



---

## **Analisis Performansi VLAN Pada Jaringan Software Defined Network (SDN)**

Rohmat Tulloh

Program Studi D3 Teknik Telekomunikasi, Fakultas Ilmu Terapan, Universitas Telkom  
Jalan Telekomunikasi Terusan Buah Batu, Bandung 40257, Indonesia  
Email korespondensi: rohmatht@telkomuniversity.ac.id

Dikirim 19 Oktober 2017, Direvisi 06 November 2017, Diterima 08 November 2017

---

**Abstrak –** *Software defined network (SDN)* adalah sebuah paradigma baru dalam dunia jaringan yang mampu memusatkan fungsi beberapa *control plane* pada *layer 2* maupun di *layer 3* secara terprogram, hal tersebut menyebabkan jaringan akan bersifat lebih fleksibel dan terskala. Dengan jumlah pertumbuhan pengguna internet yang semakin tinggi maka hal tersebut akan berbanding lurus terhadap kompleksitas dari jaringan internet itu sendiri. Sehingga paradigma SDN ini menjadi salah satu solusi yang muncul. Penerapan *Virtual Local Area Network (VLAN)* pada jaringan tradisional telah menjadi hal yang penting dan banyak diterapkan. Fungsi VLAN adalah untuk membatasi *broadcast* trafik dari suatu *host*, sehingga hanya dapat mengirim data kepada VLAN ID yang sama. Penelitian ini menganalisis performansi VLAN di jaringan SDN. Terjadi penurunan hampir 60% pada angka jumlah paket yang dapat terkirim (*data transfer*) dan nilai *throughput* pada sebuah VLAN ID karena terdapat pengaruh dari VLAN ID yang berbeda. Pada pengujian membandingkan VLAN dengan *non VLAN over Netwok Functions Virtualization (NFV)* didapatkan bahwa nilai *data transfer* dan *throughput* yang diperoleh pada VLAN lebih besar hampir 30%. Hasil analisis dari seluruh pengujian penambahan *traffic* terlihat bahwa kinerja VLAN pada SDN akan membebani kinerja jaringan pada VLAN yang berbeda.

**Kata kunci –** *Software Defined Network, VLAN, Virtualization.*

---

**Abstract -** Software-defined network (SDN) is a new paradigm in the networking world capable of centralizing multiple control plane functions on layer 2 as well as in layer 3 programmatically, making the network more flexible and scalable. With the growing number of Internet users, it will be directly proportional to the complexity of the Internet network itself. So this SDN paradigm becomes one of the emerging solutions. Application of Virtual Local Area Network (VLAN) on traditional networks has become an important and widely applied. The VLAN function is to restrict broadcast traffic from a host, so it can only send data to the same VLAN ID. This study analyzes the performance of VLANs in the SDN network. There is a decrease almost 60% in the number of packets that can be sent (data transfer) and the throughput value of a VLAN ID because of the influence of different VLAN IDs. In the test compare the VLAN with non-VLAN over Network Functions Virtualization (NFV) found that the value of data transfer and throughput obtained on VLAN is greater almost 30%. The analysis result from all of the traffic addition test shows that VLAN performance on SDN will burden the network performance on different VLAN.

**Keywords -** Software Defined Network, VLAN, Virtualization.

### I. PENDAHULUAN

Pada zaman yang mendahuluikan teknologi seperti saat ini, SDN (*Software defined network*) dipercaya sebagai kunci dari berkembangnya teknologi masa depan. Hal ini dikarenakan perbedaan arsitektur SDN dari arsitektur jaringan-jaringan sebelumnya. Perkembangan pada SDN ini disebabkan adanya kebutuhan dalam kebebasan pergerakan dan

