



**Deploying End-to-End Quality of Service in  
Telecommunication Networks and Multiple Label  
Switching Virtual Private Networks**

**A Thesis Presented**

**by**

**Bertukan Hussien**

**to**

**The Faculty of Informatics**

**of**

**St. Mary's University**

**In Partial Fulfillment of the Requirements  
for the Degree of Master of Science**

**in**

**Computer Science**

**January 2023**

**Deploying End-to-End Quality of Service in Telecommunication  
Networks and Multiple Label Switching Virtual Private Networks**

**By Bertukan Hussien**

**Accepted by the Faculty of Informatics, St. Mary's University, in  
partial fulfillment of the requirements for the degree of Master of  
Science in Computer Science**

**Thesis Examination Committee:**

Dr. Alemebante Mulu

---

**Internal Examiner**  
**{Full Name, Signature and Date}**

Dr. Eng. Yihenew Wondie



23/02/2023

---

**External Examiner**  
**{Full Name, Signature and Date}**

---

**Dean, Faculty of Informatics**  
**{Full Name, Signature and Date}**

January, 2023

## DECLARATION

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

Bertukan Hussien Yimam  
Full Name of Student

---

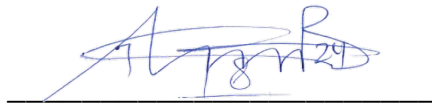
Signature

Addis Ababa

Ethiopia

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

Dr. Asrat Mulatu  
Full Name of Advisor



---

Signature

Addis Ababa

Ethiopia

January, 2023

## **Acknowledgments**

First and foremost, I want to give Allah honor and thanks for guiding me through this challenging but inspiring job and for giving me the inspiration and patience necessary for the successful completion of this thesis.

Every day, I have felt your guidance. I was able to complete my thesis thanks to you.

I would also like to express my heartfelt gratitude and appreciation to my advisor, Dr. Asrat Mulatu, for his guidance, patience, encouragement, and advice that he has provided throughout the project's development, as well as for being an extraordinary mentor. Without his assistance, this project would not be nearly as good.

Finally, I'd like to express my gratitude to my family and friends for their unending support and encouragement.

## Table of Contents

DECLARATION .....	iii
List of Acronyms and Abbreviations .....	viii
List of Figures .....	ix
List of Tables .....	x
Abstract .....	xi
Chapter One: Introduction .....	1
1.1. Background .....	1
1.2. Statement of the Problem .....	4
1.3. Research Questions .....	4
1.4 Objectives of the Study .....	5
1.4.1 General Objective .....	5
1.4.2 Specific Objectives .....	5
5. Methodology and Tools .....	5
1.6 Significance of the study / Contribution .....	7
1.7. Scope and Limitation of the Study .....	7
1.7.1 Scope of the Thesis .....	7
1.8 Organization of the Thesis .....	8
Chapter Two: Review of Literature and Related Works .....	9
2.1 Review of Literature .....	9
2.1.1 Multi-Protocol Level Switching (MPLS) .....	9
2.1.2. MPLS Label Distribution Protocol .....	11
2.1.2.1 MPLS Architecture .....	12
2.1.2.2. Control Plane .....	13
2.1.2.3. Data Plane .....	13
2.1.2.4. MPLS Network Applications .....	14
2.1.3. Virtual private network (VPN) .....	14
2.1.3.1 Basic of VPN technologies .....	15
2.1.4. Multiple Protocol Label Switching-Virtual Private Network .....	17
(MPLS VPN) .....	17
2.1.4.1 MPLS Layer 2 VPNs .....	17
2.1.4.2 MPLS Layer 3 VPN .....	17
2.1.4.3. MPLS VPN Architecture .....	19

2.1.6. Border Gateway Protocol (BGP) .....	20
2.1.6. MP-BGP MPLS VPN .....	21
2.1.7. Quality of Service .....	22
2.1.8. VPN QoS - MPLS QoS Application on MPLS VPNs.....	23
2.1.9. QoS Specifications.....	23
2.1.9.1 Bandwidth.....	23
2.1.9.2. End-to-end delay.....	24
2.1.9.3. Jitter (Delay Variation) .....	24
2.1.9.4. Packet loss.....	25
2.1.10. Recommended IP QoS in Telecommunication network.....	25
2.1.11. Mechanisms of Improving QoS of VPN.....	25
2.1.12. End-to-End QoS Service Models.....	26
2.1.12.1. Best-Effort Model .....	26
2.1.12.2. Integrated Services.....	27
2.1.12.3. Differentiated Services.....	28
2.1.13. DiffServ QoS Implementation over MPLS VPN.....	28
2.1.14. Traffic Classification .....	29
2.1.15. VPN Traffic Marking.....	30
2.1.16. Per-Hop Behavior (PHB).....	31
2.1.17. Traffic Shaping and Policy .....	31
2.1.18. Congestion Management .....	32
2.2 Review of Related Works .....	32
Chapter Three: Simulation Design and Analysis.....	38
3.1 Introduction.....	38
3.3 Simulation Network Topology .....	38
3.3.1 IP addresses.....	39
3.3.2. Configuration an IP address for each interface.....	41
3.3.3. Interior Gateway Protocol (IGP) Interconnection.....	41
3.3.4. MPLS and MP BGP Interconnection.....	42
3.4. Designed QoS of Proposed network architectures.....	43
3.4.1. Define Access Control List rules .....	43
3.4.2. Apply the traffic policies .....	44
Chapter Four: Simulation Result and Analysis.....	45
4.1 Experimental Result and Analysis .....	45

4.1.1. IGP protocol (OSPF).....	45
4.1.2. MPLS LDP Operation.....	46
4.1.3. BGP Protocol Operation .....	46
4.1.4. VPNs QoS Operation.....	47
4.1.5. Performance among L2VPN Service.....	48
4.1.6. Performance among L3VPN Service.....	49
4.2. Representation of Experimental Discussions with Table and Graph.....	50
Chapter Five: Conclusions and Future Works .....	55
4.1. Conclusions.....	55
5.2. Future Works .....	56
References.....	57
Appendix.....	62

## **List of Acronyms and Abbreviations**

ACL	Access control list
AS	Autonomous Systems
CE	Customer Edge
BA	Behavior aggregates
L2VPN	Layer 2 Virtual Private Network
L3VPN	Layer 3 Virtual Private Network
LLQ	Low Latency Queuing
NGN	Next Generation Network
MPLS	Multiprotocol Label Switching
OSPF	Open Shortest Path First
P	Provider
PC	Personal Computer
PE	Provider Edge
P2P	Point to Point
PHB	Per-hop behavior
QOS	Quality of service
RD	Route Distinguisher
RT	Route Targets
RR	Route reflector
RSVP	Resource reservation protocol
SLA	Service Level Agreement
TCP	transport control protocol
ToS	Type of Service
VPN	Virtual Private Network
VRF	Virtual Routing Forwarding
VoIP	Voice over Internet Protocol
WAN	Wide Area Network
WFQ	Weighted Fair Queuing



## List of Figures

Figure 1.1: proposed flowchart for the VPN QoS Research Method .....	6
Figure 2.1: Multi-Protocol Label Switching based network [12] .....	11
Figure 2.2: MPLS label distribution Protocol [20] .....	12
Figure 2.3: MPLS Architecture [12] .....	13
Figure 2.4: MPLS Layer 3 VPN Component Terminology [57] .....	18
Figure 2.5: BGP MPLS VPN components and working principles [34] .....	22
Figure 2.6: Traffic classification [52]. .....	29
Figure 3.1: Simplified Proposed BGP MPLS VPN network architecture with end-to-end QoS. .....	39
Figure 4.4: This shows the Access-list operation. ....	47
Figure 4.5 :This shows the Class map operation .....	47
Figure 4.6: Shows How differentiated service code point (DSCP) operation. ....	47
Figure 4.7: Defined QoS. ....	48
Figure 4.8: Shows L2VPN service operation. ....	48
Figure 4.9: Defined QoS. ....	49
Figure 4.10: Shows L3VPN service operation. ....	49
Figure 4.11: Defined QoS. ....	50
Figure 4.13: L3VPN Measurement Comparison. ....	52

## **List of Tables**

Table 2.1: Telecom recommended QoS targets [38]. .....	25
Table 2.1 Summary and Gap Analysis from Related Works.....	35
Table 3.1 - IP addressing scheme of the designed network architectures .....	40
Table 4.1 The similarities and differences between existing and proposed network architecture. .....	50
Table 4.2 Exist and proposed network architecture numerical QoS results for LVPN service.	54

## **Abstract**

To deliver adequate services to users, the major goals of Quality of Service (QoS) include bandwidth management, regulated jitter, latency, and better packet loss characteristics. The service provider must shape network optimization. Among the best practices for implementing network QoS is improving the current network's physical and logical designs.

This work attempted to investigate the end-to-end QoS parameters of MPLS VPN services (Layer 2 VPN and Layer 3 VPN services) networks using the differentiated service (DiffServ) paradigm to manage end-to-end traffic delay, jitter, and packet loss. The traffic is categorized and labeled based on its priority. The suggested network design utilizes weighted fair queuing for congestion management and weighted random early detection for congestion avoidance. The network configurations were designed, demonstrated, and analyzed using GNS3 and Wireshark. When the existing works are compared with the proposed network design constructed utilizing the DiffServ model it is found an improved L2VPN latency results of 7% and the L3VPN delay is reduced by 9.1%. Furthermore, packet loss and jitter are reduced by 18.71% and 4%, respectively.

**Keywords:** - *Quality of Service, Virtual Private Network, Multiprotocol Label Switching, Multiprotocol Border Gateway Protocol, Label Distribution Protocol, Differentiated Service Model.*

# Chapter One

## Introduction

### 1.1. Background

As new services increase the demands on IP networks' service capabilities, QoS becomes more important in the network. Every day, new telecommunications technologies are being developed. Businesses use these new technologies to improve network services while cutting expenses. The need for timely delivery of real-time applications like telephony, video conferencing, or guaranteed bandwidth for mission-critical applications has led to a high demand for end-to-end quality of service (QoS) guarantees such as delay, Jitter, and packet loss [1] [2]. QoS requirements put new challenges to service providers. QoS does not create capacity, but only supports the priorities of traffic and allocation of resources under the terms of congestion [1]. New alternatives to private wide area networks include virtual private networks (VPN) and multiprotocol label switching (MPLS) (WAN). Enterprise clients are turning to service providers who offer MPLS VPNs because they are effective. The key reason for this move is MPLS VPN's ability to provide built-in security measures and end-to-end connection. The most crucial factor is service quality [3].

MPLS is a technique used by service providers to provide better and single network infrastructure for real-time traffic such as voice and video. The main advantage of utilizing MPLS is to create Virtual Private Networks. MPLS can develop both Layer 2 and Layer 3 MPLS VPNs

MPLS is a high-performance packet forwarding technology that combines the scalability, flexibility, and performance of the network layer with the performance and traffic management capabilities of the data link layer (layer 2). (Layer 3) routing to avoid complex lookups in a routing table, MPLS directs data from one network node to the next using short path labels rather than long network addresses. Instead of endpoints, the labels identify virtual links (paths) between distant nodes. MPLS is capable of encapsulating packets from various network protocols [5].

Multiprotocol Label Switching (MPLS) is the primary technology used in Service Provider Networks because it allows packets to be sent fast. MPLS is a novel technique to improve the speed, capability, and service provisioning capabilities of transmission resources. This technology is used by service provider networks to connect several remote sites.

MPLS technology delivers decreased network latency, an effective forwarding mechanism, and ascendable and predictable service performance, making it more suitable for carrying out real-time applications such as voice and video. MPLS may transmit any form of data, whether it is layer 2 data (frame relay, Ethernet, ATM data, etc.) or layer 3 data (IPV4, IPV6) [5].

MPLS VPN is a form of VPN infrastructure that uses multiprotocol label-switching techniques to deliver services. It is a set of MPLS-based VPN technologies that enable the creation and management of different protocols and technologies in a VPN environment [6]. A virtual private network (VPN) is a network that provides user connectivity to many sites via a shared infrastructure while adhering to the same administrative regulations as a private network.

The Policy can also determine (wholly or partially) the path between two systems in a VPN, as well as the features of that path. It is also a question of policy whether a system in one VPN is authorized to communicate with systems in another VPN [7].

In MPLS VPN, a VPN normally consists of a collection of sites that are interconnected by way of an MPLS provider core network, but it is also possible to apply different policies to different systems that are located at the same site. Policies can also be implemented in dial-in systems; the policies chosen would be based on the dial-in authentication processes [7].

A given set of systems may be a member of one or many VPNs. A VPN can be made up of sites (or systems) the same enterprise (intranet) or from other enterprises (extranet); it can be made up of sites (or systems) the same service provider backbone or from various service provider backbones [7].

Many Telecommunication enterprise customers have signed up for MPL VPN services. These enterprise customers have an end-to-end QoS service level agreement (SLA) with the company. The company is also working on it by establishing SLA goals. However, there is a discrepancy between the company's SLA targets and what SLA enterprise customers have received [5].

The bandwidth of interfaces is used to arrange traffic in traditional traffic management. As a result, traffic management is sensitive to service classes but not to users, which is appropriate for network core traffic but not for service access traffic. Traditional traffic management has a hard time controlling various services for many users at the same time.

To address the aforementioned difficulties and provide a better QoS solution, a QoS system

capable of controlling user traffic and scheduling traffic based on the priority of user services is urgently needed. QoS technology ensures service quality from beginning to end based on the needs of various services. It is a system that allows different types of traffic to preempt network resources based on their priorities, resulting in more efficient network resource utilization.

The capacity of a service provider to guarantee the degree of service required by a customer's traffic from beginning to end is defined by QoS. It assesses a network's packet transmission capacity. A service provider offers a wide range of services. As a result, QoS assesses services in terms of bandwidth, transmission delay, availability, jitter, speed, and packet loss ratio during packet transmission. In a nutshell, QoS is the ability to provide different applications, users, and data flows with varying priorities or to guarantee a specific degree of performance for a data flow.

VPN QoS Models are provided for user services to ensure QoS based on the user's requirements and network quality. The following are examples of common service models: Best Effort service model, integrated service model, and Differentiated service model are all examples of service models. The Best Quality Model is another name for the Best Effort service model. It is mostly the network's default model. It offers equal service, such as priority and bandwidth, to all types of traffic. It is simple to implement, all packets are treated the same at the same level, and no different types of sensitive real-time Multimedia traffics are treated differently in terms of end-to-end packet delay and packet loss. IntServ is a service model that guarantees a certain level of traffic during a specific time. The IntServ constraints are as follows: Because each router must contain a large amount of state information, it operates on a small-scale network. As the network grows, it may become difficult to store all traces of all reservations [10]. It was created by the IETF (Internet Engineering Task Force, 1998) working group for specific standards and definitions of services that fall under Differentiated QoS [11]. MPLS is a mature technology that allows us to provide VPN services by speeding up network traffic and improving service quality by utilizing BGP MPLS VPN TE and DiffServ. In general, the main goal of this thesis is to improve Virtual Private Network Services Quality of Service (VPN QoS), which will aid in ensuring end-to-end VPN QoS delivery. VPN QoS concerns end-user or service provider perception as well as network performance. The best way to suit and increase network performance or VPN QoS is to optimize the VPN QoS network using different algorithms. Finally, improving network performance improves end-user and service provider perception.

In this paper, an attempt was made to investigate the end-to-end QoS parameters of a telecommunication network and Multiprotocol Label Switching Virtual Private Network Service to manage end-to-end traffic delay, jitter, and packet loss. The traffic is classified and labeled based on its priority.

The major aims of Quality of Service (QoS) include dedicated-line bandwidth provisioning, packet loss ratio reduction, network congestion management and avoidance, network traffic control, and packet priority modification. As a result, QoS is developed to meet such criteria, ensuring end-to-end service delivery for users. The service provider's ability to shape network optimization is critical. Optimizing the current network's physical and logical architectures is one of the best practices for implementing network QoS.

## **1.2. Statement of the Problem**

With the growing popularity of triple-play services, new services such as IPTV and VoIP place more demands on the IP network's service capability. Users are no longer content with mere packet transport to their destination.

They have higher expectations for better service, such as dedicated-line bandwidth provisioning, packet loss ratio reduction, network congestion management and avoidance, network traffic control, and packet priority adjustment.

Telecom clients have an increasing demand for Data, Internet, and Voice services. IP MPLS networks employ data, internet, and voice to connect clients in different places. However, according to a literature review conducted on the level of Telecommunication QoS in various countries, faced various challenges such as low bandwidth, high jitter, high packet loss, and high packet delay, all of which significantly degrade the quality of service and overall network performance parameters.

Customers can use MPLS VPN as one of the Telecommunication services. These services are often used to connect remote VPN sites for clients in IP MPLS networks. Companies, on the other hand, encountered various obstacles in offering these services, including low bandwidth, high jitter, high packet losses, and high packet delay, all of which harmed service quality and network performance. It happened because of QoS issues, with the failure to deploy end-to-end quality-of-service solutions being the root cause.

## **1.3. Research Questions**

As a result of the problem statement, literature review, and gap analysis, the researcher focuses on answering the following questions:

RQ1: What are the issues with VPN MPLS services?

RQ2. What measures are utilized to guarantee Multiprotocol Label Switching Virtual Private Networks Quality of Service in the Telecom network environment and avoid unmanageable networks, high jitter, high packet losses, and high packet delay?

RQ3. What are the network characteristics that determine MPLS VPN service quality?

RQ4. What improvements in MPLS VPN QoS have been observed in the Telecom network since the deployment of the End-to-End QoS Model?

RQ5: How can an end-to-end QoS be ensured and controlled?

## **1.4 Objectives of the Study**

### **1.4.1 General Objective**

The overall purpose of this research is to improve clients' telecommunication networks and MPLS VPNs so that jitter, packet losses, and packet delay are minimized.

### **1.4.2 Specific Objectives**

The specific objectives of the research are summarized as follows:

- Identify the gap in service quality for Multiprotocol Label Switching Virtual Private Network Service services.
- Propose a solution to the company's difficulties in improving the quality of Multiprotocol Label Switching Virtual Private Network Service offerings.
- Design, develop the Artifact demonstrate, evaluate, and communicate ways to improve Telecom's Multiprotocol Label Switching Virtual Private Network Service Quality of Service for its clients.
- Multiprotocol Label Switching Virtual Private Network Service Quality of Service was investigated using ITU standard threshold metrics such as packet loss, delay, and jitter, as well as bandwidth link.
- Recommend Telecom concepts or methods for improving the quality of Multiprotocol Label Switching Virtual Private Network Service.

## **5. Methodology and Tools**

The study's research method is classified as experimental research and design tools, network simulators, and the GNS3 tool, which is used for simulation. To improve the VPN Quality of Service, the appropriate VPN protocol, routing, and switching strategies must be chosen after to achieve the study's main and clear purpose, the researcher conducted a Literature Review on my topic from several sources.

