ANALISIS KINERJA JARINGAN L3VPN MPLS MENGGUNAKAN SDN CONTROLLER ONOS

ANALYSIS OF L3VPN MPLS NETWORK PERFORMANCE USING ONOS SDN CONTROLLER

Ivan Ramadhan[1], Umar Ali Ahmad[2], Aliwarman Tarihoran[3]

[1,2,3] Universitas Telkom, Bandung
[1]**ivanramadhan@student.telkomuniversity.ac.id**, [2]**umar@telkomuniversity.ac.id**,
[3]**aliwarmantarihoran@telkomuniversity.ac.id**

Abstrak

Layer 3 Virtual Private Network (L3VPN) merupakan layanan yang disediakan pada jaringan Multiprotocol Label Switching (MPLS) untuk memberikan koneksi virtual private network yang aman dan cepat. L3VPN pada jaringan MPLS konvensional dinilai sulit dikelola dengan bertambahnya demand penggunaan layanan. Penggunaan Software Defined Network (SDN) pada jaringan L3VPN dapat mengatasi masalah tersebut, membuat jaringan mudah dikelola dan meningkatkan performansinya. Pada penelitian ini akan, dibahas perbandingan performansi yang dilakukan untuk mengetahui apakah penggunaan SDN pada jaringan L3VPN dapat mengatasi masalah yang sudah disebutkan. Pengukuran performansi dilakukan dengan parameter Setup Time atau mengukur seberapa cepat SDN dapat membantu pembuatan layanan L3VPN. Pada akhir penelitian ini telah dilakukan pengukuran Setup Time layanan L3VPN MPLS pada kedua sistem dengan beberapa skenario pengujian. Dari hasil yang didapat, penggunaan SDN dapat mempercepat pembuatan layanan L3VPN MPLS 757,14% hingga 1246% dibandingkan Konvensional. Hasil dari penelitian ini telah menunjukkan bahwa penggunaan SDN pada layanan L3VPN MPLS dapat meningkatkan kecepatan pembuatan layanan, mempermudah pengelolaan layanan, dan membuka peluang pada jaringan konvensional untuk lebih programmable.

Kata kunci : L3VPN, MPLS, SDN, Performansi.

Abstract

Layer 3 Virtual Private Network (L3VPN) is a service provided on a Multiprotocol Label Switching (MPLS) network to provide a secure and fast virtual private network connection. L3VPN on conventional MPLS networks is considered difficult to manage with the increasing demand for service usage. The use of Software Defined Network (SDN) on the L3VPN network can overcome these problems, make the network easy to manage and improve its performance. Performance measurement is carried out with the Setup Time parameter or measuring how fast SDN can help create L3VPN services. At the end of this study, the L3VPN MPLS service Setup Time measurement has been carried out on both systems with several test scenarios. From the results obtained, the use of SDN can speed up the creation of L3VPN MPLS services from 757.14% to 1246% compared to conventional. The results of this study have shown that the use of SDN in the L3VPN MPLS service can increase the speed of service creation, simplify service management, and open up opportunities for conventional networks to be more programmable.

Keywords: L3VPN, MPLS, SDN, Performance.

1. Pendahuluan

Berkembangnya teknologi *internet* yang semakin pesat saat ini, semakin memudahkan kebutuhan manusia. Hal ini terbukti dengan semakin banyaknya pengguna yang terhubung dengan jaringan *internet*. Semakin banyaknya penggunaan jaringan *internet* maka diperlukan akses *internet* yang semakin cepat dan aman. Penyediaan layanan *internet* (ISP) dituntut dapat memberikan jaringan *backbone* yang dapat memenuhi kebutuhan tersebut. Teknologi yang dapat memenuhi kebutuhan akses *internet* cepat tersebut adalah MPLS, sedangkan untuk memberikan akses jaringan *internet* yang aman dapat dipenuhi dengan teknologi VPN.

