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

Asrat Mulatu Beyene[1](✉) and Shimelis Asrat Argaw[2]

[1] Addis Ababa Science and Technology University, Addis Ababa, Ethiopia
asrat.mulatu@aastu.edu.et
[2] St. Mary's University, Addis Ababa, Ethiopia
shimelisas@gmail.com

Abstract. The primary goals of Quality of Service (QoS) are managed bandwidth, controlled jitter, minimized latency, and improved packet loss characteristics to provide satisfactory services for users. Shaping network optimization is crucial for the service provider, too. To implement QoS mechanisms optimizing the current network physical and logical architectures is among the best practices. In this paper, an attempt has been made to investigate the end-to-end QoS parameters of multiprotocol border gateway protocol multiprotocol label switching virtual private network (MP-BGP MPLS VPN) EthioTelecom service level agreement (SLA) customers. That is done using differentiated service (DiffServ) model to manage end-to-end traffic delay, jitter, and packet losses. The traffics are classified and marked depending on their priorities. The proposed network architecture has used weighted fair queueing (WFQ) for congestion management and weighted random early detection (WRED) for congestion avoidance. The Huawei's Enterprise Network Simulation Platform (eNSP) and Wireshark are used to design, demonstrate and evaluate the network architectures. When the results of the existing network are compared with the proposed network architecture its delay, jitter, packet loss and traffic utilization have shown improvements.

Keywords: Quality of Service · Virtual private network · Multiprotocol label switching · Multiprotocol border gateway protocol · Service level agreement · Differentiated service model

1 Introduction

Every day new telecommunication technologies are being developed. Enterprises use these new technologies to upgrade their network services and reduce cost.

F. Mekuria et al. (Eds.): ICT4DA 2019, CCIS 1026, pp. 278–288, 2019.
https://doi.org/10.1007/978-3-030-26630-1_24

Now a day, different kinds 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 QoS is one the challenges [1]. MP-BGP MPLS VPN is one alternative solution to private wide area networks (WAN) to assure end-to-end QoS.

In existing networks there is significant problem of meeting consumers QoS demands. This is discussed in [1–3]. Moreover, a preliminary investigation based on data collected from EthioTelecom MP-BGP VPN customers shows there were many verified complaints of end-to-end QoS problems. The primary reasons for this are EthioTelecom uses best effort policy to guarantee QoS demands, first in first out (FIFO) to manage congestion, tail drop to avoid congestion. This can be improved in many different ways. Here, we have implemented the DiffServ QoS model, WFQ for congestion management, WRED for congestion avoidance on EthioTelecom MP-BGP MPLS VPN customers network to better meet QoS expectation based on the SLA. To do that, in this research work, a simplified network architecture is built as shown in Fig. 1. It covers the main steps in designing QoS of MP-BGP MPLS VPN networks. The New Generation Network (NGN) network architecture was chosen according to the requirements of designing networks with service provision and end-to-end QoS implementation.

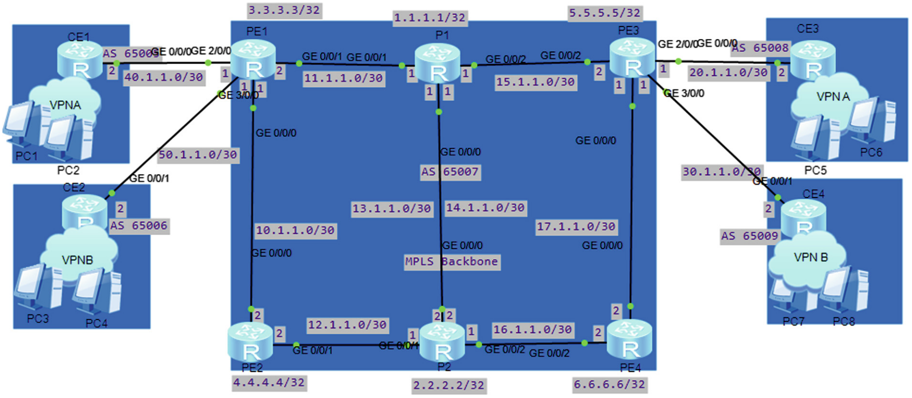

Fig. 1. Simplified MP-BGP MPLS VPN network architecture with end-to-end QoS.