This literature study will help you understand what factors affect Layer 2VPN and L3VPN QoS and



select proper VPN protocol, routing, and switching approaches to improve 2VPN and L3VPN QoS. Second, the researcher employed design science research methodologies to collect data on the problem of 2VPN and L3VPN Quality of Service. Third, the researcher examines the results from the VPN quality of service measurement in relation to the ITU threshold values. Fourth, to improve the 2VPN and L3VPN QoS. The proposed flowchart for the VPN QoS Research Method is shown in Fig.1.1.

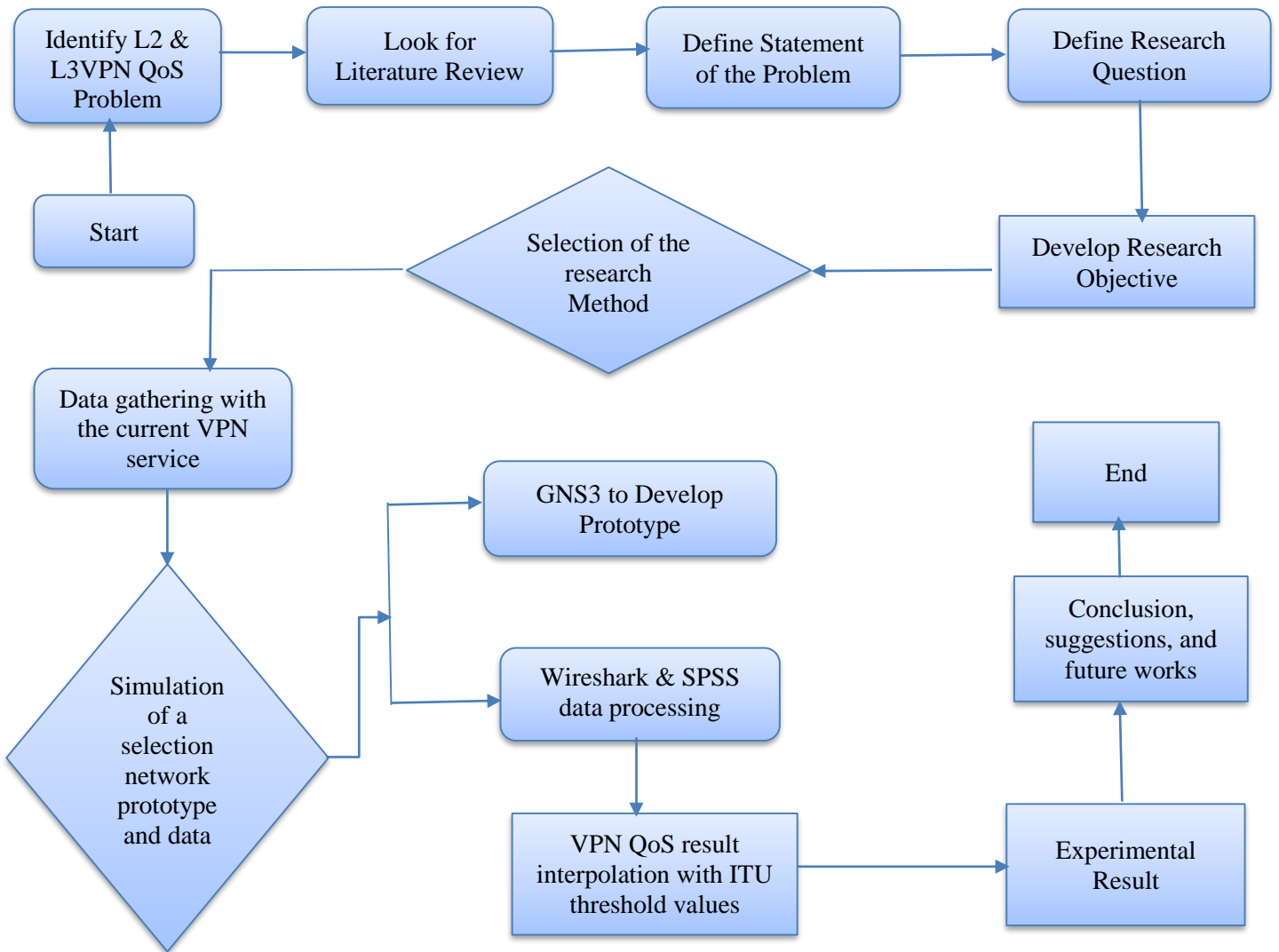


Figure 1.1: proposed flowchart for the VPN QoS Research Method

## 1.6 Motivation

Companies operate in a global market that necessitates the dissemination of information across multiple geographical zones. The ability to transmit information between locations that are geographically separated allows the organization to operate flatly. Regional branches connect openly with their headquarters, regularly transmitting all types of traffic. Customers typically desire high quality, flexible, safe, manageable, scalable, and low-cost networking solutions that let them to access all of a company's information and services.

Multi-Protocol Label Switching (MPLS) has recently been suggested as a means of ensuring an effective and scalable solution for huge networks. In addition to the commonly available layer 2 transport systems and protocols, it uses layer 3 routing protocols. The implementing QoS MPLS Layer 2 and Layer 3 VPNs working group's goal was to standardize the use of protocols that minimize jitter, delay, and packet loss. Network performance is optimized with the QoS function. Based on the following characteristics, QoS classifies incoming traffic into traffic classes: Configuration of a device, interface for egress, content of a packet.

In order to maintain its popularity, MPLS has provided significant additional capabilities in four areas: QoS (Quality of Service) support, Traffic Engineering, Virtual Private Network, and Multiprotocol Support.

### **1.7 Significance of the study / Contribution**

The role of thesis research is to improve the Multiprotocol Label Switching Virtual Private Network Service Quality-of-Service (MPLS L2VPN and L3VPNS). In the telecommunications industry, most areas of study require very strict follow-up. Meanwhile, Telecom offers MPLS L2VPN and L3VPNS to its Enterprise customers. This is due to the fact that every L2VPN and L3VPN customer requires continuous services to support their day-to-day activities. This, in turn, necessitates end-to-end network traffic optimization. As a result, efforts must be made to improve the QoS of MPLS L2VPN and L3VPNS. Continuous and organized traffic optimization on end-to-end networks is required to use the network's maximum capacity and to understand its usage after deployment. This research helped to improve the QoS of L2VPN and L3VPNS Telecom customers' connections. This is accomplished through traffic classification, marking, shaping, and policing based on various KPIs. Using computer-aided tools, the proposed solution was designed, developed, simulated, analyzed, and evaluated.

### **1.8. Scope and Limitation of the Study**

#### **1.6.1 Scope of the Thesis**

The current quality of VPN Telecom core site edge routers to connection across put was analyzed in this thesis investigation. Following the evaluation, the researchers compare the current Telecom VPN quality of service to the company's aims and ITU VPN QoS standards (standard threshold values).

The researcher selects L2VPN and L3VPN Quality of Service Difficulties as input and builds the test-based prototype to tackle the problem of L2VPN and L3VPN quality of services based

on variance found from VPN objectives and ITU VPN QoS standards.

The final recommended solution has been well-organized and designed, demonstrated, and assessed utilizing computer-aided tools GNS3. To demonstrate how MPLS, VPN, and MPLS LDP, work together to improve L3VPN Quality of Service, the researcher used GNS3 with Cisco IOS images of switches and routers. However, traffic management and queuing algorithms are used to improve the overall QoS of the existing infrastructure.

### **1.7 Organization of the Thesis**

There are four parts to this thesis. In the first chapter, the thesis is presented. It includes the research title, study background, problem statement, and references. Hypotheses/research questions the study's purpose, Scope of the study, Importance of the study, Study Limitations, The format of the paper, Timeline, budget, and cost breakdown

The MPLS, VPN, and QoS models are discussed in Chapter 2. It also shed some light on what other authors and researchers have to say about how to improve the quality of service of MPLS VPNs. In chapter three, the suggested network design was given. This explains how the DiffServ model was used to build, demonstrate, and evaluate MPLS, VPN, and QoS. The findings and discussions from the experiments were also presented.

Finally, the chapter included the paper's conclusions as well as future recommendations.

## **Chapter Two**

### **Review of Literature and Related Works**

#### **2.1 Review of Literature**

This section explores the current state of knowledge about the improvement of QoS in MPLS VPN networks utilizing various methodologies and models, such as best effort, integrated service, and differentiated service models. To comprehend earlier efforts to enhance MPLS VPN client communication performance. This section's goal enables us to identify research gaps and broaden our understanding of the study area's statistical landscape. BGP, MPLS, VPN, QoS threshold, QoS model, traffic shaping, and congestion control have all been properly reviewed. The papers on MPLS, VPN, QoS, and BGP have been reviewed.

On BGP MPLS VPN networks, QoS ensures end-to-end service quality to satisfy the various requirements of various services [13]. The elements that impact QoS are bandwidth, latency, jitter, and packet loss rate. Quality assurance for important service components is provided by QoS measurement based on these variables.

Through various service models, QoS offers consumers end-to-end services based on network quality and user requirements. The BGP MPLS VPN network employs the best effort, integrated service, and differentiated service models [14]. To ensure QoS in accordance with user needs and network quality, many service models are offered for user services. Techniques used to ensure the QoS for BGP MPLS VPN networks include traffic categorization, traffic policing, traffic shaping, congestion management, congestion avoidance, resource reservation protocol, and the link efficiency mechanism [16].

##### **2.1.1 Multi-Protocol Level Switching (MPLS)**

In traditional IP networks, routing protocols are used to distribute Layer 3 routing information. The destination address dictates how packets are routed. As a result, when a packet is delivered to the router, the next-hop address is determined by combining the destination IP address with details of the routing table [17]. This processing step will be carried out from source to destination. Router, repeat at each hop On the MPLS network, data packets are forwarded based on their label. The label may refer to the destination IP address as well as other parameters such as QoS classes and other parameters. The origin address MPLS is a network architecture designed to meet the needs of a [17]. A large-scale carrier network MPLS is a layer 2.5 technology. It is located between L2 and L3 and supports both data types. The network layer and the data link layer perform L3 routing as well as L2 routing at the MPLS network's edge. Within the MPLS network routing, it is a data forwarding packet forwarding technology. Label-

based decisions in the network, packets are assigned to an FEC (Forwarding Equivalence Class). Ingress LER (Label Edge Router), and a unidirectional LSP are built between ingress and each FEC. and egress routers; these LSPs are commonly referred to as "tunnels". LSPs are constructed in one of two ways. IGP shortest paths, link costs, and other optimization criteria It has QoS and network support. Scalability and the integration of various network types (such as IP and Asynchronous Transfer Protocol) Mode) in a network, as well as the establishment of interoperable networks [18] [19].

The three main components of MPLS are the Label Switch Router (LSR), the Edge Router, and the Label Distribution Protocol. Labels are assigned and removed from packets by the Label Switching Router, which is part of the MPLS network. The Edge Router is a high-speed router that communicates with the LAN via MPLS. Label Distribution Protocol is a protocol used to send labels and binding information to Label Switch Routers. The Edge Router examines, grades, and labels packets as they reach the MPLS network's edge. Each node employs the label, and as the packet travels along the path, each Label Switch Router employs the label. The label (rather than other information such as the IP header) is used to make routing decisions, keeping the packet on the Label Switched Paths. At each Label Switch Router, the incoming label is interrogated, and if it is found to be unacceptable, it is replaced with a new label so that the packet can proceed to the next hop, and then it is sent to the next Label Switch Router. This procedure is repeated until the packet reaches an Edge Router. The label-related information is removed by either the last Label Switch Router on the path or the Edge Router. This is significant because the packet could then be identified using an IP header rather than an MPLS label [18]. The basic elements of an MPLS network are depicted in Figure 2.1. network elements:

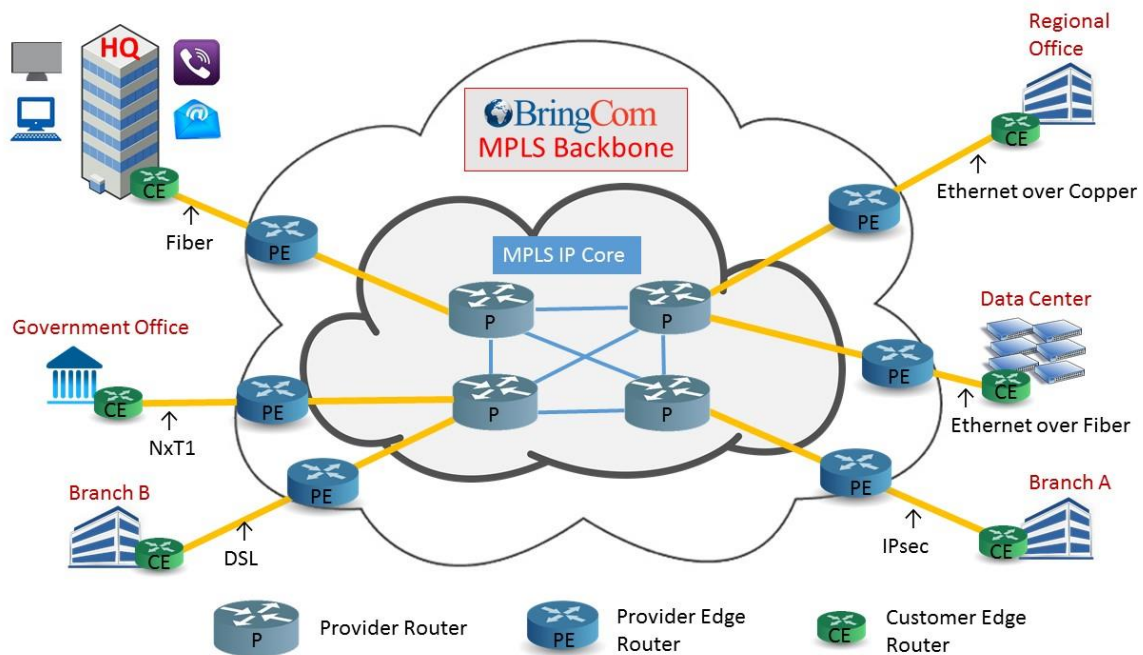


Figure 2.1: Multi-Protocol Label Switching based network [12]

MPLS packet header, which has 32 bits, 20 bits for the label, 3-bits EXP, which is not defined in the protocol but is typically used for COS, 1-bit S to mark stack bottom, and 8 bits for TTL [12]. The following are the major packet routing operations in an MPLS network:

- Label switching router (LSR): an MPLS-capable network device that serves as the foundation of an MPLS network. An MPLS domain is made up of a series of continuous LSRs.
- Core LSR: resides within an MPLS domain and only connects to LSRs within the domain.
- Label edge router (LER): A label edge router (LER) is located at the edge of an MPLS domain and connects to one or more MPLS-incapable nodes.

An LSP can be established between any two LERs on an MPLS network to forward packets that enter an MPLS domain and can pass through one or more core LSRs. As a result, an LSP's ingress and egress are LERs, and transit nodes are core LSRs.

### 2.1.2. MPLS Label Distribution Protocol

LDP is a protocol that generates and exchanges labels between routers automatically. Each router will produce labels for its prefixes locally and then broadcast the label values to its neighbors. The label switch path (LSP) tunnel is used in the MPLS network [20] [14] to

forward packets that must transit through the network. When a packet arrives at an MPLS network, the Ingress router receives it, adds an MPLS label to it, and sends it to the next hop based on the destination address in the packet. Due to the possibility of several LSRs between Ingress and Egress routers, when a packet reaches an LSR, it swaps labels and passes it to the next LSR. When a packet arrives at the Egress router, it is stripped of any labels and forwarded to the outgoing router.

All LSRs support interior gateway routing (IGP). To complete this task, adjacent LSRs must agree on a label that will be used as the IGP prefix, and each LSR must understand which label should be swapped for incoming and outgoing packets. This demonstrates the need for a mechanism to inform routers about which label to use when forwarding a packet. Each pair of router labels is unique to the network and has no global significance. To exchange label information, there must be some communication between the two adjacent routers. Otherwise, the routers have no idea which incoming label should match which outgoing label. Label distribution protocol is required for this purpose.

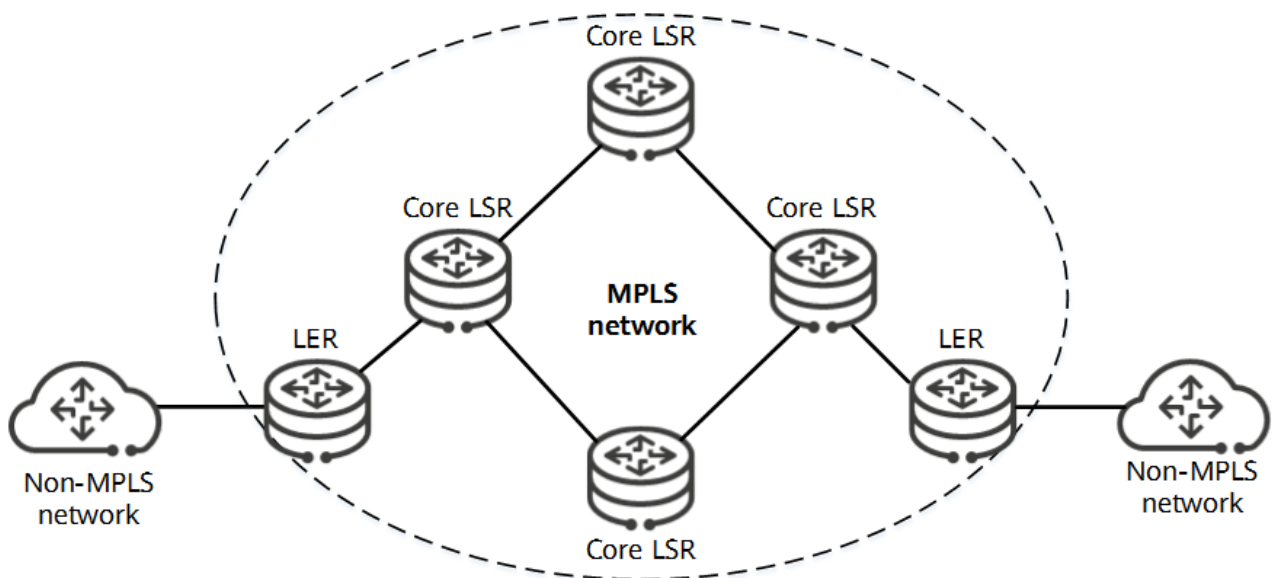


Figure 2.2: MPLS Label Distribution Protocol [20]

### 2.1.2.1 MPLS Architecture

MPLS's control and forwarding planes are separated. LSPs are configured on the control plane based on IP routes. Where necessary, MPLS can borrow the flexibility and reliability mechanisms of IP routes. Packets are transmitted over LSPs on the connection-oriented forwarding plane. MPLS can also effectively implement TE and QoS.