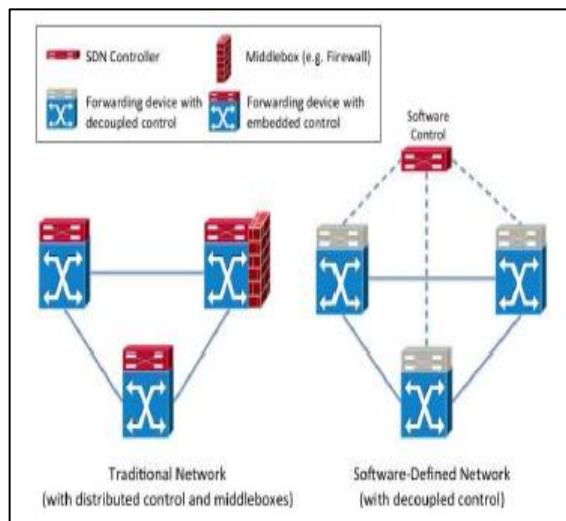
kemudahan dalam memperluas jaringan komputer yang tidak dapat dicapai dengan teknologi jaringan yang ‘tradisional’, hal ini dicapai dengan membuat manajemen jaringan dengan lebih mudah. Riset dalam perkembangan jaringan masa depan banyak dilakukan di seluruh dunia. Namun dari beberapa penelitian yang telah dilakukan, makin banyak peneliti merasa perkembangan jaringan masa depan terhambat pada keterbatasan jaringan yang ada sekarang ini. Hal inilah

yang menyebabkan adanya perubahan arsitektur pada teknologi masa depan [1].

Jaringan Konvensional yang cenderung bersifat tertutup serta terdistribusi diubah oleh paradigma baru SDN menjadi bersifat terbuka (*Open Source*), dapat diprogram dan dapat dikontrol secara terpusat. Hal ini membuat konsep SDN sangat menarik bagi para peneliti atau administrator jaringan karena mereka dapat mengatur jaringan berdasarkan kebutuhan. Selama ini pengembangan terhambat karena setiap perangkat telah diatur *protocol*, API dan standar-nya oleh *vendor*. SDN menawarkan konsep virtualisasi topologi jaringan dan memungkinkan administrator melakukan pengaturan pada *control plane* [2].

Hal ini juga membuat SDN bersifat *managable*, dimana apabila ada suatu *maintenance*, seorang admin tidak perlu untuk mengurus tiap-tiap *switch*, cukup dengan hanya mengkonfigurasi di *controller*-nya saja. Selain itu, SDN juga dapat menjanjikan *bandwidth* yang lebar, *cost-effective*, dan *manageable* [3].

*Open Networking Foundation* (ONF) adalah lembaga non-profit yang mengembangkan, membuat standar, dan membuat komersil dari SDN. Dengan adanya pemisahan antara *control plane* dan *data plane*, SDN menawarkan kontrol jaringan yang lebih baik melalui pemrograman, sehingga dapat meningkatkan konfigurasi, performansi, dan peningkatan arsitektur serta operasi jaringan [3].



Gambar 1. Perbedaan SDN dan Jaringan Tradisional [4]

Konsep SDN tersebut dapat diaplikasikan pada berbagai mekanisme jaringan komputer, salah satunya adalah pada konsep *Virtual Local Area Network* (VLAN). Teknologi VLAN membagi jaringan secara logika menjadi beberapa VLAN ID. VLAN mengijinkan banyak VLAN ID di dalam suatu jaringan. VLAN ini bertujuan untuk membatasi *broadcast traffic* hanya untuk penerima yang memiliki VLAN ID. Jaringan dikonfigurasikan secara virtual dan tidak tergantung pada lokasi perangkat secara fisik. VLAN dipilih karena mengatur jaringan berdasarkan teknik

pengklasifikasianya, yaitu melalui pengalamatan MAC, *port*, dan sebagainya yang menjadikan jaringan VLAN fleksibel. Proses pengklasifikasian disimpan ke dalam suatu tabel yang berisi pengalamatan suatu VLAN (*tagging*), dimana apabila pengalamatan berdasarkan *port* yang digunakan, maka *port tersebut* harus dapat diindikasi oleh *database* [5].

