Interoperability and Reliability of Multiplatform MPLS VPN: Comparison of Traffic Engineering with RSVP-TE Protocol and LDP Protocol

Nanang IsmaiI[1], Eki Ahmad Zaki H[2], and M. Arghifary[3]
[1]Electrical Engineering Department, [2]Faculty of Science & Technology,
[3]UIN Sunan Gunung Djati, Bandung 40614, Indonesia
Email: [1]nanang.is@uinsgd.ac.id, [2]ekiahmadzaki@uinsgd.ac.id, [3]arghifary.m@gmail.com

***Abstract*—One of the alternatives to overcome network scalability problem and maintaining reliability is using MPLS VPN network. In reallity, the current network is already using a multiplatform of several different hardware vendors, i.e., Cisco and Juniper platforms. This paper discusses the comparison of the simulation results to see interoperability of multiplatform MPLS VPN and reliability through traffic engineering using RSVP-TE and LDP protocols. Both the RSVP and LDP protocols are tested on a stable network and in a recovery mode, as well as non-load conditions and with additional traffic load. The recovery mode is the condition after the failover due to termination of one of the links in the network. The no-load condition means that the network is not filled with additional traffic. There is only traffic from the measurement activity itself. While network conditions with an additional load are conditions where there is an additional UDP packet traffic load of 4.5 Mbps in addition to the measurement load itself. On a stable network and without additional traffic load, the average delay on LDP protocol is 59.41 ms, 2.06 ms jitter, 0.08% packet loss, and 8.99 Mbps throughput. Meanwhile, on RSVP protocol, the average delay is 52.40 ms, 2.39 ms jitter, 12.18% packet loss, and 7.80 Mbps throughput. When failover occurs and on recovery mode, LDP protocol is 48% of packet loss per 100 sent packets while on RSVP packet loss percentage is 35.5% per 100 sent packets. Both protocols have interoperability on the third layer of multiplatform MPLS VPN, but on heavy loaded traffic condition, RSVP protocol has better reliability than the LDP protocol.**

***Index Terms*—Interoperability, Reliability, Traffic Engineering, MPLS VPN, RSVP Protocol, LDP Protocol**

I. Introduction

SERVICE provider is the main player in the provision of systems and data communications channels. The convergence of Internet with telecommunication allows the use of provider's network resource optimally. For instance, Virtual Private Network (VPN) allows a private data link on public network with high scalability and security [1]. By VPN, providers can utilize their network on the Internet to be used as private data communication for users as long as the users are connected to provider's Point of Presence (PoP) [1, 2].

The Internet Engineering Task Force (IETF) standardizes a solution such as Multiprotocol Label Switch (MPLS) as an expansion of VPN to increase the performance of forwarding and traffic engineering intelligence on packet based network [2–4]. MPLS combines the advantage of the second OSI layer of forwarding and routing efficiency on the third OSI layer to increase the performance by label switching. This mechanism is consecutively used as a method to control traffic flow on the network to ensure the rigidity of traffic that is known as traffic engineering. Traffic engineering can overcome standard routing protocols such as RIP, OSPF, IGRP, and others on MPLS network because they seek the nearest and shortest route [2, 4–6].

There are two protocols supporting the traffic engineering, namely Resource Reservation Protocol (RSVP) and Constraint-Based Routed Label Distribution Protocol (CR-LDP). These protocols offer the same functions but different mechanisms. However, RSVP shows an advantage on data transport because it uses UDP so it is connectionless. On the other hand, several platforms deny UDP access so in the level of data transport, availability, and accessibility determine which protocols to be used [7–10].

Researchers have tested traffic engineering methods on MPLS network using several approaches [3, 4, 11–16]. Reference [14] applied tunneling and explicit route traffic engineering and analyzed the QoS for multicast

Received: 29 Mar. 2017; received in revised form: 20 Aug. 2017; accepted: 23 Oct. 2017; available online: 28 Nov. 2017.

data transfer on MPLS network. They revealed VPN on MPLS network by traffic engineering could support multicast network with appropriate expected QoS [14]. Reference [8] compared the RSVP and CR-LDP protocol parameters as traffic engineering protocol on MPLS network. Meanwhile, Ref. [9] compared frame error rate, throughput, and normalized data rate between RSVP and non-RSVP network. The analyzed data were voiced on the same physical network. The result revealed that the RSVP network had a lower frame error rate with a high throughput and normalized data rate compared to non-RSVP [9]. Reference [13] compared the memory usability of LDP and RSVP together with the advance of MPLS. The tested data packet on the network was Point to Multi-Point (P2MP) multicast data. The result showed RSVP-TE was better in utilizing network resource while LDP offered constant scalability within an expanding network.