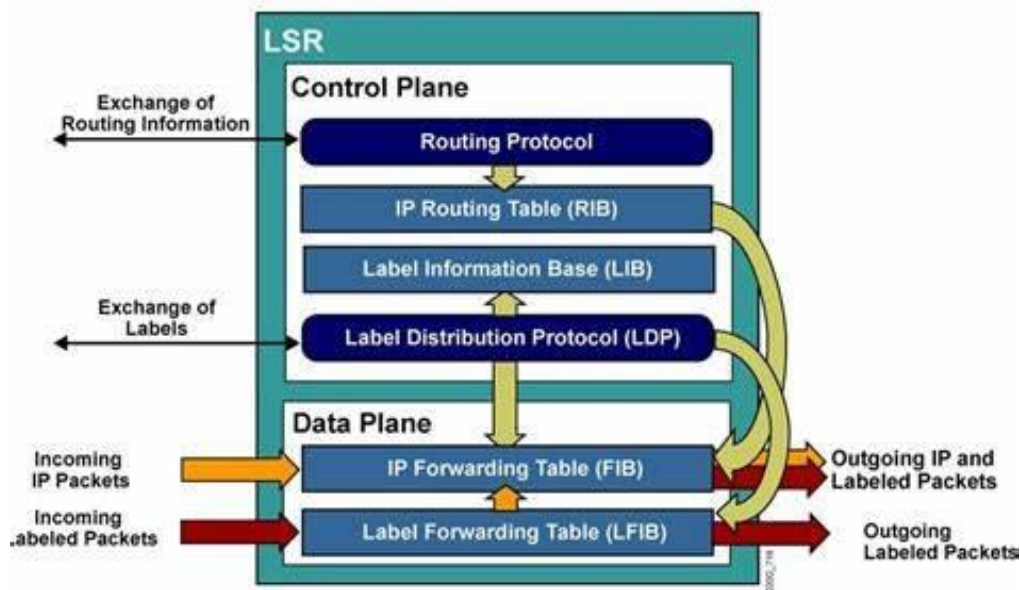


Figure 2.3: MPLS Architecture [12]

### 2.1.2.2. Control Plane

The control plane is in charge of exchanging routing information and labeling information with neighboring routers. Link state routing protocols distribute routing information among routers that are not necessarily adjacent, whereas label-binding information is distributed only to adjacent routers. [21]. There are two types of protocols in the control plane. Routing protocols and label exchange protocols are two types of information protocols. Protocols for label exchange are also required by the control plane, such as:

- Tag Distribution Protocol
- Label Distribution Protocol
- BGP MPLS VPNs
- Resource-Reservation Protocol and
- Traffic Engineering.

### 2.1.2.3. Data Plane

The MPLS data plane has a simple forwarding engine based on labeled information. Each MPLS router has two tables: label information base (LIB) and label forwarding information base (LFIB) [20]. To forward labeled packets, the data plane makes use of an LFIB maintained by the MPLS-enabled router. The LIB table stores all the local labels assigned by the local routers as well as the mapping of the labels received from the adjacent MPLS routers. For actual packet forwarding, the LFIB employs a subset of the labels contained in the LIB [20]. MPLS enabled routers use LFIB and label value information to make forwarding decisions [21].



#### **2.1.2.4. MPLS Network Applications**

a measure of how many services and programs may be installed on an MPLS network to enable virtual private networks, quality of service, and security. Because MP-BGP is protocol-independent, end-to-end circuits can be built using any protocol across any kind of transport media. MPLS Traffic Engineering (MPLS-TE): IS-IS or OSPF-based customized link-state routing protocols are used to locate resources and distribute attributes throughout the network. Control processes the FEC binding through RSVP, and the FIB is changed in accordance with the MPLS labels [23]. Network utilization may be minimized, and traffic routing can be controlled with MPLS-TE. In MPLS VPNs, FIBs are formed for one or more VPN customers. Customer routing data and MPLS labels are distributed throughout the network via Multiprotocol BGP (MBGP) [22, 23]. Any Transport over MPLS, a Layer 2 circuit over MPLS, can be used to establish Layer 2 VPNs (AToM). Services offered by Layer-2 VPNs include management, QoS, and auto-configuration. BGP is utilized for Layer-3 VPN in the network of the service provider (SP), and IP routing or static routing protocols are used between SPs and customers. MPLS QoS is a technique for differentiating services that makes it possible to build LSPs with guaranteed bandwidth [22] [23]. Each IP prefix in ATM networks receives four labels through customized LDP, enabling several QoS classes for each label. Some of the technologies that serve as the basis for MPLS applications and services include Layer 3 VPNs, traffic engineering, differentiated services, and Layer 2 VPNs. Multicast, GMPLS, and IPv6 the common framework incorporates a number of MPLS applications, each with its own unique set of properties. LSRs can integrate with new MPLS applications while keeping up with current services by sharing a common LFIB. [22] [23].

#### **2.1.3. Virtual private network (VPN)**

The majority of traditional private network requirements are as follows: security, availability, QoS, reliability, compatibility, and manageability. The primary goal of the VPN is to address three basic requirements, which are as follows: Access to network resources at any time for remote and mobile users, interconnectivity between remote offices, and controlled access to network resources. A virtual private network (VPN) is a technology that allows a secure and encrypted connection to be established over a less secure network, such as the internet. VPN technology was created to provide remote users and branch offices with secure access to corporate applications and other resources. Data travels through secure tunnels to ensure security, and VPN users must use authentication methods such as passwords, tokens, and other unique identification methods to gain access to the VPN [22]. VPN establishes a private

network across an infrastructure. VPNs provide a transparent network infrastructure that allows multiple customer sites, regardless of geographical location, to communicate over a shared backbone network as if they were using their private network. Each small company most likely has one VPN network, and if the company is large, there may be more than one VPN network, and these VPNs are mostly connected to the ISPs. VPN requires Internet connectivity, which is provided by default if it is connected to an MPLS VPN. The ISP has reaped the greatest benefit from the VPN and application services provided to its enterprise customers. Corporate Intranet, mail services, and VoIP telephony are common applications that run across an organization's VPN. VPNs are divided into two types: IP-based VPNs and MPLS-based VPNs [24].

### **2.1.3.1 Basic of VPN technologies**

There are many different VPN technologies to choose from, and network operators need to put together a list of their requirements and pick a solution that meets these requirements. For a VPN user, such a list will typically include the following criteria.

- **VPN Service.** The VPN service must match the type of service required by the VPN user. Different VPN solutions offer either layer 2 or layer 3 connectivity between VPN sites.
- **Quality of Service.** The VPN user may require a certain quality of service (QoS) for the connections between VPN sites (for example, the VPN user may require a minimum guaranteed bandwidth). If this is the case, the service provider backbone must support the provisioning of QoS-constrained tunnels, and the VPN solution must be able to make use of these tunnels.
- **Security.** If sensitive data is to be sent across the backbone between VPN sites, then the solution should support encryption, authentication, and integrity checking of data in the VPN tunnels. In addition, it is a further advantage if the routing information distributed in the provider network is also protected, to prevent the VPN network topology from being exposed to prying eyes.
- **Capital Cost (to the VPN user).** The VPN user may require a solution that does not involve a costly replacement of their existing hardware. Therefore, any VPN solution offered by a service provider must not require expensive extra functions to be added to the customer edge devices. Ideally, the solution will be fully interwork able with the VPN user's existing switches and routers.
- **Manageability.** The VPN user will want a solution that is simple to manage, and minimizes migration costs. The configuration of

the VPN solution should not be so complex that the network management personnel require extensive training. Neither should the solution require a significant overhaul of the VPN user's existing network architecture. Equally, the ongoing day-to-day management should not be too onerous – for example, it should be easy to add new sites to the VPN.

- **Maturity.** The VPN user will want a solution that has widespread industry acceptance and deployment. Less mature solutions carry the risk that the technology may not yet be thoroughly evaluated, and the architectural and interoperability issues entirely overcome. There is also the danger that they may not be offered by an acceptable range of providers, limiting the VPN user's range of choice and ability to source alternative backup solutions. At the same time, many vendors and providers may be looking to differentiate their product or service offerings by driving the establishment and deployment of new solutions

All of these criteria have focused primarily on the needs of the VPN user. However, a service provider also has some extra requirements for a VPN solution, as follows.

- **Capital Cost (to the SP).** The amount of money that needs to be spent on new equipment must be kept to a minimum. A solution will not be suitable if an SP has to upgrade every router in their network in order to deploy it!
- **Scalability.** The solution must scale well. This has two separate meanings. Firstly, the number of manual configuration required should not become unmanageable as more VPNs are supported by the SP. Secondly, the amount of extra system resources taken up on each router as VPNs are added to the backbone must be small enough not to require costly hardware upgrades or slow the routers down significantly.
- **Additional Services.** Ideally, the SP would like to be able to use the VPN offering to allow it to make a range of value-added services to the VPN user. This would offer the SP the chance to increase revenue from their customers. A number of different IP VPN solutions are discussed below, and, for each, we make reference to these criteria and assess their advantages and drawbacks.

## **2.1.4. Multiple Protocol Label Switching-Virtual Private Network (MPLS VPN)**

A group of techniques known as MPLS VPN use Multiprotocol Label Switching (MPLS) to build virtual private networks (VPNs). Using an MPLS backbone, MPLS VPN is a versatile way to carry and route different kinds of network traffic. Gold, Silver+, Silver, and Bronze are the four Classes of Service (CoS) available for MPLS VPN to provide QoS. Gold: It supports Real-time packet forwarding created to satisfy the needs of applications that are delay sensitive. The typical performance level for common applications, such as file transfers, email, and intranet a silver base Silver+ delivers an Assured Level of performance with packet-loss promises for mission-critical applications like streaming video and signaling, as well as business-critical applications like SAP, SNA, Oracle, and Telnet.

All forwarding is done using label switching with MPLS within the service provider network and labels are removed when sending traffic from Provider Edge to Customer Edge routers.

### **2.1.4.1 MPLS Layer 2 VPNs**

In this arrangement, the customer network and the service provider network are separated and no exchange of routes between the CE and PE routers is done. The division between the client and the service provider simplifies the implementation of the VPN. MPLS L2VPNs provide services for moving layer-2 frames from one client site to another. The CE devices are absolutely unaware of this method. Working with layer-2 frames enables the ISP to offer services that are not dependent on layer-3 protocols. Layer 2 VPNs do not require router equipment, and communication is assigned a MAC address rather than an IP address. Since it works at a lower layer, the latency is lower compared to a layer 3-based solution. It is also simple to deploy because it does not require any special configuration, unlike a LAN device [58]. It also has several drawbacks as a layer 2 protocol. Broadcast storms can affect Layer 2 networks. Because the service provider has no visibility, services are difficult to monitor [60].

### **2.1.4.2 MPLS Layer 3 VPN**

A provider router, a provider edge router, and a CE router comprise an MPLS Layer 3 VPN. One or more CE routers connect to one or more PE routers at each customer site. A client network is a collection of VPN sites located in different geographical areas. Each VPN Site is linked to carrier networks via the CE router, and the CE router connects to the PE via single or dual connections and connects VPN sites in different areas via carrier networks.

MPLS L3VPN can assign separate client locations to distinct VPNs in order to assign one office to a few VPNs or isolate services for VPN-shared access. Furthermore, routing information from one client is totally segregated from that of other customers and tunneled through the service provider MPLS network. MPLS L3VPN has a high level of client isolation flexibility to suit the needs of varied clients in terms of flexible networking and service security. The service provider will be involved in routing with the consumer at Layer 3. With the service provider, the customer will use appropriate IGP protocols such as BGP, OSPF, EIGRP, or any other routing protocol [59].

Routing scenarios can be complex at times, but the most frequent instance is an any-to-any topology in which any customer device can connect directly to the L3 MPLS VPN. To achieve effective tunneling and de-multiplexing across core and corporate traffic, data is packaged with MPLS labels [57].

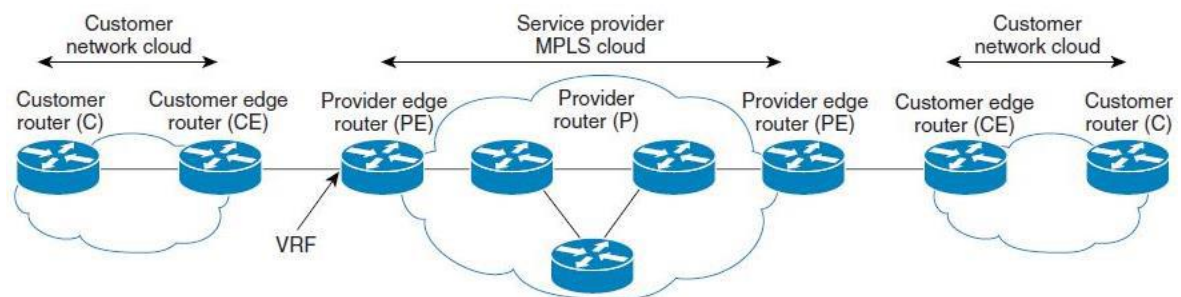


Figure 2.4: MPLS Layer 3 VPN Component Terminology [57]

MPLS Layer 3 VPN establishes a peer-to-peer VPN between customer sites (See Figure 3). It establishes Layer 3 connections with service provider routers. When client IP routes pass from Customer Edge (CE) routers to Provider Edge (PE) routers, labels are applied. Within the service provider network, all forwarding is completed using label switching with MPLS, and labels are removed when traffic is sent from Provider Edge routers to Customer Edge routers.

MPLS L3VPN employs both a GRE/IP tunnel and an MPLS tunnel. A tunnel is used to separate a client route from a provider router. A provider router is only connected to a public network route and not to a client router. Tunnel management is difficult for GRE due to the protocol's lack of support. An IP network that does not support MPLS can carry VPN service

over a GRE/IP tunnel to avoid the cost burden on the entire network.

A tunnel aim is to transfer data across a network from one node to another as though the two nodes were physically connected. This is performed by encapsulating the information - an additional header is added to information transmitted by the transmitting end of the tunnel, and information is sent by intermediate nodes based on this external header without looking at the original packet's contents.

There are various protocols that can be used to establish these tunnels, and the qualities of the tunnel have a significant impact on the overall properties of the VPN that uses that tunnel [59].

Address overlay, standard protocols for allocating labels and routes, scalable bandwidth and routing, reduced cost, intelligent QoS, any-to-any connectivity, support for a variety of topologies (Mesh, P2P, Hub-Spoke, VPN overlay, and HoVPN), and high reliability distinguish MPLS Layer 3 VPN from others.

#### **2.1.4.3. MPLS VPN Architecture**

There are some basic building blocks for the MPLS VPN at Provider edge routers. These are given below.

- Virtual Routing Forwarding (VRF)
- Route Targets (RT) and
- Route Distinguisher (RD).

VRF Virtual Routing and Forwarding (VRF) Assume that the same service provider network is being used by two different client sites with comparable IP schemes. It is the SP's duty to keep them apart. VRFs are utilized for this purpose. Every customer has their own VRF in the neighboring PE router. The service provider maintains its own routing information in the global routing table while allocating various VRFs to each client. A single interface can only be a part of one VRF; multiple interfaces can all be a part of the same VRF. [33]

A method called VRF divides a single network unit into several virtual networks. Layer 3 virtualization is used on the PE router and is called Virtual Route Forward. Multiple VRF resources in a single network component isolate virtual networks from one another. The instance of the VPN forwarding table is a virtual routing forwarding. It is a fusion of the three routing tables listed below [26]:

There is a distinct routing table for each VRF.

- VPN Routing table.
- VRF Cisco Express Forwarding table.
- PE router has an IP routing table.

**Route Distinguisher (RD):** A route distinguisher is an address qualifier that is only employed within the Multiprotocol Label Switching (MPLS) network of a single internet service provider.

It is used to differentiate between the unique VPN routes taken by various clients when they connect to the provider [32]. When VPN prefixes flow over an MPLS VPN network utilizing multiprotocol BGP, the ISP should be concerned that they are unique since IPV4 IP addressing becomes problematic if there are overlapping IP addresses being used on the client side [54]. To resolve this issue, RD is utilized. The primary function of the RD is to generate a distinct IPV4 IP in the ISPs so that there are no issues with overlapping IPs [26].

**Route Targets (RT):** In the case of the RT mechanism, there are some restrictions among the various MPLS VPN networks regarding which VPNs can communicate with one another and which cannot. In order to address these types of challenging scenarios, RT was developed to address the issue relating to processes among the VPN networks [26].

### **2.1.6. Border Gateway Protocol (BGP)**

The Border Gateway Protocol is the de facto interdomain routing technology used on the worldwide Internet to communicate reachability data between Autonomous Systems (BGP). Each Autonomous System can replace distance-based metrics with policy-based metrics when determining the best routes thanks to the path-vector protocol known as BGP. [32] Border Gateway Protocol (BGP) is a routing protocol that is utilized between autonomous systems (BGP).

A BGP speaking system's principal function is to talk with other BGP systems in order to share network reachability data. This network reachability information includes a list of Autonomous Systems (AS) that reachability information traverses. This data is sufficient to build an AS connection graph for this reachability, which can then be used to remove routing loops and enforce some policy decisions at the AS level. Classless Inter-Domain Routing (CIDR) is supported by a set of methods provided by BGP-4 [RFC1518, RFC1519]. These approaches include disabling BGP's network "class" concept and supporting the advertising of a group of destinations as an IP prefix. Additionally, BGP-4 offers capabilities for route

aggregation, including aggregation of AS pathways. Only the destination-based forwarding paradigm, which implies that a router only forwards a packet based on the destination address included in the IP header of the packet, is supported by routing information transmitted via BGP. The set of policy decisions that can (and cannot) be enforced via BGP is reflected by this in turn. Only policies that follow the destination-based forwarding paradigm can be supported by BGP.

### **2.1.6. MP-BGP MPLS VPN**

The SP network uses Multiprotocol BGP (MP-BGP) to deliver VPN routes to additional PE devices. Due to the fact that VPNs may employ overlapping address spaces, BGP may choose routes to places using the same IP prefix. Border Gateway Protocols Multi-Protocol Label Switching Virtual Private Network (BGP MPLS VPN) is a network architecture. Virtual private networks at layer 3 using BGP MPLS (L3VPN). While MPLS is used to forward VPN packets on backbone networks, it employs BGP to advertise VPN routes [34]. The following routers make up the BGP MPLS VPN model: Provider (P), Provider Edge (PE), and Customer Edge (CE) routers. In order to provide an alternative to physical full-mesh communication between two internal border gateway protocols (iBGP), a route reflector (RR) is used. Between two internal border gateway protocols (iBGP), a route reflector (RR) is used to offer an alternative logical full mesh instead of physical full-mesh connectivity to optimize the routes as shown below in Fig. 2.5 [34].



