INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2023, VOL. 69, NO. 1, PP. 115-120
Manuscript received March 4, 2022; revised February, 2023. DOI: 10.24425/ijet.2023.144339

Application of MPLS Tunnel Service L2TP-VPN Optimization Concept with Traffic Engineering Method for Looping-Protection Service Analysis

Lukman Medriavin Silalahi, Setiyo Budiyanto, Imelda Uli Vistalina Simanjuntak, Rukhi Ali Effendi, Fernando, Agus Dendi Rochendi, and Irfan Kampono

***Abstract*— This research began when observations were made on any-to-any-connection services that require QoS (Quality of Service) and tunnel measurements. Tunnel is a technique to interconnect between local networks that are separated through a public network. Research questions found looping caused by traffic issues when sending data in the MPLS service layer-2 tunneling service. Furthermore, this research hypothesis proposes optimizing QoS performance in the application of the SR-TE (Segment Routing-Traffic Engineering) method in the MPLS (Multi-Protocol Label Switching) network and analyzing traffic based on MAC addresses using the looping-protection method. This research contributes to optimizing the MPLS network and is a recommended solution for simplifying control-plane operation, especially the SR-TE method and looping-protection in the L2-VPN MPLS service. The purpose of this study is to analyze the performance of MPLS networks, as well as analyze the application of L2-VPN (Layer 2 Virtual Private Network) MPLS networks. The targeted TKT (Technology Readiness Level) is 3rd-Level, which is an analytical and experimental proof of the MPLS tunnel network model on Layer-2 VPN services. The results of the research concluded that testing the SR-TE method is a solution to simplify the process of labeling data traffic that is global labelling, then the looping-protection method is a solution to eliminate looping indications. The QoS obtained has also shown an "excellent" category based on TIPHON standards.**

***Keywords*—MPLS; SR-TE; *Looping Protection;* L2-VPN; VPN; QoS**

I. Introduction

THE rapid development of computer networks accompanied by increasingly complex human needs has made user demand for internet services higher [1]–[3]. This research discusses IP network technology which is an internal any-to-any connection data communication service that can serve information in the form of data, voice, and video [4]–[6]. Based on the survey from APJII (Asosiasi Penyelenggara Jasa Internet Indonesia) [7] that the number of National internet users is 210.03 million users from a total population of 272.68 Indonesians in 2022, this is equivalent to 77.02%. Furthermore, based on the results of a survey of the most internet users based on work in the field of academia, 99.26% of the number of internet users [8]. The results of the survey are a big challenge for ISPs (Internet Service Providers) to provide the best quality internet services and access. QoS (Quality of Service) is important for measuring the level of reliability and optimization of networks and internet services offered by ISPs [9].

MPLS (Multi-Protocol Label Switching) is an evolution of multi-layer switches developed by the IETF (Internet Engineering Task Force) to combine a label-swap mechanism at Layer-2 with routing at Layer-3 to speed up packet delivery. So that MPLS can provide services in VPLS (Virtual Private LAN Service), namely the L2-VPN (Layer2-Virtual Private Network) service that provides Multipoint-to-Multipoint connectivity to expand ethernet-based broadcast domains. The concept of L2-VPN, which is to forward routing information packets based on MAC (Media Access Control) address, VC (Virtual Circuit) identification, and switch port information. MPLS uses encapsulated data, namely LDP (Label Distribution Protocol) or LSP (Label Switched Path) The results of observations on the MPLS tunneling service show that looping-issues have been detected in sending data in Layer 2 services. This means that the data packets that will be sent to the recipient will not reach the destination due to traffic issues when sending the data. Thus, the solution to overcome this problem is to apply Traffic-Engineering (TE).

The TE concept is a technique of manipulating network traffic by selecting traffic data channels to control traffic loads on various routes and points in the network. MPLS-TE is a way to find the best path using LSP on a hop-by-hop basis based on the shortest IGP (Interior Gateway Protocol) path. Every transit router that is used as an LSP must store LSP status information and frequently exchanged status refresh messages to maintain LSP signaling and MPLS paths [10].

