St. Mary's University

Faculty of Informatics

Department of Computer Science

Improving Quality of Service of Border Gateway Protocol Multiprotocol Label Switching Virtual Private Network of EthioTelecom Service Level Agreements

By

Shimelis Asrat

Advisor

Dr. Asrat Mulatu

A Thesis Submitted to the Faculty of Informatics in Partial Fulfillment of the Requirements for the Degree of Master of Science in Computer Science

June 2018

Addis Ababa, Ethiopia

Improving Quality of Service of Border Gateway Protocol Multiprotocol Label Switching Virtual Private Network of EthioTelecom Service Level Agreements

By

Shimelis Asrat

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

Thesis Examination Committee:

Mr. Michael Melese	_____	_____
Full Name	**Signature**	**Date**
Internal Examiner		

Dr. Eng. Yihenew Wandie	_____	_____
Full Name	**Signature**	**Date**
External Examiner		

_____	_____	_____
Full Name	**Signature**	**Date**
Dean, Faculty of Informatics		

June 2018

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.

Shimelis Asrat Argaw
Full Name of Student

_____
Signature

Addis Ababa

Ethiopia

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

Dr. Asrat Mulatu
Full Name of Advisor

_____
Signature

June 2018

Addis Ababa

Ethiopia

Acknowledgment

First and foremost, my sincere gratitude goes to Almighty God for giving me the enablement and capability physically, mentally and spiritually for the completion of this thesis work.

I would like also to express my sincere thanks to my advisor Dr. Asrat Mulatu for his unreserved encouragement, excellent advice, and continuous support during the work of this thesis. Without his comment, information, guidance, and suggestion of several breakthroughs in this thesis would be impossible to be achieved.

I also want to thank EthioTelecom IP Quality of Service Management Section staffs for their provision of necessary data to prepare this thesis. At last, I would also like to take this opportunity to acknowledge Mr. Merid Nigussie for this support and encouragement. I am especially indebted to his support.

Table of Contents

List of Acronyms

ADSL	Asymmetric Digital Subscriber Line
AF	Assured Forwarding
BECN	Backward Explicit Congestion Notification
BGP	Border Gateway Protocol
BoS	Bottom of the Stack
BRAS	Broadband Remote Access Server
CAR	Committed Access Rate
CBQ	Class-based Queueing
CDMA	Code Division Multiple Access
CE	Customer Edge
CEF	Cisco Express Forwarding
CoS	Class of Service
CPE	Custom Premises Equipment
CPU	Central Processing Unit
CQ	Custom Queueing
DE	Discard Eligible
DiffServ	Differentiated Services
DSCP	Differentiated service code point
DSLAM	Digital Subscriber Line Multiplexer
eBGP	Exterior Border Gateway Protocol
EF	Expedited Forwarding
EPON	Ethernet Passive Optical Network
ER	Edge Router
FECN	Forward Explicit Congestion Notification
FIFO	First in Frist Out
GNS	Graphical Network Simulator
GPON	Gigabit Passive Optical Network
GSM	Global System for Mobile System
GTSM	Generalized TTL Security Mechanism
HTTP	Hypertext Transfer Protocol
iBGP	Interior Border Gateway Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
IntServ	Integrated Services
IP	Internet Protocol
IS-IS	Intermediate System to Intermediate System
ITU	International Telecommunication Union
KPI	Key Performance Indicator

L3VPN	Layer 3 Virtual Private Network
LAN	Local Area Network
LFB	Label Information Base
LFIB	Label Forwarding Information Base
LSP	Label Switched Path
LSR	Label Switch Router
MD5	Message Digest 5
MP	Multi-Protocol
MPLS	Multiprotocol Label Switching
MSAG	Multiple Service Access Gateway
MSAN	Multiple Service Access Node
NGN	New Generation Network
OSPF	Open Shortest Path First
P	Provider
PE	Provider Edge
PHB	Per-Hop-Behavior
PQ	Priority Queuing
OPNET	Optimized Network Engineering Tools
QoS	Quality of Service
RD	Route Distinguisher
RED	Random Early Detection
RFC	Request for Comment
RR	Route Reflector
RSVP	Resource Reservation Protocol
RT	Route Target
SLA	Service Level Agreement
SP	Service Provider
TCP	Transmission Control Protocol
TE	Traffic Engineering
TP	Traffic policing
TS	Traffic shaping
TTL	Time to Live
UDP	User Datagram Protocol
VDSL	Very high bit rate Digital Subscriber Line
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
ToS	Type of Services
WAN	Wide Area Network
WFQ	Weight Fair Queueing
WRED	Weighted Random Early Detection

List of Figures

List of Tables

Abstract

The primary goals of Quality of Service (QoS) are bandwidth management, controlled jitter, latency and improved packet loss characteristics to provide satisfactory services for users. Shaping network optimization is crucial for the service provider. To implement the network QoS, optimizing the current network physical and logical architectures is among the best practice.

In this work, an attempt has been made to investigate the end-to-end QoS parameters of EthioTelecom service level agreement (SLA) customers network by using differentiated service (DiffServ) model, to manage end-to-end traffic delay, jitter, and packet loss. The traffics are classified and marked depending on their priorities. The proposed network architecture has used weighted fair queueing for congestion management and weighted random early detection for congestion avoidance method. The eNSP and Wireshark have used been to design, demonstrate and evaluate the network architectures. When the results of the existing network are compared with the proposed network architecture that is designed using the DiffServ model; delay, jitter, and packet loss have decreased whereas the traffic utilization increased.

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

Chapter One

Introduction

1.1. Background

Every day new telecommunication technologies are being developed. Enterprises use these new technologies to upgrade their network services and reduce cost. Now a day different kind of traffic such as voice, video, and data are sent over the same network infrastructure. When transferring different traffic types within the same network infrastructure quality of service (QoS) is the big issue for enterprise [1]. Multiprotocol label switching (MPLS) virtual private network (VPN) are new alternatives to private wide area networks (WAN). Due to the effectiveness of MPLS VPN enterprise customers are moving to service providers that offer MPLS VPNs [1][2]. The main reason for this shifting is the capability of MPLS VPN to provide built-in security features and end-to-end connectivity [1][3]. QoS is the most important element for enterprise networks. Multiprotocol border gateway protocol (MP BGP) MPLS VPNs [4][5] assures the quality of services for these enterprises. To achieve the quality of service for different types of MPLS VPN traffic, differential service (DiffServ) QoS model can be used with MP BGP MPLS VPN. It provides a service guarantee in terms of better end-to-end bandwidth, delay, jitter, and packet loss.

Many of EthioTelecom enterprises customers have subscribed for MP BGP MPLS VPNs services. These enterprise customers have a service level agreement (SLA) with the company on end-to-end QoS. The company is also working on it by setting SLA targets. But there is a gap between the company's SLA targets and what SLA enterprise customers have been getting [2] [6].

QoS defines a service provider's ability to guarantee the level of service required by a customer's traffic end-to-end [4][6]. It evaluates the capabilities of a network to transmit packets. A service provider provides many kinds of services. So, QoS evaluates services from various aspects, including the bandwidth, transmission delay, availability, jitter, speed and packet loss ratio during packet transmission. Shortly, QoS is the ability to provide different priorities to different applications, users, data flows or to guarantee a certain level of performance to a data flow[2][3].

VPN extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the

private network [5]. Applications running across the VPN may benefit from the functionality, security, cost, and management of the private network [8] [11]. VPN services are widely used for interconnecting branches of an organization or a company located in multiple areas. There are two different methods to construct VPNs across IP backbone [1][3], that is custom premises equipment (CPE) based and network-based. Most current VPN implementations are based on CPE equipment. VPN capabilities are being integrated into a wide variety of CPE devices, ranging from firewalls to WAN edge routers. On the other hand, there is significant interest in network-based VPNs where the operation of the VPN is outsourced to service providers.

MPLS is a high-performance packet forwarding technology that integrates the performance and traffic management capabilities of data link layer (layer 2), switching with scalability, flexibility, and performance of network layer (layer 3) routing [5][3]. MPLS directs data from one network node to the next based on short path labels rather than long network addresses, to avoid complex lookups in a routing table[5][7]. The labels identify virtual links (paths) between distant nodes rather than endpoints. MPLS can encapsulate packets of various network protocols.

BGP is often classified as a path vector protocol[3][12]. But it is sometimes also classified as a distance vector routing protocol. The BGP makes routing decisions based on paths, network policies or rule sets configured by a network administrator and is involved in making core routing decisions. BGP may be used for routing within an autonomous system.

BGP MPLS VPN is a layer 3 virtual private network (L3VPN) [1][3]. A BGP MPLS VPN uses the BGP to advertise VPN routes and uses MPLS to forward VPN packets on backbone networks. The BGP MPLS VPN model consists of Provider (P), Provider Edge (PE) and Customer Edge (CE) routers. Between two internal border gateway protocol (iBGP), route reflector (RR) is used to offer an alternative logical full mesh instead of physical full mesh connectivity to optimize the routes as shown in Fig.1.1 [3].

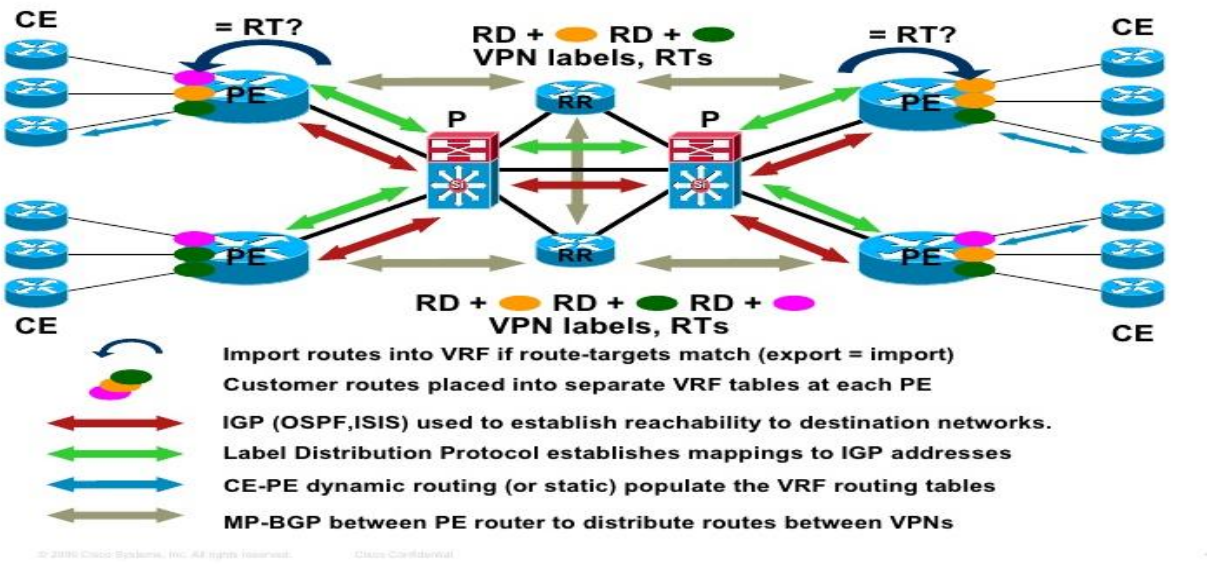

Fig.1.1: BGP MPLS VPN components and working principles [3].

A BGP MPLS VPN uses a peer model that enables a service provider (SP) and customers to exchange routing information [3][6]. The SPs are responsible for forwarding data of customers, without the participation of the customers. A BGP MPLS VPN is more scalable and easier to manage than a traditional VPN. When a new site is added a network administrator only needs to modify the configuration of the edge nodes serving the new site.

BGP MPLS VPN allows overlapping address spaces and overlapping VPNs so that VPNs can be flexibly deployed and expanded [1][2][3]. BGP MPLS VPN supports MPLS QoS and MPLS traffic engineering (TE). Because of these merits, BGP MPLS VPN becomes an approach for IP network carriers to provide value-added services.

In BGP MPLS VPN application CE and PE devices are responsible for advertising VPN routes, whereas provider devices only need to maintain routes of the backbone network without knowing VPN routes. Generally, PE devices maintain all VPN routes.

VPN routes are advertised from the local CE device to the ingress PE device, from the ingress PE device to the egress PE device and from the egress PE device to the remote CE device. After the whole route advertisement process is complete, the local and remote CE devices have reachable routes to each other and VPN routes can be advertised on the backbone network.

BGP MPLS VPN service models are provided for user services to ensure QoS according to the user's requirements and the quality of the network [1][4] [10]. The common service models are as follows:

- Best Effort service model
- Integrated service model and
- Differentiated service model.

The Best Effort service model is applicable to the services that are insensitive to delay and has lower requirements for reliability [4] [10]. It is realized through the FIFO mechanism. The integrated service model is the application program applies to the network for specific service and does not send packets until the arrival of confirmation that the network has reserved resources for it [4] [14]. In the differentiated service model, the application program does not need to send its request for network resources before sending packets [4] [15]. Instead, the application program notifies network nodes of its QoS requirements by setting QoS parameters in the IP header as shown in Fig.1.2. The application program informs network nodes of its demand for QoS by using QoS parameters in the IP packet header.

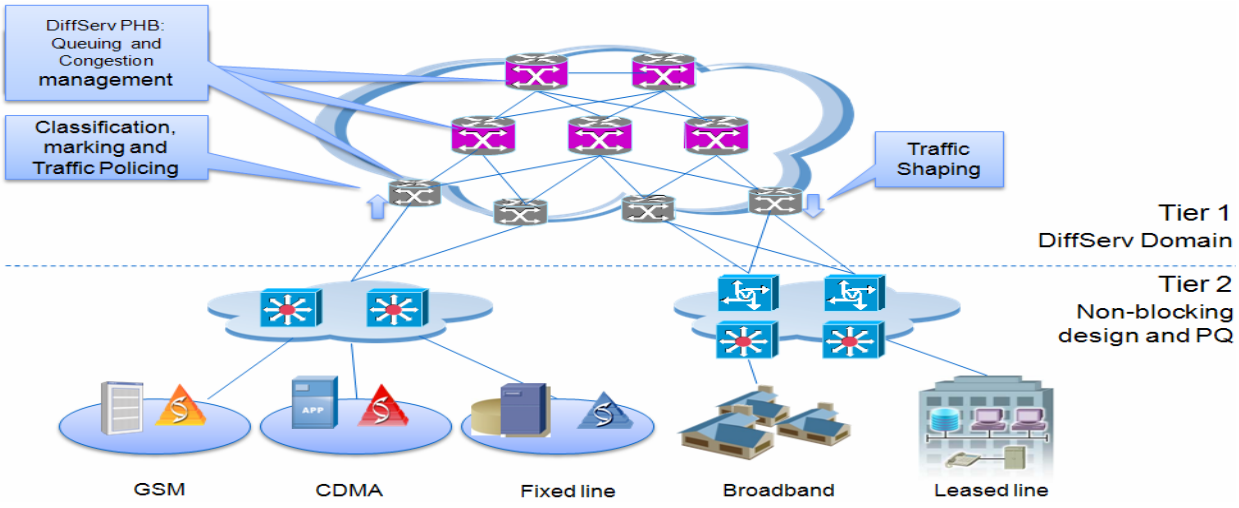

Fig.1.2: QoS differentiated service model [3].

Generally, the main goal of improving QoS is to guarantee end-to-end service delivery. QoS includes end-user perception, service provider perception, and network performance issues. Optimization of the network by using different queueing algorithm is the best suit to increase the network QoS. Increasing network performance increases end-user perception and service provider perception.

1.2. Statement of the Problem

BGP MPLS VPN is one of the services provided by EthioTelecom for its SLA customers. These services are widely used in IP MPLS networks for connecting customers' remote VPN sites. But according to the literature review done on company's QoS level in [5] [32] [35], companies faced many challenges such as low bandwidth, high jitter, high packet drops and high packet delay which degrade the quality of service and overall network performances to provide these services. In addition to this, as shown in the questionnaires conducted from the company's BGP MPLS VPN SLA customers 45 % of their connection has QoS problems.

To provide QoS for its customers, EthioTelecom has done continuous optimization on MPLS VPN SLA customers network. Moreover, the company did continuous expansion projects in its networks [5] [32]. For example, it has recently expanded the existing network of IP backhaul, multiple service access gateway (MSAG) and multiple service access node (MSAN) plantation projects for broadband VPN and Internet customers and yet an end-to-end QoS is not guaranteed.

There is a detailed analysis done by EthioTelecom IP QoS management team [5] [31] [32], on QoS of BGP MPLS VPN of SLA customers. The analysis result shows that there are some disparities between the company's SLA targets and analysis results (what customers getting). This might be because of improper network optimization and customer LAN side problems.

In addition, there are several VPN complaints from end users across the country on poor bandwidth, high packet drops, high packet delay and high jitter as suggested by the fixed access network, operation, and maintenance team in [31] [32]. It has happened because there were QoS problems. The cause of these problems is EthioTelecom hasn't optimized their network architecture logically as shown in Fig.1.3.

In the existing network architecture, there are three types of routers, two P, four PE and two CE routers. These routers have their own functionalities in the optimization BGP MPLS VPN traffic flow.

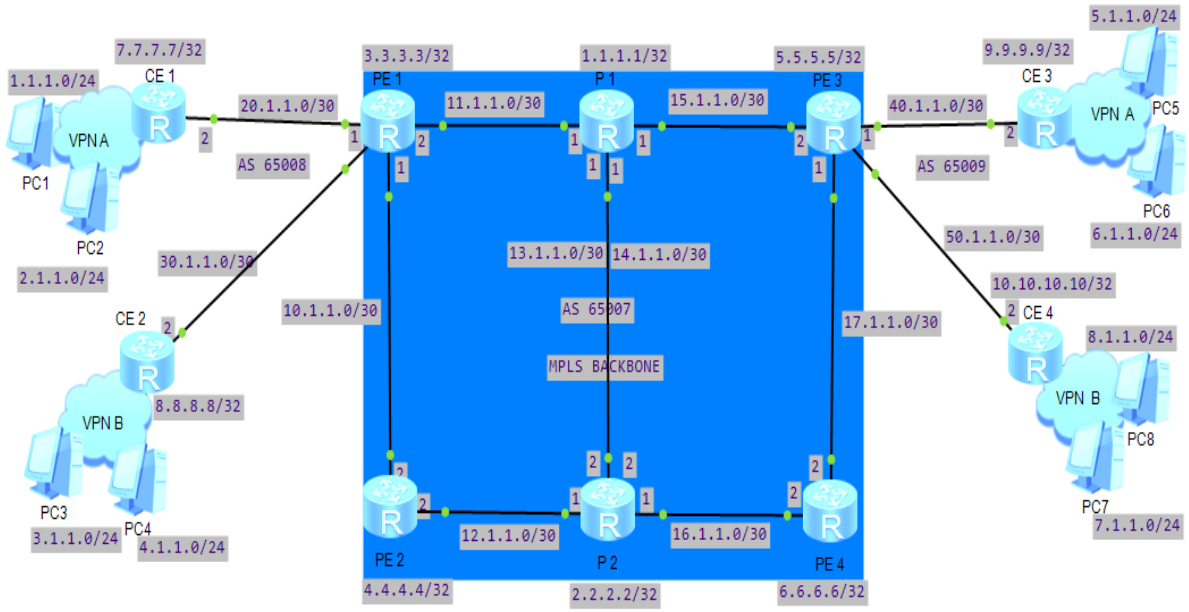

Fig.1.3: Existing BGP MPLS VPN network architecture [31].

Currently EthioTelecom treaties all customers (SLA, major and residential) network equally which lead to QoS problems. These are because the company uses the Best Effort QoS model, FIFO for congestion management and tail drop for congestion avoidance. Because of this gap, the research is motivated to address the above problems by optimizing the network logically using differentiated Service QoS model.

1.3. Objectives

1.3.1. General Objective

The general objective of this study is to identify EthioTelecom BGP MPLS VPN of SLA customer's QoS complaints, analyze the result with respect to the company's SLA targets and ITU threshold values, design solution to improve it and evaluate the proposed solution.

1.3.2. Specific Objectives

The specific objectives of the research are summarized as follows:

- Identify EthioTelecom BGP MPLS VPN of SLA customer's QoS complaints.
- Analyze the result of the QoS measurement with respect to the company's SLA targets and ITU threshold values.
- Propose the solution to improve QoS of BGP MPLS VPN of company's SLA customer's problems.