Pada penelitian sebelumnya [5] telah dilakukan simulasi *Virtual Local Area Network* (VLAN) berbasis SDN menggunakan POX Controller, namun penelitian tersebut tidak mengukur QoS dan hanya menganalisis pengaruh penambahan jumlah VLAN ID pada SDN. Kemudian pada paper [6] menggunakan VLAN sebagai metode pemulihan cepat untuk kegagalan *link* SDN. Berdasarkan mekanisme proteksi, ia menghitung jalur cadangan untuk setiap tautan, dan menyimpan rute ini dengan bantuan VLAN ID. Mereka hanya fokus untuk meminimalkan waktu yang dibutuhkan untuk *recovery link*. Pada [7] juga melakukan penelitian analisis kuantitatif aliran data berdasarkan model data yang diajukan. Keuntungan dari VLAN dan dampak dari kesalahan sistem, serta topologi jaringan, pada jaringan berbasis VLAN dievaluasi, dan disimulasikan menggunakan OPNET Modeler. Selain itu paper [8] juga telah melakukan penelitian penyebaran otonom "VLAN filtering and segmentation" di atas jaringan reguler dan jaringan SDN, yang membuktikan bahwa paradigma SDN menawarkan kepada para administrator perbaikan dalam tugas kontrol dan manajemen, dengan terjemahan bisnis yang ketat ke dalam jaringan produksi. Berdasarkan paper di atas menunjukkan bahwa implementasi VLAN pada SDN dibutuhkan untuk menambah performa jaringan, namun belum ada yang menganalisis saat jumlah VLAN bertambah apakah akan menurunkan performa VLAN lainnya di dalam jaringan SDN. Hal ini yang dianalisis lebih lanjut di dalam paper ini, terutama pengaruhnya terhadap QoS.

Pada penelitian ini, diterapkan *Network Functions Virtualisation (NFV)* yang merupakan konsep baru untuk mendesain, mengembangkan, dan mengelola layanan jaringan dengan memvirtualisasi fungsi arsitektur jaringan sepenuhnya [9].

Dalam NFV terdapat tiga komponen utama [10], yaitu:

- a) *Network Functions Virtualisation Infrastructure (NFVI)*, menyediakan virtual komponen hardware dan software untuk mendukung VNF.
- b) *Virtualised Network Function (VNF)*, bentuk *software* implementasi yang digunakan pada NFVI.
- c) *Management and Orchestration (NFV M&O)*, menjalankan tugas *orchestration* dan *lifecycle management* dari *physical* dan *software* yang mendukung infrastruktur virtualisasi dan VNF.

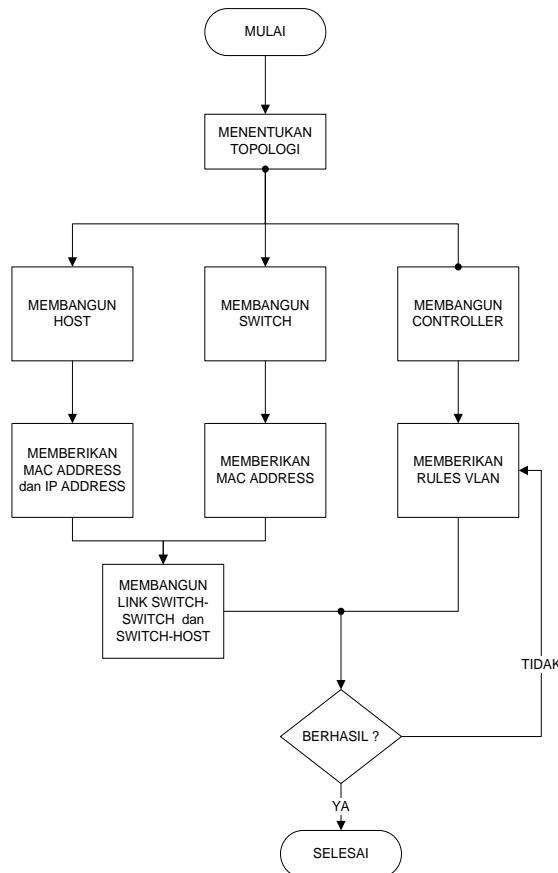
*Hypervisor* atau yang disebut juga *Virtual Machine Monitor* adalah sebuah *software* komputer, *firmware* ataupun *hardware* yang dapat menciptakan dan