SR-TE (Segment Routing - Traffic Engineering) and looping-protection are proposed methods of this research. 1st method is SR (Segment Routing) which is a control-plane operation simplification technique that is effectively used in the TE concept [11]. This method uses the routing concept calculated by the ingress node and each node is identified by a SID (Segment Identifier), so that along the SR-TE path there is no need to store any state information. Unlike on the MPLS network when SR (Segment Routing) sets flow-traffic only on ingress-nodes, then segment-list is applied with RSVP-TE (Reservation Protocol-Traffic Engineering) to set forwarding-

The first, second, third, fourth, and fifth authors are with Universitas Mercu Buana, Indonesia (email: lukman.medriavin@mercubuana.ac.id, sbudiyanto@mercubuana.ac.id, imelda.simanjuntak@mercubuana.ac.id, rukhiali10@gmail.com, nandodoang26@gmail.com).

The sixth and seventh authors are with Badan Riset dan Inovasi Nasional Republik Indonesia, Indonesia (email: agus105@brin.go.id, irfa005@brin.go.id).

© The Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0, https://creativecommons.org/licenses/by/4.0/), which permits use, distribution, and reproduction in any medium, provided that the Article is properly cited.

table on transit-nodes [12]. The routing algorithm is more flexible and simpler, so it only makes the segment-list less burdensome for routers along the SR-TE path. In addition, to be able to optimize QoS in the SR-TE method, a Virtual Private Network (VPN) method is also applied to make it more efficient in using bandwidth capacity [13].

The 2nd method is looping protection which is based on the problem of sending quality data without the occurrence of looping cases. There are variations of router devices such as Nokia, Cisco, etc. This research uses Nokia routers because it has the ability to perform MPLS tunneling techniques and analyze service verification, QoS Throughput and Delay parameters.

The expected result is to be able to create a private and secure L2-VPN services network system, produce analysis of the parameters tested into novelty-research for the MPLS-TE network system and establish looping protection that occurs in the MPLS network tunneling service. The purpose of the research is to analyze the working principle of L2-VPN MPLS by analyzing the process of forming a path label on each SR, QoS analysis of the application of the L2-VPN MPLS network scenario with the SR-TE method and the looping protection method.

II. Research Method

A. Literature Review

According to [13] it discusses leaks in network security systems, and accessing network sources remotely. The proposed method is the testing of L2-VPN hybrid networks using WAN emulators on routers, and end devices. Thus, the results of this study state that the encryption capabilities of VPN protocols are very important because they determine the level of privacy and security protection. Load testing, showing that VPN tunnels can degrade the performance of the overhead and encryption methods used.

According to [14] it raises the issue of ISPs to provide connectivity to their users through topologies that operate on the data link layer. The proposed method is to design two network topologies along with the protocols used for looping anticipation, namely a topology with MSTP (Multiple Spanning Tree Protocol) and a topology with ITU-T (International Telecommunication Union-Telecommunication) G.8032 Finally, this research issued an average packet loss range of between 320-385 milliseconds in the MSTP topology, and an average packet loss range between 218-286 milliseconds in the ITU-T G.8032 topology.

According to [15] it is about the decentralization of the BGP (Border Gateway Protocol) protocol on Autonomous Systems-Decision Routing (AS-DR) using routing loop detection. The proposed method is a simulation using SS-BGP (Self-Stable BGP) and ESS-BGP (Enhanced Self-Stable BGP) loop routing methods through a realistic internet topology by performing 100 different simulations to generate delay across links.

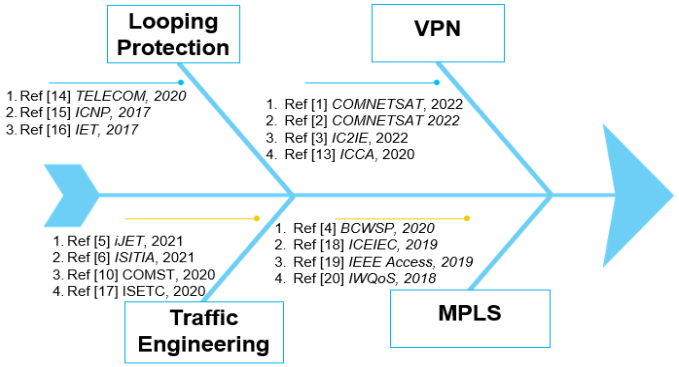

Fig. 1. Block diagram system

According to [16] discuss about WMN (Wireless Mesh Networks) built by the US with hop-by-hop communication performance. The proposed method is a simulation of the hybrid loop-free routing approach and hybrid metric methods under lossy/not lossy area topology conditions. Finally, this research states that the hybrid loop-free method can prevent loops from occurring and can achieve loopfreeness.