- Develop the artifact (prototype) for the proposed solution.
- Design, demonstrate and evaluate the solution to improve the QoS of BGP MPLS VPN of SLA customers.

1.4. Methodology

To do this research work effectively, the general approach and specific method, type of data and source, sample size and sampling techniques, instruments and procedures for data collection, process and analysis, methods of data analysis and evaluation approaches are stated hereunder**.**

1.4.1. General Approach and specific method

The method of research that was used for studying the problem was design science [38], where the researcher interacts with the participant through questionnaires to gather data regarding the status and conditions of the services. Moreover, literature review and related work have been made to determine the state of art in the area. Then the design, development, demonstration, and evaluation of improved QoS of MPLS VPN of EthioTelecom SLA customers have been done.

In this study questionnaires approach is appropriate to collect precise information concerning the status of QoS of MPLS VPN of EthioTelecom SLA customers. Moreover, it helps to demonstrate the association between QoS MPLS VPN and bandwidth, delay, jitter and packet loss ratio. A literature review is the best suit to compare the QoS of EthioTelecom that has been promised in its SLA and what the customers are getting. It is also to cross check with ITU QoS threshold values.

Therefore, a literature review is the best method to identify and analyze the existing conditions of QoS of BGP MPLS VPN of SLA customers, compare the existing conditions with SLA and ITU target values in short and brief manner. Because of this, the researcher was interested to use these research methods.

1.4.2. Data type and source

The sources of data for the study were both primary and secondary. Regarding the primary source, data was collected from twenty EthioTelecom BGP MPLS VPN of SLA customers randomly out of one hundred seven as a sample from different parts of the country. Moreover, secondary data was gathered from relevant documents such as SLA charter, QoS guide, network element configuration guide, achieved configuration, and empirical studies through literature review.

1.4.3. Sample size and sampling Techniques

The total sample size involved in this study was twenty EthioTelecom BGP MPLS VPN of SLA customers from different parts of the country as shown in Table 1.1. The researcher takes a sample of 18 % SLA customers from those that use different types of networks using random sampling technique.

Table 1.1: Total BGP MPS VPN EthioTelecom SLA customers and Sample size [39].

Types of Network	Total Customers	Sample Size Selected
ADSL/VDSL	3	1
EPON	31	6
GPON	23	4
DIRECT FIBER	29	5
AIRONET	17	3
VSAT	4	1
TOTAL	107	20

1.4.4. Instruments and procedures for Data collection, Process, and Analysis

The data for this study was collected from both primary and secondary sources. As a primary source, a questionnaire was used. The questionnaire is a close-ended type. Before distributing the questionnaire, to determine the quality and reliability of the questionnaire, the researcher distributed the questionnaire to four participants who were not included in the actual study to check if there is any unclear idea or statement. As a result, based on the feedback obtained some questions were rephrased or rewritten which lacked clarity. The secondary data was conducted from archived database management of EthioTelecom SLA charter, QoS guide, network element configuration guide and CPE configuration guide through literature review.

The collected data through close-ended questionnaires were analyzed and compared with QoS of EthioTelecom SLA targets and ITU threshold values. By taking the analyzed data as input and the researcher has modeled the traffic flows by using different network modeling and simulation tools.

1.4.5. Design and Evolution Procedures

By taking the gap of analyzed data as input, the researcher has modeled the QoS of EthioTelecom BGP MPLS VPN of SLA customers. The researcher used the DiffServ model by giving priority to the class of services at network and data link layers. The researcher used weighted fair queueing and weighted random early detection algorithms for congestion management and congestion avoidance respectively.

Th**e** traffic flows were studied using network modeling and simulations tools such as Wireshark and eNSP. The simulation part covered end-to-end QoS delivery. Bandwidth and QoS parameters have been reviewed with respect to the QoS of EthioTelecom's SLA targets and ITU QoS threshold values.

1.5. The significance of the study

This study has shown the numerical analysis of QoS of BGP MPLS VPN of EthioTelecom SLA customer's status. Then this numerical result has compared with to SLA targets and ITU standard threshold values. By taking the numerical results as input the study has proposed a way of improving QoS of BGP MPLS VPN of company's SLA customers. For the proposed solution practical modeling and demonstration of the EthioTelecom high speed and optimized network usage have conducted. Then the study has designed, demonstrated and evaluated the solution to improve the QoS of BGP MPLS VPN of SLA customers.

1.6. Contributions

QoS of BGP MPLS VPN is one of the areas that need very strict follow up in telecommunication industries. This is because every SLA customer needs uninterrupted services to support their day to day activities. This, in turn, demands network traffic optimization end-to-end. Hence, attention must be given to improving QoS of BGP MPLS VPN. To utilize the maximum possible capacity of the network and know its usage after deploying the network, there should be continuous and organized traffic optimization on end-to-end networks.

This research work contributed, to improving the QoS of BGP MPLS VPN of EthioTelecom's SLA customer's connection. This is done by traffic classification, marking, shaping and policing using different KPIs by DiffServ QoS model. The proposed solution has been designed, developed, demonstrated and evaluated using computer-aided tools.

1.7. Scope and Limitations

1.7.1. The scope of the Study

This study has evaluated the existing quality of services of BGP MPLS VPN of twenty EthioTelecom SLA customer's connection. After the evaluation, comparing the level of existing quality of services with respect to the company's SLA targets and ITU standard threshold values. Then the study has taken the gap in existing QoS as input and developed a porotype design to improve QoS. The proposed solution has designed, demonstrated and evaluated using computer-aided tools in detail manner. However, the overall process of improving QoS of the existing infrastructure is done by using traffic management and queueing algorithm.

1.7.2. Limitations of the Study

Implementing end-to-end QoS of BGP MPLS VPN could be done by optimizing the current network physical and logical architectures. But this study has not focused on the physical design architectures to improve the existing QoS of BGP MPLS VPN of SLA customers.

In addition to this, the simulation has used developed sample models and randomly selected variables for packet arrival rate. But on the real traffic, there is an additional configuration such as for bidirectional forwarding, time synchronization, and fast route recover. These variables are generated after close inspection of the real network scenario.

1.8. Organization of the Thesis

This thesis paper contains four chapters. Chapter one deals with the introduction of the whole thesis. It clearly alludes to the statement of the problem, objectives, methodology, thesis contribution, scopes, and limitations. Chapter two presents the MPLS, BGP, VPN and QoS model used. It also showed some light on what other authors and researchers have forward their own ideas on the area of improving QoS of MP BGP MPLS VPNs were presented.

The proposed network architecture was presented in chapter three. This includes how BGP, MPLS, VPN, and QoS were designed, demonstrated and evaluated with DiffServ model. The experimental results and discussions were also presented. Finally, the chapter concluded the paper by presenting the conclusions and future recommendations.

Chapter Two

Review of Literature and Related Works

2.1. Review of Literature

This gives a review of earlier contributions on improving QoS of BGP MPLS VPN using different approaches and different model such as best effort, integrated service, differential service models. The objective is to understand the problem and emphasize the research gap in relation to the study. The proper review has been made on BGP, MPLS, VPN, QoS threshold, QoS model, traffic shaping and congestion management.

QoS guarantees end-to-end service quality, to meet different requirements of various services on BGP MPLS VPN networks [7] [10]. The bandwidth, latency, jitter, and packet loss rate are the factors that affect QoS. QoS measurement based on these factors provides quality assurance for key factors of services.

Based on network quality and user requirements, QoS provides end-to-end services for users through different service models. Best effort, integrated service, and differentiated service model are used for BGP MPLS VPN network [4] [10]. Different service models are provided for user services to ensure QoS according to users' requirements and the quality of the network. Traffic classification, traffic policing, traffic shaping, congestion management, congestion avoidance, resource reservation protocol and the link efficiency mechanism are techniques used to guarantee the QoS for BGP MPLS VPN networks [15].

2.1.1. Border Gateway Protocol (BGP)

BGP is a path vector protocol that allows devices between autonomous systems (ASs) to communicate and selects optimal routes [15]. A network is divided into different ASs to facilitate the management of the network.

On a BGP network, unauthorized users may not modify data packets or forge packets for authorized users to attack the BGP network. To ensure service security on the BGP network, configure BGP Message Digest 5 (MD5) authentication, BGP keychain authentication, or Generalized TTL Security Mechanism (GTSM) [10] [14].

Within an AS, routes received from an iBGP peer are not advertised to the other iBGP peers [10]. To ensure the connectivity between iBGP peers in an AS, full-mesh connections must be established between iBGP peers on a BGP network. When there are a large number of iBGP peers on the network, the peer configuration is complex, and many network resources and CPU resources need to be consumed. To reduce the number of iBGP connections on the BGP network, configure a route reflector (RR) and confederation [1] [17].

When there are multiple routes with the same destination address but of different routing protocol types, BGP selects the optimal route based on the routing protocol priority. To change the BGP route selection sequence in an IP routing table set the BGP priority.

There may be multiple routes to the same destination in a BGP routing table [6] [15]. To guide route selection, BGP defines the next-hop selection policy and route selection rules. The next-hop policy takes precedence over route selection rules. After performing the next-hop policy, BGP selects the optimal route based on the rules.

2.1.2. Multi-Protocol Label Switching

MPLS is a technology developed by the Internet engraining task force (IETF) to overcome the problems of traditional IP routing and to make routing fast, manageable, able to carry heavy traffic and accept new routing architectures [8] [17]. MPLS is a modern technique for forwarding network data. In an MPLS network packets are assigned labels and the labels are used to make forwarding decisions without IP lookups at each node. It is called multiprotocol because it supports any layer 3 network protocols. MPLS work between layer 2 and layer 3 which is called layer 2.5 technologies. MPLS provides the scalability for the VPNs and supports for end-to-end QoS [6].

MPLS routing process in larger networks. There are two types of routers [6] edge routers and core routers. The routing decisions are made only at the edge routers and the core routers forward packets based on the labels. These two functions provide fast forwarding method of packets. The core router then swaps the label with a new label and sends the packet to edge router. The edge router performs routing lookups and removes the label and sends it to the destination as a simple IP packet. The packet goes through the path called the Label Switched Path (LSP).

The MPLS header consists of 32 bits [**7**]. The first 20 bits are used for the actual label and these bits are called label bits. The three bits are called experimental bits, these bits are used by defining a class of service (CoS). MPLS enabled routers might need to insert multiple labels to send packets through the MPLS network. To determine which label is the last label in the packet, a bottom of the stack (BoS) bit is used, if the bit is 1 it means that it is the last label. The last 8 bits are used to time to live (TTL) they have the same function as the usual IP header.

Label	**EXP**	**S**	**TTL**
20 Bits	3 Bits	1 Bits	8 Bits

Fig. 2.1: MPLS header [**7**].

2.1.2.1. MPLS Architecture

MPLS architecture has a control plane and data plane [6][8]. Control plane takes care of the routing information exchange and the label exchange between adjacent devices whereas Data plane takes care of forwarding either based on destination addresses or labels.

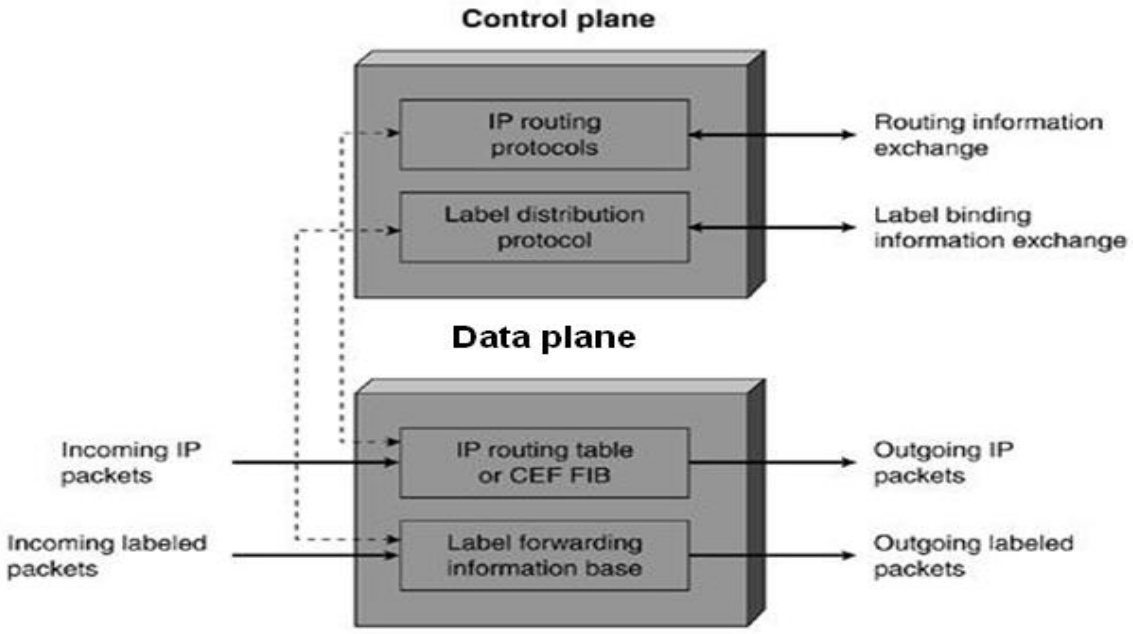

Fig.2.2: MPLS Architecture [8]

2.1.2.2. Control Plane

The control plane is responsible for the routing information exchanges and the label information exchanges with the adjacent routers. Link state routing protocols advertise routing information among the routers that are not necessarily adjacent, whereas label binding information distribution is limited to adjacent routers. [8]. Control plane consists of two types of protocols. The routing protocols and label exchange information protocols. The control plane also requires protocols to exchange labels, 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 the information attached with labels. There are two tables on each MPLS router, label information base (LIB) and label forwarding information base (LFIB) [7][8]. The data plane uses an LFIB maintained by the MPLS enabled router to forward labeled packets. The LIB table contains all the local labels assigned by the local routers and mapping of the labels that it receives from the adjacent MPLS routers. The LFIB uses a subset of the labels contained in the LIB for actual packet forwarding [8]. The MPLS enabled routers to use information in LFIB and label value to make forwarding decisions [8].

A label switch router (LSR) [6] [8] is a router that supports MPLS. These routers have the ability to understand the MPLS labels and they can receive and transmit labeled packets. There are three kinds of LSR's ingress, egress, and intermediate LSR. Ingress LSR's [7] receive an unlabeled packet, insert a label in front of the packet and send it to a data link. Egresses LSR's [7] receive a labeled packet and remove the label and send it to the data link. Ingress and egress routers are edge routers. Intermediate LSR's receive an incoming labeled packet, perform an operation on it, switch the packet, and send the packet on the correct data link [7]. Label switch path (LSP) [7] is the path that a packet passes through from ingress LSR to the intermediate LSR and then the egress LSR.

2.1.2.4. MPLS Label Distribution

The packet in the MPLS network [6] [7] that must pass through the network is forwarded over the label switch path (LSP) tunnel. When the packet reaches the MPLS network then the Ingress router

receives the packet and puts MPLS label in the packet and sends it to the next hop according to the destination address in the packet. There can be many LSRs between Ingress and Egress routers, so when the packet reaches an LSR it swaps the labels and sends it to the next LSR. When the packet reaches the Egress router, it strips off all the labels and sends it to outgo. All the LSRs have interior gateway routing (IGP). To accomplish this task, the adjacent LSRs must agree on a label that will be used as the prefix of IGP and each LSR must know which label should be swapped for incoming and outgoing packets. This shows that we need a mechanism to tell routers which label will be used when forwarding a packet. Each pair of router labels is local, and they do not have any global meaning across the network. There must be some communication between the two adjacent routers to exchange label information. Otherwise, the routers do not know which incoming label need to match with which outgoing label. For this purpose, label distribution protocol is needed.

2.1.3. Multiprotocol Label Switching and Virtual Private Network

MPLS VPN is a network that connects private networks over the public network [6] [8]. MPLS VPNs provide connectivity on OSI layer 2 and layer 3. Service providers use VPNs to interconnect different sites that belong to the same corporation. A requirement of a corporation's private network is that all their customer sites VPNs remain separate from the other corporation VPNs [7].

At the IP layer, VPN models might require that different VPNs are required to connect with one another and also provide connectivity to the internet. MPLS VPN provides this functionality. Service providers use MPLS in their backbone network which supplies a decoupling of the forwarding (data) plane and the control plane that IP does not [7]. There are two types of VPNs.

- L2VPN and
- L3VPN.

2.1.3.1. MPLS VPN Architecture

There are some basic building blocks for the MPLS VPN at Provider edge routers. These are given below [7].

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

2.1.3.2. Virtual Routing Forwarding

The combination of the VPN IP routing table and the associated VPN IP forwarding table is called the VPN routing and VRF [9]. VRF is used to make the MPLS VPN networks private. The VRF makes sure that the routing information is kept separate from different customers and that the backbone of the MPLS network makes sure that the packet forwarding is based on label information and not on the information in the IP header.

VRF is the routing and forwarding instance of VPN. It is a combination of the VPN routing table, the VRF table and IP routing protocols on the PE router. A PE router contains a VRF instance for each VPN that is attached to it.

On PE routers each VPN has its own separate routing table and this routing table is called the VRF routing table. A PE router interface that is towards the CE router only has one VRF, so that all IP packets coming to that interface will be considered as they are belonging to that VRF. It is because there is a separate routing table per VPN. There is a separate Cisco Express Forwarding (CEF) table per VPN to forward these packets on the PE router which is called the VRF CEF table. As with the global routing table and the global CEF table, the VRF CEF table is derived from the VRF routing table [7] [9].

VRF parameters are valid locally [9]. The created VPN VRF must bound to the ingress interfaces of VPN services. An interface can only assign to one VRF, but several interfaces can be assigned to the same VRF. The PE router then creates a VRF and CEF table. The VRF routing table is similar like regular routing table and it is used for a set of VPN sites and is separated from all other routing tables.

2.1.3.3. Route Distinguisher

The VPN uses MP-BGP to propagate its prefixes in MPLS VPN networks. The IPv4 prefixes must be unique when they cross the service providers' network. If there is an overlapping in customers IP addressing, then routing is a problem. To overcome this problem, the concept of route distinguishers (RD) is used to make the IPv4 prefix unique. It distinguishes the same route between different VPN. The combination of IPv4 and RD is called VPNv4 prefix. MP BGP is used to carry this VPNv4 prefixed between the PE routers [7] [9].

The RD is a 64-bit field [7] [8]. One RD must be assigned to each VRF at the PE router. The 64-bit value can have two formats IP Address: nn or ASN: nn, where nn is number and ASN, is the

autonomous system number. Most service providers use ASN: nn. ASN is assigned by IANA to the service provider and "nn" is unique assigns to VRF by the service provider. RD and IPv4 prefix provide a VPNv4 prefix and it is 96-bit long address and subnet mask is 32-bit long [7].

2.1.3.4. Route Target

A route distinguisher works fine but the problem is that they can only communicate with one VPN. To overcome the problem router targets (RT) are introduced. RTs are able to communicate between complex VPN topologies.

RT is attached as an additional attribute to VPNv4 BGP routes to indicate the VPN membership. RT indicates which route should be imported from the MP-BGP into the VRF. The RT that is attached with the route is called the export route and configured separately for each virtual routing table in a PE router. In MPLS VPN architecture the RTs at PE routers are attached with the customer route when it is converted from IPV4 to VPNv4 route [7].

Route target properties are divide into the export target and import target [7] [10]. In the export target after learning IPv4 from directly connected sites, the local PE converts the IPv4 into VPN IPv4 routes and fix the export target properties for this route. As an expanded community property of BGP, the export target property is advertised with the routes. When receiving a VPN IPv4 route advertise by another PE, the PE checks the export property of the route. When the property is consistent with the import target property of certain VRF on the PE, the PE adds the route to the routing table of the VRF.

When a PE router propagates the VPNv4 address to other PE routers, those routers have to select the best router to import into their virtual routing table. This selection is based on import RT. At the PE routers, each virtual routing table has several import RTs that identify the set of VPNs that the virtual routing table is accepting routes from neighbors [10].