In the proposed network architecture solution there are two provider (P) routers, four provider edge (PE) routers and four customer edge (CE) routers. The P routers are the backbone routers. They provide MPLS label forwarding and maintain 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. They also do label popping and imposition. CE routers are customer edge routers where the customer's routers or personal computers (PCs) are directly connected.

VPN A and VPN B routers are traffic generators. The two VPN pairs, VPN As and VPN Bs, traffic was evaluated. Both are MPLS based on resource reservation protocol traffic engineering (RSVP-TE) for signaling and tunneling. They use intermediate system to intermediate system (IS-IS) for interior gateway-protocol (IGP) interconnection. Both VPNs use the same networking devices. The P routers in the core network are realized as core routers and route reflectors (RR). These devices are logically divided into two logical systems. These systems are act 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 networks 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. To test the QoS applied in the traffic flow Wireshark and eNSP are used. The two VPNs provide random traffic generation, fixed or non-fixed packet size, and simultaneous generation of multiple traffic flows.

1.1 MP-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 of BGP MPLS VPN there are 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 and public network labels. VPN packet forwarding is used for encapsulation, outer packet forwarding on a public network and inner label instructing inner sites of packets [1–3].

1.2 Quality of Service (QoS)

QoS is the mechanism of networks to provide different services to different traffic types [4]. Service providers offer their network service with varying quality levels. To do that they define SLAs. An 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 not the functionality of a single device and it is an end-to-end mechanism. It provides the intelligence to network devices to treat the different application's traffic as they are defined in the SLA. QoS combines different technologies together such as classifying, marking, scheduling, queuing, allocating and prioritizing bandwidth that are commonly used to provide a scalable end-to-end service [5]. QoS is used to manage the main network performance elements like bandwidth, delay, jitter and packet loss [4,6].

Bandwidth. The amount of data that can be transmitted over the link is bandwidth [4,9]. 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 [5,10]. Due to the low bandwidth users experience delay, jitter and packet loss in the communication.

Delay. End-to-end delay is the total time that a packet takes from source to destination [6,7]. End-to-end delay is the sum of processing, queuing, serialization, and propagation delays.

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 loads on different timings. For voice and video, it is necessary to receive the packets in the same sequence to achieve good quality [10].

Packet Loss. Packet loss occurs due to the low buffer space [8,9]. When the buffer space of interfaces are full packets are dropped. In queue scheduling packet loss occur when the queue is full. Packet loss creates extended delays and jitter. Packet loss can be controlled by applying techniques like tail drop, random early detection, weighted random early detection and traffic shaping and policing [9].

Generally, QoS doesn't depend only on bandwidth, delay, packet loss and delay [10]. It also depends on end-user perception of telecommunication services such as trends, advertising, tariffs and costs which are interrelated with customers' expectation of QoS. Figure 2 shows how end-user perception reaches the QoS satisfaction level.

QoS can be divided into two viewpoints [11,12]. 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 Fig. 3.

Generally, if network performance was well optimized, service provider viewpoint reaches the highest level. Moreover, if service provider affords quality services to its customer, customer viewpoint escalates which increases customer quality of experiences.

2 Designed QoS of MP-BGP MPLS VPN

The designed QoS-based network architecture provides different levels of service quality based on end-to-end QoS targets and International Telecommunication Union (ITU) threshold quality requirements for different VPNs. Managing