According to [17], [18] discusses solutions for using simultaneous application traffic tunnels (e.g voice and data) simultaneously. To avoid congestion/delay, customer routes must provide space for resource allocation for various communication sessions. The research method is TE (Traffic Engineering) of MPLS hybrid network on Cisco 9-router configurations using the MPLS-VPN protocol. The experimental results show that the TE method is much less output received, when compared to MPLS-VPN networks without engineering traffic and still categorized as low [19], [20].

Based on literacy studies, this research proposes looping protection methods [14]–[16] and SR-TE methods that simplify control plane operations [5], [6], [10], [17] at tunnel L2-VPN [1]–[3], [13] on MPLS network [4], [18]–[20] using mesh topologies to solve the problem of QoS ISPs and reduce the occurrence of simplified looping in the fishbone diagram shown on the fig. 1.

B. Research Method

This research proposes 2-methods that aim to compare interconnections in L2-VPN within the MPLS network which aims to save costs derived from using resources to be more efficient and help reduce total operational costs. In addition, it can also be used to provide protection in case of link or node failures by providing tunnel backups.

First, proposed using SR-TE method, TE-information in MPLS is carried by the Resource Reservation Protocol (RSVP). RSVP is used to signal LSP (Label Switched Path) in TE tunnels constructed by dynamic path or explicit path. TE is used to change LSP by default selected by IGP via the shortest path.

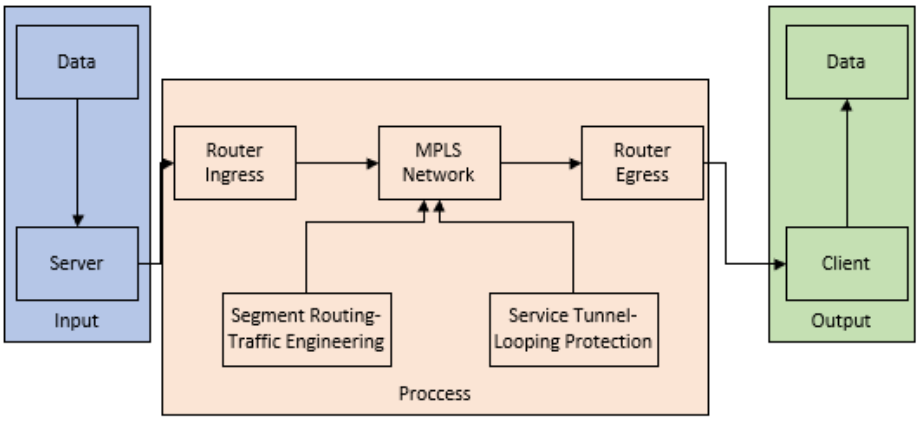

Fig. 2. Block diagram system

The first, proposed design using the SR-TE method, where the TE information in MPLS is carried by the Resource Reservation Protocol (RSVP). RSVP is used in MPLS-TE to signal LSP (Label Switched Path) in TE tunnels constructed by dynamic path or explicit path. TE is used to change LSP by default selected by IGP via the shortest path.

Then, the second proposal using the looping protection method which is a form of protection or anticipating the occurrence of a traffic reverse rotation event from a node back to the node and is not stopped or also where data packets will be sent back to the recipient so that data packets do not reach their destination or because of problems with the traffic of sending data or known as looping.

Figure 2 shows the scenario planning that has been designed in the diagram block. The input block informs that the data is transmitted through the server and then continued into the MPLS network through the ingress router. On the MPLS network, the SR-TE method has been implemented with service tunnel-looping protection. After arriving at the router egrees the data packet will be forwarded to the client and the original data packet will be received.