2.1.4. MP BGP MPLS VPN

In the BGP MPLS VPN, BGP is used to transfer VPN private network route information on the carrier backbone network and MPLS to forward VPN service steams. Depending on the working principles BGP MPLS VPN is three aspects. Route information advertisement, label distribution and packet forwarding [2] [3].

Route information advertisement is used for the exchange of information from the local CE to the ingress PE, from ingress PE to egress PE and egress PE to local CE. Label distribution distributes

private network label and public network label. VPN packet forwarding is used for encapsulation, outer packet forwarding on a public network and inner label instructing inner sites of packets [1] [2] [3].

2.1.5. Quality of Service (QoS)

QoS is the mechanism of the network to provide different service level to a different traffic type as business need [11]. Service providers offer their network service with quality. They define an SLA. SLA provides the details of all QoS parameters. It defines the parameters such as end-to-end delay, end-to-end jitter, and packet loss. QoS is no single device functionality and it is an end-to-end mechanism. It provides the intelligence to network devices to treat the different application's traffic as their defined service level by SLA. QoS combines different technologies together such as classification, marking, scheduling, queuing, bandwidth allocation and prioritization that are commonly used to provide a scalable end-to-end service [8].

QoS is a generic term. It provides the different level of treatment to the different types of traffic or applications that flows over the network. QoS is required to provide the good management of network resources that makes the sophisticated usage of resources and gives comfort to the network user. Business networks are widely expended with different types of applications. These applications have different network requirements. It needs to lead for different administrative policies that control applications as per their requirements individually. QoS within a network is essential to guarantee the requirements of today's converged networks. QoS provides that different levels of service for business-critical application and delay-sensitive applications. QoS is to manage the following network elements [7] [9].

- Bandwidth
- Delay
- Jitter and
- Packet loss.

To m guarantee, these networks must provide perfect service capabilities. QoS is designed to provide a different level of service quality based on different requirements to guarantee users' requirements for different services.

2.1.5.1. Bandwidth

The amount of data that can be transmitted over the link is bandwidth [11]. On the network, IP Packets travel through the best route. The maximum bandwidth of the route is equal to the smallest value of bandwidth on the route.

The available bandwidth is the path bandwidth divided by several traffic flows [11] [7]. Due to the low bandwidth users experience delay, jitter and packet loss in the communication. This problem can be overcome by following multiple ways.

- Increase link bandwidth: - This is effective but costly.
- Classify and mark traffic and apply to the queue: - Forward important packet first.
- Use Compression technique: - Layer 2 payload compression, TCP header compression, and compressed RTP (cRTP) are some examples [11]. Usage of hardware compression is preferable over software-based compression because compressions are CPU intensive and create a delay.

2.1.5.2. Delay

End-to-end delay is the total time that a packet takes from source to destination [11]. End-to-end delay is the sum of all the following delays.

- Processing delay
- Queuing delay
- Serialization delay and
- Propagation delay.

2.1.5.3. Jitter

Variation in delay is jitter. Packets for the same destination may not arrive at the same rate. Jitter can occur due to different traffic load on different timings. For voice and video, it is necessary to receive the packets in the same sequence to achieve good quality [11].

2.1.5.4. Packet loss

Packet loss occurs due to the low buffer space [8] [10]. When the buffers space of the interface full then packets are dropped. In queue scheduling, packet loss will occur if the queue is full. Packet loss creates extended delays and jitter. Packet loss can be controlled by applying some techniques such as tail drop, random early detection, weighted random early detection and traffic shaping and policing [8].

Generally, QoS is not depended only on the four-pillar bandwidth, delay, packet loss and delay [37]. It also depends on the end-user perception of telecommunication services such as trends, advertising, tariffs and costs which are interrelated to the customer expectation of the QoS. Shortly the below framework shows how end-user perception reaches the QoS satisfaction level.

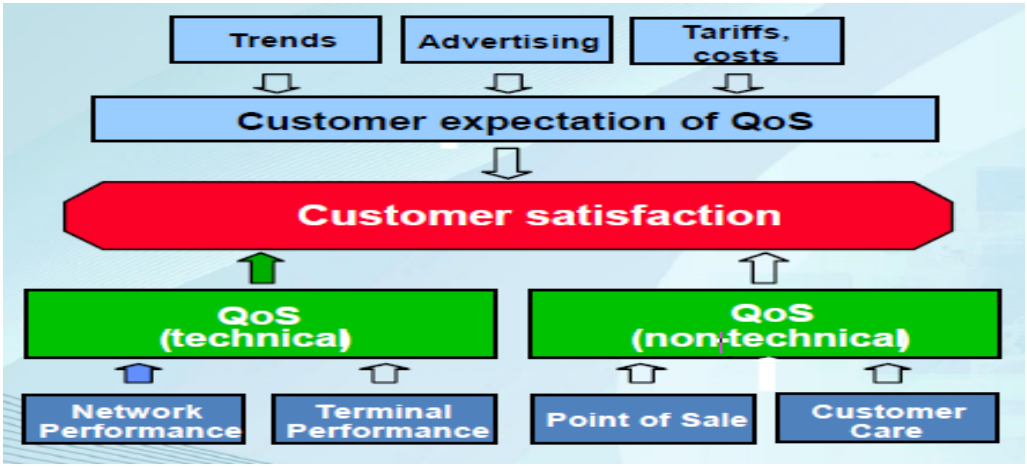

Fig.2.3: User perception of end-to-end QoS delivery framework [37] [39].

QoS can be divided into two viewpoints [37] [39]. Customer viewpoints and Service provider viewpoints. Customer viewpoints include QoS requirements and perception whereas service provider viewpoints include QoS offered and QoS achieved as shown in detail in the below framework.

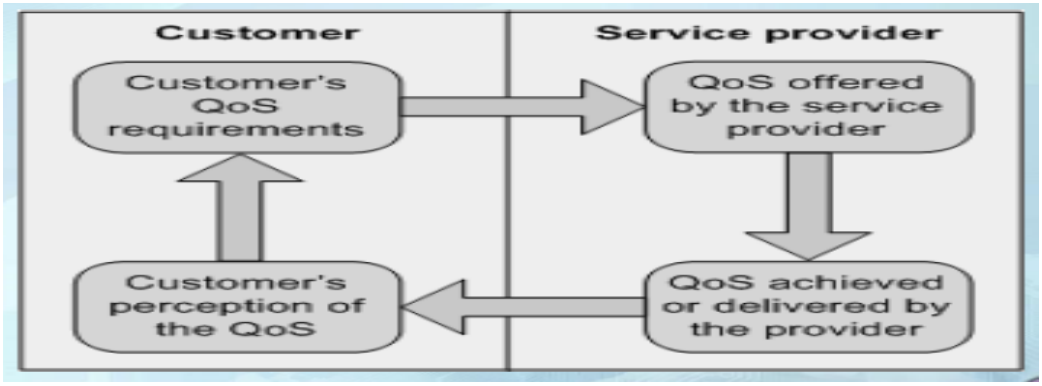

Fig.2.4: QoS viewpoints framework [39].

Network QoS is not well defined by itself [37] [39]. It is used with network performance and quality of experience. For example, quality of experience impacts QoS and network performance even though end-user subjective.

Generally, if network performance was well optimized, service provider viewpoint reaches a high level. If Service provider affords quality services to its customer, customer viewpoint was reached at a high level which increases the quality of experience.

2.1.5.5. ITU-T Y.1541 Recommended QoS Targets

The intent of this recommendation is to provide guidance on the key factors that influence QoS from the end-user perspective [30]. By considering a range of applications involving the media, voice, video, image, and data the parameters that govern end-user satisfaction for these applications and broad classification of end-user QoS categories is determined. It is intended that these categories are used as the basis for deriving realistic QoS classes and associated QoS control mechanisms for the underlying networks.

A typical user is not concerned with how a particular service is implemented. However, the user is interested in comparing the same service offered by different providers in terms of universal, user-oriented performance parameters. This implies that performance should be expressed by parameters.

Table 2.1: ITU-T Y.1541 recommended QoS targets [30].

Medium	Application	Degree of symmetry	Typical amount of data	Key performance parameters and target values		
				One-way delay (Note)	**Delay variation**	**Information loss**
Data	Web-browsing – HTML	Primarily one-way	~10 KB	Preferred < 2 s /page Acceptable < 4 s /page	N.A.	Zero
Data	Bulk data transfer/retrieval	Primarily one-way	10 KB -10 MB	Preferred < 15 s Acceptable < 60 s	N.A.	Zero
Data	Transaction services – high priority	Two-way	< 10 KB	Preferred < 2 s Acceptable < 4 s	N.A.	Zero
Data	E-mail (server access)	Primarily one-way	< 10 KB	Preferred < 2 s Acceptable < 4 s	N.A.	Zero
Data	Low priority transactions	Primarily one-way	10 KB	< 30 s	N.A.	Zero
NOTE - In some cases, it may be more appropriate to consider these values as response times.						

2.1.5.6. Recommended IP QoS in EthioTelecom network

QoS is a configuration which prioritizes data traffic based on traffic type or destination. So that in the event of congestion on a network, a site's critical traffic has higher priority over other traffic [31] [32] [33]. Currently, in EthioTelecom network, all packets form all customers are treated equitably, thereby a generalized IP network performance targets are set (recommended) as shown in the table below.

Table 2.2: EthioTelecom recommended QoS targets [32].

QoS parameters	Across backbone (ER to ER)	VPN end to end (CPE to CPE across backbone)	Internet connection as measured from the connected BRAS or ER (or from speedtest.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 BW	75% or more of subscribed BW

2.1.5.7. The way of Enhancing QoS

The network QoS can be enhanced with the following methods [12] [34]:

- Increasing the link bandwidth
- Use rational queue scheduling and congestion avoidance mechanism and
- Improve processing process.

When the available bandwidth increase, the link ensures QoS of the traffic [34]. It reduces the transmission delay and jitter. In addition, when the link bandwidth increases the packet loss ratio is lowered and less packet is dropped. In the rational queue scheduling and congestion avoidance mechanism, data of various services are allocated depending on their priorities [12]. Delay sensitive data are got higher priorities than low delay sensitive data. This avoids the congestion by the different queueing mechanism. Improve processing processes such as CPU and memory increase the processing performance and reduce packet delay and loss [12].

2.1.5.6. QoS Models

Network application requires successful end-to-end communication. Traffic may travel multiple routes or one network or multiple networks before reaching the destination host. To provide end-to-end QoS, an overall network deployment is required. Service models are used to provide an end-to-end QoS guarantee based on specific requirements. There are three QoS models, that are [11] [13]:

- Best-Effort Model
- Integrated Services (IntServ) Model and
- Differentiated Services (DiffServ) Model.

2.1.5.6.1. Best-Effort Model

When we talk about Best-Effort model its mean no QoS is configured [13]. In this model, all the traffic is treated in the same manner and all are equally important. No classification and no differentiation in different applications. Best-Effort model provides scalability and eases to handle but it has a lack of service guarantee and lack of service differentiation.

2.1.5.6.2. Integrated Service Model (IntServ)

Integrated Service (IntServ) model was the first model that was developed to achieve end-to-end QoS [13]. It was developed to fulfill the requirement for real-time applications. Basic idea was to reserve the network resources for applications by guaranteeing bandwidth, delay, and packet loss. Reservation of network resources to provide the service level resource reservation protocol (RSVP) is used [11]. It provides the signaling and reserves end-to-end network resources for the application. It is also called the hard QoS model. If it cannot reserve the resources as per the policy, it refuses to let the application operate. It is a virtual circuit and flow-based model [13].

2.1.5.6.3. Differentiated Service Model (DiffServ)

Differentiated Service Model comes after IntServ QoS model [12]. It overcomes the limitation of the IntServ model. DiffServ is also called the “Soft QoS” model [5] [12]. IntServ model guarantees for the end-to-end resource reservation before application take the start. It uses the RSVP for signaling and end-to-end resource reservation. DiffServ does not use the signaling protocols. It uses the per-hop-behavior (PHB). Each node in the network provides the specific level of service for each traffic class. PHB does not require end-to-end resource reservation while the decision is being made at each hop and provides the service level to the traffic class [12].

IntServ and DiffServ are two mechanisms to achieve QoS. They have different architectures [12]. There are differences in their structure and configurations. IntServ model was the first attempt to achieve QoS. It is based on per-flow operations. It uses admission control to provide the guaranteed QoS for a specific flow. It reserves bandwidth throughout the path and then allows the application to start if there is the availability of resources. It uses RSVP for reservation of resources. When RSVP reserves the bandwidth, that bandwidth cannot be used by another transmission. Each flow is isolated from one another. It works like private leased lines and it provides the guaranteed QoS.

DiffServ model has a different mechanism to provide QoS [12]. It does not provide a guaranteed QoS, but it is more flexible, it is like statistical multiplexing. It does not reserve the resource for each flow. Traffic treatment decisions are being made at each hop. It does not use any signaling protocol it uses per-hop behavior to provide QoS. All the devices on the network are preprogrammed to provide QoS for a specific class of traffic. It is more flexible and scalable because it does not reserve end-to-end bandwidth for a specific flow.

2.1.5.7. DiffServ QoS Implementation over MPLS VPN

To achieve service quality in MPLS VPN environment that choose the DiffServ QoS model because it is widely used in industry due to its scalability [10] [12]. DiffServ model consists of four components. Traffic classification, marking, congestion management and congestion avoidance. These were used to control network traffic, resource allocation in different ways and allow the system to provide differentiated services. To use the DiffServ QoS model first step is classification. It is to classify the traffic into different classes. After classification each class is marked, this process is called marking. After marking, business policy for each class is configured as per SLA.

2.1.5.8. Traffic Classification

Traffic classification is the process of dividing the traffic into different category [20]. Each category is called a traffic class. Classification is the most fundamental part to achieve the QoS using the DiffServ model. After making traffic classes, traffic becomes ready for further handling to achieve QoS. Classification is a processor intensive process, but it happens once at customer edge router normally. The total effect of the classification process does make a major impact on end-to-end delay. Classification can be done by [20]:

- 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).

QoS classification is implemented by marking the type of service (TOS) field in the IP packet precedence as shown in fig.2.5 [10] [34]. IP data stream can be classified based on the different RFC standards. RFC 791[34] defines the IP precedence field to divide the IP application int0 8 categories. RFC 1394 defines the TOS field is divided into 16 categories. RFC 2472 redefines TOS to divide services into 64 categories (DSCP).

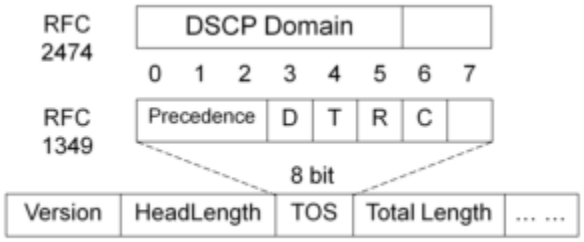

Fig.2.5: Traffic classification [34].

RFC 1349 defines bits in the TOS; bits 0 to 2 refer to precedence. The value ranges from 0 to 7. The larger the value, the higher the precedence. The D bit refers to the delay, T bit refers to the throughput, R bit refers to reliability and C bit refers to the monetary cost. Bits 6 and 7 are reserved.

2.1.5.9. Traffic Marking

In simple word marking is coloring the packet, so that they are recognized [8] [10]. Marking is to place a value in the DSCP field [8]. With the help of marking, traffic is identified for the next action to achieve QoS. Each hop individually identified the incoming traffic on the physical interface and provides the service level. Traffic marking can have done on the data link layer and on the network layer.

Traffic marking at data link layer can be done the following [8]:

- 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 network layer can be done the following [8]:

- IP precedence or DSCP on IP header IP precedence. DSCP uses 8-bit field ToS in IP header [20] 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.

2.1.5.10. Per-Hop Behavior (PHB)

Per-Hop Behavior (PHB) is a mechanism that is used by the DiffServ model to allocate the resource at each node in the path [13]. PHB is one that guarantees 99.999% allocation of the network resource (bandwidth, delay, reliability) to behavior aggregate at each node [16]. This can be measured in a variety of competing for traffic conditions. This allocation of a resource depends on business requirements. These PHBs are like building blocks and are grouped together to achieve QoS according to SLAs. PHBs are configured at each node in the network in terms of buffer allocation and packet scheduling mechanisms. IETF defines the following PHBs [18]:

- Best Effort (BE) PHB: Default PHB, which is used for used for best-effort service.
- Expedited Forwarding (EF)PHB: Used for low-delay service.
- Assured Forwarding (AF)PHB: Used for guaranteed bandwidth service.
- Class-selector (CS) PHB: Used for backward compatibility with the non-DiffServ compliant device.

2.1.5.11. Traffic Shaping and Policy

Traffic shaping is used to restrict the total traffic and burst traffic that leaves a network, providing basic QoS functions to ensure network stability [18]. Traffic shaping (TS) is an active way to adjust the traffic output rate. A typical application of TS is to control the volume and burst of outgoing traffic based on the network connection. Thus, the packets can be transmitted at a uniform rate. TS is implemented by using the buffer and token bucket as shown on fig.2.6 [18].

The Committed Access Rate (CAR) [13] is applied to limit certain categories of traffic. For example, Hypertext Transfer Protocol (HTTP) packets can be kept from taking up more than 50% of the network bandwidth. Packets are first classified according to the pre-defined matching rules. Packets that comply with the specified rate limit are forwarded directly. Packets that exceed the specifications are dropped or have their priorities re-set.

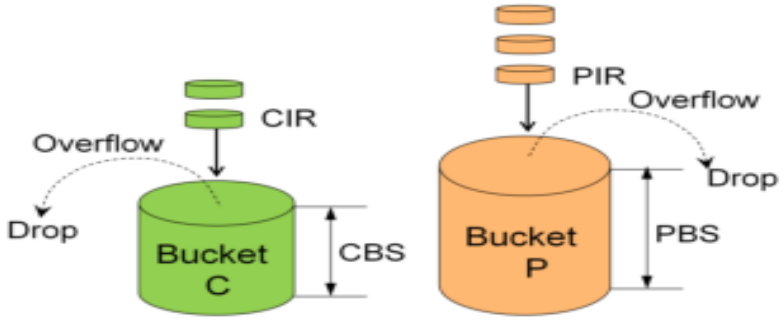

Fig.2.6: Token Bucket implementation of traffic shaping [18].

In the token bucket committed information rate (CIR) indicates the rate at which tokens are placed into the bucket, committed burst size (CBS) indicate the capacity of token burst, peak information rate (PIR) indicates maximum rate at which interface allow packets to pass and peak burst size (PBS) indicate the maximum volume of traffic that an interface allows to pass through in the interface burst shortly.

Traffic policing is used to restrict the total traffic and burst traffic that enters a network, which provides basic QoS functions to ensure network stability [13]. Traffic policing (TP) is used to monitor the specifications of the traffic that enters a network and keep it within a reasonable range. In addition, TP optimizes network resources and protects the interests of carriers by restricting the traffic that exceeds the rate limit.

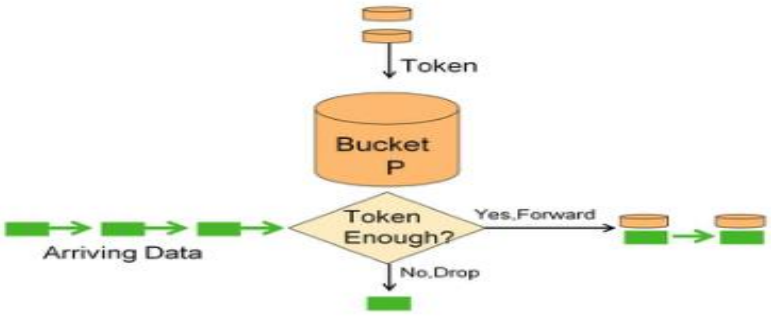

Fig.2.7: Implementation of traffic Policing [34].

Traffic policing uses committed access rate (CAR) to control the traffic. CAR uses token buckets to meter the traffic rate. Based on the metering forward, discard, change priority before forwarding and send to the next level policing action can implement.

Traffic shaping can delay the traffic to avoid many packets from being dropped and avoid the congestion at the egress. So, traffic shaping increases the delay. The simple implementation of traffic shaping is shown in fig.3.8 [13] [34].