menjalankan *virtual machine* di atasnya. Pada *hypervisor*, istilah *host machine* ditujukan kepada *hardware* yang menjalankan *hypervisor* tersebut. Sedangkan *guest machine* ditujukan untuk *virtual machines* yang berjalan diatas *host machine* itu sendiri [11].

## II. METODE PENELITIAN

Tujuan utama penelitian ini adalah menganalisis performansi konsep jaringan VLAN berbasis SDN berdasarkan hasil *transfer rate* dan *throughput* yang diperoleh dengan mengubah *traffic* pada jaringan VLAN tersebut, kemudian dibandingkan dengan performa jaringan *non VLAN* yang dibangun berbasis NFV.

Proses perancangan dan pembangunan sistem dengan menggunakan 1 buah PC yang bertindak sebagai *host* dan masing-masing *host* dibangun *hypervisor VirtualBox*. Untuk memudahkan pemahaman dalam proses perancangan, maka perlu dibuat diagram alir seperti pada Gambar 2.

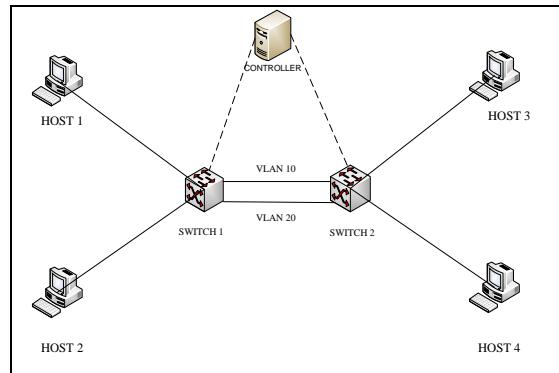


Gambar 2. Proses Pembangunan Sistem

### A. Topologi

Topologi yang digunakan adalah dua topologi *ring* yang terhubung, seperti pada Gambar 1. Topologi terdiri dari dua *switch* dan empat *host* dimana ditunjukkan pada Gambar 3. Pemilihan topologi didasarkan pada jumlah *loop* dan jumlah *switch* yang bersesuaian dengan kriteria pengujian. Keempat *host* dijalankan di dalam mininet dan terdapat dua *virtual*

*switch* yang dihubungkan kepada *controller*, lalu diberi jalur VLAN pada topologi tersebut yang menghubungkan semua *host* melalui *switch*.



Gambar 3. Topologi yang Digunakan

### B. Simulasi

#### a) Skenario Pengujian

Untuk pengujian, disiapkan tiga pengujian berbeda. Parameter *data transfer* dan *throughput* akan diamati pada semua skenario. Data yang dikirimkan pada H1 adalah layanan data UDP dan TCP dengan distribusi Weibull. Distribusi Weibull mirip dengan distribusi normal. Skenario yang dilakukan pada proses simulasi ini yaitu,

- Pengujian pertama, dilakukan pengamatan terhadap panjang paket karena penambahan paket *header* 802.1Q. Paket yang dilewatkan adalah TCP, UDP dan ICMP.
- Pengujian kedua, dilakukan pengamatan terhadap pengaruh dari *setting* dua VLAN yang berbeda yaitu VLAN 10 dan 20, lalu ukur parameter *data transfer* dan *throughput*. Skenario pengujian dilakukan selama 60 detik dengan memberikan *traffic* sebesar 10 sampai 100 Mb pada VLAN 20 sedangkan pada VLAN 10 *bandwidth* konstan yaitu sebesar 50 Mb.
- Pengujian ketiga, dilakukan pengamatan terhadap jaringan VLAN dengan *non VLAN* dengan skenario yang sama seperti pengujian dua, lalu diukur parameter *data transfer* dan *throughput*.