MPLS memiliki prinsip operasi berbasis pertukaran label. Dengan prinsip operasi pertukaran label membuat MPLS memiliki kemampuan paket *forwarding* yang cepat. MPLS menawarkan layanan VPN untuk beroperasi di atasnya, salah satunya adalah L3VPN. L3VPN pada jaringan MPLS konvensional dinilai sulit dikelola dengan bertambahnya *demand* penggunaan layanan. Penggunaan *Software Defined Network* (SDN) pada jaringan L3VPN dapat mengatasi masalah tersebut, membuat jaringan mudah dikelola dan meningkatkan performansinya.

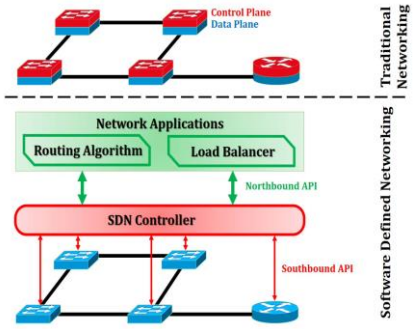
SDN merupakan konsep baru dalam membuat arsitektur jaringan. Konsep utamanya adalah pemisahan antara *control plane* dan *data plane* dalam suatu perangkat. Kecerdasan dalam perangkat dihilangkan dan diganti suatu kontrol terpusat[1]. Hadirnya teknologi SDN tidak menghilangkan teknologi yang sudah ada seperti MPLS, akan tetapi mendampingi dan meningkatkan performansi, *skalabilitas*, dan *programmability*.

Pada penelitian-penelitian sebelumnya seperti pada penelitian [2] dan [3] sudah dilakukan implementasi antara SDN dengan L3VPN MPLS menggunakan *controller* SDN Opendaylight dan Ryu, akan tetapi belum ada yang melakukan evaluasi performansi pembuatan layanan L3VPN pada ONOS. Oleh karena itu pada penelitian ini akan dilakukan analisis performansi antara L3VPN MPLS konvensional dan L3VPN MPLS yang sudah menggunakan SDN *Controller*. Evaluasi performansi dilakukan dengan pengukuran kecepatan *setup time* atau pembuatan layanan L3VPN MPLS.

2. Dasar Teori

2.1 SDN

Software Defined Network (SDN) adalah sebuah paradigma baru dalam membangun jaringan komputer yang mana terdapat pemisahan antara *control plane* dan *data plane* pada suatu perangkat jaringan seperti *router* dan *switch* [4]. Konsep pemisahan fungsi tersebut membuat *control plane* dan *data plane* memerlukan protokol komunikasi untuk saling berkomunikasi, protokol komunikasi yang digunakan pada SDN seperti *Openflow*, NETCONF, OVSDB, dan SNMP[5].



Gambar 1. Perbedaan arsitektur jaringan tradisional dengan SDN[6].

2.2 ONOS

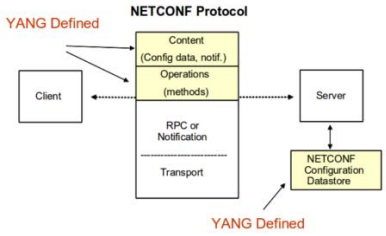
Open Network Operating System (ONOS) merupakan SDN *Controller* yang bersifat *open source* dan didesain untuk melayani layanan jaringan dengan skala besar berkat desain arsitektur terdistribusinya[7]. Penggunaan ONOS lebih diperuntukkan untuk penyedia layanan jaringan *internet* (ISP)[8].

2.3 NETCONF

NETCONF adalah *protocol* yang memiliki kemampuan untuk memasang, memanipulasi, dan menghapus konfigurasi pada perangkat jaringan. Menggunakan RPC untuk komunikasinya dan XML sebagai data konfigurasi [9].

2.4 YANG Data Model

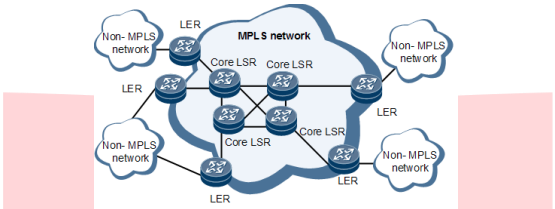
Yet Another Next Generation (YANG) adalah bahasa pemodelan data yang digunakan untuk mendefinisikan data yang dikirim melalui protokol pengelola jaringan seperti NETCONF [10].