In reality, the Internet is not always a single platform but multiplatform from different hardware vendors such as Cisco and Juniper. Every vendor has its scalability rule for each of their hardware. Therefore, hardware vendors and network providers must share the same information to determine which protocols to be implemented on MPLS network considering protocol determination becomes a crucial factor to rank the manufacturers devices and network providers [11].

This paper is the further development of the previous work of Ref. [17] that discusses the performance of the RSVP-TE protocol in Multiplatform MPLS VPN. This paper compares the results of traffic engineering by adjusting traffic flows (override traffic routes) by setting and controlling RSVE-TE and LDP protocols on multiplatform MPLS network. The goal is to compare the interoperability and reliability of RSVP and LDP protocols on multiplatform MPLS networks. The reliability will be seen by testing the performance of services (QoS).

II. Research Method

The research procedure is of the following:

1) System modeling
2) System configuration
3) Testing
   a) Connectivity testing
   b) Performance parameter testing
4) Analysis

A. System Modeling

We consider a model of a small company, which has one head office and two branch offices. They are connected through a VPN network by a provider. Each branch office has two networks and the head office has only one network. The network provider applies the MPLS on their own core network [17]. The model of the system is depicted in Fig. 1.

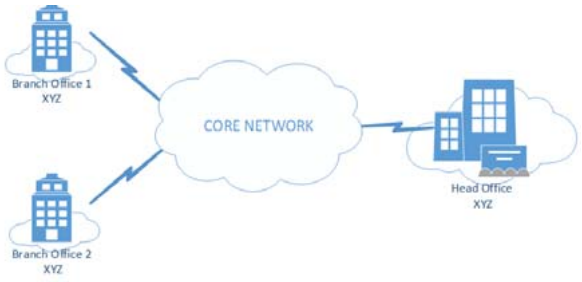

Fig. 1. VPN model [17].

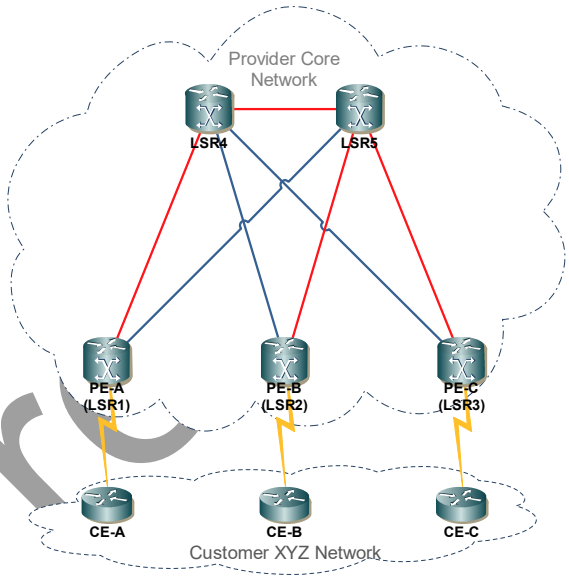

Fig. 2. System topology [17].

This network simulates three customer edges (CE), three provider edges (PE), and five routers as a core network from the provider. In the multiplatform test, CE router is from Cisco, and on core network routers and PE are from both Cisco and Juniper.

On every network in each business location, a router acts as a gateway to connect to the provider network with PoP. Graphically, the system topology is depicted in Fig. 2.

The topology has three main components of the system, CE, PR, and Label Switch Router (LSR). The three components will be configured to simulate traffic engineering on the third OSI layer VPN MPLS network. The variation of platforms is presented in Table I.

Cite this article as: N. Ismail, E. A. Zaki, and M. Arghifary "Interoperability and Reliability of Multiplatform MPLS VPN: Comparison of Traffic Engineering With RSVP-TE Protocol and LDP Protocol", CommIT (Communication & Information Technology) Journal 11(2), 57–65, 2017.

TABLE I
VARIATION OF PLATFORMS [17].

No	Node	Platform
1	CE-A, CE-B, CE-C, PE-A (LSR1), LSR4	Cisco
2	PE-B, PE-C, LSR5	Juniper

B. System Configuration

Basically, the traffic engineering in our simulation is materialized by adjusting the traffic flow (overriding traffic routes) determined by IGP to prevent traffic congestions on certain routes by routing protocol controlling on multiplatform MPLS network. In this research, the RSVP protocol is used for traffic engineering on MPLS network so that network congestion can be avoided on certain links.

With the LDP protocol, the selection of a path in the network following that of IGP. LDP duty is to give the packet label entering the MPLS network. In this simulation, the format of the LDP on a Cisco router configuration is shown in Listing 1.

Listing 1. Format of LDP Configuration on Cisco router.
```
Router(config)#mpls label protocol LDP
Router(config)#mpls ldp router-id [loopback]
```

Listing 2 shows an example configuration of LDP in LSR4.