#### b) Spesifikasi Hardware

Tabel 1 menjabarkan spesifikasi perangkat yang digunakan dalam proses simulasi.

Tabel 1. Spesifikasi Perangkat

Hardware	Lenovo T410s Specification
Processor	IntelCore i7
RAM	6GB DDR3-1066
Hard Drive	128GB SSD

Perangkat lunak yang dipakai dalam simulasi ini adalah,

- Dua *Oracle Virtual Machine* yang digunakan sebagai control plane dan data plane.
- Iperf untuk membangkitkan *traffic*.
- Wireshark*, digunakan untuk melihat data trafik *overhead*.

*Mininet* sebagai *network emulator* yang menciptakan *virtual host, switch, controller* dan *link*. *Mininet host* menjalankan standar perangkat lunak jaringan Linux, dan *switch* yang mendukung OpenFlow untuk *custom routing* yang sangat fleksibel dan SDN.

### III. HASIL DAN PEMBAHASAN

Bagian berikut menjelaskan hasil yang diperoleh dengan mensimulasikan tiga skenario di lingkungan *Mininet*.

#### A. Pengujian Pertama

Pengujian pertama dilakukan untuk melihat penambahan *header* paket VLAN pada paket yang dikirim. Topologi yang digunakan adalah topologi linear seperti Gambar 3 yang terhubung pada 2 *switch*.

Tabel 2. Hasil Pengamatan Penambahan Paket

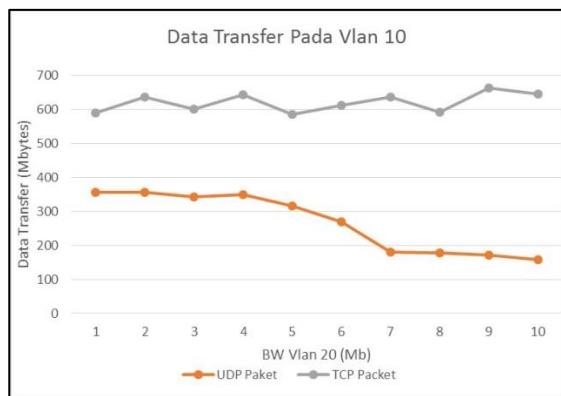
Paket	Frame Length	Frame Length menggunakan VLAN
ICMP	98 Bytes	102 Bytes
UDP	1512 Bytes	1516 Bytes
TCP	14546 Bytes	14550 Bytes

Pada Tabel 2 menunjukkan adanya penambahan *header* VLAN sebesar 4 bytes dari panjang *frame* yang sebenarnya. Percobaan dilakukan dengan melewatkkan jenis *traffic* yang berbeda untuk kemudian dilakukan pengamatan terhadap panjang paket karena penambahan paket *header* 802.1Q. Pada percobaan paket yang pertama, *ICMP Packet* dilewatkkan dan di *capture* melalui dua *interface* yang berbeda, yaitu *interface* pada *sender* secara langsung dan *interface* pada *switch* yang menjadi *trunk VLAN*. Hal serupa dilakukan pada paket UDP dan TCP yang dilewatkkan dan mendapatkan hasil yang sama yaitu penambahan paket sebesar 4 bytes.