Gambar 2. Operasi NETCONF dan YANG[11]

2.5 MPLS

Multiprotocol Label Switching (MPLS) merupakan protokol yang digunakan pada jaringan *backbone* IP, memiliki prinsip kerja berdasarkan pertukaran label di atas jaringan IP [12].



Gambar 3. Jaringan MPLS[13]

2.6 L3VPN

Layer 3 Virtual Private Network (L3VPN) adalah layanan *virtual private network* yang mengimplementasikan model *peer-to-peer* untuk menghubungkan *site* [15]. Dengan L3VPN, beberapa *site* pelanggan dapat terhubung melalui penyedia layanan jaringan IP/MPLS [16].

2.7 OSPF

Open Shortest Path First (OSPF) merupakan protokol *routing Interior Gateway* yang bekerja di dalam satu *autonomous system* yang sama menggunakan *routing* protokol *link-state* untuk menentukan jalur terbaik [18].

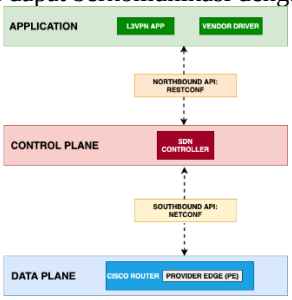
2.8 BGP

Border Gateway Protocol (BGP) merupakan *routing* protokol antar *Autonomous System*. BGP termasuk sebuah protokol *Exterior Gateway*. BGP menggunakan protokol *path-vector* untuk menentukan jalurnya[19].

3. Perancangan Sistem

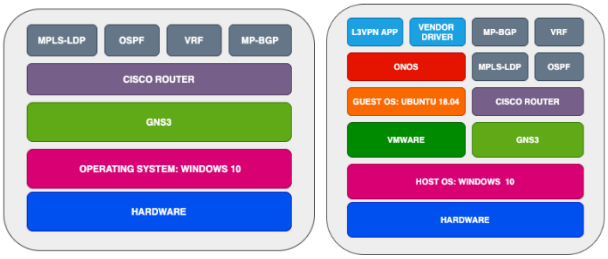
3.1. Desain Sistem

Desain sistem pada Gambar 3.1 adalah desain sistem untuk L3VPN MPLS dengan SDN. Secara umum komponen-komponennya terbagi menjadi *Application*, *Control Plane*, dan *Data Plane*. Komponen *Application* adalah layanan yang dijalankan oleh SDN *Controller*. Layanan yang akan dijalankan pada penelitian tugas akhir ini adalah layanan L3VPN yang digunakan untuk mengatur pembuatan VPN pada jaringan dan layanan *Vendor Driver* yang digunakan agar perangkat *router* yang berbasis *vendor* tertentu dapat berkomunikasi dengan *controller*.



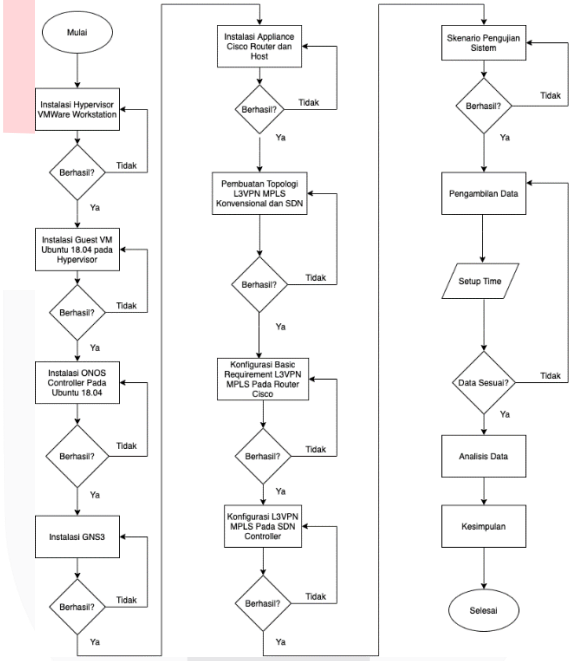
Gambar 4. Desain Sistem

Arsitektur sistem yang akan digunakan ada dua, yaitu arsitektur sistem L3VPN konvensional dan sistem L3VPN dengan SDN.