# MPLS VPN Operation

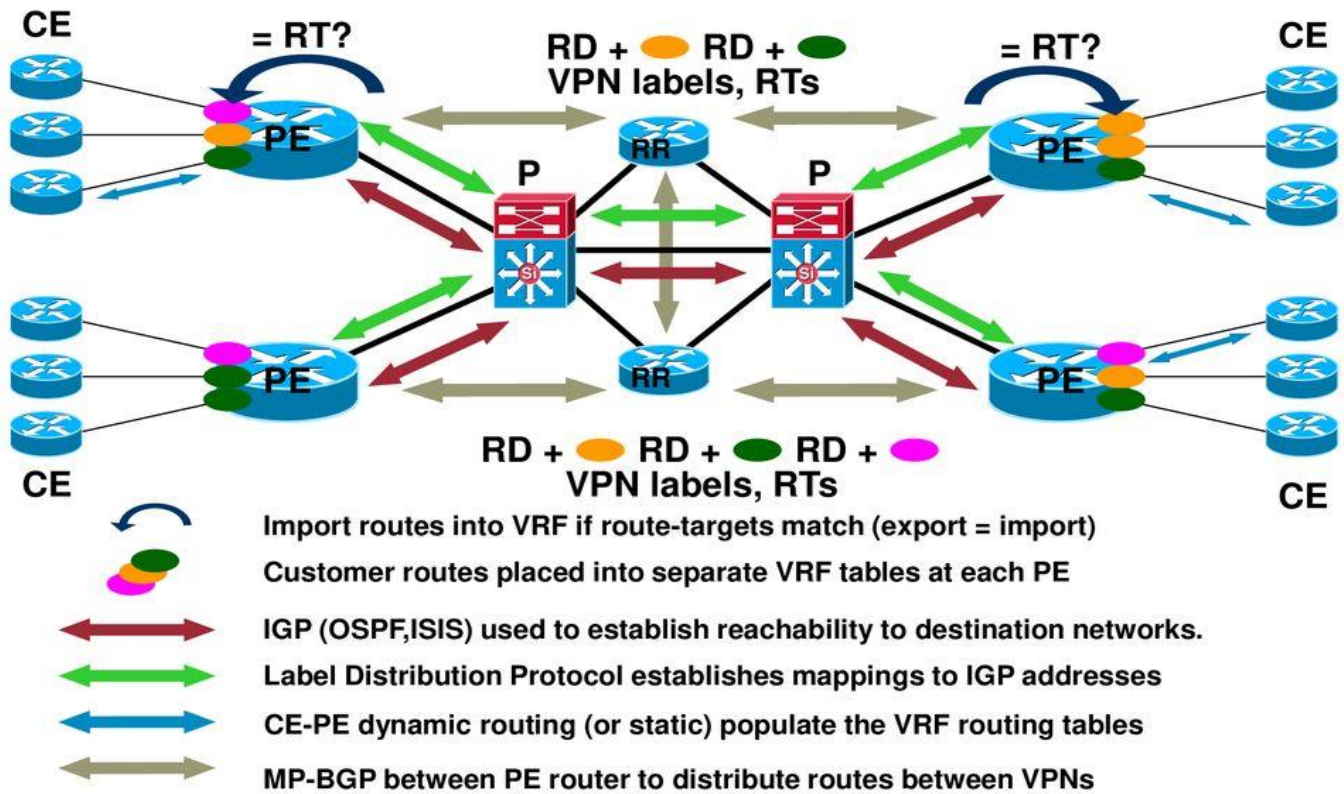


Figure 2.5: BGP MPLS VPN components and working principles [34]

## 2.1.7. Quality of Service

The term "the quality of service that a flow seeks to attain" is Quality of Service or QoS. A specific degree of performance for a data flow through a network can be ensured via QoS, even when different users, applications, and data flows may have varying priorities. The goal of QoS is to guarantee that a network can produce the intended results. A network management system is employed in a network to guarantee that the networks are performing at their best [36]. It is possible to describe QoS and the network's capacity to guarantee performance. Performance in a communication system relates to how quickly and consistently various sorts of load data are delivered. The effectiveness of computer networks can vary significantly due to a number of problems, including packet loss, delay (latency), jitter, and throughput. These problems can have a big influence on many applications. Users will become agitated when an

application streams data packets across a network with insufficient bandwidth, unpredictable delays, or significant jitter, for example, when using voice communications (such as IP Telephony or VoIP) or streaming video. It is possible to estimate and match packet loss, delay (latency), jitter, and throughput to the needs of the applications. These factors, which include packet loss, delay (latency), jitter, and throughput, can be forecasted and tailored to the needs of the present using applications. QoS is increasingly crucial for the new generation of internet applications because the majority of them employ the Internet of Things definition. Because customers expect quality assurance from their ISPs, QoS is more important in the client-ISP relationship. Network traffic has an impact on QoS quality when data is transmitted over the network from source to destination

### **2.1.8.VPN QoS - MPLS QoS Application on MPLS VPNs**

VPN QoS combines MPLS QoS and MPLS VPN to serve networking that bears services of various priorities. VPN QoS distinguishes services of different priorities and ensures that high-priority services are forwarded preferentially. This guarantees the QoS for important services on VPNs.

DiffServ, MPLS-LDP, and MPLS VPN can be jointly used based on actual requirements to isolate services, distinguish services of different priorities, ensure bandwidth resources for important services or important VPNs, and forwards packets on VPNs or MPLS-LDP tunnels based on packet priorities. This provides a solid technical basis for carriers to develop voice, video, and VPN services.

### **2.1.9. QoS Specifications**

QoS provides customized service guarantees based on the following specifications:

- Bandwidth/throughput
- Delay
- Delay variations (Jitter)
- Packet loss rate

#### **2.1.9.1 Bandwidth**

The term "bandwidth," also known as "throughput," describes the greatest amount of data that can be sent between two points in a single second or the average speed at which a certain data flow is sent between two network nodes. Bit/s units are used to measure bandwidth.

Internet users anticipate higher bandwidths as services become more varied, allowing them to experience a wide range of popular applications in addition to news browsing. New and

appealing applications, like IPTV, databases, and new-generation multimedia, are constantly being produced by the epoch-making information evolution. These applications all require extraordinarily high bandwidths. As a result, bandwidth is always the primary consideration in network planning and a crucial foundation for network research [27].

#### **2.1.9.2. End-to-end delay**

The time it takes for a packet to get from its source to its destination is referred to as a delay. As an illustration, consider voice transmission. The interval between speaking and hearing words is referred to as a delay. When there is a considerable delay, voices get muddled or cut off. The majority of users are insensitive to delays of under 100 Ms. The speaker can detect brief pauses in the responder's response if there is a delay of between 100 and 300 milliseconds, which can be irritating to both parties. Both the speaker and the responder must wait for responses if there is a delay of more than 300 milliseconds. Voices bleed into one another if the speaker cannot wait and repeats what has been stated. When a speaker can't wait and repeats what they just said, voices meld together and the conversation's quality drastically declines.

There are some common types of delay, including [37].

- Processing Delay: Routers require some time to process packet headers.
- Queuing Delay: The number of delays, including the time it takes to insert a packet into the network and send the packet to its destination address.
- Transmission Delay: The time required to push packet bits into the connection.
- Propagation Delay: the time it takes for a signal to travel through a medium after it has been delivered.

#### **2.1.9.3. Jitter (Delay Variation)**

When packets in the same flow have different delays, this is referred to as a jitter. Jitters happen and the service quality suffers when the time it takes for a packet to reach a device to be delivered by that device varies from one packet to another in a flow. Jitters can cause interruptions in some services, most notably audio and video services, which are zero-tolerant of them. Transmission of protocol packets is also impacted by jitters. At regular intervals, specific protocol packets are exchanged. Such protocols switch between Up and Down if there are a lot of jitters, which is bad for quality. Networks are a haven for jitter, but as long as jitter levels stay within a certain tolerance, service quality is unaffected. Buffers can reduce excessive jitter but increase delay times [37].

#### 2.1.9.4. Packet loss

When a packet or packets fail to arrive at their destination after traveling through a network, this is known as packet loss. Services are unaffected by slight packet loss. Users, for instance, are not aware when a bit or a packet is lost during voice transfers. The image on the screen briefly becomes jumbled if a bit or packet is lost during video transmission, but it recovers fairly rapidly.

Even if TCP is used to transport data, a little amount of packet loss is unimportant because TCP immediately retransmits the missed packets. However, the effectiveness of packet transmission is hampered by high packet loss. The severity of service interruptions on networks is indicated by the packet loss rate, which worries users [37].

#### 2.1.10. Recommended IP QoS in Telecommunication network

Data traffic can be prioritized according to its nature or destination using a QoS configuration. In order to give a site's vital traffic higher priority over other traffic in the event of network congestion. Since all packets from all clients are currently processed equally in the telecom network, generic IP network performance targets are advised, as indicated in the table below

Table 2.1: Telecom recommended QoS targets [38].

QoS Parameter	Across backbone PE to PE	VPN end-to-end CPE to CPE across backbone)	Internet connection as measured from the connected BRAS or PE (or speed test.net)
Latency	50ms or less	200ms or less	150ms or less
Jitter	15ms or less	50ms or less	N. A
Packet loss	0.1% or less	2% or less	1% or less
Availability	99.9% or more	90% or more	90% or more
Throughput	N. A	75% or more of subscribed bandwidth	75% or more of subscribed bandwidth.

#### 2.1.11. Mechanisms of Improving QoS of VPN

Bandwidth, network latency, jitter, and data packet loss are the primary problems that the QoS aspect should focus on in order to transport virtual private networks effectively. We explain

how VPN QoS issues might be resolved in the following section to ensure the necessary QoS for voice traffic. By using several mechanisms, this issue can be resolved, and VPN QoS can be improved [39]:

- Compress and fragmentize packets
- Increase bandwidth.
- Use rational queue scheduling and congestion avoidance mechanism
- Improve processing performance.

By increasing the current bandwidth and the link, which directly affects or ensures the QoS of the traffic flow, it is possible to deliver successful VPN QoS [39].

Additionally, it shortens the transmission jitter, lowers the packet loss ratio, and drops fewer packets. Delay-sensitive traffic prioritization, traffic compression, queue scheduling, and congestion avoidance are other methods for enhancing VPN QoS. Processing performance is increased by optimizing memory and CPU operations, which also decreases latency and data packet loss [39].

### **2.1.12. End-to-End QoS Service Models**

Successful end-to-end communication is a need for network applications. Before reaching the destination host, traffic may pass via many routers on a single network or even multiple networks. Therefore, a comprehensive network implementation is needed to assure end-to-end QoS. Based on specific requirements, service models are utilized to provide an end-to-end QoS guarantee.

The following service model categories are offered by QoS:

- Best-Effort Service Model
- Integrated Service Model
- Differentiated Service Model

#### **2.1.12.1. Best-Effort Model**

The Best-Effort service model governs numerous network applications, including email and FTP, and it is the standard service model on the Internet. [40] The simplest service model is this one.

Any number of packets can be sent at any moment by an application without network authorization or notification. The network then sends the packets with its best effort, but it provides no performance promises. applications of the Best-Effort model include services with

minimal criteria for dependability and latency

### **2.1.12.2. Integrated Services**

Per-flow QoS assurances for individual application sessions are provided by the integrated service (IntServ) framework. Its goal is to offer IP networks the closest approach to circuit emulation.

It also marks a substantial shift from the Internet's best-effort service by aiming to deliver the maximum level of QoS in terms of service guarantees, the granularity of resource allocation, and the detail of feedback [42]. The number of service classes that characterize specific service attributes required by various application types has been specified by the IntServ working group.

End applications are instructed by IntServ to make the necessary QoS requests of routers along their data path. This is achieved through RSVP (resource reservation protocol), which uses a two-way handshake to create and maintain a secure connection. This is done by establishing and maintaining a sender-receiver connection via RSVP (resource reservation protocol) [14], which uses a two-way handshake to ensure a given level of service [45]. Additionally, RSVP is a very flexible general-purpose signaling protocol that enables the release of resources that are no longer needed and the reservation of additional resources inside an existing connection. RSVP is referred to as a "soft state" protocol, which is described as a state that may be modified by specific RSVP messages in routers and end nodes. Path and reservation messages establish soft states and frequently refresh them. If no matching refresh messages arrive before a cleanup timeout expires, it is erased. IntServ nodes are required to separately save, update, and retain all states of their flows in addition to exchanging soft states messages.

The main problem with the IntServ/RSVP architecture is scalability. The model does not scale well in the Internet core primarily because [46]: -

1. Huge storage and processing overhead is placed on the routers since the amount of state information in the routers increases proportionally with the number of flows,
2. The requirement on routers is very high, each router must implement RSVP, admission control, classification, and packet scheduling.

### **2.1.12.3. Differentiated Services**

To overcome the disadvantages of IntServ, a new architecture for the Internet has been proposed [3], which is called Differentiated Services (DiffServ). Therefore, DiffServ is more scalable, manageable, and easily deployable for service differentiation in IP networks. In this scheme, the complexity is pushed out to the edge routers and the core routers are maintained as simply as possible. DiffServ architecture [43] is manageable since traffic flows entering a network are admitted and conditioned by the network's BB, then classified and scheduled at the boundaries of the network as seen in Figure (1) [47]. Therefore, individual microflows are aggregated at the edge routers into one of the classes or Per-Hop-Behaviors (PHB) defined by the approach. A PHB is identified by a short label in the IP header which is called Differentiated Service Code Point (DSCP) which is 6 bits of IPv4 or IPv6 header. Incoming packets are marked using code points as belonging to one of the many pre-defined classes and injected into the network. The core routers forward packets by examining the DSCP code. This code is also used to schedule traffic flows packets. First, the classifier uses the IP header to do multifiled classification. Then, the Type of Service (ToS) field is used for behavior aggregate classification to identify priority level since DiffServ defines certain behaviors that packets can receive at each hop. All packets with the same DSCP are grouped and are known as behavior aggregates (BA) and they get the same processing treatment. DiffServ admission control does not call upon data flows to reserve a complete path, nor does it assert that routers maintain flow states. Instead, it requires end hosts to continuously monitor the given QoS. In spite outperforming of IntServ, DiffServ has the following disadvantages: -

1. Individual flows within a DiffServ class cannot be differentiated since the only number of pre-defined classes is used to classify incoming traffic packets [48].
2. Mapping packets to pre-defined classes using DSCP produces more delay that affects the end-to-end delay

### **2.1.13. DiffServ QoS Implementation over MPLS VPN**

Because of its scalability, the DiffServ QoS model is preferred in MPLS VPN environments to achieve service quality [49]. There are four elements in the DiffServ model. Classification, marking, control, and prevention of traffic jams. These were used to manage network traffic,

allocate resources in various ways, and enable the system to offer a variety of services.

Classification is the initial stage in using the DiffServ QoS model. Its purpose is to divide traffic into various classes. Each class is marked after categorization; this procedure is known as marking. Following grading, each class's business policy is set up in accordance with the VPN.

### **2.1.14. Traffic Classification**

The process of categorizing traffic is known as traffic classification [50]. A traffic class is a name given to each category. The most essential step in using the DiffServ paradigm to achieve QoS is classification. Traffic is prepared for additional handling to achieve QoS after being classified. Although classification requires a lot of processing power, it typically occurs at the client edge router. End-to-end delay is significantly affected by the classification process' overall influence. Classification is possible using [51]:

- Incoming interface
- IP precedence
- Differentiated service code point (DSCP)
- Source or destination IP address
- Application and
- Five Tuple (source and destination IP address, IP protocol number, TCP/UDP source, and destination port numbers).

The type of service (TOS) field in the IP packet priority is marked to implement QoS categorization, as shown in fig. 2.6 [52]. The various RFC standards can be used to classify IP data streams. The IP precedence field is described in RFC 791[53] and is used to categorize IP applications into 8 groups. The TOS field is separated into 16 groups according to RFC 1394. RFC 2472 redefines the TOS and categorizes services into 64 groups (DSCP).

The type of service (TOS) field in the IP packet precedence, as shown in fig. 2.6 [52], is marked to implement QoS classification. Based on the many RFC standards, IP data streams can be categorized. The IP precedence field is defined in RFC 791[34] to classify the IP application into 8 groups. According to RFC 1394, there are 16 categories in the TOS field. Using 64 categories, RFC 2472 redefines the TOS for services (DSCP).

QoS classification is implemented by marking the Type of Service field in the IP packet header.



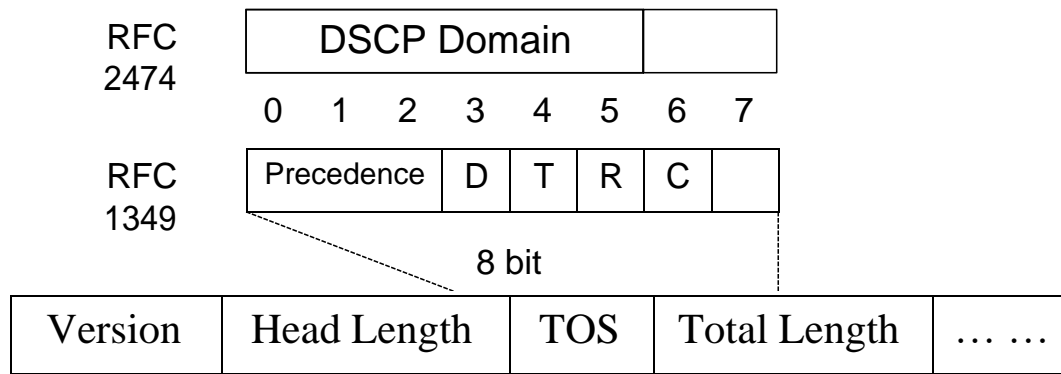


Figure 2.6: Traffic classification [52].

Bits are defined in RFC 1349; bits 0 to 2 denote precedence. The value is between 0 and 7. The precedence increases with increasing value. The D bit stands for the delay, the T bit for throughput, the R bit for reliability, and the C bit for cost in dollars. Bits 6 and 7 are set aside.

### 2.1.15. VPN Traffic Marking

Traffic marking involves coloring the packet so that the subsequent nodes may easily recognize it.

As soon as the nodes have recognized and categorized the VPN packets, they should mark the packets. Adding a value to the DSCP field is known as marking. Traffic is detected using marking for the subsequent action to achieve QoS [53]. Every hop in the network can typically categorize and identify VPN packets (by port or ToS byte), and then those hops can give each VPN packet the necessary QoS. Then, by compressing the 40-byte IP plus UDP plus RTP header to 2 to 4 bytes, you can use specific algorithms to enable priority queueing to ensure that large data packets do not interfere with voice transmission and to reduce bandwidth requirements [54]. To identify traffic as VPN traffic in the majority of IP networks, marking IP Precedence or DSCP should be sufficient. Data link layer and network layer traffic tagging are also possible [54]. The method of marking involves the node setting one of the options listed below [54]:

Traffic marking at the data link layer can be done the following:

- CoS value on IEEE 802.1p [8]: -Three bits in IEEE 802.1P frame are reserved for QoS.
- MPLS experimental (EXP) bits [8]: - Three-bit field (MPLS EXP) is reserved for QoS purpose
- Frame Relay: - Forward explicit congestion notification (FECN), backward explicit congestion notification (BECN), and discard eligible (DE) fields are used

for congestion management and congestion avoidance. Traffic marking at the network layer can be done the following [8]:

- IP precedence or DSCP on IP header IP precedence. DSCP uses an 8-bit field ToS in IP header IP precedence uses 3 most significant bits and DSCP uses 6 most significant bits. DSCP is backward compatible with IP precedence.
- Source or destination IP address Source and destination IP address in IP can be used for marking the IP packets.