#### B. Pengujian Kedua

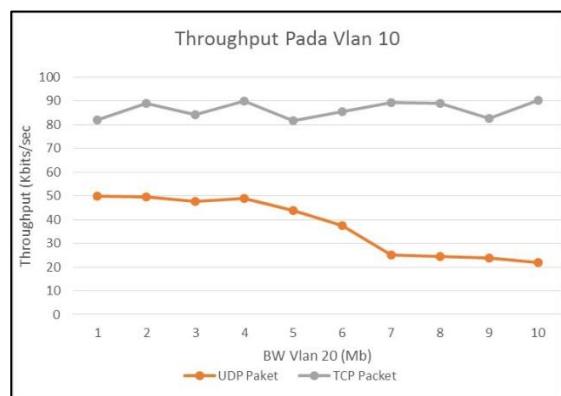
Pada bagian ini, dilakukan analisis terhadap pengaruh dari *setting* dua VLAN yang berbeda. Skenario pengujian dilakukan selama 60 detik dengan membangkitkan *traffic* sebesar 10 sampai dengan 100 Mb pada VLAN 20 sedangkan pada VLAN 10 *bandwidth* konstan yaitu sebesar 50 Mb. Tujuan dari perubahan skenario tersebut adalah untuk melihat apakah terjadi pengaruh dari VLAN yang lain. Berdasarkan Gambar 4 terjadi penurunan angka jumlah paket UDP yang dapat terkirim (*transfer rate*) pada VLAN 10, hal ini membuktikan bahwa terdapat pengaruh dari VLAN ID 20. Kondisi ini juga dibuktikan pada hasil *throughput* paket UDP di Gambar

5 yang juga mengalami penurunan sejalan dengan meningkatnya *traffic* pada VLAN 20.



Gambar 4. Grafik Pengaruh Nilai Data Transfer VLAN ID Terhadap VLAN ID Lain

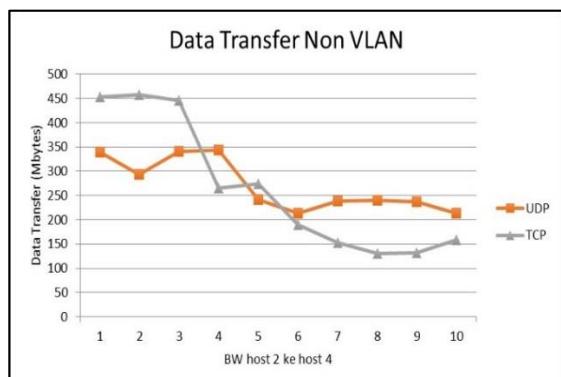
Sedangkan pada Gambar 4 dan Gambar 5 untuk skenario paket TCP sebagai objek pengamatan, didapatkan *transfer rate* dan *throughput* yang tidak terlalu signifikan dikarenakan pada protokol TCP terdapat *retransmit packet* apabila paket yang dikirim tidak sampai ke penerima.



Gambar 5. Grafik Pengaruh Nilai Throughput VLAN ID Terhadap VLAN ID Lain

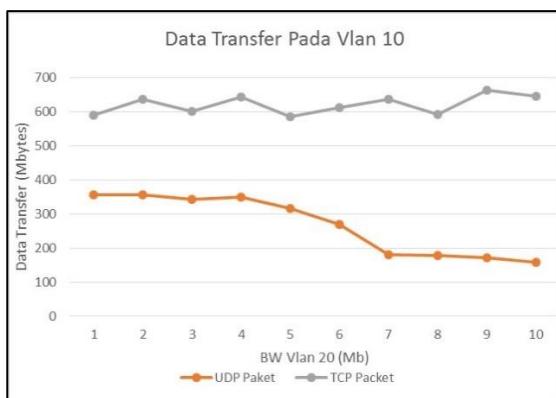
#### C. Pengujian Ketiga

Pengujian kali ini dilakukan untuk membandingkan *platform SDN* yang menggunakan VLAN dan tanpa VLAN. Skenario menggunakan L2\_learning pada *pox-controller* sebagai pembanding.



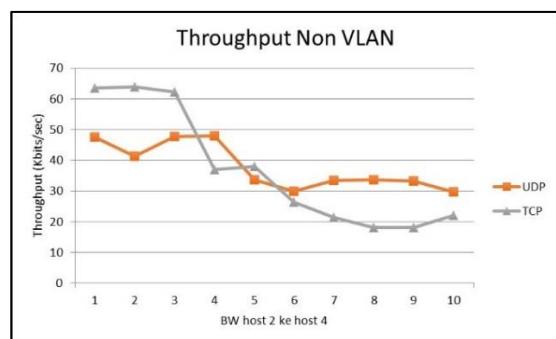
Gambar 6. Grafik Data Transfer Pada Non VLAN

Pada Gambar 6 dapat dilihat bahwa nilai *data transfer* paket TCP dan UDP pada jaringan SDN tanpa VLAN tidak stabil. Khususnya untuk paket TCP yang terus menurun seiring bertambahnya *traffic*. Hal ini tentu sangat tidak mendukung untuk karakteristik paket TCP yang *reliable* dan *loss intolerant*.