Gambar 5. Arsitektur L3VPN MPLS Konvensional dan SDN

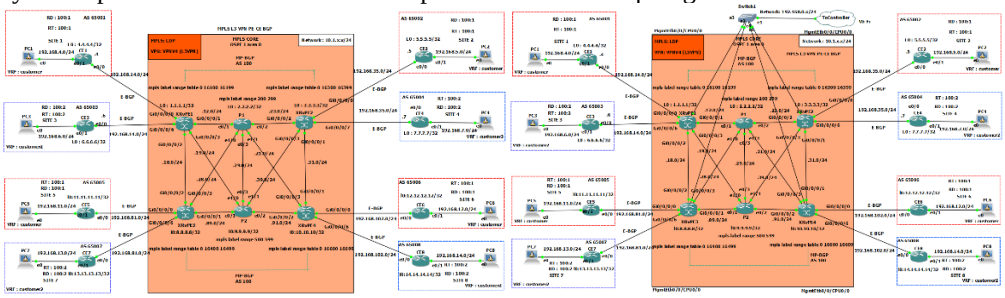
Pengerjaan penelitian dilakukan berdasarkan rancangan diagram alir yang sudah dibuat seperti pada Gambar 6. Pada diagram alir telah dipaparkan langkah-langkah pengerjaan mulai dari melakukan instalasi sistem hingga melakukan analisis data pengujian.



Gambar 6. *Flowchart* Sistem

3.2. Desain Topologi Sistem

Dalam penelitian ini kedua sistem L3VPN MPLS konvensional dan L3VPN MPLS dengan SDN yang dibangun menggunakan topologi *mesh*. Pada topologi ini digunakan 6 *router* inti yang terdiri dari 4 *router* PE (*Provider Edge*) dan 2 *router* P (*Provider*), serta 8 *router* CE (*Customer Edge*) yang terhubung dengan sisi *client*. Perbedaan antara topologi sistem konvensional dan SDN hanya terdapat tambahan SDN *controller* pada PE di dalam topologi sistem SDN.