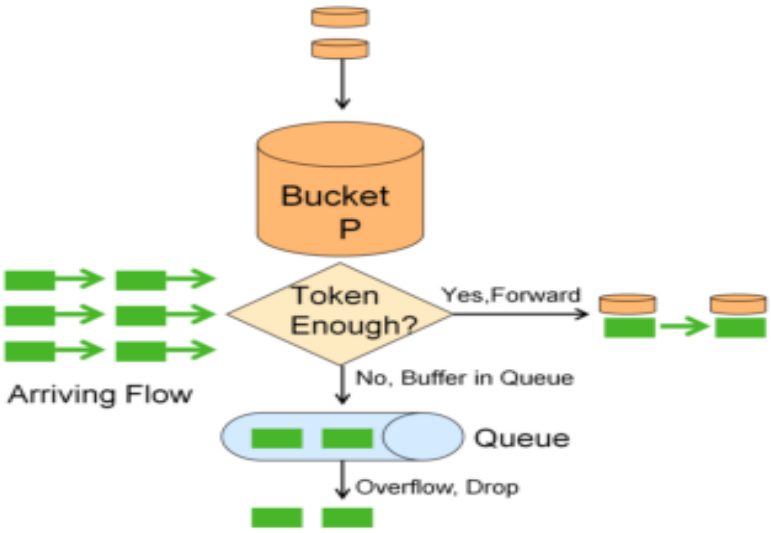

Fig.2.8: Implementation of traffic shaping [34].

2.1.5.12. Congestion Management Mechanisms

When the network is congested, managing it by queue scheduling technologies to base on the priority of various queues. There is different queue scheduling for congestion mechanism in the MPLS VPN network [18].

- First in first out (FIFO)
- Priority Queueing (PQ) and
- Weight Fair Queueing (WFQ).

FIFO does not classify the packets. It is the default queueing mechanism. It is simple, fast, low in delay and does not require any additional configuration. It allows the packets to leave the queue in arrival order to the packet. A packet that arrives early can leave queue early shown in fig.3.9 [13] [18] [34]. However, bandwidth allocation does not are able to realize using it.

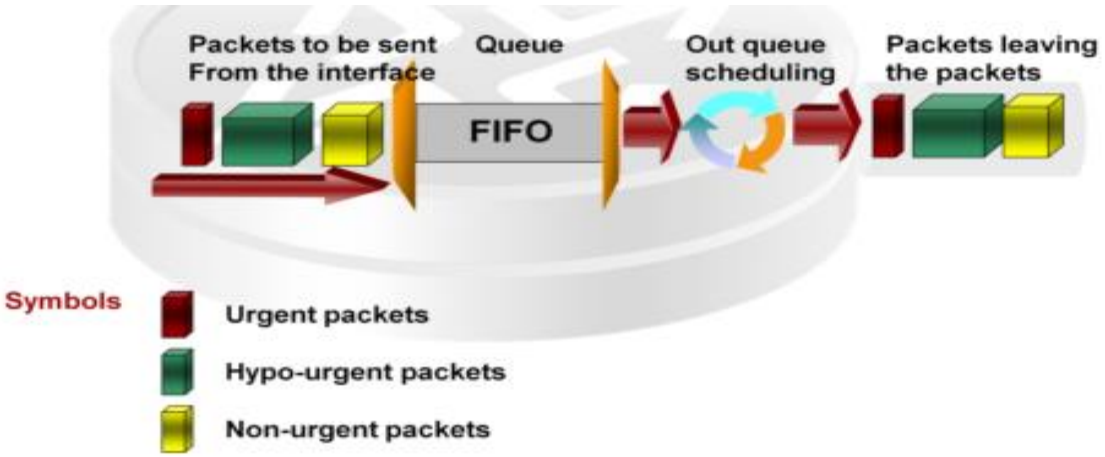

Fig.2.9: Implementation of a FIFO scheduling algorithm [13] [34].

In PQ packets in high priority queue are scheduled preferentially [12]. Packets in higher priority queue are sent first. PQ definitely able to secure the data transmission of higher importance service which is placed at a higher priority. However, if the bandwidth of the higher priority is not restricted, low priority packets cannot obtain bandwidth and reserved out as shown in fig.3.10 [12] [34].

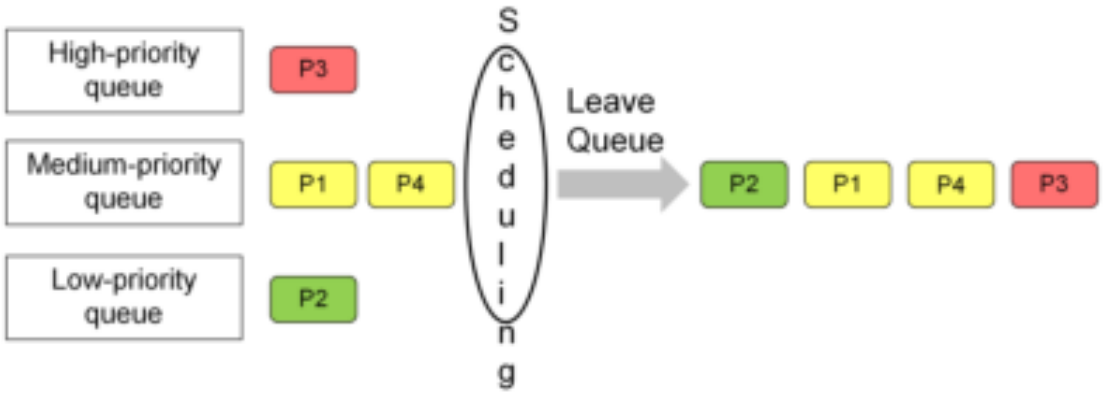

Fig.2.10: Implementation of priority queue scheduling algorithm [12] [34].

WFQ allocates specific bandwidth to flows based on the weight. In addition, to allocating bandwidth fairly to flows, it schedules packets in bits. The WFQ mechanism has two major purposes, to provide fair scheduling of flows and to secure that flow high IP precedence obtain a high bandwidth. However, no fixed bandwidth can be ensured. WFQ implementation are shortly described in fig.2.11 [13] [34].

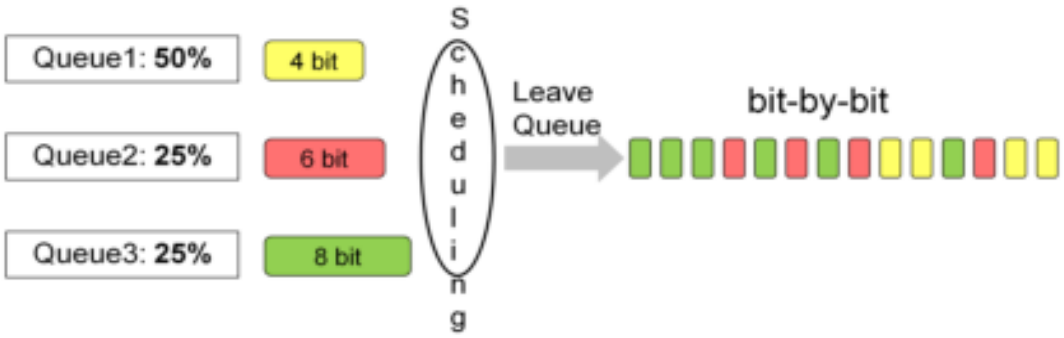

Fig.2.11: Simple Implementation of Weight Fair Queueing [13] [34].

Depending on the designed network appropriate queue scheduling mechanism can be used to guarantees QoS parameters such as bandwidth, delay, jitter, and packet drop rate.

2.1.5.13. Congestion Avoidance Mechanisms

Congestion avoidance is a traffic control mechanism that uses traffic scheduling to prevent the network from being overloaded [18]. With this mechanism, the device can monitor the usage of network resources such as queues and buffer areas in the memory and discard packets when network congestion is intensifying. The traditional packet drop policy uses the tail drop mechanism, which may lead to global TCP synchronization. Tail drop, random early detection and weighted random early detection are introduced to prevent global TCP synchronization. To avoid congestion, the following algorithms are introduced [18]:

- Tail Drop
- Random Early Detection (RED) and
- Weighted Random Early Detection (WRED).

In the traditional tail-drop policy [19], all the newly received packets are dropped when a queue reaches its maximum length. This policy may lead to global TCP synchronization. When queues drop the packets of several TCP connections at the same time, the TCP connections start to adjust their traffic simultaneously. There is a possibility that all the TCP connection sources begin the slow start process to perform congestion avoidance. Then, all the TCP connection sources start to build up traffic, causing the traffic to peak at a certain time. Therefore, traffic on the network fluctuates cyclically.

RED and WRED employ the random packet drop policy to avoid global TCP synchronization [19]. When the packets of a TCP connection are dropped and sent at a lower rate, the packets of other TCP connections are still being sent at a relatively higher rate. There are always some TCP connections whose packets are sent at a relatively higher rate, improving the utilization of network bandwidth. RED has three drop modes [19] [22]; green packet not dropped, yellow packet dropped at the certain possibility and red packet dropped at all.

If packets are dropped by directly comparing the length of queues with the upper and lower limits (which set the absolute length of the queue threshold), the transmission of burst data stream is affected. The average queue length is hence used to set the relative value to compare the queue threshold and the average queue length. The average length of a queue is the average length of the queues passing through a low pass filter. It reflects queue changes and is not affected by the burst change in queue length. This prevents adverse impact on the burst data stream.

2.2. Related Works

There are several authors and researchers that have worked on the area of improving quality of service of MP BGP MPLS VPNs. Some of them have tried to describe the QoS of MPLS VPN from the customer LAN side, provider edge (PE) to the customer side, network backbone and others end-to-end QoS perspectives. In this section, notable related works are reviewed to lay the foundation for this study.

Sebastian N. and Desta D., in [21] worked on quality of service of access layer networks. They have optimized the network through physical and logical architectures to improve the end-to-end QoS. They have used weighted random early detection (WRED) algorithms for the logical architecture and minimum spanning tree for the physical and data link layers' architecture to increase effective bandwidth utilization and to improve the performances of the networks. According to their result, VPN technology can be used to improving the quality of service for customers. They advocated that the BGP MPLS protocol has its own benefits in network speed, stability, quality of services. They indicated that it can be used to detect denial of services (DoS) attacks.

The implementation of traffic engineering and addressing QoS in MPLS VPN based IP backbone has been done by Mushtaq A. et al, in [22]. They have verified that QoS and TE of IP based and MPLS based backbone network of service providers with their advantages and disadvantages.

They have demonstrated that QoS and TE of MPLS at the backbone of the service provider network using the graphical network simulator 3 (GNS3) simulator. They configured open shortest path first (OSPF) on the client side, both OSPF and MPLS on the service provider side, created a virtual route and forwarding (VRF) A and B for primary and backup connections, interconnected them by using MP BGP via importing and redistributing the route to BGP. When they compared the result obtained by conventional service provider networks with MPLS based service provider networks, a clear improvement in performance has been observed. By taking this as an input, they have resolute that MPLS is a better choice by service providers in their backbone networks to forward packets from source to destination for an optimal path with guaranteed delivery, assured bandwidth and minimum or even without jitter. Hence, it is possible to make end-to-end communicating users feel like as if they are on the same local area network.

Farsin S. et al., in [23], articulated that VPN in MPLS network with MP BGP to assure end-to-end QoS. They conducted simulation using GNS3 by configuring two companies with different VPN sites on the same backbone. They used Wireshark to monitor the traffic flow and quality of service. From their investigation, they identified that MP BGP MPLS VPN is the most popular standard [23]. This technology uses BGP as a control plane to provide VPN routing and MPLS as a transport technique to achieve isolation between customers traffic. Its popularity is from the fact that its capability to support quality of service, traffic engineering and a high number of customer's support (thousands of customers and hundreds of thousands of VPNs sites).

Gustavo L. and Lilia C. from Intelligent Internet Research Group in [24], worked on a framework that focuses on router reflector (RR) concepts for scalability, optimal network resource utilization and improving quality of services of BGP MPLS VPN. They have implemented BGP MPLS VPN networks according to RFC 4364 [25] using the OPNET simulator. They advised that BGP MPLS IP VPN solution can handle a growing size in the deployment of a VPN (in terms of VPN, sites, and routes).

Mohamed E. et al., in [26], proposed an efficient quality of services scheme for MPLS VPN services to met user's peak demands. They have made six kinds of tests on MPLS VPN. From their tests, they proposed a better quality of services structure for MPLS VPN. This structure has the possibility to exceed the customer contracted bandwidth if residual bandwidth is available in the link.

A detailed review was done by Kanchan D. and Alam S. in [27] on quality of service improvement with MPLS mechanism in the next generation networks (NGNs). It is stated that the increased demand for new and broaden network in terms of quality of service plays an important role in providing better services for consumers. Hence, MPLS VPN techniques enabled to improve the quality of service. MPLS VPN is one of the simplest, scalable, flexible and dynamic ways to provide a better quality of service to users in a degraded condition, with fast failure node recovery and traffic engineering. These improved network performances and an end-to-end quality of services.

Radostina G. in [15], has worked on end-to-end network QoS guarantee. He has designed IP based and MPLS based network architectures. He built and evaluated both IP based and MPLS based network architectures. After the whole evaluation was made, it was seen that the MPLS architecture has much more benefits than IP based architecture. In the MPLS network, architecture end-to-end QoS has improved. This is due to the opportunity for traffic-engineering in the network, which helps for better traffic management end-to-end QoS.

Here the researcher tried to combine different methods and procedures that are used in the above-mentioned work as input and works on improving the quality of services of EthioTelecom MP BGP MPLS VPN SLA customers by using rational queue scheduling and congestion avoidance mechanism.

Chapter Three

Proposed Network Architectures

3.1. Introduction

For this present research, a simplified network architecture is built as showed (Fig. 3.1). It covers the main steps in designing QoS of BGP MPLS VPN network. The New Generation Network (NGN) network architecture was chosen according to the requirements for the design of networks with service provisioning and implemented end-to-end QoS. The proposed NGN network architecture can be easily scaled with simply appending new devices in the network.

In the proposed network architecture solution there are three types of routers, two P, four PE and two CE routers. P routers are the backbone routers. It provides MPLS label forwarding and maintains public network routing information. PE routers are directly connected with CE routers. The functions of PE routers are maintaining and processing VPN route information, forwarding VPN, running MP-BGP and MPLS protocols. It also has done label popping and imposition. CE routers are the edge router where customer's routers or personal computers (PCs) are connected.

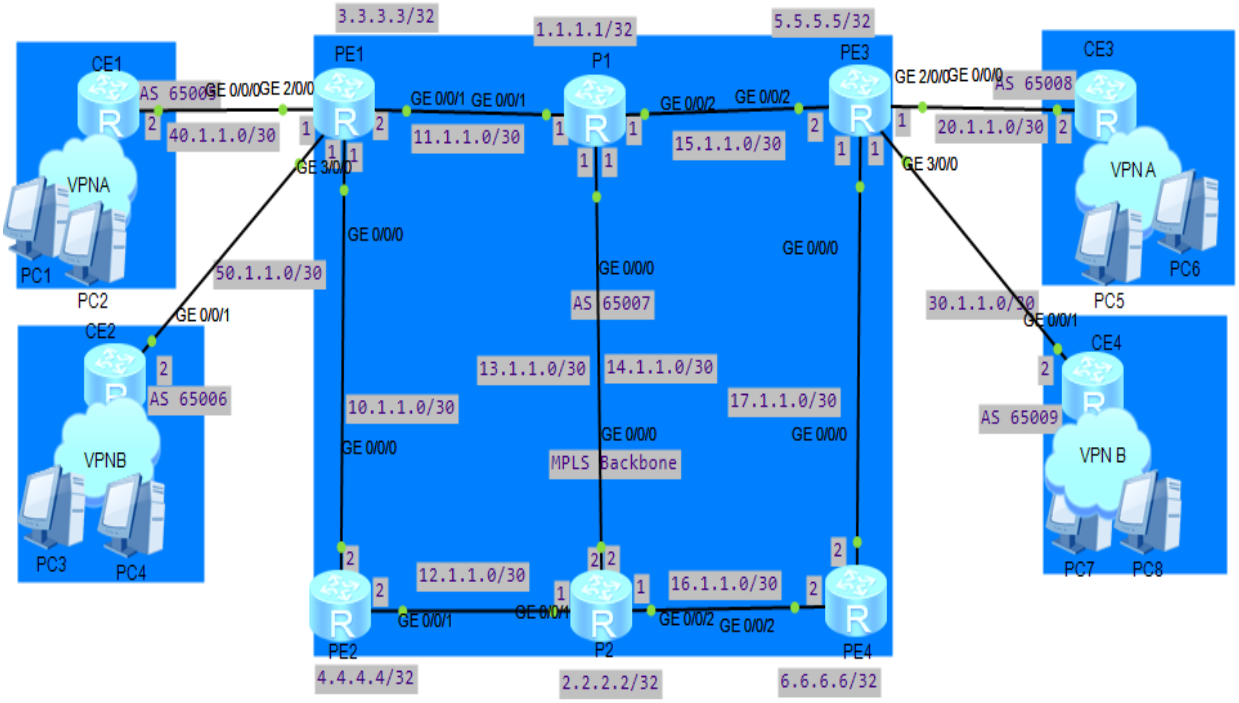

Fig.3.1: Simplified Proposed BGP MPLS VPN network architecture with end-to-end QoS.

The proposed network model is slightly modified for the purposes of testing congestion analysis. The VPN A and VPN Brouters are traffic generators. Two VPNs (both VPN As and both VPN Bs) were evaluated. Both are MPLS based with RSVP-TE signaling and tunneling and uses IS-IS for IGP interconnection. Both VPNs use the same networking equipment. The links and interfaces are similar in both VPN models. The QoS applied to the traffic running through the network is similar in both solutions.

The core network is realized as a core router and route reflector. The device is logically divided into two logical systems. These systems are acting like separate routers. They have full functional capabilities of two separate hardware devices. The connections between the two logical systems are made with peering the interfaces. The links with the other devices in the network are recognized with general Gigabit Ethernet interfaces.

The access and aggregation networks are made with secure service routers. They are working in multiprotocol label popping and positioning mode instead of the default packet flow, due to the MPLS architecture. The devices are working with Gigabit Ethernet interfaces. The links with the core networks are through Gigabit Ethernet and the links with the end devices are also with full Gigabit Ethernet.

The access and aggregation routers apply the QoS to the traffic from the end devices. The two VPN routers are traffic generators. For testing, the QoS applied in the traffic flow Wireshark is used. These modules provide functions as random traffic generation, fixed or non-fixed packet size, simultaneous generation of multiple traffic flows.

The uniform network entities for both VPNs networks of BGP MPLS VPN architectures tested are given in the following description. These units are IP address allocation, interface connections, and configuration, as well as the QoS, applied on the network.

3.2. Designed BGP MPLS VPN

3.2.1. Network IP Address

The IP address spaces in the network are described in the following steps. Most networks are private from the Internet's point of view and they have just a couple of uplink points connected to the internet. These uplink points are dedicated interfaces, which have public IP addresses and are assumed as external interfaces (external part of the network). This gives the opportunity to use private IP address spaces in the internal interfaces in the network.

To simplify IP addressing scheme in the proposed network different private IP address spaces are used. The class A network is dedicated for the connections between core routers, between core and aggregation routers, between aggregation and aggregation routers, between aggregation and access routers and for users in VPN A and VPN B interconnection. This address space is split into IP address spaces between different interfaces of the core, aggregation and access device and Loopback IP Addresses.

IP address spaces between Core, Aggregation, Access routers and End devices in the proposed network.

The IP address spaces for the connections between core, aggregation, access routers and End devices in the proposed network are chosen to be a class A networks. This gives an opportunity for scaling the network.

The connection between core routers (P1 and P2)

Host Range:	13.1.1.1 – 13.1.1.6
Broadcast address:	13.1.1.7
Host Range:	14.1.1.1 – 14.1.1.6
Broadcast address:	14.1.1.7

The connection between core routers (P1 and P2) and Aggregation routers (PE1, PE2, PE3, and PE4)

Host Range:	11.1.1.1 – 11.1.1.6	For interconnection between P1 and PE1.
Broadcast address:	11.1.1.7	
Host Range:	12.1.1.1 – 12.1.1.6	For interconnection between P2 and PE2.
Broadcast address:	12.1.1.7	
Host Range:	15.1.1.1 – 15.1.1.6	For interconnection between P1 and PE3.
Broadcast address:	15.1.1.7	

Host Range: 16.1.1.1 – 16.1.1.6 For interconnection between P2 and PE4.

