, "QoS in The MPLS-DIFFSERV NETWORK," *2012 6th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT)*, 2012.

[10]. N. Roddav, K. Streit, G. D. Rodosek, and A. Pras, "On the usage of dscp and ecn codepoints in internet backbone traffic traces for ipv4 and ipv6," *2019 International Symposium on Networks, Computers and Communications (ISNCC)*, 2019.

[11]. Kumera, H. (2018). Analysing Impact of Seamless MPLS on QoS Analysing Impact of Seamless MPLS on QoS.

[12]. Konstantin Muhhin, "QoS Implementation on Network Devices." (2010).

[13]. B. R. Patil, M. Moharir, P. K. Mohanty, S. G, and S. S, "Ostinato - a powerful traffic generator," *2017 2nd International Conference on Computational Systems and Information Technology for Sustainable Solution (CSITSS)*, 2017.

[14]. Adewale, A. A., Adagunodo, R. E., John, N. S., & Ndujiuba, C. (2016). A Comparative Simulation Study of IP, MPLS, MPLS-TE for Latency and Packet Loss Reduction over a WAN. *International Journal of Networks and Communications*, *6*(1), 1–7.

[15]. Technology, I. (n.d.). "Evaluation Study for Delay and Link Utilization with the New - Additive Increase Multiplicative Decrease Congestion Avoidance and Algorithm." 1–15.

[16]. A. Hassidim, D. Raz, M. Segalov, and A. Shaqed, "Network utilization: The flow view," *2013 Proceedings IEEE INFOCOM*, 2013.

[17]. Various. (2005). What is MPLS? Network, 1–31.

[18]. S. Mehraban, K. B. Vora, and D. Upadhyay, "Deploy multi-protocol label Switching (MPLS) using VIRTUAL routing and FORWARDING (VRF)," *2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI)*, 2018.

[19]. R. Fuller, D. Jansen, M. McPherson, and K. Corbin, *NX-OS and Cisco Nexus SWITCHING: Next-generation data center architectures*. Indianapolis, IN: Cisco Press, 2013.

[20]. "Building a fully connected, intelligent world," huawei, 20-Jul-2021. [Online]. Available: http://www.huawei.com/. [Accessed: 11-Jun-2021].

[21]. "Find and share research," ResearchGate. [Online]. Available: https://www.researchgate.net/. [Accessed: 02-Oct-2021].