### **2.1.16. Per-Hop Behavior (PHB)**

The DiffServ architecture distributes resources at each node along the path using Per-Hop Behavior (PHB). PHB assures that each node's behavior aggregate receives 99.999% of the network resource (bandwidth, latency, and reliability). This can be determined by observing the various competing traffic circumstances. This resource allocation is decided by business demands. These PHBs are connected together and utilized as building blocks to establish QoS in compliance with SLAs. Each network node's PHBs are set up with appropriate buffer allocation and packet scheduling rules. [56] Class-selector (CS) PHB: Used for backward compatibility with the non-DiffServ compliant device.

The following PHBs are defined by IETF:

- The IETF has defined the following PHBs:
- Best Effort (BE) PHB: The default PHB that is utilized for best-effort service.
- Expedited Forwarding (EF)PHB: A low-latency service.
- Assured Forwarding (AF)PHB: Used for guaranteed bandwidth service.

### **2.1.17. Traffic Shaping and Policy**

Traffic policing regulates the rate at which incoming packets arrive to guarantee that network resources are correctly allocated. If a connection's traffic rate exceeds the interface's standards, traffic policing allows the interface to discard extra packets or re-mark the packet priority to maximize network resource consumption and safeguard carriers' revenues. Limiting the rate of HTTP packets to 50% of network capacity is one example of this technique.) Traffic shaping regulates the rate at which outgoing packets are sent in order to match the downstream device's traffic flow. When traffic is transferred from a high-speed link to a low-speed link, the inbound interface of the low-speed link is vulnerable to substantial data loss to avoid this issue,

implement traffic shaping on the outbound interface of the device connected to the low-speed network [55].

### **2.1.18. Congestion Management**

By temporarily keeping extra packets on an interface of a network device until there is adequate bandwidth to forward them, queuing can alleviate brief interface congestion. The queue depth being full can cause certain packets to be dropped occasionally [55]. Congestion management is the best method for reducing data packet loss. By establishing how and when the queue depth is full, congestion management enables the administrator to regulate congestion. Congestion Management can be implemented in several ways [55].

- Priority Queuing (PQ): This mechanism allows one to give priority to certain traffic while allowing others to be dropped when the queue depths are full.
- Custom Queuing: It allows us to reserve queue space in the router or switch buffer for the traffic type.
  - Weighted Fair Queuing (WFQ): This allows the sharing of bandwidth with prioritization given to some traffic.
  - Class-based Weighted Fair Queuing (CBWFQ): This extends the functionality of WFQ to provide support for the user-defined class.
  - Low Latency Queuing (LLQ): This is a combination of CBWFQ and PQ. It can give traffic that requires low delay the required bandwidth it needs while also giving data the needed bandwidth. It solves the starvation problem associated with PQ.

## **2.2 Review of Related Works**

The quality of service of MPLS VPNs has been improved by several writers and researchers. From the customer LAN side, the provider edge (PE) to the customer side, the network backbone, and other end-to-end QoS views, some people have tried to explain MPLS VPN QoS. To set the framework for this investigation, this section evaluates significant connected studies.

In [8] Beyene, A.M., et al., attempted to investigate the end-to-end QoS parameters of Ethio Telecom service level agreement (SLA) customers network by using differentiated service

(DiffServ) model, to manage end-to-end traffic delay, jitter, and packet loss. The traffic is classified and labeled based on its priority. Weighted fair queueing was used for congestion management in the proposed network architecture, and weighted random early detection was used for congestion avoidance. The network architectures were designed, demonstrated, and evaluated using GNS3 and Wireshark. When the existing network's results are compared to the proposed network architecture designed using the DiffServ model, delay, jitter, and packet loss have decreased while traffic utilization has increased.

According to H. Lee., et al [9] They require VPN mechanisms that operate over deployed backbones that have already been installed and that can also be transferred to new backbones like MPLS. The most recent development in multilayer switching over the Internet is MPLS. They are attempting to make it clear how MPLS may be used to build VPNs. They investigated an architectural design for creating VPNs within an MPLS domain for that purpose. The suggested approach makes use of both peering and packet switching at the network layer as well as circuit and per-stream switching at the link layer. It includes an implementation process and a design plan for the VPN service in the MPLS system. And after that, they go over the MPLS-based VPN service operations. Additionally, they outline MPLS VPN plans that must function with current network backbones and offer a broad range of QoS characteristics.

P. Zhang., et al., [10] worked on Recently, MPLS has been utilized to create MPLS VPNs or VPNs over an IP backbone. they examine problems with QoS routing—finding routes in MPLS VPNs that meet QoS requirements. They begin by providing background information on QoS routing and MPLS VPNs. Then they talk about the advantages and drawbacks of adding QoS routing to MPLS VPNs. About operating QoS routing in MPLS VPNs, specifically provide an architecture for MPLS VPNs with QoS routing functionality.

K. Okukpujie., et al., [11] Using simulation tests conducted on the OPNET network, a comparison between the performance of the MPLS-VPN network and a traditional VPN network is made. End-to-end delay, voice packet sent/received, and label-switched path traffic is the performance measures that were compared. The test platform for the simulation study was Voice over Internet Protocol (VoIP). The study's findings demonstrated that MPLS-based VPN networks function better than conventional VPN networks.

Without rerouting already admitted flows, the researcher D. Ionescu., et al., [12] propose to address the combined routing and admission control challenge for IP traffic flows in MPLS networks. They offer two mathematical programming methods as solutions to this issue. End-to-end latency constraints are part of the first model, and end-to-end packet loss constraints are part of the second. These end-to-end QoS restrictions are put in place for all admitted flows in the network as well as the new traffic flow. Both approaches' primary goal is to reduce the end-to-end delay for the new flow.

The researchers S. Yada., et al. [13] worked on traffic-engineered MPLS VPN for Protected Traffic using GNS Simulator and they present an approach to MPLS VPN along with VPN with OSPF and MP-BGP to isolate the customer and manageable. Finally, they provide a design for designing a traffic-engineered MPLS VPN network with path protection, and what they conclude is the implementation of the proposed design will surely reduce parameters like packet loss and delay. The solution they proposed has applicable to intra-domain VPN communication. The usage of traffic tunnels on the interdomain has not been addressed.

By integrating MPLS Network with TE, K. Jeevan., et al., [14] explain how to enhance the performance of Voice over Internet Protocol and implement QoS. In order to decrease congestion, load balancing, and management of network resources, MPLS can offer traffic engineering (TE). They are implementing QoS on a network by employing scheduling techniques. On top of the MPLS-TE network, Differentiated Service (DiffServ) architecture is used to implement Coevolution of performance taking into account the network's end-to-end delay, jitter, and packet loss factors. OPNET modeler 16.0 was used for the simulation, and the outcomes were examined.

A VPN network simulation model was looked at by N. Rikli., et al., [15] and is based on an existing network and will be developed using the MPLS protocol. The implementation of various queueing strategies will be used to assess how well the end-to-end QoS criteria for different traffic kinds are met. Real-world data-based input traffic was employed. After a thorough examination of the policies, the benefits, and drawbacks of each are identified, and recommendations are made along with suggestions for future research.

The QoS performance for several services, including VoIP, real-time video, and best-effort

data traffic, was examined by D. Zhang., et al., [16]. The results show that while guaranteed bandwidth services can offer excellent QoS for real-time traffic like VoIP, they can offer subpar QoS for variable video traffic. Guaranteed quality of service is expected to be provided by the combined usage of differentiated services (DiffServ) and multiprotocol label switching (MPLS) technologies (QoS). Prior to forwarding data, Traffic Engineering (TE), which uses MPLS, configures an end-to-end routing path. MPLS TE can't offer QoS for differentiated services because it only reserves resources for one aggregated class. By fusing the features of both DiffServ and TE, MPLS DiffServ-aware TE makes MPLS TE aware of QoS.

B. Soewito, et al., [17] provide a solution to the combined routing and admission control difficulty for IP traffic flows in MPLS networks without rerouting already accepted flows. They propose two approaches to mathematical programming to address this problem. The first model includes end-to-end latency limitations, whereas the second model includes end-to-end packet loss constraints. All accepted flows in the network and the new traffic flow are subject to these end-to-end QoS constraints. The reduction of the new flow's end-to-end delay is the main objective of both strategies.

The discussion of D. Kanchan., et al., [19] examination of the MPLS's basic operation. They place a lot of emphasis on the significance of MPLS as a means of transporting IP datagrams and other types of traffic, as well as the benefits of using MPLS in IMS platforms to ensure QoS from start to finish. This review paper's conclusion mentions the outcomes of an MPLS network simulation.

Here, the researcher attempted to combine various approaches and techniques utilized in the study as input and strives to enhance the caliber of services provided to MPLS VPN users by employing various algorithms and congestion avoidance mechanisms.

### **3. Summary and Gap Analysis of Related Works**

Related research discoveries, which they then incorporated into their current work or improved. as shown in Tables 2.1 and 2.2.

Table 2.1 Summary and Gap Analysis from Related Works

Ref.	E2E QoS Model	MPLS VPN QoS Improvement	Gap Analysis
Oulai, D., et al., [17]	mathematical programming models	Reduces significantly the mean end-to-end delay (or the mean packet loss rate).	Only the end-to-end delay and packet loss were considered in the study; throughput, latency, and jitter were left out.
Lee, H., et al., [9]	Differentiated service (DiffServ),	To provide VPN tunnels for backbone networks with QoS assurances.	Instead of providing a solution to the issue, it just makes an assumption and a proposal.
Beyene, A.M., et al., [8]	Differentiated service (DiffServ),	End-to-end QoS was achieved using DiffServ models, which led to lower end-to-end latency, guaranteed QoS over IP/MPLS networks, and greater VPN throughput.	The researcher only uses Layer 3 VPN, although he can also implement Layer 2 VPN because VPN services include both Layer 2 and Layer 3 VPN.
Jeevan, K., et al., [14]	Differentiated service (DiffServ),	MPLS decreases latency, jitter, and packet delay only for voice communication.	It assesses the outcome for ITU QoS of network metrics like latency, jitter, packet delay, and loss but does not identify the QoS technique.
Rilke, N., et al., [15]	Queuing policies in Differentiated service (DiffServ)	It is intended to deliver a guaranteed quality of service by utilizing MPLS and DiffServ technology (QoS).	The researcher does not apply VRF to isolate customers and the sharing of IP addresses. not implement traffic engineering (TE) to control traffic.

Table 2.2 Summary and Gap Analysis from Related Works

Ref.	Routing Technology	QoS Feature	Metrics Used	Network Features	Improvement Achieved	Gap Analysis
Beyene, A.M., et al., [8]	Differentiated service (DiffServ), weighted fair queueing, weighted random early detection, eNSP, and Wireshark	To provide users with adequate services, bandwidth management, controlled jitter, latency, and better packet loss characteristics are used.	Delay, Jitter, packet loss, and traffic utilization	The network can expand in the future to include more dependability features.	used to achieve end-to-end QoS, decreased end-to-end latency, guaranteed QoS over IP/MPLS networks, and higher VPN throughput.	The researcher doesn't use L2VPN; only L3VPN is implemented with QoS.
Mushtaq, A., et al., [4]	MPLS introduction, MPLS VPN, Traffic Engineering, MPLS QoS in MPLS IP backbone, and GNS3 for simulator	For the purpose of ensuring MPLS QoS delivery with minimal jitter and fixed bandwidth	Jitter and bandwidth	IP network at the edges achieves the core network, robustness of routing protocol, and scalability.	It is intended to deliver a guaranteed quality of service by utilizing MPLS and DiffServ technology (QoS).	The researcher did not focus on QoS models.
Rilke, N., et al., [15]	MPLS protocol and queueing policies	provision of the end-to-end QoS over Virtual Private Networks (VPN)	Latency, jitter, and packet delay	flexible and scalable network	analyze the end-to-end QoS requirements for different traffic types are being met.	The researcher does not apply VRF to isolate customers and the sharing of IP addresses.
Jeevan, K., et al., [14]	MPLS VPN-TE & DiffServ Model.	MPLS has the capacity to provide Traffic Engineering (TE), which is essential for reducing congestion and use of the network	Latency, jitter, end-to-end delay, and packet delay	The ability of routing systems to balance and manage network resources.	Compared to using TE exclusively for voice traffic, MPLS reduces latency, jitter, and packet delay.	It assesses the outcome for ITU QoS of the network but does not identify the QoS technique.
Kanchan, D., et al., [19]	Next Generation Network (MPLS), (QoS), Label Switch Router (LSR), Label Edge Router (LER).	offer high-quality services end-to-end	low throughput and high latency, jitter	Simple, scalable, dynamic, and fast failure node recovery network features	They offer the design for design of an MPLS VPN network with traffic engineering.	More concentrated on the Review than it was on providing a resolution.



## **Chapter Three**

### **Simulation Design and Analysis**

#### **3.1 Introduction**

The suggested NGN network architecture is easily saleable by simply adding new network devices. There are three types of routers in the proposed network design solution: two P, four PE, and two CE routers. Backbone routers are P routers. It manages public network routing information and provides MPLS label forwarding. PE routers are linked directly to CE routers. PE routers maintain and process VPN route information, forward VPN traffic, and operate MP-BGP and MPLS protocols. It has also performed label popping and imposition. CE routers are the edge routers that link to client routers or personal computers (PCs).

As shown, a simple network architecture is used in this study (Fig. 3.1). It describes the key phases in designing the QoS of a BGP MPLS VPN network. The New Generation Network (NGN) network architecture was chosen based on the needs for network design with service provisioning and end-to-end QoS implementation.

#### **3.2 Simulation Tools**

The scenario will be implemented using the Graphical Network Simulator 3 simulation application (GNS3). The GNS3 platform is a graphical network simulator that allows for the design of complex network topologies as well as the process of testing a designed model on a platform that simulates the real world. It can also be used to experiment with Cisco IOS features or to test configurations that will be deployed later on real routers. could select a newer Router model with additional features.

#### **3.3 Simulation Network Topology**

There are two P (Provider) routers, four PE (Provider Edge) routers, and two CE routers in the Provider's core (see Figure 3.1). It manages public network routing information and provides MPLS label forwarding. PE routers are linked directly to CE routers. PE routers maintain and process VPN route information, forward VPN traffic, and operate MP-BGP and MPLS protocols. It has also performed label popping and imposition. CE routers are the edge routers that link to client routers or personal computers (PCs).

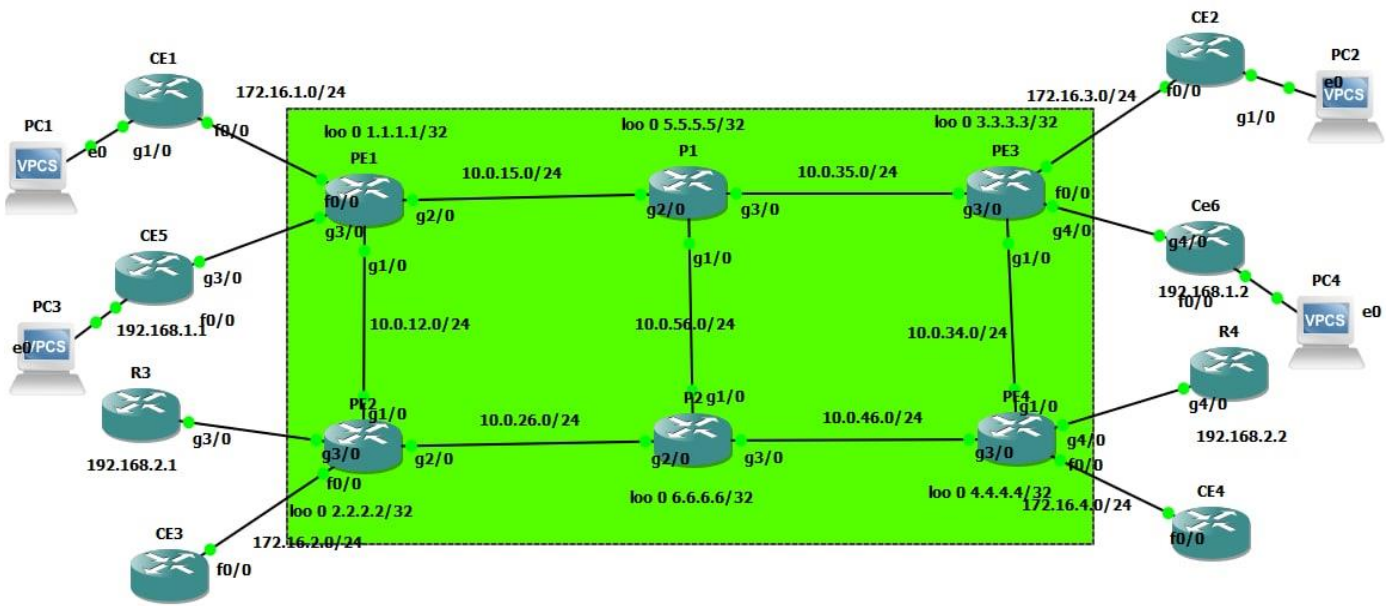


Figure 3.1: Simplified Proposed BGP MPLS VPN network architecture with end-to-end QoS.

Traffic is generated by VPN A and VPN B routers. Two VPNs (both VPN A and VPN B) were tested. Both employ MPLS for the OSPF and use the IGP protocol to advertise their subnets to the Routers of the Core network between them (such as directly connected networks and Loopback IP addresses). Both VPNs make use of the same networking hardware. Both VPN models use comparable connectivity and interfaces. In both methods, QoS is applied to network traffic in a similar manner.

Secure service routers are used to build access and aggregation networks. Because of the MPLS architecture, they are operating in multiprotocol label popping and positioning mode rather than the typical packet flow. The gadgets employ Gigabit Ethernet interfaces. The connections to the core networks are Gigabit Ethernet, and the connections to the end devices are also Gigabit Ethernet.

QoS is applied to traffic from end devices by access and aggregation routers. The two VPN routers generate traffic. Wireshark is used for checking the QoS applied in the traffic flow. These modules perform functions such as random traffic generation, fixed or variable packet size, and concurrent generation of various traffic flows.

The following description includes the uniform network entities for both VPN networks of the BGP MPLS VPN topologies examined. These modules include IP address allocation, interface connections, and setup, as well as the network's QoS.

### 3.3.1 IP addresses

IP addresses to be used for all Routers and CEs in this scenario are as the following and all ports are configured by them.