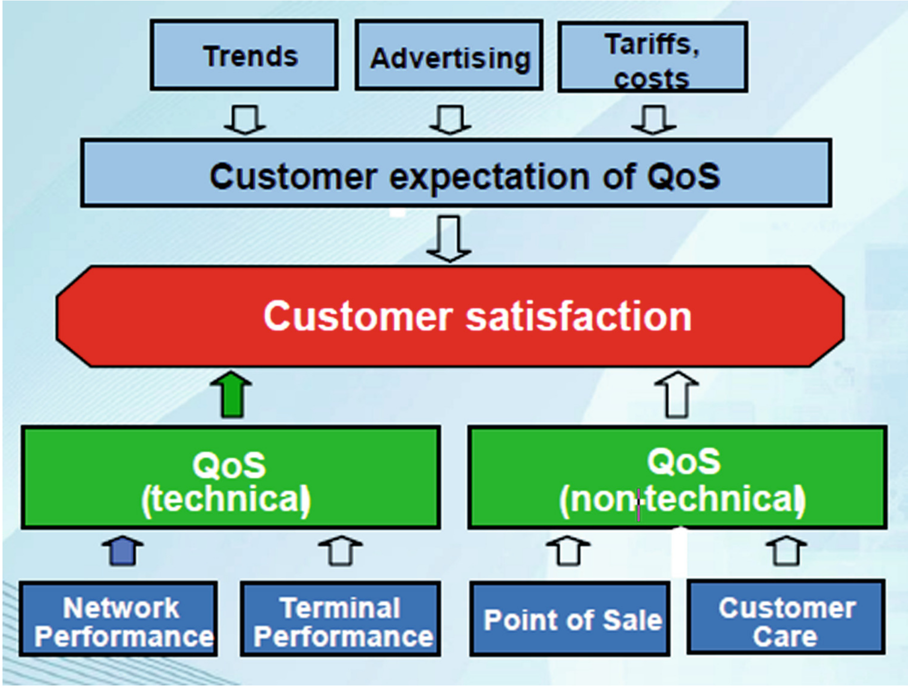

Fig. 2. User perception of end-to-end QoS delivery framework [11,12].

maximum receivable bandwidth, reducing transmission, queueing and processing delay, minimizing jitter and packet loss are the main focus of the design. End-to-end QoS assurance is achieved based on existing resources by using rational scheduling and congestion avoidance methods. DiffServ is used to classify, mark and shape network traffic based on existing SLA agreements. Applying end-to-end QoS using DiffServ can follow the following step by step processes:

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

2.1 Experimental Resuts

The designed MP-BGP MPLS VPN end-to-end QoS applied on the network architecture depicted in Fig. 1 is fully operational. That means

- All protocols are fully operational,
- Proper implementation of the designed QoS is made,

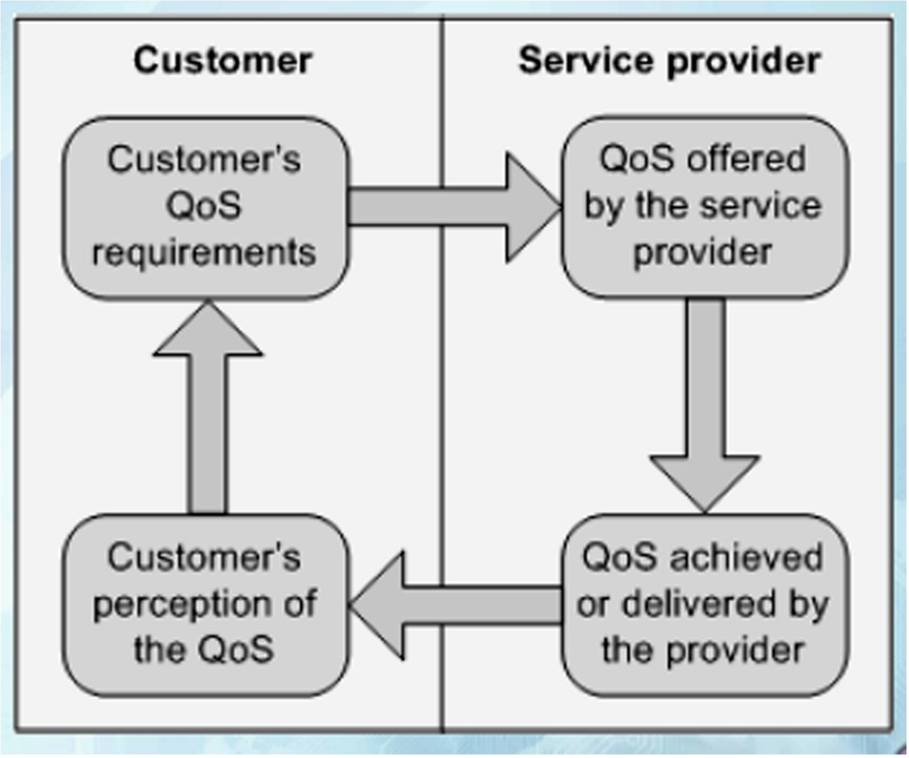
Customer
Service provider
Customer's QoS requirements
QoS offered by the service provider
QoS achieved or delivered by the provider
Customer's perception of the QoS