Listing 2. LDP configuration on LSR4.
```
LSR4(config)#mpls label protocol LDP
LSR4(config)#mpls ldp router-id 4.4.4.4
```

Different from the Cisco router, in the Juniper router, LDP should explicitly configure such as OSPF protocols. In addition, MPLS must also be redefined in the sub of protocol configuration. Listing 3 shows the format of the LDP and MPLS configurations on Juniper routers.

Listing 3. Format of LDP configuration on Juniper Router.
```
root@#set protocols ldp interface [interface]
root@#set protocols mpls interface [interface]
```

Listing 4 shows an example configuration of LDP and MPLS on LSR5 router.

Listing 4. LDP and MPLS configuration on LSR5.
```
root@LSR5#set protocols ldp interface ge-0/0/0.0
root@LSR5#set protocols ldp interface ge-0/0/1.0
root@LSR5#set protocols ldp interface ge-0/0/2.0
root@LSR5#set protocols ldp interface ge-0/0/3.0
root@LSR5#set protocols mpls interface ge-0/0/0.0
root@LSR5#set protocols mpls interface ge-0/0/1.0
root@LSR5#set protocols mpls interface ge-0/0/2.0
root@LSR5#set protocols mpls interface ge-0/0/3.0
```

In the LSR5 router, all interfaces used by IGP incorporate into LDP protocols and MPLS. It is because all interfaces are used in MPLS networks.

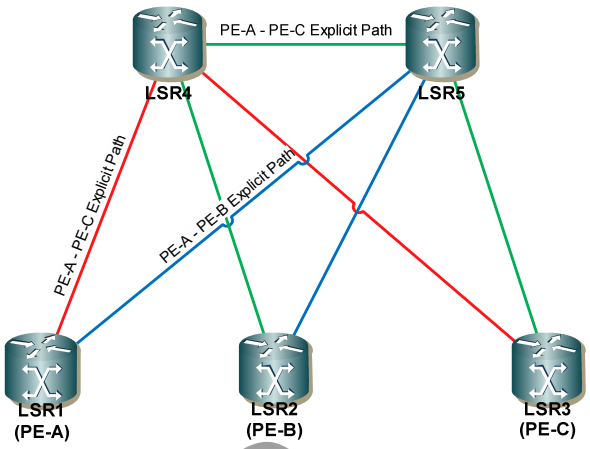

Fig. 3. RSVP explicit path. The red edges are PE-A–PE-C primary paths. The blue edges are PE-A–PE-B primary paths. The green edges are PE-B–PE-C primary paths.

The path determination used in this research is Explicit Path and Dynamic Path. Explicit path is used as a main path in transporting data from each PE and Dynamic Path acts as redundancy in case one node fails to work. The Explicit Path is depicted in Fig. 3.

The configuration format in Cisco router appointed to activate traffic engineering feature on MPLS network is depicted in Listing 5.

Listing 5. RSVP configuration format on cisco router.
```
Router(config)#mpls traffic-eng tunnels
Router(config)#interface [interface]
Router(config)#mpls traffic-eng tunnels
Router(config)#router [ospf]
Router(config)#mpls traffic-eng router-id lo0
Router(config)#mpls traffic-eng area 0
```

Listing 6 shows the configuration required for path determination taken by each PE.

Listing 6. Label Switched Path (LSP) Configuration Format.
```
LSR1(config)#mpls traffic-eng tunnels
LSR1(config)#interface Ethernet1/1
LSR1(config)#mpls traffic-eng tunnels
LSR1(config)#interface Ethernet1/2
LSR1(config)#mpls traffic-eng tunnels
LSR1(config)#router ospf 10
LSR1(config)#mpls traffic-eng router-id lo0
LSR1(config)#mpls traffic-eng area 0
```

In MPLS network, the path connecting LSR is called Label Switched Path (LSP) [7]. The configuration on Listing 6 is a configuration to form LSP traffic engineering on Cisco router. The address to be passed by LSP is determined by separate tunnel interface. Listing 7 shows the configuration for traffic engineering at LSR1 (Cisco).

With a similar method, configuration on Juniper router is done so the network can be set based on the plan.

Listing 7. Traffic Engineering Configuration.

```
Router(config)#interface [tunnel interface]
Router(config)#ip unnumbered [loopback]
Router(config)#tunnel mode mpls traffic-eng
Router(config)#tunnel destination [Destination Address]
Router(config)#tunnel mpls traffic-eng autoroute announce
Router(config)#tunnel mpls traffic-eng priotity [priority number]
Router(config)# tunnel mpls traffic-eng path-option 1 explicit name [path-name]
Router(config)# tunnel mpls traffic-eng path-option 2 dynamic
Router(config)# tunnel mpls traffic-eng record-route
Router(config)#ip explicit-path name [path-name]
Router(config)#next-address
```

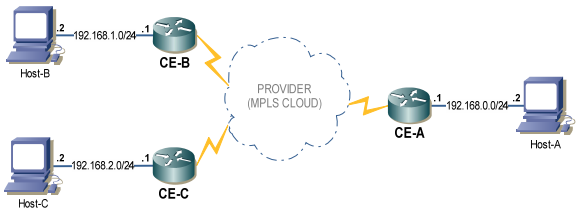

Fig. 4. Testing model.