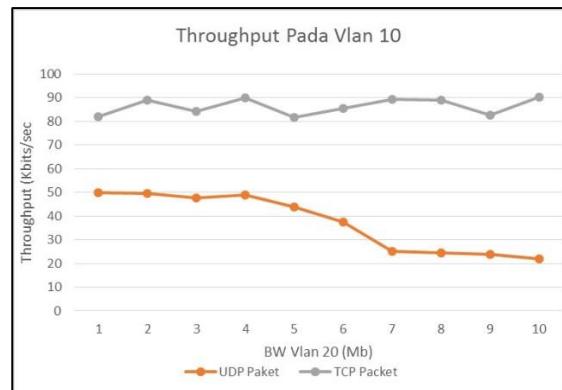
Gambar 7. Grafik *Data Transfer* Dengan Menggunakan VLAN

Pada Gambar 7 hasil yang didapatkan jauh berbeda dimana paket TCP relatif stabil dan besar data transfer juga meningkat, namun untuk paket UDP tetap mengalami penurunan.



Gambar 8. Grafik Data Nilai *Throughput* Pada Non VLAN

Pada Gambar 8 dan Gambar 9 dapat dilihat bahwa jaringan dengan menggunakan VLAN memiliki nilai *throughput* secara keseluruhan lebih besar daripada non VLAN. Hal ini dikarenakan terjadinya penambahan *header* paket 802.1Q sebesar 4 bytes pada masing-masing *sequencial* paket yang dikirim, sehingga jumlah paket yang dapat terkirim secara keseluruhan akan menjadi lebih besar. Nilai *throughput* pada pengiriman paket TCP maupun UDP non VLAN mengalami penurunan seiring dengan besarnya pembebangan *traffic* yang diberikan. Namun nilai *throughput* pada pengiriman paket TCP pada jaringan dengan menggunakan VLAN memiliki nilai konstan secara keseluruhan karena pada paket TCP, paket akan dikirimkan ulang apabila terjadi kesalahan, sehingga tidak adanya *packet loss* yang terjadi, namun pada penelitian kali ini nilai *throughput* pada pengiriman paket TCP tersebut masih bernilai fluktuatif dikarenakan faktor lain seperti perangkat, kesalahan, dan sebagainya.



Gambar 9. Grafik Nilai *Throughput* Dengan Menggunakan VLAN

#### IV. PENUTUP

##### A. Kesimpulan

Pada pengujian VLAN, *ICMP Packet* dilewatkan dan *di-capture* melalui dua *interface* yang berbeda, yaitu *interface* pada *sender* secara langsung dan *interface* pada *switch* yang menjadi *trunk vlan*. Hal serupa dilakukan pada paket *UDP* dan *TCP* yang dilewatkan dan mendapatkan hasil yang sama yaitu penambahan paket sebesar 4 bytes. Adanya *traffic* pada suatu VLAN ID dapat mempengaruhi performansi VLAN ID yang lainnya. Hal tersebut dapat dibuktikan dengan terjadinya penurunan angka jumlah paket yang dapat terkirim (*data transfer*) dan nilai *throughput* pada VLAN 10, karena terdapat pengaruh dari VLAN ID 20. Dari 50 Mb data UDP dan TCP yang dikirimkan pada VLAN 10 terjadi penurunan *throughput* mencapai 60% yang menunjukkan bahwa ada pengaruh oleh VLAN 20. Sedangkan pada skenario yang menggunakan TCP sebagai objek pengamatan, didapatkan *data transfer* dan *throughput* yang cukup stabil dikarenakan pada protokol TCP terdapat *retransmit packet* apabila paket yang dikirim tidak sampai ke penerima. Pada pengujian ketiga, nilai *throughput* dan *data transfer* yang diperoleh dengan menggunakan VLAN menghasilkan nilai yang lebih besar daripada non VLAN seiring dengan adanya pemberian *traffic*. Hal tersebut dikarenakan terjadinya penambahan *header* paket 802.1Q sebesar 4 bytes pada masing-masing *sequencial* paket yang dikirim, sehingga jumlah paket yang dapat terkirim secara keseluruhan akan menjadi lebih besar. Pada skenario non VLAN, terjadi penurunan sampai 43% untuk paket UDP dan 67% untuk paket TCP.