Gambar 7. Topologi L3VPN MPLS Konvensional dan SDN

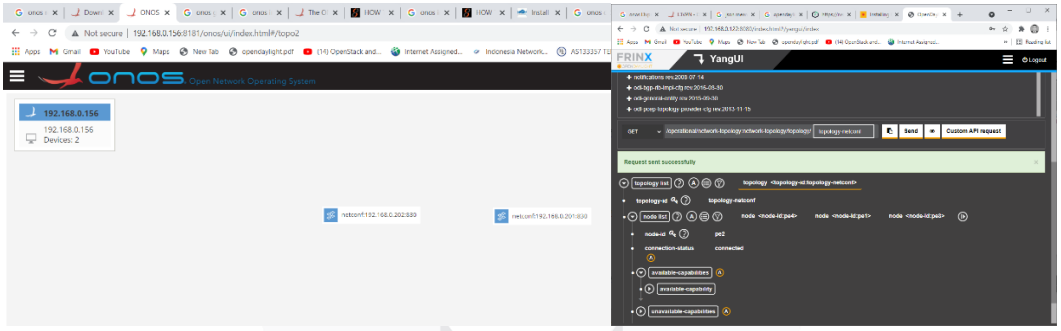
3.3. Skenario Pengujian

Skenario pengujian dimulai dengan melakukan pengujian terhadap fungsionalitas layanan L3VPN dan dilanjutkan dengan menguji performansi melalui pengukuran *setup time*. Uji fungsionalitas L3VPN MPLS memastikan bahwa setiap *client* yang berada pada daerah VPN yang sama dapat saling berkomunikasi dan memastikan setiap *client* pada daerah VPN yang berbeda tidak dapat saling berkomunikasi. Pengujian *setup time* diukur pada kedua sistem yaitu L3VPN MPLS Konvensional dan L3VPN MPLS dengan SDN. Karena pada jaringan SDN hanya mendukung pembuatan L3VPN antara PE *Router* dan CE *Router*, maka hanya saat pembuatan L3VPN saja yang diukur. Beberapa skenario yang akan dilakukan pada pengujian seperti melakukan setup 1 VPN dengan 2 PE dan 2 *Site*, 2 VPN dengan 2 PE dan 4 *Site*, 2 VPN dengan 4 PE dan 6 *Site*, serta 2 VPN dengan 4 PE dan 8 *Site* yang masih memungkinkan untuk dilakukan pengukuran sesuai dengan topologi yang telah dibuat.

4. Pengujian

4.1. Pengujian L3VPN Pada Jaringan Konvensional dan SDN

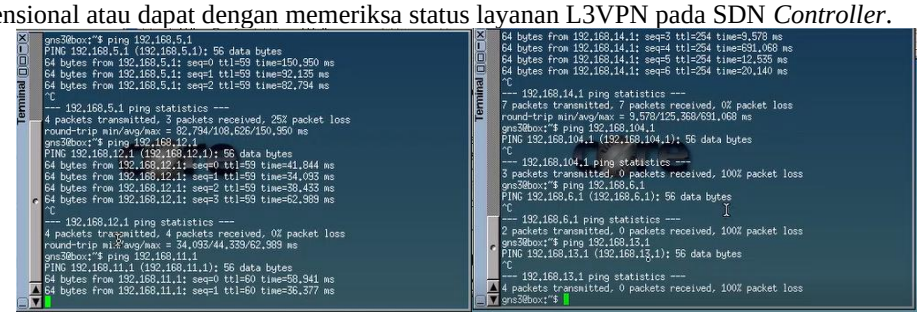
ONOS dapat menyediakan L3VPN *Module* pada saat ini, akan tetapi konfigurasi dinamis yang memungkinkan eksekusi pembuatan L3VPN masih dalam tahap pengembangan. Oleh karena itu digunakan alternatif SDN *Controller* lain yang memungkinkan pembuatan layanan L3VPN yaitu FRINX ODL. Dalam melakukan penerapan layanan L3VPN menggunakan SDN langkah-langkah yang diperlukan seperti mengaktifkan fitur-fitur L3VPN yang diperlukan pada *controller*, menghubungkan PE *router* dengan SDN *controller* melalui NETCONF, membuat layanan L3VPN melalui *controller*, membuat *Site* pada VPN untuk *customer*, dan yang terakhir melakukan *commit* pembuatan L3VPN. Penerapan L3VPN secara konvensional dilakukan dengan melakukan konfigurasi langsung pada terminal setiap *router*.