Broadcast address: 16.1.1.7

The connection between Aggregation routers (PE1, PE2, PE3, and PE4)

Host Range: 10.1.1.1 – 10.1.1.6 For interconnection between PE1 and PE2.

Broadcast address: 10.1.1.7

Host Range: 17.1.1.1 – 17.1.1.6 For interconnection between PE3 and PE4.

Broadcast address: 17.1.1.7

The connection between Aggregation routers (PE1and PE3) and Access routers (CE1, CE2, CE3, and CE4)

Host Range: 20.1.1.1 – 20.1.1.6 For interconnection between PE1 and CE1.

Broadcast address: 20.1.1.7

Host Range: 30.1.1.1 – 30.1.1.6 For interconnection between PE1 and CE2.

Broadcast address: 30.1.1.7

Host Range: 40.1.1.1 – 40.1.1.6 For interconnection between PE3 and CE3.

Broadcast address: 40.1.1.7

Host Range: 50.1.1.1 – 50.1.1.6 For interconnection between PE3 and CE4.

Broadcast address: 50.1.1.7

Network Routers Loopback IP Addresses

P1 Loopback – 1.1.1.1/32

P2 Loopback – 2.2.2.2/32

PE1 Loopback – 3.3.3.3/32

PE2 Loopback – 4.4.4.4/32

PE3 Loopback – 5.5.5.5/32

PE2 Loopback – 6.6.6.6/32

CE1 Loopback – 7.7.7.7/32

CE2 Loopback – 8.8.8.8/32

CE3 Loopback – 9.9.9.9.9/32

CE2 Loopback – 10.10.10.10/32

3.2.2. Interfaces in the designed evaluation network architecture

The interfaces in the proposed network architecture are established with the following steps. The configuration is almost common for all interfaces. Only loopback have distinct differences in the way of their configuration. The loopback interfaces can't contain Mpls, Mpls LDP, Mpls te and Mpls rsvp-te configuration. The logical tunnel interfaces must contain peer unit in their configuration to establish a connection between all routers interfaces. The following command is the most common format to configure given Interfaces:

```
[PE1] interface Gigabit Ethernet 0/0/0

[PE1-GigabitEthernet0/0/0]ip address 10.1.1.1  30

[PE1-GigabitEthernet0/0/0]isis enable 1

[PE1-GigabitEthernet0/0/0]mpls

[PE1-GigabitEthernet0/0/0]mpls ldp

[PE1-GigabitEthernet0/0/0]mpls te

[PE1-GigabitEthernet0/0/0]mpls rsvp-te
```

But the interfaces between the core, aggregation, and access routers have shaped depending upon the QoS policy applied to the interfaces.

3.2.3. Interior Gateway Protocol (IGP) Interconnection

In the proposed network for the interconnection between P and PE routers, the IS-IS protocol has used. This is because of IS-IS protocol is more convergent. The following command is the most common format to configure IS-IS protocol.

```
[PE1] isis 1
[PE1-isis-1] is-level level-2
[PE1-isis-1] cost-style wide
[PE1-isis-1] network-entity 49.0001.0000.0000.0003.00
```

3.2.4. MPLS and MP BGP Interconnection

MPLS protocol is used for label switching and distribution. The following command is the most common format to configure MPLS globally.

```
[PE] Mpls user-id 3.3.3.3
[PE1] mpls
[PE1-mpls] quit
[PE1] Mpls ldp
[LSRA-mpls-ldp] quit
```

MP BGP protocol is used to create the peer relationship between different types of routers. The following command is the most common format to configure MP BGP.

```
[PE1] bgp 65007
[PE1] router-id 3.3.3.3
[PE1-bgp] peer 1.1.1.1 as-number 65007
[PE1-bgp] peer 1.1.1.1 Connect-interface loopback 0
[PE1-bgp] ipv4-family vpnv4
[PE1-bgp-af-vpnv4] peer 1.1.1.1 enable
[PE1-bgp-af-vpnv4] quit
[PE1-bgp] quit
```

3.2.5. Configuring a VPN instance Using MPLS RSVP-TE Tunnel

MPLS RSVP-TE is used to establish a TE tunnel from one router to another. It limits the maximum receivable bandwidth for links along the tunnel. TE tunnel has bandwidth constraints model such bandwidth allocation method.

To configure TE tunnel firstly enable MPLS, MPLS TE, and RSVP-TE globally on each router, enable MPLS, MPLS TE, and RSVP-TE on all tunnel interfaces, and enable CSPF in the system view on the ingress routers. The following command is the most common format to enable MPLS, MPLS TE, and RSVP-TE globally and interfaces.

```
[PE1] Mpls user-id 3.3.3.3
[PE1] mpls
[PE1-mpls] Mpls te
[PE1-mpls] Mpls rsvp-te
[PE1-mpls] Mpls te cspf
[PE1-mpls] quit
[PE1] interface gigabitethernet 0/0/0
[PE1-GigabitEthernet0/0/0] mpls
[PE1-GigabitEthernet0/0/0] Mpls te
[PE1-GigabitEthernet1/0/0] Mpls rsvp-te
[PE1-GigabitEthernet1/0/0] quit
```

Configure IS-IS TE and maximum receivable bandwidth and the maximum usable (BC0) bandwidth, creates the TE tunnel and limits the maximum receivable bandwidth on all tunnel interfaces. The following command is the most common format to in order configure IS-IS TE and maximum receivable bandwidth.

```
[PE1] isis 1
[PE1-isis-1] cost-style wide
[PE1-isis-1] traffic-engineering level-2
[PE1-isis-1] quit
[PE1] interface gigabitethernet 1/0/0
[PE1-GigabitEthernet0/0/0] Mpls te bandwidth max-reservable-bandwidth 150000
[PE1-GigabitEthernet0/0/0] Mpls te bandwidth bc0 150000
[PE1-GigabitEthernet0/0/0] quit
```

Create tunnel interfaces on the ingress routers. Then configure IP addresses for the tunnel interfaces, tunnel protocol, destination address, tunnel ID, dynamic signaling protocol and tunnel bandwidth. Finally, commit the configurations to validate them using the Mpls te commit command. The following command is the most common format to create a tunnel and configure IP addresses for the tunnel.

```
[PE1] interface tunnel 1/0/0
```

[PE1-Tunnel1/0/0] ip address unnumbered interface loopback 0

[PE1-Tunnel1/0/0] tunnel-protocol mpls te

[PE1-Tunnel1/0/0] destination 5.5.5.5

[PE1-Tunnel1/0/0] mpls te tunnel-id 100

[PE1-Tunnel1/0/0] mpls te signal-protocol rsvp-te

[PE1-Tunnel1/0/0] mpls te bandwidth ct0 20000

[PE1-Tunnel1/0/0] mpls te commit

[PE1-Tunnel1/0/0] quit

3.2.6. Configure VPN instances on PEs

VPN instances has VPN name, route distinguisher and route target. After configuring VPN instances and bind the instances to the CE interfaces. The following command are the most common format to configure VPN instance and bind the instance to the interfaces.

[PE1] ip vpn-instance CBE

[PE1-vpn-instance-vpna] ipv4-family

[PE1-vpn-instance-vpna-af-ipv4] route-distinguisher 100:1

[PE1-vpn-instance-vpna-af-ipv4] vpn-target 111:1 both

[PE1-vpn-instance-vpna-af-ipv4] quit

[PE1-vpn-instance-vpna] quit

[PE1] ip vpn-instance NBE

[PE1-vpn-instance-vpnb] ipv4-family

[PE1-vpn-instance-vpnb-af-ipv4] route-distinguisher 100:2

[PE1-vpn-instance-vpnb-af-ipv4] vpn-target 222:2 both

[PE1-vpn-instance-vpnb-af-ipv4] quit

[PE1-vpn-instance-vpnb] quit

[PE1] interface gigabitethernet 1/0/0

[PE1-GigabitEthernet1/0/0] ip binding vpn-instance CBE

[PE1-GigabitEthernet1/0/0] ip address 20.1.1.1 30

[PE1-GigabitEthernet1/0/0] quit

[PE1] interface gigabitethernet 2/0/0

[PE1-GigabitEthernet2/0/0] ip binding vpn-instance NBE

[PE1-GigabitEthernet2/0/0] ip address 30.1.1.1 30

[PE1-GigabitEthernet2/0/0] quit

3.2.7. Creating EBGP peer relationship between the PE and CE routers

To establish the EBGP peer relationship between the PE and CE to import VPN routes on CEs routers and PEs routers. The following command are the most common format to enable EBGP peer relationship.

```
[CE1] bgp 65008
[CE1-bgp] peer 20.1.1.2 as-number 65007
[CE1-bgp] import-route direct
[CE1-bgp] quit
[PE1] bgp 65007
[PE1-bgp] ipv4-family vpn-instance CBE
[PE1-bgp-vpna] peer 20.1.1.1 as-number 65008
[PE1-bgp-vpna] import-route direct
[PE1-bgp-vpna] quit
[PE1-bgp] ipv4-family vpn-instance NBE
[PE1-bgp-vpnb] peer 30.1.1.1 as-number 65008
```

3.3. Designed QoS of Proposed network architectures

The designed QoS is to provide different levels of service quality based on different requirements to met SLA targets and ITU threshold quality requirements of different VPNs. Managing maximum receivable bandwidth, reducing transmission, queueing and processing delay, managing jitter and packet loss are the main focuses of the design.

QoS assurance is designed based on the existing resources by using rational scheduling and congestion avoidance methods. Differentiated service model (DiffServ) have used to classify, mark and shape the networks based on the existing SLA agreements. This can have applied by the following step by step processes.

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

The QoS assurance initially must have basic BGP MPLS VPN designed conditions for their design and evaluation.

3.3.1. Define Access Control List rules

ACLs are used specify which VPNs are granted to guarantee the required services quality within the time. Define ACL rules Configure complex traffic classification on CE routers to control the traffic that accesses CEs from the local networks. The following command is the most common format to define ACL.

```
[CE1] acl number 2001
[CE1-acl-basic-2001] rule permit source 1.1.1.0 0.0.0.255
[CE1-acl-basic-2001] quit
[CE1] acl number 2002
[CE1-acl-basic-2002] rule permit source 2.1.1.0 0.0.0.255
[CE1-acl-basic-2002] quit
[CE1] acl number 2003
[CE1-acl-basic-2003] rule permit source 3.1.1.0 0.0.0.255
[CE1-acl-basic-2003] quit
[CE1] acl number 3001
[CE1-acl-basic-3001] rule 0 permit UDP destination-port eq DNS
[CE1-acl-basic-3001] rule 1 permit UDP destination-port eq snmp
[CE1-acl-basic-3001] rule 2 permit UDP destination-port eq SNMP trap
[CE1-acl-basic-3001] rule 3 permit UDP destination-port eq Syslog
[CE1-acl-basic-3001] quit
[CE1] acl number 3002
[CE1-acl-basic-3002] rule 4 permit up
[CE1-acl-basic-3002] quit
```

3.3.2. Define traffic classifiers

In the proposed network QoS classification is implemented by marking types of the services. Classification classifies the packets while packets unchanged. It is based on the DiffServ Code Point (DSCP) values of IP packets. The traffic of different service level can be identified. Then the defined ACL can have applied to it. The following command is the most common format to define traffic classifiers.

[CE1] traffic classifier a

[CE1-classifier-a] if-match all 2001

[CE1-classifier-a] quit

[CE1] traffic classifier b

[CE1-classifier-b] if-match all 2002

[CE1-classifier-b] quit

[CE1] traffic classifier up limit

[CE1-classifier-udplimit] if-match all 3001

[CE1-classifier-udplimit] quit

[CE1] traffic classifier udplimit1

[CE1-classifier-udplimit1] if-match all 3002

[CE1-classifier-udplimit1] quit

3.3.3. Define traffic behavior

In the proposed network traffic behavior is used to ensure the capability of the devices support DSCP. It includes configuring traffic policing and re-marks DSCP values. Committed information rate (CIR) indicates the rate at which the tokens are placed into the bucket. Committed burst size (CBS) indicates the capacity of the bucket, whereas packet burst size (PBS), shows the maximum volume of the traffic that can the interface allows to pass through the traffic burst. Then the Committed access rate (CAR) used to policing specific excess traffics are dropped or remarked. All packets are marked according to predefined traffic classifier match rule. The following command is the most common format to define traffic behavior.

[CE1] traffic behavior e

[CE1-behavior-e] car car 10000 CBS 150000 PBS 0

[CE1-behavior-e] remark dscp 40

[CE1-behavior-e] quit

[CE1] traffic behavior f

[CE1-behavior-f] car car 5000 CBS 100000 PBS 0

[CE1-behavior-f] remark dscp 26

[CE1-behavior-f] quit

[CE1] traffic behavior g

[CE1-behavior-g] car car 2000 CBS 100000 PBS 0

[CE1-behavior-g] remark dscp 0

[CE1-behavior-g] quit

[CE1] traffic behavior up limit

[CE1-behavior-udplimit] permit

[CE1-behavior-udplimit] quit

[CE1] traffic behavior udplimit1

[CE1-behavior-udplimit1] car 5000 CBS 100000 PBS 150000 green pass yellow discard red discard

[CE1-behavior-udplimit1] quit

3.3.4. Define traffic policies

Traffic policing control the rate of the incoming packet to ensure the network resources are properly allocated. When the traffic rate of the connection exceeds the specification on an interface, it allows remarking the excess packet depending on the priority to maximize the network resource usage.

Traffic policy implements on the QoS requirement defined in the SLA. The SLA contains parameters such as CIR, CAR, PBS and CBS which are predefined on the traffic behavior. The following command is the most common format to define traffic policies.

[CE1] traffic policy 1

[CE1-trafficpolicy-1] classifier a behavior e

[CE1-trafficpolicy-1] quit

[CE1] traffic policy 2

[CE1-trafficpolicy-2] classifier b behavior f

[CE1-trafficpolicy-2] quit

[CE1] traffic policy 3

[CE1-trafficpolicy-3] classifier c behavior g

[CE1-trafficpolicy-3] quit

[CE1] traffic policy up limit

[CE1-trafficpolicy-udplimit] classifier UDP limit behavior up limit

[CE1-trafficpolicy-udplimit] classifier udplimit1 behavior udplimit1

[CE1-trafficpolicy-3] quit

3.3.5. Apply the traffic policies

Applying the predefined policies to the inbound interfaces routers. The predefined policies are used to guarantee the service requirements of SLA. The following command is the most common format to apply traffic policies to the inbound interfaces.

```
[CE1] interface gigabitethernet 1/0/0
[CE1-GigabitEthernet1/0/0] undo shutdown
[CE1-GigabitEthernet1/0/0] traffic-policy 1 inbound
[CE1-GigabitEthernet1/0/0] quit
[CE1] interface gigabitethernet 3/0/0
[CE1-GigabitEthernet3/0/0] undo shutdown
[CE1-GigabitEthernet3/0/0] traffic-policy 2 inbound
[CE1-GigabitEthernet3/0/0] quit
[CE1] interface gigabitethernet 4/0/0
[CE1-GigabitEthernet4/0/0] undo shutdown
[CE1-GigabitEthernet4/0/0] traffic-policy 3 inbound
[CE1] interface gigabitethernet 2/0/0
[CE1-GigabitEthernet2/0/0] undo shutdown
[CE1-GigabitEthernet2/0/0] traffic-policy UDP limit outbound
```

3.4. Experimental Results of Proposed Architecture

The proper functioning of the designed QoS of BGP MPLS VPN network architectures include:

- All protocols are fully operating
- Proper implementation of the designed QoS
- Provisioning of the necessary services ensuring L3VPN operation and
- Redundancy of network resources which includes rerouting in case of link or node failure.

The necessities for fulfilling these requirements have discussed with the relevant tests for each of them. To be entrusted the proper functioning of the network first the basic components have checked.

3.4.1. IGP protocol (IS-IS)

In proposed architectures first, the IS-IS operation is checked. Since it is one of the basic components of the designed models. Checking IS-IS routing protocol involves testing its routing information, established neighbors, link state database, and interface enabled with IS-IS.

To check the IS-IS routing information “display isis route” command is used. It checks whether routes are learned by other routers. Route information includes all direct routes and the routes to loopback interfaces.

```
<PE1>display isis route

                Route information for ISIS(1)
                -----------------------------

               ISIS(1) Level-2 Forwarding Table
               --------------------------------

IPV4 Destination    IntCost    ExtCost ExitInterface   NextHop        Flags
-------------------------------------------------------------------------------
3.3.3.3/32          0          NULL    Loop0           Direct         D/-/L/-
6.6.6.6/32          30         NULL    GE0/0/1         11.1.1.1       A/-/-/-
                               GE0/0/0         10.1.1.2
2.2.2.2/32          20         NULL    GE0/0/1         11.1.1.1       A/-/-/-
                               GE0/0/0         10.1.1.2
5.5.5.5/32          20         NULL    GE0/0/1         11.1.1.1       A/-/-/-
1.1.1.1/32          10         NULL    GE0/0/1         11.1.1.1       A/-/-/-
10.1.1.0/30         10         NULL    GE0/0/0         Direct         D/-/L/-
11.1.1.0/30         10         NULL    GE0/0/1         Direct         D/-/L/-
12.1.1.0/30         20         NULL    GE0/0/0         10.1.1.2       A/-/-/-
13.1.1.0/30         20         NULL    GE0/0/1         11.1.1.1       A/-/-/-
14.1.1.0/30         20         NULL    GE0/0/1         11.1.1.1       A/-/-/-
15.1.1.0/30         20         NULL    GE0/0/1         11.1.1.1       A/-/-/-
16.1.1.0/30         30         NULL    GE0/0/1         11.1.1.1       A/-/-/-
                               GE0/0/0         10.1.1.2
17.1.1.0/30         30         NULL    GE0/0/1         11.1.1.1       A/-/-/-
4.4.4.4/32          10         NULL    GE0/0/0         10.1.1.2       A/-/-/-
    Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
                   U-Up/Down Bit Set
```

Fig.3.2: IS-IS route information.

To check the IS-IS neighbor relationship information “display isis peer verbose” command is used. It checks the adjacency relationship.

```
<PE1>dis isis peer  verbose

                  Peer information for ISIS(1)

  System Id     Interface         Circuit Id       State HoldTime Type     PRI
------------------------------------------------------------------------------
0000.0000.0004  GE0/0/0           0000.0000.0003.01 Up   27s      L2       64

  MT IDs supported     : 0(UP)
  Local MT IDs         : 0
  Area Address(es)     : 49.0001
  Peer IP Address(es)  : 10.1.1.2
  Uptime               : 00:26:32
  Adj Protocol         : IPV4
  Restart Capable      : YES
  Suppressed Adj       : NO
  Peer System Id       : 0000.0000.0004

0000.0000.0001  GE0/0/1           0000.0000.0001.03 Up   9s       L2       64

  MT IDs supported     : 0(UP)
  Local MT IDs         : 0
  Area Address(es)     : 49.0001
  Peer IP Address(es)  : 11.1.1.1
  Uptime               : 00:26:38
  Adj Protocol         : IPV4
  Restart Capable      : YES
  Suppressed Adj       : NO
  Peer System Id       : 0000.0000.0001


Total Peer(s): 2
```

Fig.3.3: IS-IS neighbor relationship.