Table 3.1: IP addressing scheme of the designed network architectures

IP addresses for each Router and CEs				
Device	Port	IP Address	Loopback	Gateway
P1	g2/0	10.0.15.5	5.5.5.5	-
	g3/0	10.0.35.5		-
	g1/0	10.0.56.5		-
P2	g2/0	10.0.26.6	6.6.6.6	-
	g3/0	10.0.46.6		-
	g1/0	10.0.56.6		-
PE1	g2/0	10.0.15.1	1.1.1.1	-
	g1/0	10.0.12.1		-
	f0/0	172.16.1.1		-
	g3/0	-		-
PE2	g2/0	10.0.26.2	2.2.2.2	-
	g1/0	10.0.12.2		-
	f0/0	172.16.2.1		-
	g4/0	-		-
PE3	g3/0	10.0.35.3	3.3.3.3	-
	g1/0	10.0.34.3		-
	f0/0	172.16.3.1		-
	g3/0	-		-
PE4	g1/0	10.0.34.4	4.4.4.4	-
	g3/0	10.0.46.4		-
	f0/0	172.16.4.1		-
	g4/0	-		-
CE1	f0/0	172.16.1.2	-	172.16.1.1/24
CE2	f0/0	172.16.2.2	-	172.16.2.1/24
CE3	f0/0	172.16.3.2	-	172.16.3.1/24
CE4	f0/0	172.16.4.1	-	172.16.4.1/24
CE5	g3/0	192.168.1.1	-	-
CE6	g4/0	192.168.1.2	-	-
CE7	g3/0	192.168.2.1	-	-
CE8	g4/0	192.168.2.1	-	-

The loop IP addresses are used to establish a transport control protocol (TCP) peer with neighbors in the MPLS network.

### **3.3.2. Configuration of an IP address for each interface**

Private IPV4 address class A is utilized for the link between CE, PE, and P. This address range is subnet into IP address spaces across distinct CE, PE, and P interfaces, as well as Loopback IP addresses. The IP addresses listed below are being used for this research.

#### **Configure PE 1**

##### **For L3VPN service**

```
PE1(config)#mpls ip
PE1(config)#interface gigabitEthernet 2/0
PE1(config-if)#ip address 172.16.1.1 255.255.255.0
PE1(config-if)#ip ospf 1 area 0
PE1(config-if)#mpls ip
PE1(config-if)#end
PE1#
```

##### **For L2VPN services**

Enter configuration commands, one per line. End with CNTL/Z.

```
R1(config)#interface GigabitEthernet3/0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)#
R1(config-if)#end
R1#
```

The QoS policy applied to the interfaces has formed the interfaces between the core, aggregation, and access routers.

### **3.3.3. Interior Gateway Protocol (IGP) Interconnection**

In the intended network, the OSPF protocol was used to connect P and PE routers.

This is because the OSPF protocol is more convergent. The most typical format for configuring the OSPF protocol is as follows.

```
PE1#
PE1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
PE1(config)#router ospf 1
```

```
PE1(config-router)#network 172.16.1.0 0.0.0.255 area 0
PE1(config-router)#end
PE1#
```

### 3.3.4. MPLS and MP BGP Interconnection

For label switching and distribution, the MPLS protocol is utilized. The most frequent format for configuring MPLS globally is as follows.

```
PE1#conf t
PE1(config)#mpls ip
PE1(config)#end
PE1#
```

The MP BGP protocol is used to establish peer relationships between various types of routers. The most frequent format for configuring MP BGP is as follows.

```
PE1#conf t
PE1(config)#router bgp 65000
PE1(config-router)# neighbor 3.3.3.3 remote-as 65000
PE1(config-router)# neighbor 3.3.3.3 update-source Loopback0
PE1(config-router)# neighbor 4.4.4.4 remote-as 65000
PE1(config-router)# neighbor 4.4.4.4 update-source Loopback0
PE1(config-router)# address-family vpnv4
PE1(config-router-af)# neighbor 3.3.3.3 activate
PE1(config-router-af)# neighbor 3.3.3.3 send-community extended
PE1(config-router-af)# neighbor 4.4.4.4 activate
PE1(config-router-af)# neighbor 4.4.4.4 send-community extended
PE1(config-router-af)# exit-address-family
PE1(config-router)#
```

#### For L2VPN service

```
PE1#configure t
Enter configuration commands, one per line. End with CNTL/Z.
PE1(config)#inte
PE1(config)#interface GigabitEthernet3/0
PE1(config-if)#xconnect 3.3.3.3 101 encapsulation mpls pw-class L2VPN
PE1(config-if-xconn)#end
PE1#
```

### 3.4. Designed QoS of Proposed network architectures

QoS guarantee is built utilizing reasonable scheduling and congestion avoidance approaches based on current resources. Based on the current VPN services, the differentiated service model (DiffServ) has been utilized to classify, mark, and shape the networks. This can be accomplished by following step-by-step procedures.

- Define access control list (ACL) rules
- Define traffic classifiers
- Define traffic behaviors
- Define traffic policies and
- Apply traffic policies to interfaces

For the initial design and evaluation of QoS assurance, fundamental BGP MPLS VPN specified circumstances must be used.

#### 3.4.1. Define Access Control List rules

ACLs are used to specify which VPNs are granted in order to provide the required service quality within the time frame. Create ACL rules. Configure complicated traffic classification on CE routers to regulate traffic from local networks to CEs. The most frequent format for defining ACL is as follows.

For L3VPN service

```
PE1#conf t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
PE1(config)#ip access-list extended VPN_A_qos
```

```
PE1(config-ext-nacl)# permit ip 172.16.1.0 0.0.0.255 172.16.3.0 0.0.0.255
```

```
PE1(config-ext-nacl)#end
```

```
PE1#
```

L2VPN service

```
PE1#conf t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
PE1(config)#pseudowire-class L2VPN
PE1(config-pw-class)# encapsulation mpls
PE1(config-pw-class)#end
PE1#
```

### 3.4.2. Apply the traffic policies

Using pre-configured policies on inbound interface routers. Predefined policies are used to ensure service needs. The most common format for applying traffic regulations to inbound interfaces is as follows.

```
PE1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
PE1(config)#policy-map VPN_A_qos
PE1(config-pmap)# class VPN_A_qos
PE1(config-pmap-c)# set dscp ef
PE1(config-pmap-c)# set mpls experimental topmost 5
PE1(config-pmap-c)#
PE1(config-pmap-c)#end
PE1#
PE1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
PE1(config)#interface GigabitEthernet2/0
PE1(config-if)#
PE1(config-if)# service-policy output VPN_A_qos
PE1(config-if)#
PE1(config-if)#end
PE1#
```

## Chapter Four

### Simulation Result and Analysis

#### 4.1 Experimental Result and Analysis

The proper functioning of the designed VPN QoS network architectures includes:

- All protocols are fully operating and Proper implementation of the designed VPN QoS.
  - Provisioning of the necessary services ensuring L2VPNs and L3VPNs operation and
  - Redundancy of network resources, which includes rerouting in case of link or node failure.
- The requirements for meeting these requirements have been described, as have the applicable tests for each of them. To be trusted with the proper operation of the network, the basic components must first be checked.

##### 4.1.1. IGP protocol (OSPF)

The proposed designs first validate the OSPF operation. Because it is one of the fundamental components of the created models. OSPF routing protocol verification includes testing its routing information, established neighbors, link-state database, and OSPF-enabled interface. The "display IP route" command is used to inspect the OSPF routing information. It determines whether routes have been learned by other routers. Route data covers all direct routes as well as routes to loopback interfaces.

```
PE1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

 1.0.0.0/32 is subnetted, 1 subnets
 C    1.1.1.1 is directly connected, Loopback0
 3.0.0.0/32 is subnetted, 1 subnets
 O    3.3.3.3 [110/3] via 10.0.15.5, 00:20:12, GigabitEthernet2/0
 5.0.0.0/32 is subnetted, 1 subnets
 O    5.5.5.5 [110/2] via 10.0.15.5, 00:20:12, GigabitEthernet2/0
10.0.0.0/24 is subnetted, 5 subnets
 C    10.0.15.0 is directly connected, GigabitEthernet2/0
 C    10.0.12.0 is directly connected, GigabitEthernet1/0
 O    10.0.34.0 [110/3] via 10.0.15.5, 00:20:12, GigabitEthernet2/0
 O    10.0.35.0 [110/2] via 10.0.15.5, 00:20:12, GigabitEthernet2/0
 O    10.0.56.0 [110/2] via 10.0.15.5, 00:20:12, GigabitEthernet2/0
PE1#
```

Figure 4.1: This shows the IS-IS route information.



The output of these commands connects each router to the loopback addresses of the other devices, which is required for the other components of the proposed network to function properly.

The router results indicate that the OSPF protocol successfully established its network link-state database and routing table.

#### 4.1.2. MPLS LDP Operation

MPLS operation is checked by verifying its routing information, MPLS link-state protocol, and MPLS adjacency. The "display MPLS LDP neighbor" command is used to inspect the MPLS routing information.

```
PE1#show mpls ldp neighbor
Peer LDP Ident: 5.5.5.5:0; Local LDP Ident 10.0.15.1:0
TCP connection: 5.5.5.5.646 - 10.0.15.1.31837
State: Oper; Msgs sent/rcvd: 36/34; Downstream
Up time: 00:21:15
LDP discovery sources:
  GigabitEthernet2/0, Src IP addr: 10.0.15.5
Addresses bound to peer LDP Ident:
  10.0.56.5      10.0.15.5      5.5.5.5      10.0.35.5
PE1#
```

Figure 4.2: This shows the MPLS adjacency information.

The router is set up to send the data explicitly on the designated path. The router interfaces are completely operational. From. MPLS generates a distinct routing table to deliver Layer 2 and Layer 3 VPN services. For data forwarding, the pathways are labeled differently. LSP is set to create routing table entries with information about the metrics of the various paths.

#### 4.1.3. BGP Protocol Operation

BGP operation is checked by testing its route information. The "show ipv4 unicast summary" command is used to inspect the BGP neighbor relationship information.

```
PE1#show bgp vpnv4 unicast all summary
BGP router identifier 10.0.15.1, local AS number 65000
BGP table version is 5, main routing table version 5
2 network entries using 280 bytes of memory
2 path entries using 136 bytes of memory
3/2 BGP path/bestpath attribute entries using 372 bytes of memory
1 BGP extended community entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 1) using 32 bytes of memory
BGP using 844 total bytes of memory
BGP activity 3/1 prefixes, 3/1 paths, scan interval 15 secs

Neighbor      V      AS MsgRcvd MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
3.3.3.3       4 65000    27     28      5     0     0 00:22:19      1
4.4.4.4       4 65000     2      5      5     0     0 00:00:16      0
PE1#
```

Figure 4.3: Shows BGP neighbor relationship.

BGP is now fully operating and has a neighbor relationship. BGP sessions are now in place. The VPN L2VPN and L3VPN groups have been correctly indicated. The end router traffic is appropriately forwarded, and the routers in the L2VPN and L3VPN services communicate with one another.

#### 4.1.4. VPNs QoS Operation

Different parameters and methods are used to test VPN QoS operation. The following are the fundamental VPN QoS functioning confirmation methods.

To check the operation access list defined “show access-list” command is used.

```
PE1#show access-lists
Extended IP access list VPN_A_qos
 10 permit ip 172.16.1.0 0.0.0.255 172.16.3.0 0.0.0.255 (5 matches)
PE1#
```

Figure 4.4: This shows the Access-list operation.

To check the class-map “show class map” command is used.

```
PE1#show class-map
Class Map match-any class-default (id 0)
  Match any

Class Map match-all VPN_A_qos (id 1)
  Match access-group name VPN_A_qos

PE1#
```

Figure 4.5: This shows the Class map operation

To check policy-map differentiated service code point (DSCP) the traffic captured using Wireshark on bound Interfaces.

```
CE1#ping 172.16.3.2 repeat 100
Type escape sequence to abort.
sending 100, 100-byte ICMP Echos to 172.16.3.2, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 124/205/300 ms
CE1#
```

Figure 4.6: Shows How differentiated service code point (DSCP) operation.

```

> Frame 1049: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface -, id 0
> Ethernet II, Src: ca:03:48:ac:00:54 (ca:03:48:ac:00:54), Dst: ca:05:3c:ec:00:54 (ca:05:3c:ec:00:54)
v MultiProtocol Label Switching Header, Label: 500, Exp: 5, S: 0, TTL: 255
  0000 0000 0001 1111 0100 .... = MPLS Label: 500
  ..... 101. .... = MPLS Experimental Bits: 5
  ..... 0 .... = MPLS Bottom Of Label Stack: 0
  ..... 1111 1111 = MPLS TTL: 255
v MultiProtocol Label Switching Header, Label: 105, Exp: 5, S: 1, TTL: 255
  0000 0000 0000 0110 1001 .... = MPLS Label: 105
  ..... 101. .... = MPLS Experimental Bits: 5
  ..... 1 .... = MPLS Bottom Of Label Stack: 1
  ..... 1111 1111 = MPLS TTL: 255
v Internet Protocol Version 4, Src: 172.16.3.1, Dst: 172.16.1.2
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
    Total Length: 100
    Identification: 0x003a (58)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 255
    Protocol: ICMP (1)
    Header checksum: 0x5e83 [validation disabled]
    [Header checksum status: Unverified]
    Source: 172.16.3.1
    Destination: 172.16.1.2
> Internet Control Message Protocol

```

Figure 4.7: Defined QoS.

#### 4.1.5. Performance among L2VPN Service

The L2VPN services are fully functional. To check detailed routing information of them ping reachability is checked.

```

R1#ping 192.168.1.2 repeat 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 120/155/184 ms
R1#

```

Figure 4.8: Shows L2VPN call service operation.

No.	Time	Source	Destination	Protocol	Length	Info
3392	2178.128833	192.168.1.1	192.168.1.2	ICMP	140	Echo (ping) request id=0x0009, seq=94/24064, ttl=255 (reply in 3393)
3393	2178.179374	192.168.1.2	192.168.1.1	ICMP	136	Echo (ping) reply id=0x0009, seq=94/24064, ttl=255 (request in 3392)
3394	2178.209704	192.168.1.1	192.168.1.2	ICMP	140	Echo (ping) request id=0x0009, seq=95/24320, ttl=255 (reply in 3395)
3395	2178.260244	192.168.1.2	192.168.1.1	ICMP	136	Echo (ping) reply id=0x0009, seq=95/24320, ttl=255 (request in 3394)
3396	2178.290570	192.168.1.1	192.168.1.2	ICMP	140	Echo (ping) request id=0x0009, seq=96/24576, ttl=255 (reply in 3397)
3397	2178.341095	192.168.1.2	192.168.1.1	ICMP	136	Echo (ping) reply id=0x0009, seq=96/24576, ttl=255 (request in 3396)
3398	2178.371418	192.168.1.1	192.168.1.2	ICMP	140	Echo (ping) request id=0x0009, seq=97/24832, ttl=255 (reply in 3399)
3399	2178.421995	192.168.1.2	192.168.1.1	ICMP	136	Echo (ping) reply id=0x0009, seq=97/24832, ttl=255 (request in 3398)
3400	2178.452334	192.168.1.1	192.168.1.2	ICMP	140	Echo (ping) request id=0x0009, seq=98/25088, ttl=255 (reply in 3401)
3401	2178.502937	192.168.1.2	192.168.1.1	ICMP	136	Echo (ping) reply id=0x0009, seq=98/25088, ttl=255 (request in 3400)
3402	2178.533337	192.168.1.1	192.168.1.2	ICMP	140	Echo (ping) request id=0x0009, seq=99/25344, ttl=255 (reply in 3403)
3403	2178.584003	192.168.1.2	192.168.1.1	ICMP	136	Echo (ping) reply id=0x0009, seq=99/25344, ttl=255 (request in 3402)

```

> Frame 3401: 136 bytes on wire (1088 bits), 136 bytes captured (1088 bits) on interface -, id 0
> Ethernet II, Src: ca:05:3c:ec:00:38 (ca:05:3c:ec:00:38), Dst: ca:01:49:18:00:38 (ca:01:49:18:00:38)
> MultiProtocol Label Switching Header, Label: 100, Exp: 0, S: 1, TTL: 254
> PW Ethernet Control Word
> Ethernet II, Src: ca:0a:56:94:00:70 (ca:0a:56:94:00:70), Dst: ca:09:38:6c:00:54 (ca:09:38:6c:00:54)
v Internet Protocol Version 4, Src: 192.168.1.2, Dst: 192.168.1.1
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
    Total Length: 100
    Identification: 0x01ac (428)
    > Flags: 0x0000
    Fragment offset: 0
    Time to live: 255
    Protocol: ICMP (1)
    Header checksum: 0x35e1 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.2
    Destination: 192.168.1.1
  > Internet Control Message Protocol

```

Figure 4.9: Defined QoS.

When the VPN QoS of the proposed network architecture was tested using Wireshark, several parameters such as an MP-BGP MPLS, VPN, TE, and Diffserv traffic classification, policing, and shaping was found to be fully functioning.

#### 4.1.6. Performance among L3VPN Service

The L3VPN services are fully functional. To check detailed routing information of them ping reachability is checked.

```

CE3#ping 172.16.3.2 repeat 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 172.16.3.2, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 192/348/468 ms
CE3#

```

Figure 4.10: Shows L3VPN service operation.

```

No.    Time           Source           Destination      Protocol  Length  Info
-----
4572  3601.913886    172.16.3.2      172.16.2.2      ICMP     122     Echo (ping) reply  id=0x0002, seq=86/22016, ttl=254 (request in 4570)
+ 4573  3602.195782    172.16.2.2      172.16.3.2      ICMP     118     Echo (ping) request id=0x0002, seq=87/22272, ttl=254 (reply in 4574)
- 4574  3602.354763    172.16.3.2      172.16.2.2      ICMP     122     Echo (ping) reply  id=0x0002, seq=87/22272, ttl=254 (request in 4573)
- 4575  3602.636731    172.16.2.2      172.16.3.2      ICMP     118     Echo (ping) request id=0x0002, seq=88/22528, ttl=254 (reply in 4576)

> Frame 4573: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface -, id 0
> Ethernet II, Src: ca:05:3c:ec:00:54 (ca:05:3c:ec:00:54), Dst: ca:03:48:ac:00:54 (ca:03:48:ac:00:54)
v MultiProtocol Label Switching Header, Label: 305, Exp: 0, S: 1, TTL: 252
  0000 0000 0001 0011 0001 ..... = MPLS Label: 305
  ..... = MPLS Experimental Bits: 0
  ..... = MPLS Bottom Of Label Stack: 1
  ..... 1111 1100 = MPLS TTL: 252
v Internet Protocol Version 4, Src: 172.16.2.2, Dst: 172.16.3.2
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 100
  Identification: 0x011f (287)
  > Flags: 0x0000
  Fragment offset: 0
  Time to live: 254
  Protocol: ICMP (1)
  Header checksum: 0x5e55 [validation disabled]
  [Header checksum status: Unverified]
  Source: 172.16.2.2
  Destination: 172.16.3.2
> Internet Control Message Protocol

```

Figure 4.11: Defined QoS.