##### B. Saran

Skenario pengujian untuk penelitian selanjutnya dapat ditambahkan untuk dapat mengetahui lebih lanjut karakteristik VLAN pada jaringan SDN. Dapat digunakan *controller* lain selain POX pada penelitian selanjutnya untuk dapat mengetahui kinerja dan

pengaruh dari jenis *controller* yang berbeda pada VLAN di jaringan SDN. Dapat dilakukan penelitian dengan topologi yang berbeda, misalnya penambahan jumlah *switch* maupun VLAN ID agar dapat mengetahui pengaruhnya pada performansi jaringan tersebut.

#### DAFTAR PUSTAKA

- [1] P. K. I. Helebrandt, "Novel SDN Multi-domain Architecture," *IEEE International Conference on Emerging eLearning Technologies and Applications (ICETA)*, vol. 12th, pp. 139-143, 2014.
- [2] P. Göransson and C. Black, "Software defined networks A Comprehensive Approach", 1st edition, Morgan Kaufmann Publishers Inc, USA, 2014.
- [3] Y. Guo, Z. Wang, X. Yin, X. Shi, J. Wu, "Traffic Engineering in SDN/OSPF Hybrid Network", IEEE 22nd International Conference on Network Protocols (ICNP), 2014.
- [4] X. Wei, Y. Wen, C.H. Foh, D. Niyato, H. Xie, "A Survey on Software-Defined Networking", IEEE Comm Surveys & Tutorial, vol.7, 1<sup>st</sup> Quarter, 2015.
- [5] M. Caria, and A. Jukan, "Link Capacity Planning for Fault Tolerant Operation in Hybrid SDN/OSPF Networks", IEEE Global Communications Conference (GLOBECOM), 2016.
- [6] TULLOH, Rohmat; NEGARA, Ridha Muldina; HIDAYAT, Arif Nur. Simulasi Virtual Local Area Network (VLAN) Berbasis Software Defined Network (SDN) Menggunakan POX Controller. *JURNAL INFOTEL*, [S.I.], v. 7, n. 2, p. 129-136, nov. 2015. ISSN 2460-0997.
- [7] J. Chen, J. Chen, J. Ling and W. Zhang, "Failure Recovery Using Vlan-tag in SDN: High Speed with Low Memory Requirement", IEEE 35th International Performance Computing and Communications Conference (IPCCC), 2016.
- [8] Z. Zhang, X. Huang, B. Keune, Y. Cao, Senior and Y. Li, "Modeling and Simulation of Data Flow for VLAN-Based Communication in Substations", *IEEE SYSTEMS JOURNAL*, 2015.
- [9] M. B. Lehocine dan M. Batouche, "Flexibility of managing VLAN filtering and segmentation in SDN networks", International Symposium on Networks, Computers and Communications (ISNCC), 2017.
- [10] Chiosi, M., et al.: Network Functions Virtualisation – Introductory White Paper, SDN and OpenFlow World Congress, Darmstadt, Germany, October 22-24, 2012.
- [11] K. Oberle, D. Cherubini, dan T. Cucinotta, "End-to-End Service Quality for Cloud Applications", Springer International Publishing Switzerland 2013.