To check the IS-IS link-state database information “display isis lsdb” command is used.

```
<PE1>display isis lsdb

                Database information for ISIS(1)
                --------------------------------

                 Level-2 Link State Database

LSPID             Seq Num     Checksum     Holdtime     Length  ATT/P/OL
-------------------------------------------------------------------------------
0000.0000.0001.00-00  0x00000011  0x5035       1120         615     0/0/0
0000.0000.0001.03-00  0x00000003  0x5d19       1103         54      0/0/0
0000.0000.0001.04-00  0x00000003  0x84ee       1103         54      0/0/0
0000.0000.0002.00-00  0x0000000d  0xadd6       1103         615     0/0/0
0000.0000.0002.01-00  0x00000003  0x4137       1103         54      0/0/0
0000.0000.0002.02-00  0x00000003  0x3a3d       1103         54      0/0/0
0000.0000.0002.03-00  0x00000002  0x7af9       1101         54      0/0/0
0000.0000.0002.04-00  0x00000003  0x9fd0       1101         54      0/0/0
0000.0000.0003.00-00* 0x0000000d  0x6a83       1102         337     0/0/0
0000.0000.0003.01-00* 0x00000003  0x8ae8       1102         54      0/0/0
0000.0000.0004.00-00  0x0000000d  0xf1fc       1114         337     0/0/0
0000.0000.0005.00-00  0x00000010  0x9828       1103         337     0/0/0
0000.0000.0005.01-00  0x00000003  0xc0ac       1101         54      0/0/0
0000.0000.0006.00-00  0x0000000c  0x6150       1120         337     0/0/0

Total LSP(s): 14
   *(In TLV)-Leaking Route, *(By LSPID)-Self LSP, +-Self LSP(Extended),
       ATT-Attached, P-Partition, OL-Overload
```

Fig.3.4: IS-IS link-state database.

To check the IS-IS interface information “display isis interface” command is used.

```
<PE1>display isis interface

                Interface information for ISIS(1)
                ----------------------------------
Interface      Id    IPV4.State      IPV6.State     MTU  Type  DIS
GE0/0/0        001       Up            Down       1497 L1/L2 No/Yes
GE0/0/1        002       Up            Down       1497 L1/L2 No/No
Loop0          001       Up            Down       1500 L1/L2 --
```

Fig.3.5: Interface IS-IS enabled.

To check the IS-IS overall information “display isis brief” command is used.

```
<PE1>dis isis brief

              ISIS Protocol Information for ISIS(1)
              -------------------------------------
SystemId: 0000.0000.0003      System Level: L2
Area-Authentication-mode: NULL
Domain-Authentication-mode: NULL
Ipv6 is not enabled
ISIS is in invalid restart status
Level-2 Application Supported: MPLS Traffic Engineering
L2 MPLS TE is enabled
ISIS is in protocol hot standby state: Real-Time Backup

Interface: 10.1.1.1(GE0/0/0)
Cost: L1 10       L2 10           Ipv6 Cost: L1 10   L2 10
State: IPV4 Up                    IPV6 Down
Type: BROADCAST                   MTU: 1497
Priority: L1 64   L2 64
Timers:    Csnp: L1 10   L2 10   ,Retransmit: L12 5   , Hello: L1 10 L2 10  ,

Hello Multiplier: L1 3    L2 3    , LSP-Throttle Timer: L12 50

Interface: 11.1.1.2(GE0/0/1)
Cost: L1 10       L2 10           Ipv6 Cost: L1 10   L2 10
State: IPV4 Up                    IPV6 Down
Type: BROADCAST                   MTU: 1497
Priority: L1 64   L2 64
Timers:    Csnp: L1 10   L2 10   ,Retransmit: L12 5   , Hello: L1 10 L2 10  ,

Hello Multiplier: L1 3    L2 3    , LSP-Throttle Timer: L12 50

Interface: 3.3.3.3(Loop0)
Cost: L1 0        L2 0            Ipv6 Cost: L1 0    L2 0
State: IPV4 Up                    IPV6 Down
Type: P2P                        MTU: 1500
Priority: L1 64   L2  64
Timers:    Csnp: L12 10  , Retransmit: L12 5   , Hello: 10  ,
Hello Multiplier: 3          , LSP-Throttle Timer: L12 50
```

Fig.3.6: IS-IS brief information.

From the output of these commands, each router is connected to the other devices loopback addresses which is an important prerequisite for the proper functioning of the other components of the proposed network.

The outcome of the routers in Fig.3.4 means that the IS-IS protocol successfully established its link-state database of the network and built its routing table. The information about IS-IS interfaces

(Fig.3.5) is important for updating routing information when there is a change of the network topology.

The outcome of the routers (Fig.3.3) shows that the routers made a neighbor relationship with each other, and the links between them are functioning normally. From the brief information of the protocol (Fig.3.6) can be seen that the establishment of the routing table has passed. It is further understood that the protocol is configured to work with the signaling protocol RSVP-TE and MPLS TE.

3.4.2. Signaling protocol RSVP-TE

Resource reservation setup protocol with traffic engineering is used for signaling in the proposed architectures. To check the RSVP-TE overall information "display Mpls rsvp-te" command is used.

```
<PE1>dis mpls rsvp-te
LSR ID: 3.3.3.3
RSVP-TE Function Capability: Enable
Resv Confirmation Request: DISABLE
RSVP Hello Extension: DISABLE
Hello interval: 3 sec        Max Hello misses: 3
Path and Resv message refresh interval: 30 sec
Path and Resv message refresh retries count: 3
Blockade Multiplier: 4
Graceful-Restart Capability: DISABLE
Bfd Enabled: DISABLE              Bfd Min-Tx: 1000
Bfd Min-Rx: 1000                  Bfd Detect-Multi: 3
```

Fig.3.7: RSVP-TE detail information.

3.4.3. MPLS TE Tunnel

MPLS TE is used to control the excess traffic and avoid congestion in the proposed network. It solves the process of the certain link being overloaded where the other idle. It also ensures full utilization of bandwidth resources. Checking MPLS TE functionality includes tunnel information, tunnel status of MPLS TE constraint shortest path database and MPLS TE session. To check the MPLS TE tunnel information "display interface tunnel" command is used.

```
<PE1>display interface tunnel
Tunnel0/0/0 current state : UP
Line protocol current state : UP
Last line protocol up time : 2018-04-16 21:19:00 UTC-08:00
Description:HUAWEI, AR Series, Tunnel0/0/0 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is unnumbered, using address of LoopBack0(3.3.3.3/32)
Encapsulation is TUNNEL, loopback not set
Tunnel destination 5.5.5.5
Tunnel up/down statistics 1
Tunnel protocol/transport MPLS/MPLS, ILM is available,
primary tunnel id is 0x2, secondary tunnel id is 0x0
Current system time: 2018-04-16 22:25:40-08:00
   300 seconds output rate 0 bits/sec, 0 packets/sec
   0 seconds output rate 0 bits/sec, 0 packets/sec
   0 packets output,  0 bytes
   0 output error
   0 output drop
   ct0:0 packets output,  0 bytes
      0 output error
      0 packets output drop
   Input bandwidth utilization  : --
   Output bandwidth utilization : --
```

Fig.3.8: MPLS TE tunnel information.

To check the MPLS TE tunnel status “display Mpls te tunnel-interface tunnel 0/0/0” command is used.

```
<PE1>dis mpls te tunnel-interface Tunnel 0/0/0
  ------------------------------------------------------------------
                    Tunnel0/0/0
  ------------------------------------------------------------------
  Tunnel State Desc   : UP
  Active LSP          : Primary LSP
  Session ID          : 100
  Ingress LSR ID      : 3.3.3.3         Egress LSR ID: 5.5.5.5
  Admin State         : UP              Oper State   : UP
  Primary LSP State     : UP
    Main LSP State      : READY             LSP ID  : 4
```

Fig.3.9: MPLS TE tunnel status.

To check the MPLS TE MPLS TE constraint shortest path database “display Mpls te cspf tedb all” command is used.

```
<PE1>display mpls te cspf tedb all
Maximum Nodes Supported: 1024      Current Total Node Number: 5
Maximum Links Supported: 2048      Current Total Link Number: 12
Maximum SRLGs supported: 5120      Current Total SRLG Number: 0
ID    Router-ID       IGP    Process-ID    Area        Link-Count
1     2.2.2.2         ISIS   1             Level-2     3
2     4.4.4.4         ISIS   1             Level-2     2
3     1.1.1.1         ISIS   1             Level-2     4
4     5.5.5.5         ISIS   1             Level-2     1
5     3.3.3.3         ISIS   1             Level-2     2
```

Fig.3.10: MPLS TE tunnels constraint shortest path database.

To check the MPLS TE MPLS TE session "display Mpls te session-entry" command is used.

```
<PE1>display mpls te session-entry

 Ingress-ID              : 3.3.3.3
 Tunnel-ID               : 100
 Egress-ID               : 5.5.5.5
 Crlsp num               : 1
 First TunnelTable index  : 0
 LSP No.     : 1
 LSP ID      : 3.3.3.3:100:1
 In/Out IF   : -/GE0/0/1
 Bandwidth(Kbit/sec):
   CT0 : 20000       CT1 : 0
```

Fig.3.11: MPLS TE tunnel session.

3.4.4. MPLS Operation

Checking the operation of MPLS involves testing its routing information, MPLS link state protocol, and MPLS adjacency. To check the MPLS routing information "display Mpls route-state" command is used.

```
<PE1>display mpls route-state
Codes: B(BGP), I(IGP), L(Public Label BGP), O(Original BGP), U(Unknow)
------------------------------------------------------------------------------
Dest/Mask        Next-Hop       Out-Interface          State LSP VRF Type
------------------------------------------------------------------------------

1.1.1.1/32       11.1.1.1       GE0/0/1                READY 2   0     I
2.2.2.2/32       10.1.1.2       GE0/0/0                READY 2   0     I
2.2.2.2/32       11.1.1.1       GE0/0/1                READY 2   0     I
3.3.3.3/32       127.0.0.1      InLoop0                READY 1   0     I
4.4.4.4/32       10.1.1.2       GE0/0/0                READY 2   0     I
5.5.5.5/32       11.1.1.1       GE0/0/1                READY 2   0     I
6.6.6.6/32       10.1.1.2       GE0/0/0                READY 2   0     I
6.6.6.6/32       11.1.1.1       GE0/0/1                READY 2   0     I
```

Fig.3.12: MPLS routing information.

To check the MPLS link state protocol “display Mpls LDP LSP all” command is used.

```
<PE1>display mpls ldp lsp all

LDP LSP Information in Public network
------------------------------------------------------------------------------
DestAddress/Mask  In/OutLabel   UpstreamPeer   NextHop       OutInterface
------------------------------------------------------------------------------

1.1.1.1/32       NULL/3        -            11.1.1.1      GE0/0/1
1.1.1.1/32       1031/3        1.1.1.1      11.1.1.1      GE0/0/1
1.1.1.1/32       1031/3        4.4.4.4      11.1.1.1      GE0/0/1
*1.1.1.1/32      Liberal/1030               DS/4.4.4.4
2.2.2.2/32       NULL/1025     -            10.1.1.2      GE0/0/0
                 NULL/1034     -            11.1.1.1      GE0/0/1
2.2.2.2/32       1025/1025     4.4.4.4      10.1.1.2      GE0/0/0
                 1025/1034     4.4.4.4      11.1.1.1      GE0/0/1
2.2.2.2/32       1025/1025     1.1.1.1      10.1.1.2      GE0/0/0
                 1025/1034     1.1.1.1      11.1.1.1      GE0/0/1
3.3.3.3/32       3/NULL        4.4.4.4      127.0.0.1     InLoop0
3.3.3.3/32       3/NULL        1.1.1.1      127.0.0.1     InLoop0
*3.3.3.3/32      Liberal/1026               DS/4.4.4.4
*3.3.3.3/32      Liberal/1030               DS/1.1.1.1
4.4.4.4/32       NULL/3        -            10.1.1.2      GE0/0/0
4.4.4.4/32       1026/3        4.4.4.4      10.1.1.2      GE0/0/0
4.4.4.4/32       1026/3        1.1.1.1      10.1.1.2      GE0/0/0
*4.4.4.4/32      Liberal/1031               DS/1.1.1.1
5.5.5.5/32       NULL/1032     -            11.1.1.1      GE0/0/1
5.5.5.5/32       1030/1032     1.1.1.1      11.1.1.1      GE0/0/1
5.5.5.5/32       1030/1032     4.4.4.4      11.1.1.1      GE0/0/1
*5.5.5.5/32      Liberal/1027               DS/4.4.4.4
6.6.6.6/32       NULL/1028     -            10.1.1.2      GE0/0/0
                 NULL/1033     -            11.1.1.1      GE0/0/1
6.6.6.6/32       1028/1028     4.4.4.4      10.1.1.2      GE0/0/0
                 1028/1033     4.4.4.4      11.1.1.1      GE0/0/1
6.6.6.6/32       1028/1028     1.1.1.1      10.1.1.2      GE0/0/0
                 1028/1033     1.1.1.1      11.1.1.1      GE0/0/1
------------------------------------------------------------------------------
TOTAL: 23 Normal LSP(s) Found.
TOTAL: 5 Liberal LSP(s) Found.
TOTAL: 0 Frr LSP(s) Found.
A '*' before an LSP means the LSP is not established
A '*' before a Label means the USCB or DSCB is stale
A '*' before a UpstreamPeer means the session is stale
A '*' before a DS means the session is stale
A '*' before a NextHop means the LSP is FRR LSP
```

Fig.3.13: MPLS link state protocol information.

To check the MPLS adjacency “display Mpls LDP adjacency” command is used.

```
<PE1>display mpls ldp adjacency

LDP Adjacency Information in Public Network
Codes: R: Remote Adjacency, L: Local Adjacency
A '*' before an adjacency means the adjacency is being deleted.
------------------------------------------------------------------------------
SN   SourceAddr     PeerID        VrfID AdjAge(DDDD:HH:MM) RcvdHello Type
------------------------------------------------------------------------------
 1   10.1.1.2       4.4.4.4       0    0000:00:28        347      L
 2   11.1.1.1       1.1.1.1       0    0000:00:19        230      L
------------------------------------------------------------------------------
TOTAL: 2 Record(s) found.
```

Fig.3.14: MPLS adjacency information

The router is configured to send the information explicitly on the path established. Fig.3.14 shows that the interfaces of the routers are fully functional. From the outputs of the devices in Fig.3.13, It can be concluded that it established LSPs function correctly.

When functioning, MPLS creates routing table entries (Fig.3.12). To provide Layer 3 VPN service MPLS creates a separate routing table. The paths have different labels assigned for forwarding data. LSP configured to create their own entries in the routing table that contain information about the metrics of the different paths.

3.4.5. BGP Protocol

Five AS number (AS 65005, AS 65006, AS 65007, AS 65008 and AS 65009) are used in the proposed network architecture. AS numbers are used since their count is ceasing fast with the rapid growth of networks and network users.

To check the BGP neighbor relationship information "display BGP peer" command is used.

```
<PE1>dis bgp peer

BGP local router ID : 10.1.1.1
Local AS number : 65007
Total number of peers : 3                 Peers in established state : 2

 Peer        V       AS  MsgRcvd  MsgSent  OutQ  Up/Down       State Pre
fRcv

 4.4.4.4     4    65007       0        0     0 00:03:14        Idle
 0
 5.5.5.5     4    65007       4        7     0 00:02:40 Established
 0
 6.6.6.6     4    65007       4        7     0 00:02:31 Established
 0
```

Fig.3.15: BGP neighbor relationship.

Fig.3.15 shows that BGP is fully operational and has established a neighbor relationship. BGP sessions are established. The L3VPN groups are properly signaled. The end routers traffic is properly forwarded and there is communication between the routers in the L3VPN services.

3.4.6. Performance of established L3VPN Service

The two L3VPN services are fully functional. To check detail routing information of the two L3VPN "display in VPN-instance verbose" command is used.

```
<PE1>display ip vpn-instance verbose
Total VPN-Instances configured      : 2
Total IPv4 VPN-Instances configured : 2
Total IPv6 VPN-Instances configured : 0

VPN-Instance Name and ID : CBE, 1
 Interfaces : GigabitEthernet0/0/2
Address family ipv4
 Create date : 2018/04/17 08:54:18 UTC-08:00
 Up time : 0 days, 00 hours, 10 minutes and 42 seconds
 Route Distinguisher : 100:1
 Export VPN Targets :  111:1
 Import VPN Targets :  111:1
 Label Policy : label per route
 Log Interval : 5

VPN-Instance Name and ID : NBE, 2
 Interfaces : GigabitEthernet3/0/0
Address family ipv4
 Create date : 2018/04/17 08:54:18 UTC-08:00
 Up time : 0 days, 00 hours, 10 minutes and 42 seconds
 Route Distinguisher : 100:2
 Export VPN Targets :  222:2
 Import VPN Targets :  222:2
 Label Policy : label per route
 Log Interval : 5
```

Fig.3.16: VPN instances routing information.

When the interfaces on routers are bound to the same VPN instance can exchange the information. The same VPN instance can ping each other. To check the reachability of the same VPN instance "ping VPN-instance CBE 20.1.1.2" command is used

```
<PE1>ping -vpn-instance CBE 20.1.1.2
  PING 20.1.1.2: 56  data bytes, press CTRL_C to break
    Reply from 20.1.1.2: bytes=56 Sequence=1 ttl=255 time=200 ms
    Reply from 20.1.1.2: bytes=56 Sequence=2 ttl=255 time=40 ms
    Reply from 20.1.1.2: bytes=56 Sequence=3 ttl=255 time=20 ms
    Reply from 20.1.1.2: bytes=56 Sequence=4 ttl=255 time=60 ms
    Reply from 20.1.1.2: bytes=56 Sequence=5 ttl=255 time=30 ms

  --- 20.1.1.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 20/70/200 ms
```

Fig.3.17: VPN instances reachability to access router.

```
<PE1>ping -vpn-instance NBE 50.1.1.1
 PING 50.1.1.1: 56  data bytes, press CTRL_C to break
   Reply from 50.1.1.1: bytes=56 Sequence=1 ttl=254 time=320 ms
   Reply from 50.1.1.1: bytes=56 Sequence=2 ttl=254 time=60 ms
   Reply from 50.1.1.1: bytes=56 Sequence=3 ttl=254 time=40 ms
   Reply from 50.1.1.1: bytes=56 Sequence=4 ttl=254 time=50 ms
   Reply from 50.1.1.1: bytes=56 Sequence=5 ttl=254 time=40 ms

 --- 50.1.1.1 ping statistics ---
   5 packet(s) transmitted
   5 packet(s) received
   0.00% packet loss
   round-trip min/avg/max = 40/102/320 ms
```

Fig.3.18: VPN instances reachability to aggregation router.

3.4.7. Quality of Service of proposed network architectures

The applied QoS in proposed network architectures is fully functional. to view the traffic policies, traffic classifiers defined in the traffic policies, and the traffic behaviors associated with the traffic classifiers “display traffic policy user-defined” command is used.

```
<PE1>display traffic policy user-defined
  User Defined Traffic Policy Information:
  Policy: pe
    Classifier: pe
     Operator: OR
      Behavior: pe
       Committed Access Rate:
         CIR 15000 (Kbps), PIR 20000 (Kbps), CBS 300000 (byte), PBS 500000 (byte)
         Color Mode: color Blind
         Conform Action: pass
         Yellow  Action: pass
         Exceed  Action: discard
```

Fig.3.19: user-defined QoS.

When the QoS of the proposed network architecture was verified from Wireshark, different parameters such as a frame, Ethernet, MPLS, TCP, BGP, and IP are functioning fully. Under IP the defined QoS, differentiated service field is operational with its parameters.

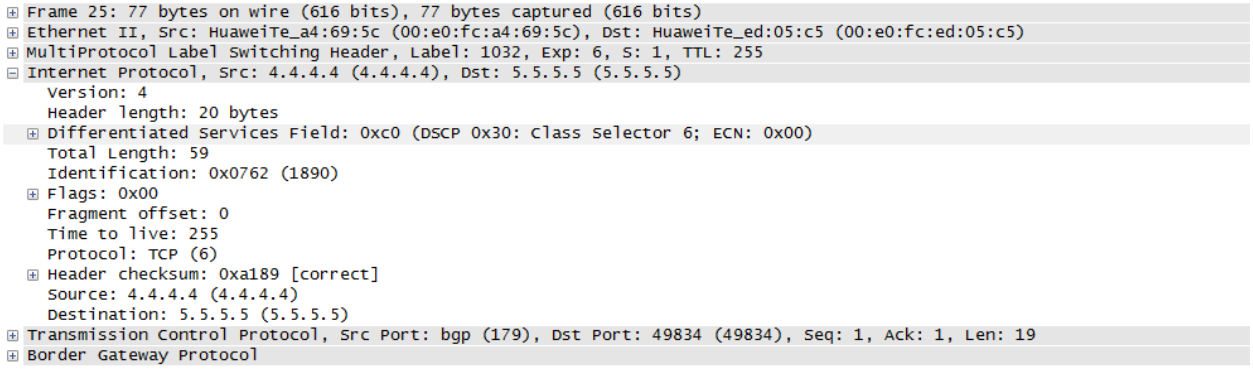

Fig.3.20: Defined QoS.