## 4.2. Representation of Experimental Discussions with Table and Graph

In terms of devices and physical connections, the present and planned network designs are identical. However, there are distinctions, particularly in QoS design. Table 4.1 details the similarities and differences between the existing and planned network architectures.

Table 4.1 The similarities and differences between existing and proposed network architecture.

	Exit Network Architecture	Proposed Network Architecture
Traffic Type	BGP MPLS VPN	BGP MPLS VPN
Service Type	L2VPN and L3VPN	L2VPN and L3VPN
IGP Routing Protocol	OSPF	OSPF
NGN Backbone	MPLS	MPLS
QoS Model	Best effort model	Differentiated services model
Congestion Management	FIFO	Weighted fair queueing

DiffServ QoS is used in the suggested network design for VPN QoS. Distinct modes of transportation have different priorities. The more traffic processed first. For congestion management, the architecture employs a weighted fair queueing algorithm, and for congestion avoidance, a weighted random early detection algorithm. In this situation, the traffic was categorized and given priority based on its customer level. Then, on an aggregation router's outward interface, traffic policies were designed and applied. The generated traffic in this example comprises two VPN instance application traffic streams. The two VPN instance traffic flows represent two end nodes that are linked to the CE routers. TCP is used for the traffic streams, which have speeds of 10 and 15 Mbps, respectively. The first test is performed between CE1 and CE2 routers, the second test is performed between CE3 and CE4 routers for L3VPN services and CE5 and CE6 routers, and the second test is performed between CE7 and CE8 routers for L2VPN services. This experiment's results are shown in Fig.4.12.

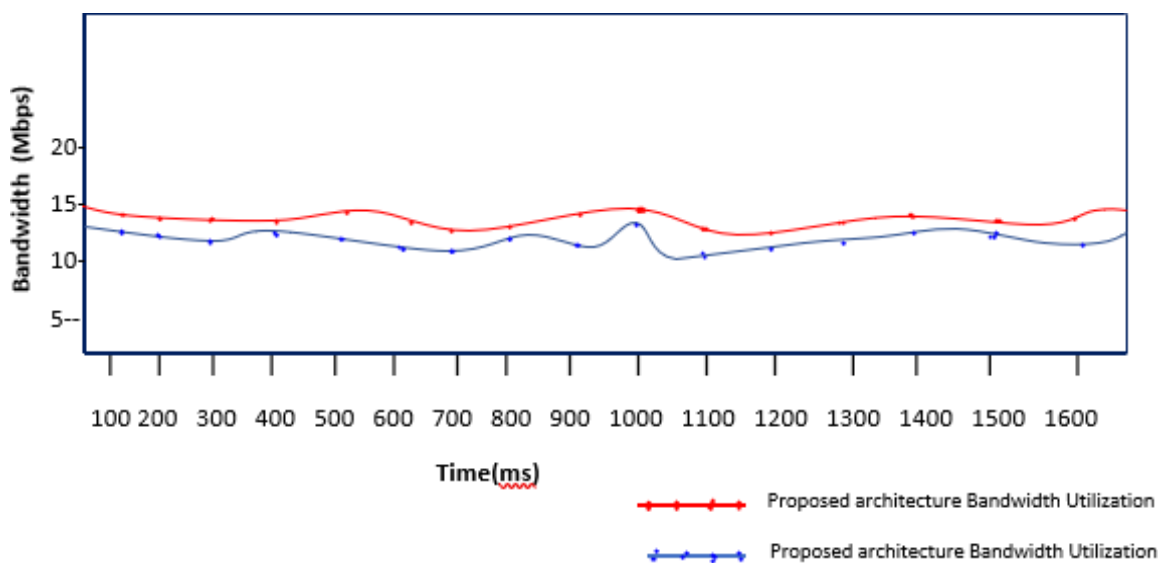


Figure 4.12: Bandwidth Utilization Measurement Comparison

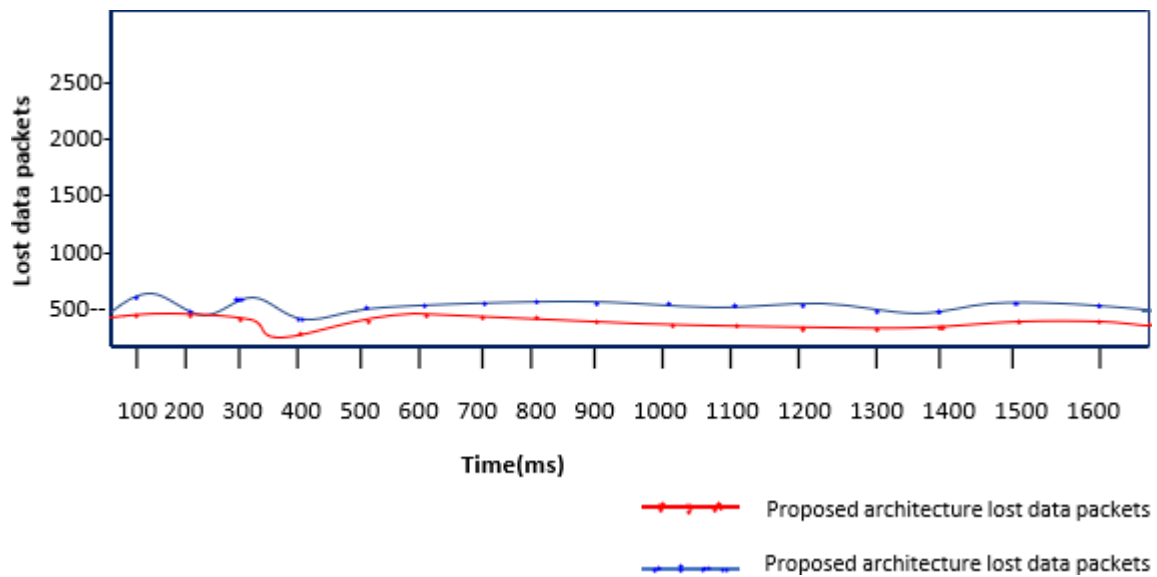


Figure 4.13: Packet Loss Measurement Comparison.

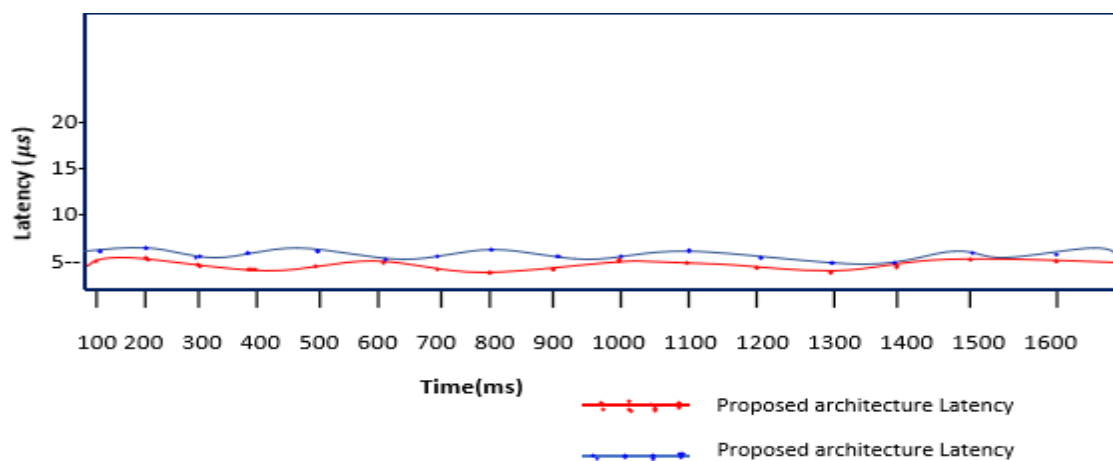


Figure 4.14: Latency Measurement Comparison.

As shown in the assessment testing of Fig.4.12, Fig.4.13 and Fig.4.14, the suggested network topologies, the implementation of DiffServ has numerous advantages for packet loss when compared to the best effort. DiffServ model routers must save traffic and QoS data every aggregation. This provides sufficient buffer space in the routers' queue. Incoming interface buffers, system buffers, and outgoing interface buffers are common on routers. In the event of congestion, traffic is marked and stored in buffer space to avoid packet loss. However, in the best-effort QoS paradigm, routers simply route packets until they reach their destination. Other packets are discarded, resulting in a greater percentage of packet loss.

The DiffServ QoS approach has advantages in terms of minimizing traffic loss. In the event of traffic congestion, this model prioritizes the traffic. The traffic is labeled and shaped based on the router's maximum data transmission rate. Some traffic is transferred, while excess traffic is noted and transmitted later. The packet loss ratio is reduced as a result.

The latency is the amount of time that a packet waits before being sent. The proposed network architecture has reduced latency than the existing network architecture. This is because the DiffServ paradigm can guarantee traffic per aggregation.

The latency is the time that a packet waits before being transmitted. It can be seen from Figure 4.11 and Figure 4.12; the proposed network architecture shows lower latency compared to the existing network architecture. The reason for this is that the DiffServ model can guarantee the traffic per aggregation.

When we look at the numerical results obtained from both the existing and proposed network is shown in Table 4.1 and Table 4.1 and Table 4.2. Most of the results were as expected. The difference between delay and jitter in existing and proposed network architecture was visible.

Table 4.2 and Table 4.3 displays the numerical findings derived from both the current and proposed networks. The majority of the outcomes were as expected. The present and proposed network architectures differed in terms of packet loss and bandwidth. However, the difference between end-to-end delay and jitter was not discernible. This occurred because we only employed ten routers across both network designs. This speed up transmission, serialization, queueing, and processing. The difference became apparent as the number of routers (nodes) increased.



Table 4.2 Exist and proposed network architecture numerical QoS results for L2VPN service

Parameters	Exit Network (Best Effort)			Proposed Network (DiffServ)		
	Result	VPN Targets	ITU threshold	Result	VPN Targets	ITU threshold
Packet loss (%)	1.897%	Out of Range	Out of Range	0.026%	Within Range	Out of Range
Delay(sec)	0.192 %	Within Range	Out of Range	0.12 %	Within Range	Within Range
Jitter (sec)	0.0056%	Within Range	Out of Range	0.0007747%	Within Range	Within Range

Table 4.3 Exist and proposed network architecture numerical QoS results for L3VPN service

Parameters	Exit Network (Best Effort)			Proposed Network (DiffServ)		
	Result	VPN Targets	ITU threshold	Result	VPN Targets	ITU threshold
Packet loss (%)	1.897%	Out of Range	Out of Range	0.026%	Within Range	Out of Range
Delay(sec)	0.12%	Within Range	Out of Range	0.029%	Within Range	Within Range
Jitter (sec)	0.0013%	Within Range	Out of Range	0.00035%	Within Range	Within Range

## **Chapter Five**

### **Conclusions and Future Works**

#### **4.1. Conclusions**

In this research, the DiffServ model for the design of BGP MPLS VPN (L2VPN and L3VPN) networks with end-to-end QoS was debated. This sort of network is suitable for the implementation of QoS for VPN networks. A simple network topology was constructed, network architectures were conceived, implemented, and assessed utilizing generic telecommunication equipment. First, the current BGP MPLS VPN network which employed the best-effort QoS model was easy installed and tested. Secondly, the proposed BGP MPLS VPN architecture which used the DiffServ QoS model was created and tested. End-to-end QoS was created and implemented in both network types. The implemented services were Layer 2 VPN and Layer 3 VPN services to manage traffic from end nodes in the proposed architecture. Both network designs were fully functioning. Verification of the applied end-to-end QoS settings was made and results were received.

Bandwidth usage, packet loss, delay, and jitter measurements were done for the network model (Fig.3.1). Following the completion of all assessments, it is clear that the proposed BGP MPLS VPN network architecture has significantly more benefits because the network allows for the classification of services and traffic engineering, which aids in better traffic management and the deployment of appropriate end-to-end QoS. The proposed BGP MPLS VPN architecture which employed DiffServ QoS model architecture might be applied in various mission-critical applications. The ability to easily scale the network is extremely beneficial in today's quickly increasing VPN networks. Because of the low latency and packet loss throughout the network, this technique is appropriate for higher-priority services.

Better network productivity can be gained using the proposed DiffServ QoS model. The developed BGP MPLS VPN architecture which uses DiffServ QoS model network architecture is easy to scale and debug. The insertion of new network end devices is simplified, with just minor configuration changes necessary. The problem of a rapidly diminishing number of accessible ASs is avoided by employing a single AS number in the core network design. The influence on network flow is eliminated due to the installed failure procedures in the event of a link failure. To reduce traffic loss, traffic entering the network is routed over backup routes while new paths are created.

With the careful design of the applied QoS, the traffic requirements of the implemented applications are served.

All services received the appropriate traffic handling in the proposed BGP MPLS VPN design, which utilized the DiffServ QoS model architecture. The BGP MPLS VPN network model that was created can easily be used for L2VPN and L3VPN services in both centralized and distributed architectures. End-to-end MPLS solutions for NGN applications are provided with ease.

In general, we find that the DiffServ QoS model was more dependable than the best-effort QoS model for the Telecommunication BGP MPLS VPN network based on the analysis and results obtained. The key work that passed through the study process was traffic engineering, network optimization, and proper network use. The developed QoS used the DiffServ paradigm, which guaranteed all of the company's VPN QoS thresholds. Finally, the developed network offers a method of boosting network performance based on the DiffServ QoS paradigm. A high QoS service provider has a high network performance. Customers who receive high-quality service are satisfied and have a positive experience.

## **5.2. Future Works**

At the level of this activity, the QoS has been ensured with respect to the company's SLA QoS target. But in the future, the network can be extended with more reliable functions. These functions include chassis clustering for access and aggregation devices, high availability feature implementation, and LDP implementation for MPLS label down streaming on demand. Extended DiffServ services with more application-specific QoS can be implemented. EVPN and segment routing can be included as a service in the network architecture. This can increase the scalability, availability, and managed network

## References

- [1] H. Kumera, "Analysing Impact of Seamless MPLS on QoS," AAiT, 2018.
- [2] T. Hobfeld, R. Schatz, M. Varela, and C. Timmerer, "Challenges of QoE management for cloud applications," *IEEE Communications Magazine*, vol. 50, no. 4, pp. 28–36, 2012.
- [3] Dr. Ahmad A., Talal A." Performance Analysis DiffServ based Quality of Service in MPLS Network's", *International Journal of Scientific and Engineering Research*, Volume 6, September 2015.
- [4]. A. B. Mushtaq Ahmed, "Implementation of Traffic Engineering and Addressing," *International*, vol. Vol 5, no. 6, pp. 9-14, June 2014
- [5]. EthioTelecom, "QoS Document" MPLS VPN Services Quality and Customer Experience Related Issues and Complaint Analysis, Version 02, 2017.
- [6]. Huawei technologies co. ltd, "Configuration Guide VPN", Huawei technologies- Cloud Engine 12800 Series Switches, volume 06, September 2017.
- [7]. MPLSs based VPN Internet: Introduction to Cisco MPLS VPN Technology - Cisco, July 07, 2022
- [8] Beyene, A.M., et al., "Improving Quality of Service of Border Gateway Protocol Multiprotocol Label Switching Virtual Private Network of EthioTelecom Service Level Agreements," vol. vol 1026, 02 August 2019.
- [9] H Lee, J Hwang, B Kang, and K Jun, "End-To-End QoS Architecture for VPNs: MPLS VPN Deployment in a Backbone Network," pp. 479-483, 02 April 2000.
- [10] Hang, R. K., et al., *Building MPLS VPNs with QoS Routing Capability*. (S. 1. Telscom AG, Ed.) , 28 September 2001
- [11]. K Okokpujie, O Shobayo. "Performance of MPLS-based virtual private networks and classic virtual private networks using advanced metrics," pp. 2073-2081, 2018).
- [12]. Mushtaq A. et al, in. "Implementation of Traffic Engineering and Addressing QoS in MPLS VPN Based IP Backbone", *International Journal of Computer Science and Telecommunications*, Volume 5, June 2014.
- [13] S. Yadav and A. Jeyakumar, "Design of traffic engineered MPLS VPN for protected traffic using GNS simulator," *Proc. 2016 IEEE Int. Conf. Wirel. Commun. Signal Process.*

Networking, WiSPNET 2016, pp. 405–409, 2016, doi: 10.1109/WiSPNET.2016.7566165.

[14]. J.Kharel and D.Adhikari, “Performance Evaluation of Voice Traffic over MPLS Network with TE and QoS Implementation”, MS. Thesis University of Karlskrona, Sweden, PP 144,November 2011.

[15]. N. Rikli, S. Almogari, "Efficient priority schemes for the provision of end-to-end quality of service for multimedia traffic over MPLS VPN networks," vol. Vol 25, pp. 89-98, 1 January 2013.

[16]. D Zhang, D. I. QoS performance analysis in deployment of DiffServ-aware MPLS Traffic Engineering. 963-967, 2007.

[17] B. Soewito, F. E. Gunawan, S. Afdhal, and A. Antonyova, “Analysis of quality network using MPLS and non MPLS,” 2017 Int. Semin. Intell. Technol. Its Appl. Strength. Link Between Univ. Res. Ind. to Support ASEAN Energy Sect. ISITIA 2017 - Proceeding, vol. 2017-Janua, pp. 1–4, 2017, doi: 10.1109/ISITIA.2017.8124044.

[18] N. S. Rajput, “Investigation of Multi-Protocol Label Switching for Intelligent Transportation Systems,” 2019 6th Int. Conf. Signal Process. Integr. Networks, SPIN 2019, pp. 230–233, 2019, doi: 10.1109/SPIN.2019.8711718.

[19] C. Risso, C. Mayr, and E. Grampin, “A Combined BGP and IP/MPLS Resilient Transit Backbone Design,” Proc. 2019 11th Int. Work. Resilient Networks Des. Model. RNDM 2019, pp. 1–8, 2019, doi: 10.1109/RNDM48015.2019.8949099.

[20]. J. Lawrence, “Designing Multiprotocol Label Switching Networks”, Communications Magazine, IEEE, July 2012.

[21]. V.Alwayn,” Advanced MPLS Design and Implementation”, Cisco Systems, Cisco press 201, 2011.

[22]. Shahid A., Bilal Z. R., “OPNET Analysis of VoIP over MPLS VPN with IP QoS”, MS. Thesis, Karlskrona University, Sweden, March 2011.

[23] A. Albdour ,G.Kannan “Analysis of MPLS and IP Networks Performance to Improve the Qos using Opnet Simulator ”, Journal of Emerging Trends in Computing and Information Sciences, Vol. 8 No. 1, pp 1-56, January 2017.

[24]. G. H. Sabri, “QoS in MPLS and IP Networks” M.B. Thesis, University of Karlskrona,

Sweden, 9th November 2009.

[25]. F. Alsoubaie “Voice over Internet Protocol (VoIP) Best Service Provider Decision Making with Using Hierarchical Decision Model (HDM)” BS.Degree project paper, Portland State University, Dec 2018.