Fig. 3. QoS viewpoints framework [11].

- Provisioning of the required services ensuring MPLS VPN are operational, and
- Redundancy of network resources is made which includes rerouting in case of link or node failure.

The existing and proposed network architectures are the same in devices and physical interconnection. But they have different QoS designs. Table 1 shows the similarities and differences between existing and proposed network architectures.

Table 1. The similarities and differences between existing and proposed network architectures.

Parameters	Existing network architecture	Proposed network architecture
Traffic type	MP-BGP MPLS VPN	MP-BGP MPLS VPN
Service type	MPLS VPN	MPLS VPN
IGP routing protocol	IS-IS	IS-IS
NGN backbone	MPLS	MPLS
QoS model	Best effort model	DiffServ
Congestion management	FIFO	WFQ
Congestion avoidance	Tail drop	WRED

The end-to-end QoS is tested with Wireshark and eNSP tools. A couple of scenarios, based on Fig. 1, are tested with different traffic streams. In the first scenario, the existing network performance is checked. The existing network architecture uses best effort endto- end QoS. All traffic has equal priority. The architecture uses FIFO algorithm for congestion management and tail drop algorithm for congestion avoidance. In the second scenario, which is the proposed network architecture, uses the DiffServ QoS. The traffic has different priorities. The architecture uses WFQ algorithm for congestion management and WRED algorithm for congestion avoidance. In this case, the traffic was classified and prioritized depending on the underlying SLA. Then traffic policies were defined and applied on the aggregation router outbound interface. In this work, 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. Both traffic streams use TCP with speed of 15 Mbps. The existing traffic test is made between CE1 and CE3 and the proposed traffic test is made between CE2 and CE4 routers.

From Fig. 4, one can see that the existing network architecture overturns the bandwidth utilization. This is because the existing network uses the 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 of data traffic. So, mission critical traffic is transmitted first.

As can be seen from the evaluation testing of Fig. 5, the proposed network architecture, the implementation of DiffServ has many benefits for packet loss compared to the best effort. In the DiffServ model, routers must store traffic and QoS information per aggregation. This creates enough buffer space in the router's queue. A router usually has incoming interface buffers, system buffers, and outgoing interface buffers. In case of congestion, the traffic is remarked and kept in buffer space to avoid the packet loss. But in the case of best effort QoS model, the routers just route packets until they reach the destination. Other packets are dropped causing a higher percentage of packet loss.

DiffServ QoS model minimizes traffic loss. In case of congestion, this model classifies 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 transmitted later. This decreases the packet loss ratio.

Latency is the time that a packet waits before being transmitted. As it can be seen from Fig. 6, 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.