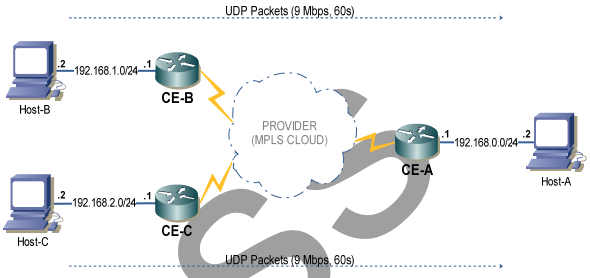

Fig. 5. No load traffic measurement model.

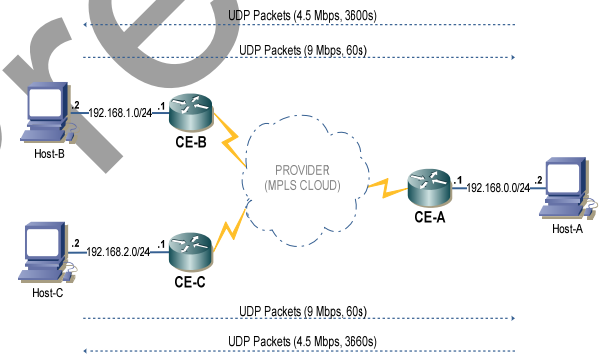

Fig. 6. Measurement model with additional traffic load.

C. Interoperability: Connectivity Test

The connectivity test is intended to check the interoperability of multiplatform of MPLS VPN. Testing is done by connecting the host to each CE router on the network as shown in Fig. 4.

The hosts which are used to test the connectivity use Ubuntu 12.04 operating system. Tools used in the testing are Ping and Traceroute. The testing process will be carried out from Host B and Host C to Host A with two scenarios for each protocol. That is when the network is stable (called as end-to-end connectivity testing) and when the network has failover (called as network recovery testing).

End-to-end connectivity test and network recovery are done on LDP and RSVP protocols. Testing is done by sending a ping request from Host B and Host C to Host A with a total of 100 packages and it can be seen how many packages are acceptable. The number of 100 packets is sufficient to see network connectivity.

D. Reliability Test

Reliability refers to the performance of the system. Network performance measurement is performed by connecting the host to each CE router. The compared performance parameters are the delay, jitter, packet loss, and throughput. Network performance measurement with LDP and RSVP protocols is done in two conditions, no load (except the measurement traffic itself) and loaded (with the additional UDP traffics). Figure 5 shows no load traffic measurement model.

To simulate loaded network, the network will be flooded by UDP traffics by 50% from maximum traffic load of 4.5 Mbps sent from Host-A to Host-B and Host-C. The loaded network measurement is depicted in Fig. 6.

The measurement is done using two tools, Ping and Iperf. Ping is used to determine delay while Iperf is used to send traffic and measure jitter, packet loss, and throughput. The measurement is done by sampling data every second during 60 s.

III. Results and Discussion

A. End-to-End Connectivity

The end-to-end connectivity is tested using the ping command on Linux OS. The purpose of this test is to ensure that the network is well connected. The results of the end-to-end connectivity test are shown in Table II.

Cite this article as: N. Ismail, E. A. Zaki, and M. Arghifary "Interoperability and Reliability of Multiplatform MPLS VPN: Comparison of Traffic Engineering With RSVP-TE Protocol and LDP Protocol", CommIT (Communication & Information Technology) Journal 11(2), 57–65, 2017.

TABLE II
END-TO-END CONNECTIVITY.

Protocol	Hosts	Packets Sent	Packet Received	Lost
LDP	B-A	100	100	0
	C-A	100	100	0
RSVP	B-A	100	100	0
	C-A	100	100	0

TABLE III
NETWORK RECOVERY CONNECTIVITY.