C. *SR-TE Materials*

The following is presented about the topology scenario using SRTE method on L2-VPN MPLS is designed as follows:

1. There are 2 end-devices, namely a server as the source provider of data packages on the network and a client as an accessor to the source data packages provided by the server.
2. All routers use the NOKIA Service Router 7750 router.
3. There is router as an EN (Edge Node) router, functioning as a router that is directly adjacent to the customer and also functions as an LSR ingress and LSR (Label Switching Router) egress on the MPLS network.
4. There are CN (Core Network) routers, functioning as ABR (Area Border Router) routers on the border of each customer area with area 0 (Backbone Area).
5. There are AN (Aggregator Network), functioning as serves as a network aggregation from the server direction.

D. *Tunneling Looping Protection Materials*

The description in the topology scenario using the looping protection method in the L2-VPN MPLS designed is as follows:

1. All routers use the NOKIA Service Router 7750 router.
2. There are 1 switch and 4 routers.
3. There are routers, functioning as routers that are directly adjacent to the customer. This CN router functions as an LSR ingress and LSR egress on an MPLS network.
4. All routers will be created a L2-VPN service where services will be streamed via the Switch towards the client.

III. Result And Discussion

This sub-chapter will compare the results of testing between Mpls service layer networks with both MPLS-TE and SR-TE methods that will provide the same design and testing scenario.

A. *System Testing*

After the network system has been built and configured according to the topological design, then the connectivity test is carried out end to the end-user (server-client). It can be seen in figure 3 and figure 4. From the results of end-to-end connectivity tests have shown reply results that indicate the network system has been converged between one router and another router, both routing protocols and other protocols have been configured perfectly on each router

```
Pinging 10.10.10.2 with 32 bytes of data:
Reply from 10.10.10.2: bytes=32 time=51ms TTL=128
Reply from 10.10.10.2: bytes=32 time=97ms TTL=128
Reply from 10.10.10.2: bytes=32 time=66ms TTL=128
Reply from 10.10.10.2: bytes=32 time=95ms TTL=128
```

Fig. 3. Ping end to end from server to client

```
Pinging 10.10.10.1 with 32 bytes of data:
Reply from 10.10.10.1: bytes=32 time=20ms TTL=128
Reply from 10.10.10.1: bytes=32 time=25ms TTL=128
Reply from 10.10.10.1: bytes=32 time=51ms TTL=128
Reply from 10.10.10.1: bytes=32 time=52ms TTL=128
```

Fig. 4. Ping end to end from client to server

```
Forwarding Database, Service 10
ServId    MAC                Source-Identifier
10        00:0c:29:b1:1d:4a sdp:26:10
10        00:0c:29:d7:c6:31 sap:1/1/1
10        00:50:56:c0:00:08 sdp:16:10
```

Fig. 5. MAC Address VPLS UMB-EN1

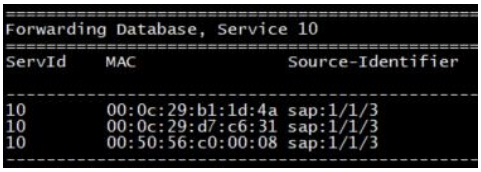

Fig. 6. MAC Address VPLS UMB-AN1

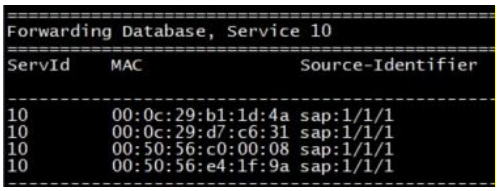

Fig. 7. MAC Address VPLS UMB-AN2

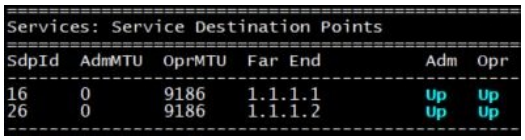

Fig. 8. Tunnel SDP SR-TE UMB-EN1

B. Service Layer 2 Testing (VPLS Service)

Service L2-VPN MPLS will use a type of VPLS service that is multipoint to multipoint. VPLS service will be configured on end-to-end MPLS network if referring to the design of end-to-end MPLS network topology. The parameters that show the vpls service is already running, namely the service can read mac addresses sent from the neighboring side that both have VPLS service and have status indicators "Admin State = UP" and "Oper State = UP", sampling capture can be seen in figure 5 - figure 7.