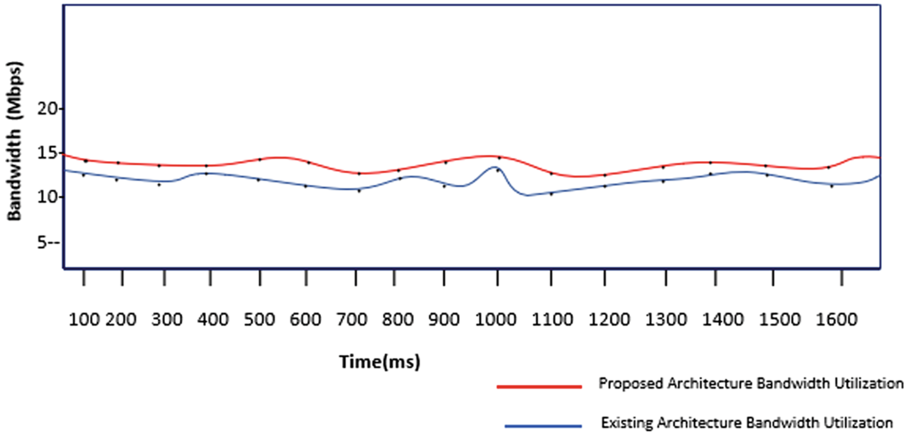

Fig. 4. The bandwidth utilization results of existing and proposed systems.

3 Discussions

The numerical results obtained from the existing and proposed networks are shown in Table 2. 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 delays. The difference increases as the number of routers (nodes) increases.

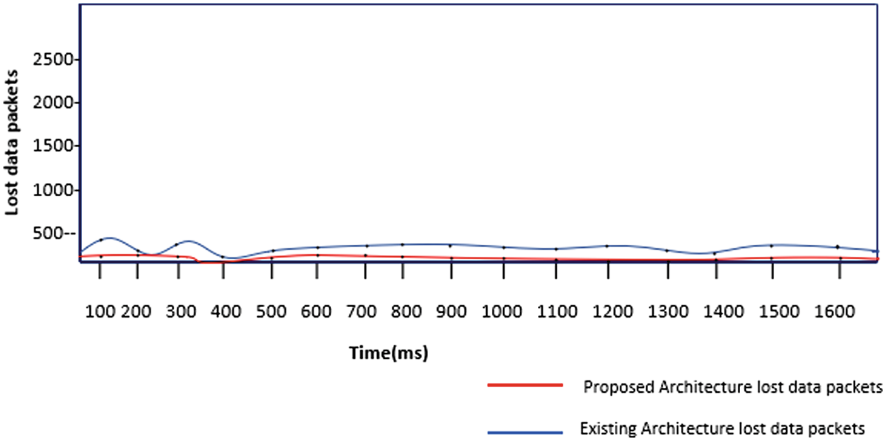

Fig. 5. Packet loss measurement comparison.

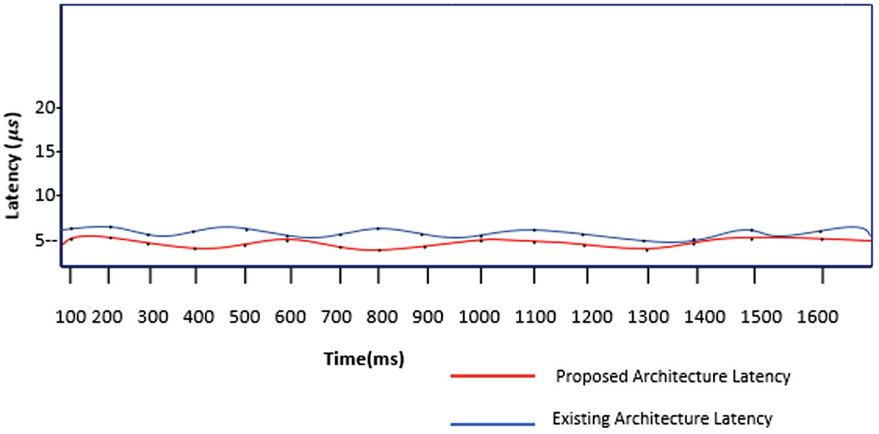

Fig. 6. Latency measurement comparison.

Table 2. Exist and proposed network architecture numerical QoS results.