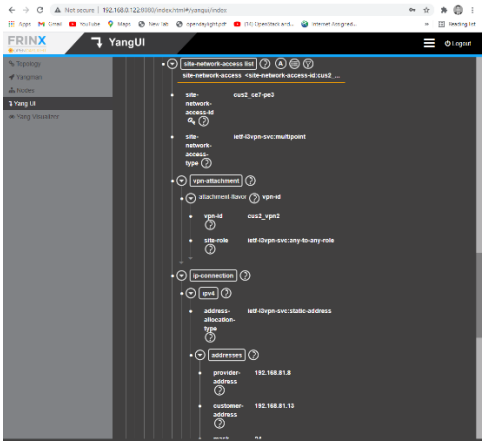
Gambar 8. Penerapan L3VPN MPLS SDN

4.2. Hasil Pengujian

Pengujian fungsionalitas L3VPN MPLS Konvensional membuktikan bahwa setiap *client* yang berada pada VPN hanya dapat berkomunikasi dengan *client* lain yang berada pada VPN yang sama. Sedangkan untuk *client* yang berada pada VPN yang berbeda tidak dapat saling berkomunikasi. Komunikasi antar *client* diuji konektivitasnya dengan cara mengirimkan paket ICMP. Pada L3VPN SDN, untuk memastikan bahwa antar *client* terhubung dalam satu VPN yang sama dapat dilakukan dengan mengirim paket ICMP untuk menguji konektivitas seperti yang telah dilakukan pada L3VPN konvensional atau dapat dengan memeriksa status layanan L3VPN pada SDN *Controller*.

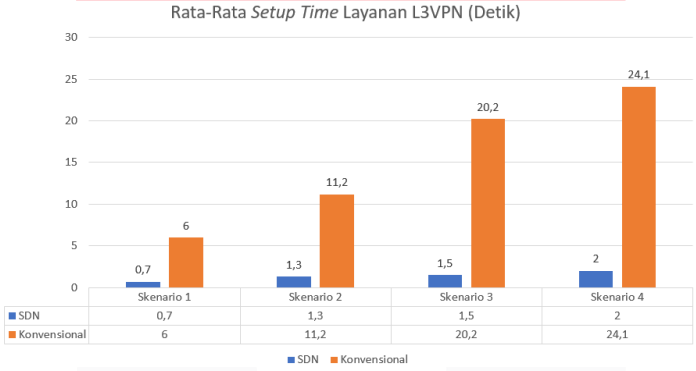


Gambar 9. Pengujian Fungsionalitas L3VPN Konvensional



Gambar 10. Pengujian Fungsionalitas L3VPN SDN

Pengujian berikutnya adalah pengujian *setup time*. *Setup time* merupakan waktu yang diperlukan untuk melakukan konfigurasi pada perangkat-perangkat jaringan hingga perangkat tersebut siap untuk memberikan layanannya. Hasil pengujian dari 4 skenario yang telah dibuat menunjukkan bahwa *setup time* pada sistem L3VPN MPLS SDN jauh lebih cepat dibandingkan dengan sistem L3VPN MPLS Konvensional.



Gambar 11. Pengujian *Setup Time* L3VPN MPLS SDN

Pada pengujian skenario 1 layanan L3VPN dengan SDN lebih cepat dibentuk dengan rata-rata *setup time* 0,7 detik. Sedangkan jika menggunakan sistem konvensional didapat rata-rata *setup time* 6 detik. Perbandingan performansi *setup time* antara MPLS L3VPN SDN dengan Konvensional pada pengujian skenario 1 adalah MPLS L3VPN SDN lebih cepat 757,14% atau 8,57 kali dalam *setup time*-nya dibandingkan Konvensional.

Pada pengujian skenario 2 layanan L3VPN dengan SDN masih lebih cepat dibentuk, akan tetapi mengalami kenaikan waktu karena bertambahnya jumlah VPN dan jumlah *site* dengan rata-rata *setup time* 1,3 detik. Sedangkan jika menggunakan sistem konvensional didapat rata-rata *setup time* yang semakin naik karena bertambahnya baris konfigurasi yaitu 11,2 detik. Perbandingan performansi *setup time* antara MPLS L3VPN SDN dengan Konvensional pada pengujian skenario 2 adalah MPLS L3VPN SDN lebih cepat 761,54% atau 8,61 kali dalam *setup time*-nya dibandingkan Konvensional.

Pada pengujian skenario 3 layanan L3VPN dengan SDN pada skenario ini meningkat tapi tidak signifikan dengan rata-rata *setup time* 1,5 detik. Sedangkan jika menggunakan sistem konvensional terlihat bahwa rata-rata *setup time* meningkat hampir dua kali lipat dari skenario sebelumnya menjadi 20,2 detik. Perbandingan performansi *setup time* antara MPLS L3VPN SDN dengan Konvensional pada pengujian skenario 3 adalah MPLS L3VPN SDN lebih cepat 1246% atau 13,46 kali dalam *setup time*-nya dibandingkan Konvensional.