C. SDP Tunnel SR-TE

SDP tunnels that have been successfully configured that run using the SR-TE protocol will show the LSP indicator "O" which means SR-OSPF which is a segment routing protocol with OSPF routing, and has the status indicators "Admin State = UP" and "Oper State = UP", the concentration of SDP tunnel SR-TE on UMB-AN1, UMB-AN2, and UMB-EN1. Sampling capture can be seen in figure 8.

TABLE I.
EXPERIMENTAL RESULTS

Data Label Pattern					
Protocol	**Scenario 1**		**Scenario 2**		**Description**
SR-TE	Global Labelling		Globang Labelling		Source Node Router
MPLS-TE	Private LFIB		Private LFIB		Individual LFIB Router
ICMP Package Comparison					
Protocol	**Scenario 1 (ms)**		**Scenario 2 (ms)**		**TIPHON Index**
SR-TE	8.775		13.57		4
MPLS-TE	8.925		13.75		4
Comparison of Service Rate SDP Tunnel					
Protocol	**Scenario 1 (ms)**		**Scenario 2 (ms)**		**TIPHON Index**
SR-TE	3.614		8.08		4
MPLS-TE	3.673		10.213		4
Comparison of QoS Throughput					
Protocol	**Scenario 1 (KBps)**				**TIPHON Index**
	Upload {25 MB)	**Upload (50 MB)**	**Download (25 MB)**	**Download (50 MB)**	
SR-TE	292.6	297.2	130	108.6	3
MPLS-TE	265.2	326.8	138.4	64.4	3
Looping Protection	#N/A	#N/A	#N/A	#N/A	
Protokol	**Scenario 2 (KBps)**				**TIPHON Index**
	Upload {25 MB)	**Upload (50 MB)**	**Download (25 MB)**	**Download (50 MB)**	
SR-TE	136.6	155.4	91.6	80	2
MPLS-TE	172.4	176.6	103.4	71	2
Looping Protection	0.1193	0.129	0.18533	0.23266	4
Comparison of QoS Delay					
Protocol	**Scenario 1 (ms)**				**TIPHON Index**
	Upload {25 MB)	**Upload (50 MB)**	**Download (25 MB)**	**Download (50 MB)**	
SR-TE	3.58	3.5	6.52	8.68	4
MPLS-TE	4.16	3.14	5.86	11.08	4
Looping Protection	#N/A	#N/A	#N/A	#N/A	
Protocol	**Scenario 2 (ms)**				**TIPHON Index**
	Upload {25 MB)	**Upload (50 MB)**	**Download (25 MB)**	**Download (50 MB)**	
SR-TE	7.78	7.18	8.46	8.86	4
MPLS-TE	6.04	5.2	8.22	10	4
Looping Protection	5.9	5.2	6.5	4.13	4

D. Analysis Data

Table 1 shows the results of tests that have been carried out based on predetermined parameters, So, further explained the analysis at each important point of the test results.

1) ICMP Packet (Ping)

The results of the network connectivity test with ping commands were tested 40 times for each protocol and scenario tested end to end (Server-Client). Networks using the SR-TE protocol show the average ping reply value parameter in scenario 1 around 8.78 ms and scenario 2 about 13.57 ms. Whereas networks using the MPLS-TE protocol show the average ping reply value parameter in scenario 1 about 8.96 ms and scenario 2 about 13.75 ms. From this connectivity test, it can be seen that networks with SR-TE protocol have better network connectivity values than networks with MPLS-TE protocols both using scenario 1 and scenario 2.

2) Service Tunnel SDP (L2VPN)

The results of the SDP tunnel testing for layer 2 of SR-TE VPN with service rate testing were tested 10 times for each protocol and scenario tested end to end MPLS Network (AN1-EN1). Networks using the SR-TE protocol show the parameters of the average service rate value in scenario 1 about 3.6 ms and scenario 2 about 8.08 ms. While networks that use the MPLS-TE protocol show the parameter value of the average service rate in scenario 1 about 3.67 ms and scenario 2 about 10.21 ms. If referring to the standard TIPHON standard delay category, The service rate value of both protocols is in an excellent category with an index of 4. From this service rate test, it can be seen that networks with SR-TE protocols have a better network tunnel service rate value than networks with MPLS-TE protocols both using scenario 1 or scenario 2.