Protocol	Hosts	Packets Sent	Packet Received	Lost
LDP	B-A	100	52	48
	C-A	100	52	48
RSVP	B-A	100	66	34
	C-A	100	63	37

In Table II, it can be seen that all submitted packets are completely received. This indicates the network connection is stable and has no issue. On the stable condition, with the LDP protocol, the traceroute result from Host B to Host A shows the path through LSR2 (PE-B) → LSR5 → LSR4 → LSR1 (PE-A). The traceroute results from Host C to Host A shows the path through LSR3 (PE-C) → LSR5 → LSR4 → LSR1 (PE-A). The paths according to the configuration that has been done previously. Traceroute testing on Host B and Host C with LDP protocol shows the path similarities through LSR5 and LSR4. It shows that the LDP protocol susceptible to congestion of traffic because traffic from LSR2 and LSR3 pass through the same path.

With the RSVP protocol, traceroute results from Host B to Host A shows the path through LSR2 (PE-B) → LSR5 → LSR1 (PE-A). The path is according to the configuration that has been done before. The traceroute results from Host C to Host A shows the path through LSR3 (PE-C) → LSR4 → LSR1 (PE-A). Traceroute testing with RSVP protocol indicates that the traffic sent from Host B and Host C, has passed through different pathways to prevent congestion of traffic in the network.

B. Network Recovery

During the process of package transmission, one of the links in the network will be removed from the topology to simulate link failover in the network. The goal is to see the speed of each protocol that can perform recovery. The results of network recovery testing using command Ping in OS Linux are shown in Table III.

In general, it appears that the number of packets lost with RSVP protocol is less than the number of

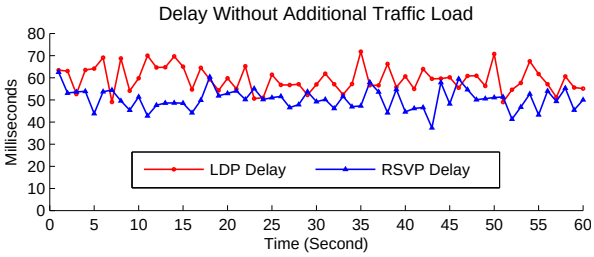

Fig. 7. Delay without additional traffic load.

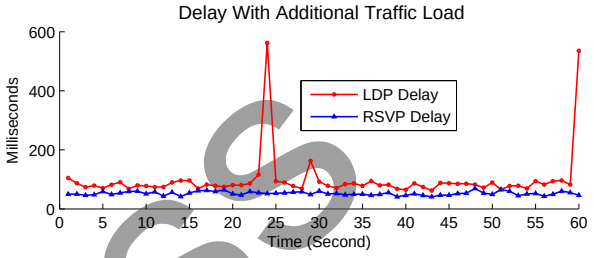

Fig. 8. Delay with additional traffic load.

packets lost with LDP protocol. The data shows that the RSVP protocol has a convergence time faster than LDP protocol, because of a number of losses to the protocol RSVP by 35.5%. Meanwhile, the number of losses by the LDP protocol are 48%. This happens because in the RSVP protocol, manufacture LSP is a make-before-break, where the LSP is made before the failover.

C. Delay

Delay is a time required by data packet from sender to recipient. The delay measurement is done using the command Ping and iPerf on the Linux OS. Command Ping functions to record delay, while iPerf works to add network traffic load at the time of measurements with additional traffic load. From 60 s of measurement, we obtain a delay for no loaded traffic from Host B and Host C to Host A as depicted in Fig. 7.

Figure 7 shows that the average of delay for 60 s between LDP and RSVP protocol. It shows no significant difference. The delay rate for LDP protocol is around 50–70 ms delay and around 40–60 ms for RSVP protocol.

Figure 8 shows the average of delay after the network is flooded with UDP traffic. This additional load is generated by iPerf of 4.5 Mbps as reverse traffic to the original sender.

On Fig. 8, a significant difference of delay can be seen on the network between using LDP protocol and RSVP protocol. With the LDP protocol, the average of delay about 80 ms and there are two packages that

TABLE IV
THE AVERAGE OF DELAY.

Condition	Protocol	Delay (ms)
Without traffic	LDP	59.41
	RSVP	50.24
With traffic load	LDP	98.82
	RSVP	52.40

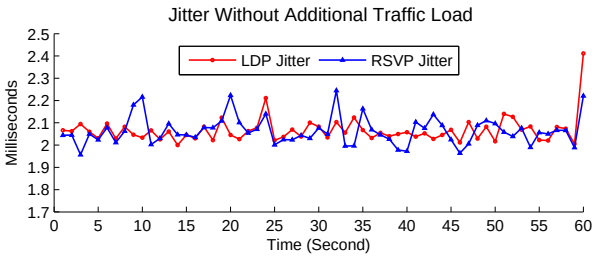

Fig. 9. Jitter without additional traffic load.

timeout marked with two points of the graph is above 500 ms. While with the RSVP protocol, the average delay is relatively stable around 50 ms. Figure 8 also shows that the RSVP protocol can manage the traffic better than the LDP protocol when the network is flooded with traffic. Table IV shows the average of delay for 60 s with LDP and RSVP protocols obtained by using command Ping on Linux OS.