Pada pengujian skenario 4 layanan L3VPN dengan SDN pada skenario ini meningkat cukup signifikan dengan rata-rata *setup time* menjadi 2 detik. Sedangkan jika menggunakan sistem konvensional terlihat bahwa rata-rata *setup time* tidak terlalu banyak bertambah dari skenario sebelumnya menjadi 24,1 detik, karena jumlah PE tetap seperti skenario sebelumnya dan hanya bertambah baris konfigurasi. Perbandingan performansi *setup time* antara MPLS L3VPN SDN

dengan Konvensional pada pengujian skenario 4 adalah MPLS L3VPN SDN lebih cepat 1105% atau 12,05 kali dalam *setup time*-nya dibandingkan Konvensional.

5. Kesimpulan dan Saran

5.1 Kesimpulan

Setelah dilakukan penelitian ini, kesimpulan yang dapat diambil pada Tugas Akhir ini adalah sebagai berikut:

1. Penggunaan L3VPN MPLS sistem konvensional maupun SDN pada pengujian berhasil memisahkan *client-client* yang berbeda VPN dan menghubungkan *client-client* yang memiliki VPN yang sama.
2. Hasil pengujian yang didapat dari beberapa skenario pengujian yang dilakukan, *setup time* pembuatan layanan L3VPN MPLS dengan SDN lebih cepat 757,14% hingga 1246 % atau 8,57 kali hingga 13,46 kali dari L3VPN MPLS Konvensional. Terbukti dengan hasil *setup time* yang didapat bahwa pembuatan layanan L3VPN dengan menggunakan SDN lebih cepat dibandingkan dengan pembuatan L3VPN Konvensional menggunakan terminal CLI.
3. Penambahan jumlah *Provider Edge* pada sistem L3VPN MPLS konvensional sangat berpengaruh terhadap *setup time* yang diperlukan. Selisih rata-rata setup time dengan 2 *Provider Edge* pada skenario 1 dan 2 adalah 5,2 detik, sedangkan selisih rata-rata *setup time* pada skenario 2 dengan 2 *Provider Edge* dan skenario 3 dengan 4 *Provider Edge* adalah 9 detik. Terdapat kenaikan selisih sebesar 73% antara skenario 2 *Provider Edge* dan 4 *Provider Edge*. Pada sistem L3VPN MPLS SDN penambahan *Provider Edge* tidak terlalu berpengaruh terhadap setup time.
4. Penambahan jumlah *Site* pada sistem L3VPN MPLS Konvensional dan L3VPN MPLS SDN tidak menambah selisih *setup time* yang diperlukan untuk membuat layanan L3VPN MPLS.

5.2 Saran

Saran penelitian yang selanjutnya dapat dilakukan terkait dengan L3VPN SDN adalah sebagai berikut:

1. Menggunakan PCEP (*Path Computation Element Communication Protocol*) dan BGP-LS (*Border Gateway Protocol – Link State*) pada perangkat *router* dan kontroler SDN untuk melakukan rekayasa jaringan dengan cara kontroler melakukan kalkulasi jalur pada jaringan dan membuat *tunnel* antara PE ke PE *router* sesuai dengan kehendak administrator jaringan.
2. Jika sudah tersedia, penelitian berikutnya dapat melakukan pembuatan layanan L3VPN pada jaringan *Openflow* sehingga dapat diukur dan dibandingkan performansi QOSnya.

REFERENSI

[1] D. B. Rawat and S. R. Reddy, “Software Defined Networking Architecture, Security and Energy Efficiency: A Survey,” *IEEE Communications Surveys and Tutorials*, vol. 19, no. 1, pp. 325–346, 2017, doi: 10.1109/COMST.2016.2618874.

[2] R. Van Der Pol, B. Gijsen, P. Zuraniewski, D. F. C. Romão, and M. Kaat, “Assessment of SDN technology for an easy-to-use VPN service,” *Future Generation Computer Systems*, vol. 56, pp. 295–302, 2016, doi: 10.1016/j.future.2015.09.010.