3) Throughput

The results of QoS testing of throughput parameters with tests conducted 5 times both in the upload and download process for each protocol and scenario tested end to the end-user (Server-Client), this test using boom traffic load of 25 MB and 50 MB, for bandwidth used which is 3 Mbps. In scenario testing 1 the average value throughput in testing both boom traffic of 25 MB and 50 MB for the process Upload sr-TE protocol about 294.9 KBps or about 78.64% of bandwidth and MPLS-TE protocol about 296 KBps or about 78.93% of bandwidth and for the process of downloading SR-TE protocol about 119.3 KBps or about 31.81% of bandwidth and MPLS-TE protocol about 101.4 KBps or about 27.04% of bandwidth. In scenario 2 testing the average throughput value in the test of both boom traffic of 25 MB and 50 MB for the SR-TE protocol upload process is about 146 KBps or about 38.93% of the bandwidth and MPLS-TE protocol is approximately 174.5 KBps or about 46.53% of bandwitdh and for the download process sr-TE protocol about 85.8 KBps or about 22.88% of bandwidth and MPLS-TE protocol about 87.2 KBps or about 23.25% of bandwidth. Overall QoS testing of SR-TE protocol throughput parameters is still better than MPLS-TE protocol both using scenario 1 or scenario 2 although in some tests MPLS-TE protocol is superior when viewed graphically every sr-TE protocol experiment has a more stable throughput graph index when compared to MPLS-TE protocol which is more drastically up and down on each test graph. When referring to the STANDARD TIPHON throughput category, the throughput values of both protocols are in the good category with index 3.

The looping protection method has been successfully resolved by adding *auto-learn-mac-protect* configuration on SAP (Service Access Point) and restrict-protected-src on the UMB-CN2 SDP (Service Destination Point) tunnel leading to UMB-CN4 and the UMB-CN4 SDP tunnel leading to UMB-CN2, so that the interconnection is normal. has successfully performed its function with MAC address protection and disabled SDP flowing on the MAC address, and it is proven that the MAC address is blocked 00:50:56:c0:00:08 which is the cause of looping originating from SDP towards JKT-CN4, so that traffic can run normally. The upload/download throughput results are shown to be stable because the looping protection method has protected traffic from the server through the VPLS service to the client.

4) Delay

The results of the QoS test parameter delay with testing conducted 5 times on both the upload and download process for each protocol and scenario tested end to end-user (Server-Client), this test using boom traffic load of 25 MB and 50 MB. The average delay value results of all trials can be seen in Table 1, from those results when referring to the TIPHON standard of the delay category, the delay values of both protocols are in the category very well with index 4. In scenario testing 1 the average delay value on testing both boom traffic of 25 MB and 50 MB for the SR-TE protocol upload process is approximately 3.54 ms and MPLS-TE protocol is about 3.65 ms, and for the sr-TE protocol download process, about 7.6 ms and MPLS-TE protocol is about 8.47 ms. In scenario 2 the average value of delay on the 25 MB or 50 MB boom traffic test for the SR-TE protocol upload process is approximately 7.48 ms and the MPLS-TE protocol is approximately 5.62 ms, and for the SR-TE protocol download process, about 8.66 ms and the MPLS-TE protocol is approximately 9.11 ms. Overall QoS testing of SR-TE protocol delay parameters is still better than MPLS-TE protocol although in some tests MPLS-TE protocol is superior when viewed graphically every protocol experiment SR-TE has a more stable delay chart index.