The differences of network performance came after the network is flooded with traffic. With the LDP protocol, all traffics from Host B and Host C to the Host A have passed through the same path, resulting in accumulation of packages on the used link. The cumulation of packets causes queues packets to be longer, so the delay increases. Meanwhile, with the RSVP protocol, traffic from Host B and Host C has passed through different pathways to prevent the congestion on the used link.

D. Jitter

Jitter is a variation of delay as a result of time difference or interval of data packet arrival at the recipient. The measurement of jitter is done using Iperf tools. Jitter measurements in no-additional traffic load conditions are performed by sending a maximum pf 9 Mbps UDP packeta generated by iPerf. From the measurement for 60 s, we obtain the packet loss percentage for no loaded traffic from Host B and Host C to Host A as seen in Fig. 9.

Figure 9 shows that the average jitter for 60 s between LDP and RSVP protocol has the same relative value which is around 2 ms. This value indicates that in

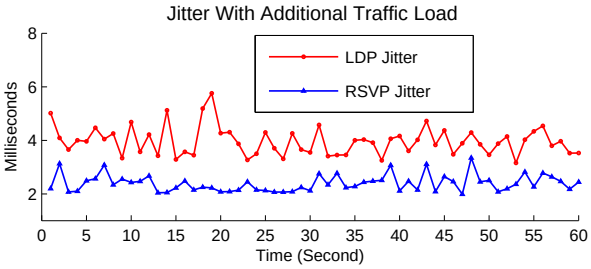

Fig. 10. Jitter with additional traffic load.

TABLE V
CONDITION PROTOCOL JITTER (MS).

Condition	Protocol	Jitter (ms)
Without traffic	LDP	2.06
	RSVP	2.06
With traffic load	LDP	3.96
	RSVP	2.39

no loaded traffic which both with the LDP and RSVP protocols, network quality is still maintained.

The measurement of jitter with additional traffic loads is done by adding 4.5 Mbps of reverse traffic load. Figure 10 shows the average jitter after the network is flooded with UDP traffic.

After the network is flooded with UDP traffic, the average of jitter with LDP and RSVP protocols is different. With the LDP protocol, the average jitter is around 4 ms, while the average jitter with RSVP protocol is around 2 ms. This shows a decreasing in the quality of the network in terms of jitter with LDP protocol when loaded traffic condition, while with the RSVP protocol, the decrease tends to be smaller. Table V shows the average of jitter for 60 s with LDP and RSVP protocols obtained by using iPerf tools.

E. Packet Loss

Packet loss is a rate to determine how much data packets are lost at the destination. The measurement of packet loss is done using Iperf tools. Packet loss measurements in no-additional traffic load conditions are performed by sending a maximum 9 Mbps UDP packets generated by iPerf. From a 60-second measurement, we obtain a packet loss for no loaded traffic from Host B and Host C to Host A as seen in Fig. 11.

Figure 11 shows the average packet loss with the LDP and RSVP protocol during the 60 s that have the same relative value of 0%. The impulse value of the initial in graph with both the LDP and RSVP protocol is possible as results of external influences, coming

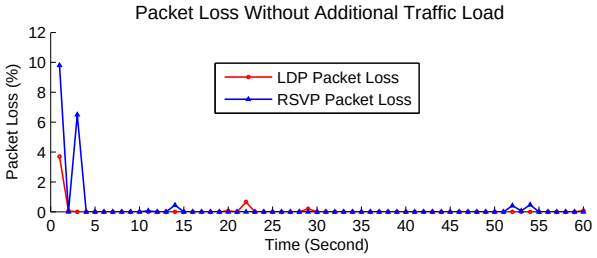

Fig. 11. Packet loss without additional traffic load.

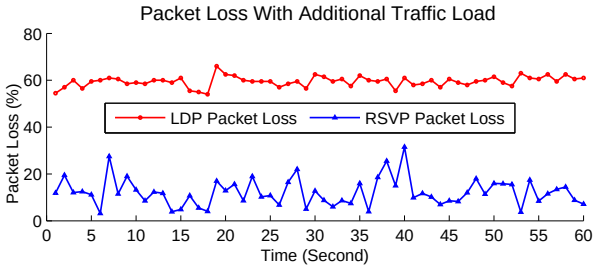

Fig. 12. Packet loss with additional traffic load.

TABLE VI
THE AVERAGE OF PACKET LOSS (%).

Condition	Protocol	Packet Loss (%)
Without traffic	LDP	0.08
	RSVP	0.30
With traffic load	LDP	59.48
	RSVP	12.18

from the system simulator. During the measurements, the computer loads as a system simulator increases. This happens because in addition to hardware simulation, the computer must simulate the traffic. Thus, the measurement process allows changes impulsively. Overall with the LDP and RSVP protocols in no loaded traffic condition, the packet loss value at both LDP and RSVP protocols is around 0%.