3.5. Discussions

The existing and proposed network architectures are the same in devices used and physical interconnection. But they have the differences, especially in QoS designing. Table 3.1 shows the similarities and differences between existing and proposed network architecture in detail manner.

Table 3.1 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	L3VPN	L3VPN
IGP Routing Protocol	IS-IS	IS-IS
NGN Backbone	MPLS	MPLS
QoS Model	Best effort model	Differentiated services model
Congestion Management	FIFO	Weighted fair queueing
Congestion Avoidance	Tail Drop	Weighted random early detection

QoS in the proposed network architectures is tested with Wireshark tool. A couple of scenarios (Fig.1.3 and Fig.3.1) are tested with different traffic streams with different parameters and speeds. In the first scenario, the existing network (Fig.1.3) performance is checked. The existing network architecture uses the best effort QoS. All traffic has equal priorities. The architecture uses a FIFO algorithm for congestion management and tail drop algorithm for congestion avoidance. In this case, the generated traffic consists of two VPN instance application traffic streams. The two VPN instance traffic flows emulate two end nodes connected to the CE routers. The traffic streams use TCP and are with speed of 10 Mbps and 15 Mbps respectively. The first test is made between CE1

and CE3 and the second test made between CE2 and CE4 routers. The results of this experiment are given on Fig.3.21.

In the second scenario (Fig.3.1) the proposed network architecture uses DiffServ QoS. The traffic has different priorities. The higher the traffic processed first. The architecture uses a weighted fair queueing algorithm for congestion management and weighted random early detection algorithm for congestion avoidance. In this case, the traffics were classified and priority is given to it depending on their SLA levels. Then traffic policies were defined and applied on an aggregation router outbound interface. In this case, the generated traffic consists of two VPN instance application traffic streams. The two VPN instance traffic flows emulate two end nodes connected to the CE routers. The traffic streams use TCP and are with speed of 10 Mbps and 15 Mbps respectively. The first test is made between CE1 and CE3 and the second test made between CE2 and CE4 routers. The results of this experiment are given on Fig.3.21.

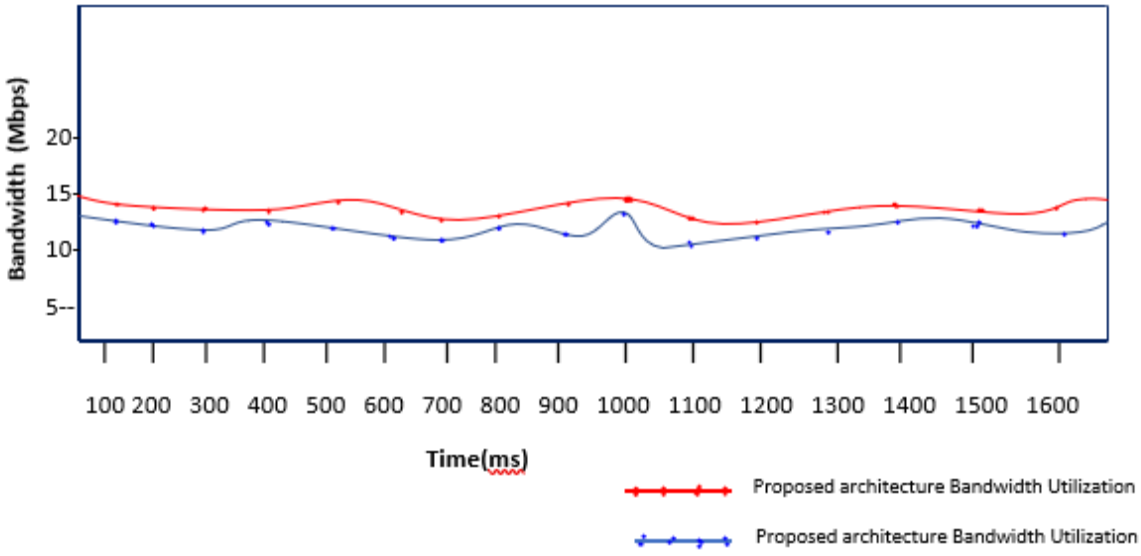

Fig.3.21: Bandwidth Utilization Measurement Comparison

From the fig.3.21 it can see that the existing network architecture overturns the bandwidth utilization. This is because of the existing network uses best effort QoS model which cannot isolate the services to guarantee the maximum data transfer. But in the proposed network architecture the bandwidth utilization is respectable. In this case, the network uses the DiffServ QoS model which isolated the network at each aggregation. The isolated aggregate guaranteed to transmit maximum number traffics. So, mission-critical traffic is transmitted firstly depending on their priorities.

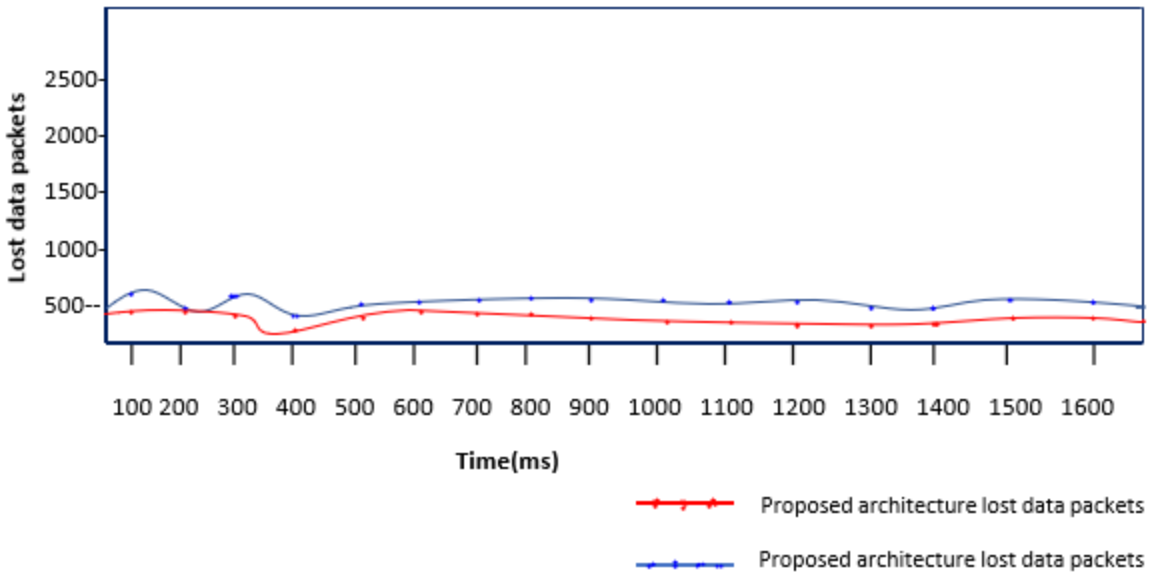

Fig.2.22: Packet Loss Measurement Comparison.

As it can be seen from the evaluation testing of Fig.3.22, the proposed network architectures, the implementation of DiffServ has many benefits for packet loss compared to the best effort. DiffServ model routers must store traffic and QoS information per aggregation. This creates enough buffer space in the routers, queue. A router usually has incoming interface buffers, system buffers, and outgoing interface buffers. In case of congestion, the traffic is remark and kept in buffer space to avoid the packet loss. But in the case of the best effort QoS model, the routers just route packets until they reach the destination. Other packets are dropped and cause a higher percentage of packet loss.

DiffServ QoS model has advantages to minimize the traffic loss. In case of congestion, this model classifies the traffic depending on their priority. The classified traffics are marked and shaped depending on the router maximum data transfer rate. Some traffic transmitted, whereas the excess traffics are remarked and transmit later. This decreases the packet loss ratio.

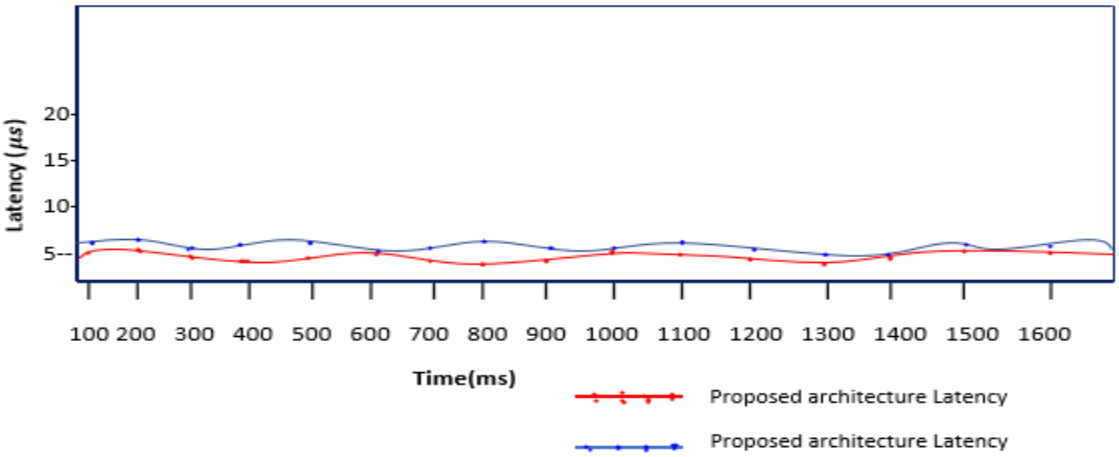

Fig.2.23: Latency Measurement Comparison.

The latency is the time that a packet waits before being transmitted. It can be seen from Fig.3.23, 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 3.1. Most of the results were as expected. The difference between packet loss and bandwidth in existing and proposed network architecture was visible. But the difference between end-to-end delay and jitter was not that much visible. This happened because we have used ten routers only on both network architectures. This reduces the transmission, serialization, queueing and processing delay. The difference was visible if the number of routers (nodes) increased.

Table 3.2 Exist and proposed network architecture numerical QoS results.

Parameters	Exit Network (Best Effort)			Proposed Network (DiffServ)		
	Result	SLA Targets	ITU threshold	Result	SLA Targets	ITU threshold
Packet loss (%)	1.897%	Out of Range	Out of Range	0.026%	Within Range	Out of Range
Delay(sec)	0.169	Within Range	Out of Range	0.14132	Within Range	Within Range
Jitter (sec)	0.001	Within Range	Out of Range	0.0007747	Within Range	Within Range
Bandwidth (bit/sec)	15068	Out of Range	Out of Range	15320	Within Range	Out of Range

Chapter Four

Conclusions and Future Works

4.1. Conclusions

In this research, the DiffServ model for the design of BGP MPLS VPN networks with end-to-end QoS was deliberated. This type of networks is suitable for implementation of QoS for VPN networks. A simplified network topology was created. Two network architectures were designed, built and evaluated with generic telecommunication equipment. Firstly, the existing BGP MPLS VPN network which used best effort QoS model was implemented and tested. Secondly, the proposed BGP MPLS VPN architecture which used the DiffServ QoS model was designed and tested. End-to-end QoS was designed and implemented in both network models. The implemented services were Layer 3 VPN services to handle traffic from end nodes in the proposed architecture. Both network architectures were fully functional. Verification of the applied end-to-end QoS parameters was made and results were obtained.

Bandwidth utilization, packet loss, latency and jitter measurements were made for both network models (Fig.1.3 and Fig.3.1). After the whole evaluations were made, it is seen that the proposed BGP MPLS VPN network architecture has much more benefits than the existing BGP MPLS VPN network architecture. This is due to the opportunity for the class of services and traffic-engineering in the network, which helps for better traffic management and provisioning of suitable end-to-end QoS. The proposed BGP MPLS VPN architecture which used DiffServ QoS model architecture could be used in many mission-critical applications. The opportunity for easy scalability of the network is in great help in today's rapidly growing VPN networks. This approach is suitable for higher priorities services, because of the low latency and low packet loss across the network.

In the proposed DiffServ QoS model better network productivity can be achieved. The designed BGP MPLS VPN architecture which used DiffServ QoS model network architecture is easy to scale and troubleshoot. The addition of new end devices in the network is simplified and just slight configuration changes are required. The problem with the fast ceasing number of available ASs is evaded by using single AS number in the core network architecture. Because of the implemented failure mechanisms in case of a link failure, the impact on network flow is ceased. The traffic

which entered the network is delivered through backup routes to minimize the traffic loss, while new paths are built. With the careful design of the applied QoS, the traffic requirements of the implemented applications are served.

In the proposed BGP MPLS VPN architecture, which used DiffServ QoS model architecture, all services got the required traffic handling. The designed BGP MPLS VPN network model can easily be used for L3VPN services in both centralized and distributed architectures. End-to-end MPLS solutions for the NGN applications are smoothly served.

The proposed approach provides more efficient use of network resources and reduction of the number of NGN nodes. It relies on a single MPLS forwarding scheme, which simplifies traffic management in the network. This way of service provisioning offers simplicity to the end nodes and depends more on the intelligent nodes in the core network. At the same time, it's implementation and maintenance are also simplified. The designed BGP MPLS VPN network can easily have implemented in the NGN core network. Then the architecture simply managed, configured and scaled with least efforts and almost without any operational costs.

Generally, based on the analysis and results gained, we conclude that the DiffServ QoS model was more reliable than the best effort QoS model for EthioTelecom BGP MPLS VPN network. As the whole research process, the main work pass through was traffic engineering, network optimization, and proper network utilization. The designed QoS used DiffServ model that have been guarantee all company's SLA QoS threshold. In a conclusion, the designed network provides a way of increasing network performance based on the DiffServ QoS model. High network performance indicates a high QoS service provider. High QoS service provider creates a satisfied and high quality of experience's customers.

4.2. Future Works

At the level of this work, the QoS has been guarantee with respect to the company's SLA QoS target. But in future, the network can be extended with more reliability functions. These functions include chassis clustering for access and aggregation devices, implementation of high availability features, implementation of LDP for MPLS label down streaming on demand.

Extended DiffServ services with more application specific QoS can be implemented. Layer 2 VPNs and VPLS can be included as a service in the network architecture. This can increase the scalability, availability, and security of layer 2 VPNs.

The good future extension is the implementation of self-organizing network architecture, such as self-learning, self-configuration and self-management, self-optimization, prediction of network congestion, prediction of traffic loops. To implement advanced extensions there are algorithms for prediction. Algorithms for adaptive training of the network such as the Widrow-Hoff algorithm can be of great use for process predictions in operating networks [40] [41]. This way the designed proposed BGP MPLS VPN architecture which used DiffServ QoS model network architecture can become optimal, which save operational and maintenance costs. It will be able to make self-optimization, based on collected data from previous network states and based on predictions. This way preventing congestion, failures, and loops.

References

[1]. Dr. Ahmad A. and Dr. Talal A.” Performance Analysis DiffServ based Quality of Service in MPLS Network's”, *International Journal of Scientific and Engineering Research*, Volume 6, September 2015.

[2]. EthioTelecom, “QoS Document” *MPLS VPN Services Quality and Customer Experience Related Issues and Complaint Analysis*, Version 02, 2017.

[3]. Huawei technologies co. ltd, “Configuration Guide VPN”, *Huawei technologies- Cloud Engine 12800 Series Switches*, volume 06, September 2017.

[4]. Cisco, “MPLS VPN QoS Design”, *End-to-End QoS Network Design, volume 3, March* 2017.

[5]. Cisco, “MPLS Layer 3 VPN”, *MPLS Layer 3 VPN Guide for Cisco ASR 9000 Series Routers, volume 6, July* 2017.

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

[7]. Luc De Ghein, “MPLS Fundamentals”, *Cisco Systems*, Cisco Press 800, 2015.

[8]. Vivek Alwayn,” Advanced MPLS Design and Implementation”, *Cisco Systems*, Cisco press 201, 2011.

[9]. Ivan Pepelnjak, Jim Guichard, *MPLS and VPN Architecture, Cisco Systems*, Cisco press 201 West 103rd Street Indianapolis, March 2001

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

[11]. Amir Ranjbar, "CCNP Certification Guide”, First *Edition, Cisco Press 800* USA, 2013,

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

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

[14]. Azhar S. and Bilal A., “MPLS VPN with DiffServ”, MS. Thesis, Halmstad University, February 2011.

[15]. Radostina G., "Network Design with Guaranteed End-to-End QoS", MS. Thesis, Aalborg University, June 2103.

[16]. Mohamed E., "Efficient QoS implementation for MPLS VPN", *International Conference on Advanced Information Networking and Applications,* IEEE, March 2016.

[17]. Gull H., "QoS in MPLS and IP Network", MS. Thesis, Karlskrona University, November 2009.

[18]. 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.

[19]. C. Huang, and Vishal S., "Building Reliable MPLS Networks Using a Path Protection Mechanism", *IEEE Communication Magazine,* Mar. 2012.

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

[21]. Dr. Sebastian N. and Desta D. "Modeling Network Optimization by Optimize the Current Network by physical and logical architectures to improve the QoS", *International Journal of Engineering Science and Computing,* Volume 7, August 2017.

[22]. Mushtaq A. and Abdul B. "Implementation of Traffic Engineering and Addressing QoS in MPLS VPN Based IP Backbone", International *Journal of Computer Science and Telecommunications,* Volume 5, June 2014.

[23]. Farsin S.et al. "VPN in MPLS network with MP BGP", *International Journal of Electronics and Communication Engineering,* March 2017.

[24]. Dr. Gustavo L. and Ing. Lilia C. "MPLS/VPN/BGP Networks Evaluation Techniques." *Institute of Electrical and Electronics Engineers (IEEE),* 2012.

[25] E. Rosen and Y. Rekhter, "BGP/MPLS IP Virtual Private Networks (VPNs)", *RFC 4364,* February 2006.

[26]. Mohamed E. and Marc-Andre B. "Efficient QoS implementation for MPLS VPN", *22nd International Conference on Advanced Information Networking and Applications IEEE Workshops,* 2008.

[27]. Kanchan D. and Alam S. “Review on QoS Improvement with MPLS Mechanism in NGN”, *International Journal of Innovative Research in Science*, Vol. 3, February 2014.

[28]. Brian M. and Neil L. "CCNP ISCW O Certification Guide", First Edition Published by Cisco Press 800, April 2016.

[29]. Mebratu D., “Traffic Analysis of Core Network in Case of EthioTelecom”, Addis Ababa University, May 2017.

[30]. ITU, “QoS Parameters”, *ITU-T Y.1541 Recommended QoS Target,* June 2012.

[31]. Ethio Telecom,”High-Level Design for NGN”, *designed network,* volume I June 2006.

[32]. Solomon T. and Hilina T.,” *EthioTelecom IP QoS parameters”,* Recommended IP-QOS performance targets, March 2015.

[33]. EthioTelecom,” Low-Level Design for IP Backhaul”, Final version, February 2013.

[34]. Huawei technologies co. ltd, “QoS Feature and Realization”, *quality of services,* volume II, May 2017.

[35]. ITU-T, “Network-based IP VPN over MPLS architecture”, *Global information infrastructure and internet protocol aspects;* 2011.

[36]. ITU-T, “Business Process Framework”, *Design document,* 2011.

[37]. Toni J., “QoS and QoE frameworks for converged services and applications”, *Regional Workshop for Europe,* November 2015, Bologna.

[38]. Ken P. et al “A Design Science Research Methodology for Information Systems Research”, *Research Guide,* Volume 24 Issue 3, Winter 2007.

[39]. EthioTelecom,” Service Provisioning Manual”, *Provisioning guide,* July 2014.

[40]. Stefanova S., “Time Series Prediction Using Linear Neural Networks”, *Annual Journal of Electronics, International Scientific Conference,* Bulgaria, September 2012.

[41]. ITU-T, “QoS support for VPN services Framework and characteristics” *Global information,* 2006.