CONCLUSION

The conclusion of this research states that the SRTE method and looping protection method have been successfully executed in L2-VPN. The SR-TE method produces data packets that are transmitted and then converted into data frames, until finally they have been identified based on the hardware MAC Address. The formation of label paths in SR-TE uses Prefix Segment categorized as Global Unique Labelling which is determined based on the allocation of SR Global Blocks, because the process is determined based on the shortest IGP path of data traffic. The looping indication has been resolved using the looping protection method due to the rotation of the MAC address originating from the SDP tunnel that connects the VPLS service on the router continuously which is directly connected to the client device. Perform configuration improvements on the router in the form of auto-learn-mac-protected in SAP as a MAC Address detector and restrict-protected-src on the SDP tunnel as an action taker to disable looping. **The results** of QoS analysis based on throughput parameters show that the SR-TE method is

better, more stable and categorized as "good" based on TIPHON standards. The average SR-TE Upload/Download in scenario-1 is 55.23% of the total bandwidth compared to MPLS-TE of 52.98% of the total bandwidth. The average SR-TE Upload/Download in scenario-2 is 30.91% of the total bandwidth compared to MPLS-TE of 34.85% of the total bandwidth. Meanwhile, the looping protection method shows an average upload of 129 bps and a download of 232.66 bps. **The results** of measurement and analysis of QoS based on delay showed that the SR-TE method was better, superior and categorized as "excellent" based on the TIPHON standard, the average SR-TE delay obtained 5.57 ms compared to the MPLS-TE obtained 6.06 ms. Pada metode looping protection rata-rata delay diperoleh 5.2 ms. The results of QoS measurement and analysis based on the ICMP package connectivity test (Ping-test), showed that the average value of ping reply upload was obtained 11,173 ms and the average ping reply download was obtained 11,338 ms so that it showed an "excellent" category based on TIPHON standards.

The looping-protection method produces an upload/ download delay in the "excellent" category according to TIPHON standards, because the looping-protection method has protected traffic from the server through the VPLS service to the client.

ACKNOWLEDGEMENTS

The first special thanks to Universitas Mercu Buana which has supported in domestic collaborative research, the second to Badan Riset dan Inovasi Nasional, and the third to PT. Datacomm Diangraha for their assistance and cooperation during this research. Hopefully, in the future there will always be new papers in collaborative research in the future.

REFERENCES

[1] S. Budiyanto, C. S. Aprihansah, L. M. Silalahi, I. U. Vistalina Simanjuntak, F. A. Silaban, and A. D. Rochendi, "Auto Discover Virtual Private Network Using Border Gateway Protocol Route Reflector," in *2022 IEEE International Conference on Communication, Networks and Satellite (COMNETSAT)*, Nov. 2022, pp. 123–129. https://doi.org/10.1109/COMNETSAT56033.2022.9994439.

[2] E. Darmawan, S. Budiyanto, and L. M. Silalahi, "QoS Analysis on VoIP with VPN using SSL and L2TP IPSec Method," in *2022 IEEE International Conference on Communication, Networks and Satellite (COMNETSAT)*, Nov. 2022, pp. 130–136. https://doi.org/10.1109/COMNETSAT56033.2022.9994572.

[3] Ubedilah, S. Budiyanto, and L. M. Silalahi, "Analysis QoS VoIP using GRE + IPSec Tunnel and IPIP Based on Session Initiation Protocol," in *2022 5th International Conference of Computer and Informatics Engineering (IC2IE)*, 2022, pp. 47–54. https://doi.org/10.1109/IC2IE56416.2022.9970120.

[4] S. Budiyanto and M. Gathmir, "Improvement of Policy Charging Control Flow Based on Internet Subscribers Behavior," in *2020 2nd International Conference on Broadband Communications, Wireless Sensors and Powering (BCWSP)*, 2020, pp. 113–118. https://doi.org/10.1109/BCWSP50066.2020.9249394.

[5] L. M. Silalahi, S. Budiyanto, F. A. Silaban, H. B. H. Sitorus, A. D. Rochendi, and M. F. Ismail, "Analysis of the effectiveness of online electronic learning system using data traffic network performance management to succeed merdeka learning--Merdeka campus during the Covid-19 pandemic," *Int. J. Electron. Telecommun.*, vol. 67, no. 4, pp. 595–601, 2021.

[6] S. Budiyanto, L. M. Silalahi, F. A. Silaban, R. Muwardi, and H. Gao, "Delivery Of Data Digital High Frequency Radio Wave Using Advanced Encryption Standard Security Mechanism," in *2021 International Seminar on Intelligent Technology and Its Applications (ISITIA)*, Jul. 2021, pp. 386–390. https://doi.org/10.1109/ISITIA52817.2021.9502262.