The measurement of packet loss with additional traffic loads is done by adding 4.5 Mbps reverse traffic load. Figure 12 shows the average of packet loss in the network after loaded with UDP traffic.

After the network flooded with UDP traffic, the average of packet loss with the LDP and RSVP protocols shows a significant difference. With LDP protocol, the average of packet loss is around 60%, while the average of packet loss with RSVP protocol is around 15%. This shows that the losses in the network with LDP protocol is larger than the RSVP protocol. Table VI illustrates the average of packet loss during the 60 s with LDP and RSVP protocols obtained by using iPerf tools.

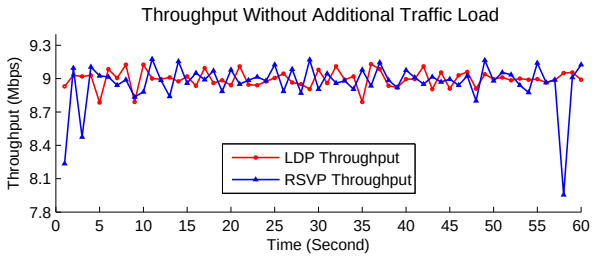

Fig. 13. Throughput without additional traffic load.

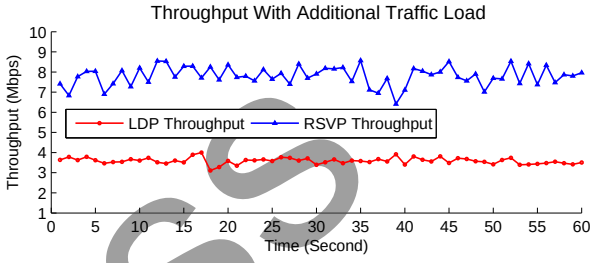

Fig. 14. Throughput without additional traffic load.

F. Throughput

Throughput are how much packets of data received by a node within certain observation interval. The value is influenced by delay, jitter, and packet loss within the network. The measurement of throughput is done using Iperf tools. Packet loss measurements in no-additional traffic load conditions are performed by sending a maximum of 9 Mbps UDP packets generated by iPerf. From a 60-second measurement, we obtain a throughput for no loaded traffic from Host B and Host C to Host A as seen in Fig. 13.

Figure 13 shows that the average of throughput with LDP and RSVP protocols has the same relative value around 9 Mbps. The impulse value of the initial in graph with both the LDP and RSVP protocol is a result of external influences. The throughput measured in the network will not reach the maximum value because the limited ability of the simulator is only 9 Mbps. With these limits, the maximum traffic that can be simulated is 9 Mbps.

The measurement of throughput with additional traffic loads is done by adding 4.5 Mbps reverse traffic load. This traffic generated by Ipref. Figure 14 shows the average of throughput in the network after loaded with UDP traffic.

After the network is flooded with UDP traffic, the average of throughput with the LDP and RSVP protocols show a significant difference. With the LDP protocol, average of throughput is around 4 Mbps, while with the RSVP protocol average throughput is around 8 Mbps. This shows the throughput on the

TABLE VII
THE AVERAGE OF THROUGHPUTS.

Condition	Protocol	Throughput (Mbps)
Without traffic	LDP	9.00
	RSVP	8.96
With traffic load	LDP	3.59
	RSVP	7.81

network with RSVP protocol is greater than the LDP protocol. Table VII illustrates the average of throughput within 60 s measurement with LDP and RSVP protocols obtained by using iPerf tools.

From VII, it can be seen that the average of throughput in the network with the LDP and RSVP protocol during the 60 s for no loaded traffic shows the value that relatively equals. To analyze the throughput in the network, it will not be separated from the packet loss on the network. In a network with no loaded traffic with the LDP and RSVP protocol, losses in the network are under 1% and the result of throughput approaches the maximum value. This occurs because of collisions in the network tend to be limited so the whole packages sent can be received well. In the network with additional traffic with the protocol LDP, losses are around 59.48%, while with the RSVP protocol, losses are around 12.18%. The high losses on LDP protocol cause the number of packets that can be accepted decrease, so a lot of data are lost due to a collision in the network. Then, with the RSVP protocol, because the traffic is routed to a different path, the collision can be minimized so that the number of data packets that can be received are greater.