Appendices

P1 Router Configuration

```
<P1>display current-configuration
#
sysname P1
#
mpls lsr-id 1.1.1.1
mpls
 mpls te
 mpls rsvp-te
#
mpls ldp
#
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher
;RJ0!+LK#L=H)H2[EInBx\`#
 local-user admin service-type http
#
isis 1
 is-level level-2
 cost-style wide
 network-entity 49.0001.0000.0000.0001.00
```

P2 Router Configuration

```
<P2>display current-configuration
#
sysname P2
#
mpls lsr-id 2.2.2.2
mpls
 mpls te
 mpls rsvp-te
#
mpls ldp
#
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher
;RJ0!+LK#L3IF$':[285x\I#
 local-user admin service-type http
#
isis 1
 is-level level-2
 cost-style wide
 network-entity 49.0001.0000.0000.0002.00
```

```
 traffic-eng level-2
#
firewall zone Local
 priority 16
#
interface GigabitEthernet0/0/0
 ip address 13.1.1.1 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 mpls rsvp-te
 mpls ldp
#
interface GigabitEthernet0/0/0.10
 ip address 14.1.1.1 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 mpls rsvp-te
 mpls ldp
#
interface GigabitEthernet0/0/1
 ip address 11.1.1.1 255.255.255.252
```

```
 traffic-eng level-2
#
firewall zone Local
 priority 16
#
interface GigabitEthernet0/0/0
 ip address 13.1.1.2 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 mpls rsvp-te
 mpls ldp
#
interface GigabitEthernet0/0/0.10
 ip address 14.1.1.2 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 mpls rsvp-te
 mpls ldp
#
interface GigabitEthernet0/0/1
 ip address 12.1.1.1 255.255.255.252
```

```
 isis enable 1
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 mpls rsvp-te
 mpls ldp
#
interface GigabitEthernet0/0/2
 ip address 15.1.1.1 255.255.255.252
 isis enable 1
 mpls
 mpls te
mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 mpls rsvp-te
 mpls ldp
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
 isis enable 1
#
user-interface con 0
user-interface vty 0 4
user-interface vty 16 20
#
return
```

```
 isis enable 1
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 mpls rsvp-te
 mpls ldp
#
interface GigabitEthernet0/0/2
 ip address 16.1.1.1 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 mpls rsvp-te
 mpls ldp
#
interface LoopBack1
 ip address 2.2.2.2 255.255.255.255
 isis enable 1
#
user-interface con 0
user-interface vty 0 4
user-interface vty 16 20
#
return
```

PE1 Router Configuration

```
<PE1>display current-configuration
[V200R003C00]
#
 sysname PE1
#
 snmp-agent local-engineid 800007DB03000000000000
 snmp-agent
#
 clock timezone China-Standard-Time minus 08:00:00
#
portal local-server load flash:/portalpage.zip
#
 drop illegal-mac alarm
#
 wlan ac-global carrier id other ac id 0
#
 set cpu-usage threshold 80 restore 75
#
ip vpn-instance CBE
 ipv4-family
  route-distinguisher 100:1
  vpn-target 111:1 export-extcommunity
  vpn-target 111:1 import-extcommunity
#
ip vpn-instance NBE
 ipv4-family
```

PE3 Router Configuration

```
<PE3>display current-configuration
[V200R003C00]
#
 sysname PE3
#
 snmp-agent local-engineid 800007DB03000000000000
 snmp-agent
#
 clock timezone China-Standard-Time minus 08:00:00
#
portal local-server load flash:/portalpage.zip
#
 drop illegal-mac alarm
#
 wlan ac-global carrier id other ac id 0
#
 set cpu-usage threshold 80 restore 75
#
ip vpn-instance CBE
 ipv4-family
  route-distinguisher 200:1
  vpn-target 111:1 export-extcommunity
  vpn-target 111:1 import-extcommunity
#
ip vpn-instance NBE
 ipv4-family
```

```
 route-distinguisher 100:2
 vpn-target 222:2 export-extcommunity
 vpn-target 222:2 import-extcommunity
#
mpls lsr-id 3.3.3.3
mpls
 mpls te
 mpls rsvp-te
#
mpls ldp
#
#
acl number 2001
 rule 5 permit source 40.1.1.0 0.0.0.248
acl number 2002
 rule 5 permit source 50.1.1.0 0.0.0.248
acl number 2003
 rule 5 permit source 60.1.1.0 0.0.0.248
#
acl number 3001
 rule 0 permit udp destination-port eq dns
 rule 1 permit udp destination-port eq snmp
 rule 2 permit udp destination-port eq
snmptrap
 rule 3 permit udp destination-port eq syslog
acl number 3002
 rule 4 permit udp
#
```

```
 route-distinguisher 200:2
 vpn-target 222:2 export-extcommunity
 vpn-target 222:2 import-extcommunity
#
mpls lsr-id 5.5.5.5
mpls
 mpls te
 mpls rsvp-te
#
mpls ldp
#
#
acl number 2001
 rule 5 permit source 20.1.1.0 0.0.0.248
acl number 2002
 rule 5 permit source 30.1.1.0 0.0.0.248
acl number 2003
 rule 5 permit source 10.1.1.0 0.0.0.248
#
acl number 3001
 rule 0 permit udp destination-port eq dns
 rule 1 permit udp destination-port eq snmp
 rule 2 permit udp destination-port eq
snmptrap
 rule 3 permit udp destination-port eq syslog
acl number 3002
 rule 4 permit udp
#
```

```
traffic classifier a operator or
 if-match acl 2001
traffic classifier udplimit operator or
 if-match acl 3001
traffic classifier udplimit1 operator or
 if-match acl 3002
traffic classifier c operator or
 if-match acl 2003
traffic classifier b operator or
 if-match acl 2002
#
traffic behavior e
 car cir 15000 cbs 300000 pbs 500000 green pass yellow pass red discard
 remark dscp cs5
traffic behavior udplimit
traffic behavior udplimit1
 car cir 15000 pir 20000 cbs 300000 pbs 500000 green pass yellow pass red discar
d
traffic behavior g
 car cir 2000 cbs 50000 pbs 500000 green pass yellow pass red discard
 remark dscp default
traffic behavior f
 car cir 10000 cbs 100000 pbs 500000 green pass yellow pass red discard
 remark dscp af33
#
traffic policy udplimit
```

```
traffic classifier a operator or
 if-match acl 2001
traffic classifier udplimit operator or
 if-match acl 3001
traffic classifier udplimit1 operator or
 if-match acl 3002
traffic classifier c operator or
 if-match acl 2003
traffic classifier b operator or
 if-match acl 2002
#
traffic behavior e
 car cir 15000 pir 20000 cbs 300000 pbs 500000 green pass yellow pass red discar
d
 remark dscp cs5
traffic behavior udplimit
traffic behavior udplimit1
 car cir 15000 pir 20000 cbs 300000 pbs 500000 green pass yellow pass red discar
d
traffic behavior g
 car cir 2000 pir 20000 cbs 50000 pbs 500000 green pass yellow pass red discard
 remark dscp default
traffic behavior f
 car cir 10000 pir 20000 cbs 100000 pbs 500000 green pass yellow pass red discar
d
 remark dscp af33
```

```
 classifier udplimit behavior udplimit
 classifier udplimit1 behavior udplimit1
traffic policy 3
 classifier c behavior g
traffic policy 2
 classifier b behavior f
traffic policy 1
 classifier a behavior e
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher
%$%$K8m.Nt84DZ}e#<0`8bmE3Uw}%$%$
 local-user admin service-type http
#
isis 1
 is-level level-2
 cost-style wide
 network-entity 49.0001.0000.0000.0003.00
 traffic-eng level-2
#
firewall zone Local
 priority 15
#
```

```
#
traffic policy udplimit
 classifier udplimit behavior udplimit
 classifier udplimit1 behavior udplimit1
traffic policy 3
 classifier c behavior g
traffic policy 2
 classifier b behavior f
traffic policy 1
 classifier a behavior e
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher
%$%$K8m.Nt84DZ}e#<0`8bmE3Uw}%$%$
 local-user admin service-type http
#
isis 1
 is-level level-2
 cost-style wide
 network-entity 49.0001.0000.0000.0005.00
 traffic-eng level-2
#
firewall zone Local
```

```
interface GigabitEthernet0/0/0
 ip address 10.1.1.1 255.255.255.252
 isis enable 1
 traffic-policy udplimit outbound
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 mpls rsvp-te
 mpls ldp
#
interface GigabitEthernet0/0/1
 ip address 11.1.1.2 255.255.255.252
 isis enable 1
 traffic-policy udplimit outbound
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 mpls rsvp-te
 mpls ldp
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet2/0/0
 ip binding vpn-instance CBE
 ip address 40.1.1.1 255.255.255.252
 priority 15
#
interface GigabitEthernet0/0/0
 ip address 17.1.1.1 255.255.255.252
 isis enable 1
 traffic-policy udplimit outbound
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 mpls rsvp-te
 mpls ldp
#
interface GigabitEthernet0/0/1
 traffic-policy udplimit outbound
#
interface GigabitEthernet0/0/2
 ip address 15.1.1.2 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
 mpls ldp
#
interface GigabitEthernet2/0/0
 ip binding vpn-instance CBE
 ip address 20.1.1.1 255.255.255.252
```

```
 traffic-policy 1 inbound
#
interface GigabitEthernet3/0/0
 ip binding vpn-instance NBE
 ip address 50.1.1.1 255.255.255.252
 traffic-policy 2 inbound
#
interface GigabitEthernet4/0/0
#
interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
 isis enable 1
#
interface Tunnel0/0/0
 description 5.5.5.5
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 mpls te tunnel-id 100
 mpls te bandwidth ct0 20000
mpls te commit
#
bgp 65007
 peer 4.4.4.4 as-number 65007
 peer 4.4.4.4 connect-interface LoopBack1
 peer 5.5.5.5 as-number 65007
 peer 5.5.5.5 connect-interface LoopBack1
 peer 6.6.6.6 as-number 65007
 peer 6.6.6.6 connect-interface LoopBack1
```

```
 traffic-policy 1 inbound
#
interface GigabitEthernet3/0/0
 ip binding vpn-instance NBE
 ip address 30.1.1.1 255.255.255.252
 traffic-policy 2 inbound
#
interface GigabitEthernet4/0/0
#
interface LoopBack1
 ip address 5.5.5.5 255.255.255.255
 isis enable 1
#
interface Tunnel0/0/0
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 3.3.3.3
 mpls te tunnel-id 200
 mpls te bandwidth ct0 20000
 mpls te commit
#
bgp 65007
 peer 3.3.3.3 as-number 65007
 peer 3.3.3.3 connect-interface LoopBack1
 peer 4.4.4.4 as-number 65007
 peer 4.4.4.4 connect-interface LoopBack1
 peer 6.6.6.6 as-number 65007
 peer 6.6.6.6 connect-interface LoopBack1
```

```
#
ipv4-family unicast
 undo synchronization
 peer 4.4.4.4 enable
 peer 5.5.5.5 enable
 peer 6.6.6.6 enable
#
ipv4-family vpnv4
 policy vpn-target
 peer 4.4.4.4 enable
 peer 5.5.5.5 enable
 peer 6.6.6.6 enable
#
ipv4-family vpn-instance CBE
 import-route direct
 peer 40.1.1.2 as-number 65005
#
ipv4-family vpn-instance NBE
 peer 50.1.1.2 as-number 65006
#
user-interface con 0
 authentication-mode password
user-interface vty 0 4
user-interface vty 16 20
#
wlan ac
#
return
```

```
#
ipv4-family unicast
 undo synchronization
 peer 3.3.3.3 enable
 peer 4.4.4.4 enable
 peer 6.6.6.6 enable
#
ipv4-family vpnv4
 policy vpn-target
 peer 3.3.3.3 enable
 peer 4.4.4.4 enable
 peer 6.6.6.6 enable
#
ipv4-family vpn-instance CBE
 import-route direct
 peer 20.1.1.2 as-number 65008
#
ipv4-family vpn-instance NBE
 peer 30.1.1.2 as-number 65009
#
user-interface con 0
 authentication-mode password
user-interface vty 0 4
user-interface vty 16 20
#
wlan ac
#
return
```

PE2 Router Configuration

<PE2>display current-configuration

[V200R003C00]

#

sysname PE2

#

snmp-agent local-engineid 800007DB03000000000000

snmp-agent

#

clock timezone China-Standard-Time minus 08:00:00

#

portal local-server load flash:/portalpage.zip

#

drop illegal-mac alarm

#

wlan ac-global carrier id other ac id 0

#

set cpu-usage threshold 80 restore 75

#

mpls lsr-id 4.4.4.4

mpls

mpls te

mpls rsvp-te

#

mpls ldp

#

PE4 Router Configuration

<PE4>display current-configuration

[V200R003C00]

#

sysname PE4

#

snmp-agent local-engineid 800007DB03000000000000

snmp-agent

#

clock timezone China-Standard-Time minus 08:00:00

#

portal local-server load flash:/portalpage.zip

#

drop illegal-mac alarm

#

wlan ac-global carrier id other ac id 0

#

set cpu-usage threshold 80 restore 75

#

mpls lsr-id 6.6.6.6

mpls

mpls te

mpls rsvp-te

#

mpls ldp

#

```
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher %$%$K8m.Nt84DZ}e#<0`8bmE3Uw}%$%$
 local-user admin service-type http
#
isis 1
 is-level level-2
 cost-style wide
 network-entity 49.0001.0000.0000.0004.00
 traffic-eng level-2
#
firewall zone Local
 priority 15
#
interface GigabitEthernet0/0/0
 ip address 10.1.1.2 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 mpls rsvp-te
```

```
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher %$%$K8m.Nt84DZ}e#<0`8bmE3Uw}%$%$
 local-user admin service-type http
#
isis 1
 is-level level-2
 cost-style wide
 network-entity 49.0001.0000.0000.0006.00
 traffic-eng level-2
#
firewall zone Local
 priority 15
#
interface GigabitEthernet0/0/0
 ip address 17.1.1.2 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 mpls rsvp-te
```

```
 mpls ldp
#
interface GigabitEthernet0/0/1
 ip address 12.1.1.2 255.255.255.252
 isis enable 1
 mpls
 mpls te
mpls te bandwidth max-reservable-bandwidth
100000
 mpls te bandwidth bc0 100000
 mpls rsvp-te
 mpls ldp
#
interface GigabitEthernet0/0/2
#
interface NULL0
#
interface LoopBack1
 ip address 4.4.4.4 255.255.255.255
 isis enable 1
#
bgp 65007
 peer 3.3.3.3 as-number 65007
 peer 3.3.3.3 connect-interface LoopBack1
 peer 5.5.5.5 as-number 65007
 peer 5.5.5.5 connect-interface LoopBack1
 peer 6.6.6.6 as-number 65007
 peer 6.6.6.6 connect-interface LoopBack1
```

```
 mpls ldp
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
 ip address 16.1.1.2 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth
100000
 mpls te bandwidth bc0 100000
 mpls rsvp-te
 mpls ldp
#
interface NULL0
#
interface LoopBack1
 ip address 6.6.6.6 255.255.255.255
 isis enable 1
#
bgp 65007
 peer 3.3.3.3 as-number 65007
 peer 3.3.3.3 connect-interface LoopBack1
 peer 4.4.4.4 as-number 65007
 peer 4.4.4.4 connect-interface LoopBack1
 peer 5.5.5.5 as-number 65007
 peer 5.5.5.5 connect-interface LoopBack1
```

```
 #
 ipv4-family unicast
  undo synchronization
  peer 3.3.3.3 enable
  peer 5.5.5.5 enable
  peer 6.6.6.6 enable
 #
 ipv4-family vpnv4
  policy vpn-target
  peer 3.3.3.3 enable
  peer 5.5.5.5 enable
  peer 6.6.6.6 enable
#
user-interface con 0
 authentication-mode password
user-interface vty 0 4
user-interface vty 16 20
#
wlan ac
#
return
```

CE1 Router Configuration

```
<CE1>display current-configuration
[V200R003C00]
#
 sysname CE1
#
```

```
 #
 ipv4-family unicast
  undo synchronization
  peer 3.3.3.3 enable
  peer 4.4.4.4 enable
  peer 5.5.5.5 enable
 #
 ipv4-family vpnv4
  policy vpn-target
  peer 3.3.3.3 enable
  peer 4.4.4.4 enable
  peer 5.5.5.5 enable
#
user-interface con 0
 authentication-mode password
user-interface vty 0 4
user-interface vty 16 20
#
wlan ac
#
return
```

CE2 Router Configuration

```
<CE3>display current-configuration
[V200R003C00]
#
 sysname CE3
#
```

```
 snmp-agent local-engineid 800007DB03000000000000
 snmp-agent
#
 clock timezone China-Standard-Time minus 08:00:00
#
portal local-server load flash:/portalpage.zip
#
 drop illegal-mac alarm
#
 wlan ac-global carrier id other ac id 0
#
 set cpu-usage threshold 80 restore 75
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher %$%$K8m.Nt84DZ}e#<0`8bmE3Uw}%$%$
 local-user admin service-type http
#
firewall zone Local
 priority 15
#
interface GigabitEthernet0/0/0
```

```
 snmp-agent local-engineid 800007DB03000000000000
 snmp-agent
#
 clock timezone China-Standard-Time minus 08:00:00
#
portal local-server load flash:/portalpage.zip
#
 drop illegal-mac alarm
#
 wlan ac-global carrier id other ac id 0
#
 set cpu-usage threshold 80 restore 75
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher %$%$K8m.Nt84DZ}e#<0`8bmE3Uw}%$%$
 local-user admin service-type http
#
firewall zone Local
 priority 15
#
interface GigabitEthernet0/0/0
```

```
 ip address 40.1.1.2 255.255.255.252
#
interface GigabitEthernet0/0/1
#
interface NULL0
#
bgp 65005
 peer 40.1.1.1 as-number 65007
 #
 ipv4-family unicast
  undo synchronization
  import-route direct
  peer 40.1.1.1 enable
#
user-interface con 0
 authentication-mode password
user-interface vty 0 4
user-interface vty 16 20
#
wlan ac
#
return
```

CE2 Router Configuration

```
<CE2>display current-configuration
[V200R003C00]
#
 sysname CE2
```

```
 ip address 20.1.1.2 255.255.255.252
#
interface GigabitEthernet0/0/1
#
interface NULL0
#
bgp 65008
 peer 20.1.1.1 as-number 65007
 #
 ipv4-family unicast
  undo synchronization
  import-route direct
  peer 20.1.1.1 enable
#
user-interface con 0
 authentication-mode password
user-interface vty 0 4
user-interface vty 16 20
#
wlan ac
#
return
```

CE4 Router Configuration

```
<CE4>display current-configuration
[V200R003C00]
#
 sysname CE4
```

```
#
 snmp-agent local-engineid 800007DB03000000000000
 snmp-agent
#
 clock timezone China-Standard-Time minus 08:00:00
#
portal local-server load flash:/portalpage.zip
#
 drop illegal-mac alarm
#
 wlan ac-global carrier id other ac id 0
#
 set cpu-usage threshold 80 restore 75
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher %$%$K8m.Nt84DZ}e#<0`8bmE3Uw}%$%$
 local-user admin service-type http
#
firewall zone Local
 priority 15
#
```

```
#
 snmp-agent local-engineid 800007DB03000000000000
 snmp-agent
#
 clock timezone China-Standard-Time minus 08:00:00
#
portal local-server load flash:/portalpage.zip
#
 drop illegal-mac alarm
#
 wlan ac-global carrier id other ac id 0
#
 set cpu-usage threshold 80 restore 75
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher %$%$K8m.Nt84DZ}e#<0`8bmE3Uw}%$%$
 local-user admin service-type http
#
firewall zone Local
 priority 15
#
```

```
interface GigabitEthernet0/0/1
 ip address 50.1.1.2 255.255.255.252
#
interface NULL0
#
bgp 65006
 peer 50.1.1.1 as-number 65007
 #
 ipv4-family unicast
  undo synchronization
  import-route direct
  peer 50.1.1.1 enable
#
user-interface con 0
 authentication-mode password
user-interface vty 0 4
user-interface vty 16 20
#
wlan ac
#
return
```

```
interface GigabitEthernet0/0/1
 ip address 30.1.1.2 255.255.255.252
#
interface NULL0
#
bgp 65009
 peer 30.1.1.1 as-number 65007
 #
 ipv4-family unicast
  undo synchronization
  import-route direct
  peer 30.1.1.1 enable
#
user-interface con 0
 authentication-mode password
user-interface vty 0 4
user-interface vty 16 20
#
wlan ac
#
return
```