[7] Asosiasi Penyelenggara Jasa Internet Indonesia, "Profil Internet Indonesia 2022," *Apji.or.Od*, no. June, p. 10, 2022, [Online]. Available: apji.or.id

[8] S. Nurhayati, A. H. Noor, S. Musa, R. Jabar, and W. J. Abdu, "A Digital Literacy Workshop Training Model for Child Parenting in a Fourth Industrial Era," *HighTech Innov. J.*, vol. 3, no. 3, pp. 297–305, 2022.

[9] L. Wang, Q. Li, L. Liu, Y. Jiang, M. Xu, and J. Wu, "S5: An Application Sensitive QoS Assurance System via SDN," *2018 IEEE 37th Int. Perform. Comput. Commun. Conf. IPCCC 2018*, pp. 1–8, 2018, https://doi.org/10.1109/PCCC.2018.8710838.

[10] P. L. Ventre *et al.*, "Segment Routing: A Comprehensive Survey of Research Activities, Standardization Efforts, and Implementation Results," *IEEE Commun. Surv. Tutorials*, no. Revision R2, 2020, https://doi.org/10.1109/COMST.2020.3036826.

[11] E. C. Filsfils, E. S. Previdi, L. Ginsberg, B. Decraene, S. Litkowski, and R. Shakir, "Segment Routing Architecture," *Internet Eng. Task Force*, no. ISSN: 2070-1721, pp. 1–32, 2018.

[12] E. S. Previdi *et al.*, "OSPF Extensions for Segment Routing," *Internet Eng. Task Force*, pp. 1–28, 2019.

[13] S. T. Aung and T. Thein, "Comparative Analysis of Site-to-Site Layer 2 Virtual Private Networks," in *2020 IEEE Conference on Computer Applications(ICCA)*, Feb. 2020, pp. 1–5. https://doi.org/10.1109/ICCA49400.2020.9022848.

[14] V. D. Dimitrov, "Implementation of Loop Prevention Protocols at the Data Link Layer in LAN," pp. 105–108, 2020, https://doi.org/10.1109/TELECOM50385.2020.9299530.

[15] D. Fialho and P. Mateus, "Stabilizing BGP Through Distributed Elimination of Recurrent Routing Loops," 2017.

[16] E. Takimoto, S. Aketa, Y. Otsuki, S. Saito, and K. Mouri, "A HYBRID LOOP-FREE ROUTING PROTOCOL FOR WIRELESS MESH NETWORKS," pp. 286–291, 2017, https://doi.org/doi:10.1109/cit.2017.45.

[17] E. M. Gales and V. Croitoru, "Traffic Engineering and QoS in a Proposed MPLS-VPN," *2020 14th Int. Symp. Electron. Telecommun. ISETC 2020 - Conf. Proc.*, pp. 3–6, 2020, https://doi.org/10.1109/ISETC50328.2020.9301135.

[18] M. A. Panhwar, K. A. Memon, A. Abro, D. Zhongliang, S. A. Khuhro, and Z. Ali, "Efficient Approach for optimization in Traffic Engineering for Multiprotocol Label Switching," in *2019 IEEE 9th International Conference on Electronics Information and Emergency Communication (ICEIEC)*, Jul. 2019, pp. 1–7. https://doi.org/10.1109/ICEIEC.2019.8784486.

[19] P. Zhang, Y. R. Gang, X. Huang, S. Zeng, and K. Xie, "Bandwidth Allocation With Utility Maximization in the Hybrid Segment Routing Network," *IEEE Access*, vol. 7, pp. 85253–85261, 2019, https://doi.org/10.1109/ACCESS.2019.2924672.

[20] N. Geng, Y. Yang, and M. Xu, "Flow-Level Traffic Engineering in Conventional Networks with Hop-by-Hop Routing," *2018 IEEE/ACM 26th Int. Symp. Qual. Serv. IWQoS 2018*, pp. 1–10, 2019, https://doi.org/10.1109/IWQoS.2018.8624179.