IV. CONCLUSIONS

Based on the network simulation of the third OSI layer multiplatform MPLS VPN with LDP protocol, we conclude that:

- both the LDP and RSVP protocols can operate in the third multiplatform MPLS VPN (Cisco and Juniper),
- in the recovery process from sending 100 packets, the rate of loss with the LDP protocol is 48% and the RSVP protocol is 35.5%,
- on no traffic load with the LDP protocol, we obtain a delay of 59.41 ms, jitter of 2.06 ms, packet loss of 0.08%, and throughput of 8.996 Mbps, and with the RSVP protocol, we obtain a delay of 50.24 ms, jitter of 2.06 ms, packet loss of 0.29%, and throughput of 8.96 Mbps,
- on the loaded traffic of 50% of maximum load with the LDP protocol, we obtain the delay rate of 98.82 ms, jitter of 3.96 ms, packet loss of 59.48%, and throughput of 3.58 Mbps, and with the RSVP protocol, we obtain the delay rate of 52.40 ms, jitter of 2.39 ms, packet loss of 12.18%, and throughput of 7.80 Mbps, and finally,
- both protocols have interoperability at the third Layer Multiplatform of MPLS VPN, but on heavy loaded traffic condition, RSVP protocol is more reliable than the LDP protocol.

REFERENCES

[1] S. Gatot, "Qos analysis on mpls-vpn: Influences of 3des/aes encryption on ip-based video telephony," Master's thesis, Universitas Indonesia: Depok, 2013.

[2] R. Safitri, "Implementation and comparison analysis of qos on mpls-based vpn network, using ripv2, eigrp and ospf protocols againts ipsec tunneling for ip-based video converence services," Master's thesis, Universitas Indonesia, 2010.

[3] A. A. Adewale, E. R. Adagunodo, S. N. John, and C. Ndujiuba, "A comparative simulation study of ip, mpls, mpls-te for latency and packet loss reduction over a wan," *International Journal of Networks and Communications*, vol. 6, no. 1, pp. 1–7, 2016.

[4] I. Mangal and D. Bajaj, "A review of multiprotocol label switching: Protocol for traffic engineering on internet," *International Journal of Computer Trends and Technology*, vol. 11, no. 3, pp. 137–140, 2014.

[5] M. Hidayat and Risanuri, "Comparison of transport protocol performance on mpls and non mpls," Master's thesis, Universitas Gajah Mada, 2009.

[6] R. T. Murade, P. M. Ingale, R. U. Kale, and S. S. Sayyad, "Comparative analysis of ip, atm and mpls with their qos," *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, vol. 2, no. 5, pp. 112–115, 2013.

[7] A. Al Mamun, T. R. Sheltami, H. Ali, and S. Anwar, "Performance evaluation of routing protocols for video conference over mpls vpn network," *Journal of Ubiquitous Systems & Pervasive Networks*, vol. 7, no. 1, pp. 01–06, 2016.

[8] M. Asif, Z. Farid, M. Lal, and J. Qayyum, "Analysis of the similarities and differences between mpls label distribution protocols rsvp and cr-ldp," *International Journal of Computer Science*, vol. 54, no. 9, pp. 96–103, 2012.

[9] D. U. E, "Penerapan resource reservation protocol pada jaringan internet protokol," *Widya Teknika*, vol. 19, no. 2, pp. 27–31, 2011.

[10] G. U. Rehman, S. Muhammad, A. Cia, M. Asif, and S. Rehman, "Scalablity analysis of mpls label distribution protocols rsvp," *VAWKUM Transactions on Computer Sciences*, vol. 4, no. 2, pp. 20–25, 2015.

[11] M. Asif, Z. Farid, M. Lal, and J. Qayyum, "Mpls-a choice of signaling protocol," *International Journal of Computer and Science*, vol. 9, pp. 289–295, 2012.

[12] K. Firdaus, "Application of multi-protocol label switching (mpls) technoogy on computer networks (case study: Elkon lab, bppt)," Bachelor Thesis, UIN Syarif Hidayatullah, 2009.

[13] M. Chaitou and H. Charara, "Multicast in multi protocol label switching: A comparison study between ldp and rsvp-te," *International Journal of Information and Network Security*, vol. 2, no. 6, pp. 471–481, 2013.

[14] R. P. Adri, G. Abdullah, and I. Y. Pratama, "Analysis and design of mpls vpn network testbed with traffic engineering and qos at the center for information and communications technology bppt," Master's thesis, Bina Nusantara University, 2010.

[15] A. Zainuri, "Implementation and analysis voip services on mpls network using traffic engineering," Master's thesis, Universitas Dian Nuswantoro, 2013.

[16] Q. Q. Zhao and H. Chen, "System and method for point to multipoint inter-domain multiprotocol label switching traffic engineering path calculation," Jan. 2013, uS Patent 8,351,418.

[17] N. Ismail, M. Arghifary, E. Zaki, and W. Dimas, "Traffic engineering simulation using rsvp-te protocol on 3rd layer multiplatform mpls vpn," in *Proceeding of SICEST*, 2016, pp. 342–346.