[26]. G. H. Sabri, “QoS in MPLS and IP Networks” M.B. Thesis, University of Karlskrona, Sweden, 9th November 2009.

[27] A. Kumar, V. Kumar, R. Kumar, S. Srivastava, and R. K. Singh, “Performance evaluation of IP network and MPLS network using NS2 simulator,” 2015 1st Int. Conf. Futur. Trends Comput. Anal. Knowl. Manag. ABLAZE 2015, pp. 369–375, 2015, doi: 10.1109/ABLAZE.2015.7155022.

[28] A. Bahnasse, F. E. Louhab, H. Ait Oulahyane, M. Talea, and A. Bakali, “Novel SDN architecture for smart MPLS Traffic Engineering-DiffServ Aware management,” *Futur. Gener. Comput. Syst.*, vol. 87, pp. 115–126, 2018, doi: 10.1016/j.future.2018.04.066.

[29] S. Malisuwan, D. Milindavanij, and W. Kaewphanuekrungsi, “Quality of Service (QoS) and Quality of Experience (QoE) of the 4G LTE Perspective,” *Int. J. Futur. Comput. Commun.*, vol. 5, no. 3, pp. 158–162, 2016, doi: 10.18178/ijfcc.2016.5.3.463.

[30] W. Sugeng, J. E. Istiyanto, K. Mustofa, and A. Ashari, “The Impact of QoS Changes towards Network Performance,” *Int. J. Comput. Networks Commun. Secur.*, vol. 3, no. 2, pp. 48–53, 2015.

[31] A. Mushtaq and M. S. Patterh, “QOS parameter comparison of DiffServ-aware MPLS network using IPv4 and IPv6,” *Int. Conf. Recent Innov. Signal Process. Embed. Syst. RISE 2017*, vol. 2018-Janua, pp. 113–118, 2018, doi: 10.1109/RISE.2017.8378136.

[32] K. Varadhan, R. Govindan, and D. Estrin. Persistent route oscillations in inter-domain routing. IS1 technical report 96-631, USC/Information Sciences Institute, 1996.

[33] M. Zeeshan Gonda, "Traffic Engineering, QoS and MP-BGP VPNs in MPLS Networks," vol. 4, pp. 1-9, MAY 2013.

[34]. Huawei technologies co. ltd, “Configuration Guide VPN”, Huawei technologies- Cloud Engine 12800 Series Switches, volume 06, pp 5-7., Sept. 2017.

[35]. Cisco press “MPLS Traffic Engineering DiffServ Configuration Guide” Cisco Systems, Inc 2011.

[36] C. J. Ghyar, M. R. Shahade, S. V Bamb, and V. B. Mankar, “Basics of Quality of Services

(QoS),” vol. 4, no. 7, pp. 105–110, 2018.

[37] S. Malisuwan, D. Milindavanij, and W. Kaewphanuekrungsi, “Quality of Service (QoS) and Quality of Experience (QoE) of the 4G LTE Perspective,” *Int. J. Futur. Comput. Commune.*, vol. 5, no. 3, pp. 158–162, 2016, doi: 10.18178/ijfcc.2016.5.3.463.

[38]. Huawei Technologies, “How to configure MPLS VPN” MPLS with BGP, May 2017.

[39]. K. Lee, MS. Thesis, “Global QoS model in the ISP networks: DiffServ-aware MPLS Traffic Engineering”, 7 Nov 2006.

[40]. R. Braden, “Integrated Services in the Internet Architecture”, An Overview RFC 1633, June 2007.

[41] E. Kumsierek, B. Choi, Z. Duan and Z. Zhang, “An Integrated Network Resource and QoS Management Framework,” *IP Operations and Management, 2002 IEEE Workshop on*, 2002 pp. 68 - 72

[42] P.P White, “RSVP and Integrated Services on the Internet: A Tutorial,” *IEEE Communication Magazine* May 1997, PP. 100-106.

[43] S. Balck, D. Black, M. Carlson, E. Davis, Z. Wang and W. Wiess, “An Architecture for Differentiated Services,” RFC 2475 1998.

[44] Fgee, E., Kenney J., Phillips, W.I., Robertson, W., Sivakumar, S.,” Implementing an IPv6 QoS management scheme using flow label & class of service fields”, *IEEE CCECE 2004. Canadian Conference*, vol 2, May 4-7, 2004, pp.851 - 854.

[45] S. Shenker and J. Wroclawski,” General characterization Parameters for Integrated Service Network Elements,” RFC 2215 (proposed standard) IETF Sep. 1997.

[46] C. Metz,” IP QoS: Traveling in First Class on the Internet.”, *IEEE Internet Computing*, vol. 3, no. 2, March-April, 1999, pp 84-88.

[47] Geoff Huston, Telstra,” Quality of Service Fact or Fiction?”, *The Internet Protocol Journal*, vol 3 no. 1, March 2000.

[48] Ray Hunt,” IP Quality of Service Architectures”, *IEEE 2001 2001*, pp. 338-343.

[49]. Huawei Technologies, “How to configure MPLS VPN” MPLS with BGP, May 2017.

[50]. Huawei Technologies, “End-to-End QoS Model “, *Huawei technologies Cloud Engine 20800 Series Switches*, volume 06, November 2017).

[51]. Antonis N., “A Multi-Gigabit FPGA-based 5-tuple classification system”. *IEEE Communications Society at ICC*, 2012.

- [52]. Huawei Technologies, “How to configure MPLS VPN” MPLS with BGP, May 2017.
- [53]. Huawei technologies co. ltd, “QoS Feature and Realization”, quality of services, volume II, May 2017.
- [54] cisco press “Quality of Service for Voice over IP”, Vol. 1. Issue 1, pp. 1-30, April 13, 2011.
- [55] K. Muhhin, “QoS Implementation on Network Devices”, Master Thesis, Tallinn University, Tallinn Estonia, May 31, 2010
- [56]. Fan Y. and Wang L., “QoS of MPLS VPN based on Log-infinitely Divisible Cascades”, IEEE, 2014 International Symposium on Computational Intelligence and Design, October. 2014.
- [57]. Networking Solutions: MPLS and VPNs - wseas.us, [www.wseas.us/elibrary/conferences/2009/budapest/MIV-SSIP/MIV-SSIP30.pdf](http://www.wseas.us/elibrary/conferences/2009/budapest/MIV-SSIP/MIV-SSIP30.pdf)
- [58]. Implementing Point to Point Layer 2 Services - Cisco, [https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k\\_r4-1/lxvpn/configuration/guide/lesc41/lesc41p2ps.pdf](https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k_r4-1/lxvpn/configuration/guide/lesc41/lesc41p2ps.pdf)
- [59]. Technical Whitepaper on MPLS L3VPN - ZTE, [http://www.google.pt/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&ved=0ahUKEwjB29zt3dvUAhXSmlQKHWNCCNwQFghJMAQ&url=http%3A%2F%2Fwww.zte.com.cn%2Fen%2Fproducts%2Fbearer%2F201308%2FP020130828527155850511.pdf&usq=AFQjCNEsW1\\_n8TSG3YjZ39mqLVQMiGotIw](http://www.google.pt/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&ved=0ahUKEwjB29zt3dvUAhXSmlQKHWNCCNwQFghJMAQ&url=http%3A%2F%2Fwww.zte.com.cn%2Fen%2Fproducts%2Fbearer%2F201308%2FP020130828527155850511.pdf&usq=AFQjCNEsW1_n8TSG3YjZ39mqLVQMiGotIw)
- [60]. <https://smallbiztrends.com/2013/09/osi-model-layer-networking.html>. Accessed 1 Jun. 2022



## Appendix

### Layer 2 and Layer 3 VPN BGP MPLS Configuration

#### P1 Router Configuration

P1#show running-config	1765	hidekeys
	1766	#
hostname P1	1767	ip tcp synwait-time 5
#	1768	#
boot-start-marker	1769	interface Loopback0
boot-end-marker	1770	ip address 5.5.5.5
#	1771	255.255.255.0
no aaa new-model	1772	#
no ip icmp rate-limit	1773	interface FastEthernet0/0
unreachable	1774	no ip address
ip cef	1775	shutdown
#	1776	duplex half
no ip domain lookup	1777	#
ip auth-proxy max-nodata-	1778	interface GigabitEthernet1/0
conns 3	1779	ip address 10.0.56.5
ip admission max-nodata-	1780	255.255.255.0
conns 3	1781	negotiation auto
#	1782	#
multilink bundle-name	1783	interface GigabitEthernet2/0
authenticated	1784	ip address 10.0.15.5
mpls label range 500 599	1785	255.255.255.0
#	1786	negotiation auto
archive	1787	mpls ip
log config		

#	1813	#
interface GigabitEthernet3/0	1814	logging alarm informational
ip address 10.0.35.5	1815	no cdp log mismatch duplex
255.255.255.0	1816	#
negotiation auto	1817	control-plane
mpls ip	1818	#
#	1819	gatekeeper
interface GigabitEthernet4/0	1820	shutdown
no ip address	1821	#
shutdown	1822	line con 0
negotiation auto	1823	exec-timeout 0 0
#	1824	privilege level 15
router ospf 1	1825	logging synchronous
log-adjacency-changes	1826	stopbits 1
network 5.5.5.5 0.0.0.0 area 0	1827	line aux 0
network 10.0.15.0 0.0.0.255	1828	exec-timeout 0 0
area 0	1829	privilege level 15
network 10.0.35.0 0.0.0.255	1830	logging synchronous
area 0	1831	stopbits 1
network 10.0.56.0 0.0.0.255	1832	line vty 0 4
#	1833	login
ip forward-protocol nd	1834	#
no ip http server	1835	end
no ip http secure-server	1836	<b>PE1 Router Configuration</b>

PE1#show running-config	1862	#
hostname PE1	1863	archive
#	1864	log config
boot-start-marker	1865	hidekeys
boot-end-marker	1866	#
#	1867	ip tcp synwait-time 5
no aaa new-model	1868	#
no ip icmp rate-limit	1869	class-map match-any
unreachable	1870	VPN_A_qos
ip cef	1871	match access-group name
#	1872	VPN_A_qos
ip vrf VPN_A	1873	match dscp ef
rd 1:1	1874	#
route-target export 1:1	1875	policy-map VPN_A_qos
route-target import 1:1	1876	class VPN_A_qos
#	1877	set mpls experimental
	1878	topmost 5
no ip domain lookup	1879	set dscp ef
ip auth-proxy max-nodata-	1880	#
conns 3		
ip admission max-nodata-	1881	pseudowire-class L2VPN
conns 3	1882	encapsulation mpls
#	1883	#
multilink bundle-name	1884	interface Loopback0
authenticated	1885	ip address 1.1.1.1
mpls label range 100 199	1886	255.255.255.255

#	1912	xconnect 3.3.3.3 101
interface FastEthernet0/0	1913	encapsulation mpls pw-class
	1914	L2VPN
ip vrf forwarding VPN_A	1915	service-policy input
ip address 172.16.1.1	1916	VPN_A_qos
255.255.255.0	1917	#
duplex half	1918	interface GigabitEthernet4/0
#	1919	no ip address
interface GigabitEthernet1/0	1920	shutdown
ip address 10.0.12.1	1921	negotiation auto
255.255.255.0	1922	#
negotiation auto	1923	router ospf 1
mpls ip	1924	log-adjacency-changes
#	1925	network 1.1.1.1 0.0.0.0 area 0
interface GigabitEthernet2/0	1926	network 10.0.12.0 0.0.0.255
ip address 10.0.15.1	1927	area 0
255.255.255.0	1928	network 10.0.15.0 0.0.0.255
ip ospf 1 area 0	1929	area 0
negotiation auto	1930	network 172.16.1.0 0.0.0.255
mpls ip	1931	area 0
service-policy output	1932	#
VPN_A_qos	1933	router bgp 65000
#	1934	no bgp default ipv4-unicast
interface GigabitEthernet3/0	1935	bgp log-neighbor-changes
no ip address	1936	neighbor 3.3.3.3 remote-as
negotiation auto	1937	65000

neighbor 4.4.4.4 remote-as 65000	1964	ip forward-protocol nd
#	1965	no ip http server
address-family ipv4	1966	no ip http secure-server
neighbor 3.3.3.3 activate	1967	#
neighbor 4.4.4.4 activate	1968	ip access-list extended
no auto-summary	1969	VPN_A_qos
no synchronization	1970	permit ip any any
exit-address-family	1971	#
#	1972	logging alarm informational
address-family vpnv4	1973	no cdp log mismatch duplex
neighbor 3.3.3.3 activate	1974	#
neighbor 3.3.3.3 send- community extended	1975	route-map AB permit 10
neighbor 4.4.4.4 activate	1976	#
neighbor 4.4.4.4 send- community extended	1977	route-map BT permit 10
exit-address-family	1978	match interface
#	1979	FastEthernet0/0
address-family ipv4 vrf VPN_A	1980	set ip precedence critical
redistribute connected metric 10	1981	#
no synchronization	1982	control-plane
exit-address-family	1983	#
#	1984	gatekeeper
	1985	shutdown
	1986	#
	1987	line con 0
	1988	exec-timeout 0 0

privilege level 15	2014	no ip domain lookup
logging synchronous	2015	ip auth-proxy max-nodata-
stopbits 1	2016	conns 3
line aux 0	2017	ip admission max-nodata-
exec-timeout 0 0	2018	conns 3
privilege level 15	2019	#
logging synchronous	2020	multilink bundle-name
stopbits 1	2021	authenticated
line vty 0 4	2022	#
login	2023	archive
#	2024	log config
end	2025	hidekeys
	2026	#
	2027	ip tcp synwait-time 5
<b>CE1 Router Configuration</b>	2028	#
CE1#show running-config	2029	interface FastEthernet0/0
hostname CE1	2030	ip address 172.16.1.2
#	2031	255.255.255.0
boot-start-marker	2032	duplex half
boot-end-marker	2033	#
#	2034	interface GigabitEthernet1/0
no aaa new-model	2035	no ip address
no ip icmp rate-limit	2036	shutdown
unreachable	2037	negotiation auto
ip cef	2038	#
#		

interface GigabitEthernet2/0	2064	#
no ip address	2065	gatekeeper
shutdown	2066	shutdown
negotiation auto	2067	#
#	2068	line con 0
interface GigabitEthernet3/0	2069	exec-timeout 0 0
no ip address	2070	privilege level 15
shutdown	2071	logging synchronous
negotiation auto	2072	stopbits 1
#	2073	line aux 0
interface GigabitEthernet4/0	2074	exec-timeout 0 0
no ip address	2075	privilege level 15
shutdown	2076	logging synchronous
negotiation auto	2077	stopbits 1
#	2078	line vty 0 4
ip forward-protocol nd	2079	login
ip route 0.0.0.0 0.0.0.0	2080	#
172.16.1.1	2081	end
no ip http server	2082	<b>CE3 Router Configuration</b>
no ip http secure-server	2083	CE3#show running-config
#	2084	hostname CE3
logging alarm informational	2085	#
no cdp log mismatch duplex	2086	boot-start-marker
#	2087	boot-end-marker
control-plane		

#	2114	interface GigabitEthernet1/0
no aaa new-model	2115	no ip address
no ip icmp rate-limit	2116	shutdown
unreachable	2117	negotiation auto
ip cef	2118	#
#	2119	interface GigabitEthernet2/0
no ip domain lookup	2120	no ip address
ip auth-proxy max-nodata-	2121	shutdown
conns 3	2122	negotiation auto
ip admission max-nodata-	2123	#
conns 3	2124	interface GigabitEthernet3/0
#	2125	no ip address
multilink bundle-name	2126	shutdown
authenticated	2127	negotiation auto
#	2128	#
archive	2129	interface GigabitEthernet4/0
log config	2130	no ip address
hidekeys	2131	shutdown
#	2132	negotiation auto
ip tcp synwait-time 5	2133	#
#	2134	ip forward-protocol nd
interface FastEthernet0/0	2135	ip route 0.0.0.0 0.0.0.0
ip address 172.16.2.2	2136	172.16.2.1
255.255.255.0	2137	no ip http server
duplex half	2138	no ip http secure-server
#		



#	2163	login
logging alarm informational	2164	#
no cdp log mismatch duplex	2165	End
#	2166	<b>CE5 Router Configuration</b>
control-plane	2167	CE5#show running-config
#	2168	hostname CE5
gatekeeper	2169	#
shutdown	2170	boot-start-marker
#	2171	boot-end-marker
line con 0	2172	#
exec-timeout 0 0	2173	no aaa new-model
privilege level 15	2174	no ip icmp rate-limit
logging synchronous	2175	unreachable
stopbits 1	2176	ip cef
line aux 0	2177	#
exec-timeout 0 0	2178	no ip domain lookup
privilege level 15	2179	ip auth-proxy max-nodata-
logging synchronous	2180	conns 3
stopbits 1	2181	ip admission max-nodata-
line vty 0 4	2182	conns 3
login	2183	#
#	2184	multilink bundle-name
end	2185	authenticated
line vty 0 4	2186	#
	2187	archive

log config	2213	shutdown
hidekeys	2214	negotiation auto
#	2215	#
ip tcp synwait-time 5	2216	interface GigabitEthernet2/0
#	2217	no ip address
class-map match-all	2218	shutdown
L2VPN_QOS	2219	negotiation auto
match access-group name	2220	#
L2VPN_QOS	2221	interface GigabitEthernet3/0
match access-group name	2222	ip address 192.168.1.1
L2VPN_QOS	2223	255.255.255.0
#	2224	negotiation auto
policy-map L2VPN_QOS	2225	service-policy output
class L2VPN_QOS	2226	L2VPN_QOS
set mpls experimental	2227	#
topmost 5	2228	interface GigabitEthernet4/0
set dscp ef	2229	no ip address
#	2230	shutdown
interface FastEthernet0/0	2231	negotiation auto
no ip address	2232	#
shutdown	2233	ip forward-protocol nd
duplex half	2234	no ip http server
#	2235	no ip http secure-server
interface GigabitEthernet1/0	2236	#
no ip address	2237	ip access-list extended

L2VPN_QOS	2262	End
permit ip any any	2263	#
#	2264	logging alarm informational
logging alarm informational	2265	no cdp log mismatch duplex
no cdp log mismatch duplex	2266	#
#	2267	control-plane
control-plane	2268	#
#	2269	gatekeeper
gatekeeper	2270	shutdown
shutdown	2271	#
#	2272	line con 0
line con 0	2273	exec-timeout 0 0
exec-timeout 0 0	2274	privilege level 15
privilege level 15	2275	logging synchronous
logging synchronous	2276	stopbits 1
stopbits 1	2277	line aux 0
line aux 0	2278	exec-timeout 0 0
exec-timeout 0 0	2279	privilege level 15
privilege level 15	2280	logging synchronous
logging synchronous	2281	stopbits 1
stopbits 1	2282	line vty 0 4
line vty 0 4	2283	login
login	2284	#
#	2285	end