[3] S. Vidal, J. R. Amaro, E. Viotti, M. Giachino, and E. Grampín, “RAUflow: Building virtual private networks with MPLS and OpenFlow,” *LANCOMM 2016 - Proceedings of the 2016 ACM SIGCOMM Workshop on Fostering Latin-American Research in Data Communication Networks, Part of SIGCOMM 2016*, pp. 25–27, 2016, doi: 10.1145/2940116.2940133.

[4] F. Hu, Q. Hao, and K. Bao, “A survey on software-defined network and OpenFlow: From concept to implementation,” *IEEE Communications Surveys and Tutorials*, vol. 16, no. 4, pp. 2181–2206, 2014, doi: 10.1109/COMST.2014.2326417.

[5] Z. Latif, K. Sharif, F. Li, M. M. Karim, and Y. Wang, "A comprehensive survey of interface protocols for software defined networks," pp. 1–30, 2019.

[6] B. R. Al-Kaseem and H. S. Al-Raweshidyhamed, "SD-NFV as an Energy Efficient Approach for M2M Networks Using Cloud-Based 6LoWPAN Testbed," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1787–1797, 2017, doi: 10.1109/JIOT.2017.2704921.

[7] S. A. R. Shah, S. Bae, A. Jaikar, and S. Y. Noh, "An adaptive load monitoring solution for logically centralized SDN controller," *18th Asia-Pacific Network Operations and Management Symposium, APNOMS 2016: Management of Softwarized Infrastructure - Proceedings*, 2016, doi: 10.1109/APNOMS.2016.7737207.

[8] A. Cortes, "Simulation of Software Defined Networks with Open Network Operating System and Mininet," *International Journal of Computer Science and Information Technology*, vol. 10, no. 5, pp. 21–32, 2018, doi: 10.5121/ijcsit.2018.10503.

[9] IETF, *Network Configuration Protocol (NETCONF)*, RFC: 6241. 2011.

[10] IETF, *YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)*, RFC: 6020. 2010.

[11] Netconf Central, "Network Configuration Protocol." http://www.netconfcentral.org/netconf_docs (accessed Nov. 25, 2020).

[12] Huawei, "Configuration Guide - MPLS." https://support.huawei.com/enterprise/en/doc/EDOC1000141937/953f01ce/overview (accessed Nov. 23, 2020).

[13] Huawei, "What Is MPLS?" https://support.huawei.com/enterprise/en/doc/EDOC1100118961 (accessed Nov. 20, 2020).

[14] L. De Ghein, *MPLS Fundamentals*. Indianapolis: Cisco Press, 2006.

[15] C. Maulana Shabirin, R. Munadi, and Y. Purwanto, *ANALISIS IMPLEMENTASI ROUTING PROTOCOL AUTHENTICATION PADA JARINGAN MPLSVPN-L3VPN*. Bandung: Universitas Telkom, 2014.

[16] T. Fadil, R. M. Negara, and T. R. Gading, "ANALISIS IMPLEMENTASI LAYANAN E-LINE , E-LAN & L3VPN BERBASIS SOFTWARE DEFINED NETWORK MENGGUNAKAN NOKIA NETWORK SERVICES PLATFORM IMPLEMENTATION ANALYSYS SERVICES E-LINE , E-LAN & L3VPN BASED," *e-Proceeding of Engineering*, vol. 5, no. 3, pp. 4407–4413, 2018.

[17] L. Lu, "L3VPN." https://wiki.onosproject.org/display/ONOS/L3VPN (accessed Nov. 25, 2020).

[18] J. Moy, "RFC2328: OSPF Version 2." RFC Editor, 1998.

[19] T. G. Griffin and G. Wilfong, "An Analysis of BGP Convergence Properties," *SIGCOMM Comput. Commun. Rev.*, vol. 29, no. 4, pp. 277–288, Aug. 1999, doi: 10.1145/316194.316231.