Parameters	Existing network (Best effort)			Proposed network (DiffServ)		
	Result	SLA targets	ITU threshold	Result	SLA targets	ITU threshold
Packet loss ()	0.169	Within range	Out of range	0.14132	Within range	Within range
Delay (sec)	0.001	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 (bps)	15068	Out of range	Out of range	15320	Within range	Out of range

4 Conclusions

In this research, the DiffServ model for the design of MP-BGP MPLS VPN networks with end-to-end QoS was deliberated. This type of networks is suitable for the implementation of QoS for MPLS 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 uses the DiffServ QoS model was designed and tested. Bandwidth utilization, packet loss, latency and jitter measurements were made for both network models. After the whole evaluations were made, it is observed that the proposed MP-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 brings better traffic management and provision of suitable end-to-end QoS. The proposed MP-BGP MPLS VPN architecture which uses DiffServ QoS model architecture could be used in many mission-critical applications.

In the proposed DiffServ QoS model better network productivity was achieved. The designed MP-BGP MPLS VPN architecture which uses 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. In the proposed BGP MPLS VPN architecture, which uses DiffServ QoS model architecture, all services have the required traffic treatment. The designed MP-BGP MPLS VPN network model can easily be used for MPLS VPN services in both centralized and distributed architectures. End-to-end MPLS solutions for the NGN applications are smoothly attended.

Generally, based on the analysis and results gained, it can be concluded that the DiffServ QoS model was more reliable than the best effort QoS model being used by EthioTelecom's MP-BGP MPLS VPN network. The designed QoS uses DiffServ model that can guarantee customers' SLA QoS thresholds. In conclusion, the designed network provides a way of increasing network performance based on the DiffServ QoS model. High network performance indicates better QoS service provision. Better QoS service provision, in turn, creates customer satisfaction and higher quality of experience to customers.

5 Future Works

Based on the scope of this work, the QoS has been guaranteed with respect to SLA QoS targets. But in the 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.

One such 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 and 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 [13,14]. This way the designed proposed BGP MPLS VPN architecture which uses DiffServ QoS model network architecture can become optimal save operational and maintenance costs. Self-optimization, based on collected data from previous network states and based on predictions can be also be attempted.

References

1. Ahmad, A., Talal, A.: Performance analysis of DiffServ-based quality of service in MPLS networks. Int. J. Sci. Eng. Res. **6**, 15–23 (2015)
2. EthioTelecom. QoS Document on MPLS VPN Services Quality and Customer Experience Related Issues and Complaint Analysis, Version 02 (2017)
3. Huawei technologies. Configuration Guide VPN - Cloud Engine 12800 Series Switches, vol. 6 (2017)
4. Szigeti, T., Hattingh, C.: End-to-End QoS Network Design. Cisco Press, Indianapolis (2005)
5. Lawrence, J.: Designing multiprotocol label switching networks. IEEE Commun. Mag. **39**(7), 134–142 (2001)

6. De Ghein, L.: MPLS Fundamentals epub. Cisco Press, Indianapolis (2016)
7. Pepelnjak, I., Guichard, J.: MPLS and VPN Architectures, vol. 1. Cisco Press, Indianapolis (2002)
8. Mohamed, J.N., Mellachervu, K.R., Ramakrishnan, S.C.: Configuration tool for MPLS virtual private network topologies. Google Patents (2012). (US Patent 8,194,570)
9. Odom, W.: CCNP Route 642–902 Official Certification Guide. Cisco Press, Indianapolis (2010)
10. Grayson, M., Gundavelli, S.: Providing integrated end-to-end architecture that includes quality of service transport for tunneled traffic. U.S Patents (2015). (Patent 9,198,209)
11. Stankiewicz, R., Jajszczyk, A.: A survey of QoE assurance in converged networks. Comput. Netw. **55**(7), 1459–1473 (2011)
12. EthioTelecom. Service Provisioning Manual, July 2014
13. Zhang, G.P.: Time series forecasting using a hybrid ARIMA and neural network model. Neurocomputing **50**, 159–175 (2003)
14. Lee, H., Hwang, J., Kang, B., Jun, K.: End-to-end QoS architecture for VPNs: MPLS VPN deployment in a backbone network. In: 2000 Proceedings of International Workshop on Parallel Processing, pp. 479–483. IEEE (2000)