Volume 6 Nomor 2 Juli 2024

JJEEE

e-ISSN : 2715-0887
p-ISSN : 2654-7813

Jambura Journal of Electrical and Electronics Engineering

Analisis dan Desain VXLAN untuk Interkoneksi Lokasi yang Berbeda di Universitas Khairun

VXLAN Analysis and Design for Interconnecting Different Locations at Khairun University

Saiful Do. Abdullah*
Prodi Informatika
Universitas Khairun
Ternate, Indonesia
saiful.abdullah@unkhair.ac.id*

Salkin Lutfi
Prodi Informatika
Universitas Khairun
Ternate, Indonesia
salkin.lutfi@unkhair.ac.id

Achmad Fuad
Prodi Informatika
Universitas Khairun
Ternate, Indonesia
achmad.fuad@unkhair.ac.id

Alan Wahyudin Nur
Prodi Informatika
Universitas Khairun
Ternate, Indonesia
alanwahyudinnur.14@gmail.com

Adelina Ibrahim
Prodi Informatika
Universitas Muhammadiyah
Ternate, Indonesia
adelinaibrahim07@gmail.com

Diterima : Mei 2024
Disetujui : Juli 2024
Dipublikasi : Juli 2024

Abstrak*— Universitas Khairun saat ini terbagi menjadi 4 kampus dengan lokasi geografis yang berbeda. Jarak antar lokasi tersebut sangat jauh, hal ini mengakibatkan setiap lokasi memiliki konfigurasi jaringan yang tidak terpusat. Penelitian ini bertujuan untuk menghubungkan jaringan pada lokasi yang berbeda secara geografis di Universitas Khairun antara Kampus Gambesi dan Kampus Jati agar terhubung menggunakan satu segmentasi IP yang terpusat. Metode penelitian ini terdiri dari tahap studi literatur, tahap perancangan topologi jaringan, tahap simulasi jaringan, tahap analisis simulasi jaringan, dan tahap analisis data. Berfokus pada VXLAN untuk menjawab tantangan bagaimana menghubungkan dua lokasi yang berbeda antara Kampus Gambesi dan Kampus Jati agar terhubung dalam satu lokasi. Dengan melakukan analisa dan perancangan melalui GNS3 dengan bantuan virtualisasi VMWare, penerapan VXLAN dapat dilakukan pada perangkat mikrotik. Pengujian ini menggunakan *ping, traceroute, packet capture,* serta *throughput.* Hasil dari penelitian ini menunjukkan bahwa VXLAN sendiri menerapkan beberapa protocol yang berjalan di layer 2 jaringan, salah satu nya yaitu Cisco Discovery Protocol (CDP). Serta *throughput* menunjukkan dengan *buffer size* 256 KB memiliki transfer data 1.5 MB dan *Bandwidth* 1.26 Mbs, *buffer size* 512 KB memiliki transfer data 2 MB dan *Bandwidth* 1.68 Mbs, serta dengan *buffer size* 1024 KB memiliki transfer data 2.5 MB dan *Bandwidth* 2.1 Mbps. Dengan kata lain VXLAN berhasil menghubungkan jaringan komputer pada lokasi yang berbeda dengan satu *subnet* IP yang sama. Walaupun tidak secara langsung terhubung ke internet namun pengiriman data antara *client* di dua lokasi yang berbeda secara geografis sukses dilakukan.

***Kata Kunci*—VXLAN; GNS3; Mikrotik; VMWare; Virtualisasi**

Abstract*— Khairun University is currently divided into 4 campuses with different geographical locations. The distance between these locations is very far, this results in each location having a network configuration that is not centralised. This research aims to connect networks in geographically different locations at Khairun University between Gambesi Campus and Jati Campus to be connected using one centralised IP segmentation. This research method consists of a literature study stage, a network topology design stage, a network simulation stage, a network simulation analysis stage, and a data analysis stage. Focusing on VXLAN to answer the challenge of how to connect two different locations between Gambesi campus and Jati campus to be connected in one location. By analyzing and designing through GNS3 with the help of VMWare virtualisation, VXLAN implementation can be done on proxy devices. This test uses ping, traceroute, packet capture, and throughput. The results of this study show that VXLAN itself implements several protocols that run at Layer 2 of the network, one of which is the Cisco Discovery Protocol (CDP). And throughput shows with a buffer size of 256 KB has a data transfer of 1.5 MB and a bandwidth of 1.26 Mbs, a buffer size of 512 KB has a data transfer of 2 MB and a bandwidth of 1.68 Mbs, and with a buffer size of 1024 KB has a data transfer of 2.5 MB and a bandwidth of 2.1 Mbps. In other words, VXLAN successfully connects computer networks in different locations with the same IP subnet. Although not directly connected to the internet, data transmission between clients in two geographically different locations was successful.

***Keywords*—VXLAN; GNS3; Mikrotik; VMWare; Virtualization**

I. PENDAHULUAN

Perkembangan teknologi saat ini menjadikan masalah keamanan, kemudahan dan kecepatan transfer (pertukaran

data) sebagai salah satu aspek penting dalam sebuah jaringan komunikasi di perusahaan berskala menengah hingga besar. Jaringan komputer merupakan solusi yang digunakan oleh perusahaan untuk mempercepat dan mempermudah arus informasi dalam Perusahaan[1]. Kemajuan jaringan komputer yang pesat saat ini mengharuskan penerapan protokol komunikasi data yang efisien. Dalam komunikasi data, sangat penting untuk memastikan bahwa data yang ditransmisikan mencapai tujuan yang diinginkan dengan cepat [2].

Universitas Khairun Ternate adalah salah satu perguruan tinggi negeri di Kota Ternate, Maluku Utara, Indonesia. Universitas Khairun memiliki 8 fakultas dan 32 program studi dengan 582 dosen tetap [3]. Universitas Khairun saat ini terbagi menjadi 4 kampus dengan lokasi geografis yang berbeda. Jarak antar lokasi tersebut sangat jauh, hal ini mengakibatkan setiap lokasi memiliki konfigurasi jaringan yang tidak terpusat. Sehingga, hal ini memunculkan tindakan analisis dan perancangan jaringan baru untuk masing-masing kampus agar dapat memiliki jaringan yang terpusat walaupun secara geografis berbeda.

Virtual Extensible LAN (VXLAN) telah menjadi teknologi yang signifikan dalam mengelola konfigurasi jaringan yang rumit, khususnya dalam konfigurasi jaringan pada Data Center dan Cloud Computing. Kapasitas VXLAN untuk memfasilitasi peningkatan fleksibilitas dan skalabilitas sangat penting[4]. VXLAN berfungsi sebagai mekanisme *overlay* Layer 2 yang diimplementasikan pada jaringan inti Layer 3[4]. Pada penelitian sebelumnya dijelaskan VXLAN seperti cara khusus untuk menciptakan jaringan terpisah bagi kelompok pengguna internet yang berbeda. Ini membantu menjaga segala sesuatu teratur dan aman dalam sistem komputer besar yang digunakan bersama oleh banyak orang[5].

Penelitian lainnya menunjukkan bahwa VXLAN, protokol virtualisasi jaringan yang tangguh, secara efektif menyelesaikan masalah yang terkait dengan administrasi segmen jaringan berskala besar [4]. Penelitian ini berfokus pada peningkatan infrastruktur jaringan dengan menggabungkan teknologi VXLAN, operasi sirkuit yang ditulis dengan Python, dan konfigurasi *Network Operating System* (NOS) yang digerakkan oleh Ansible, serta memanfaatkan GitHub untuk pencadangan konfigurasi yang aman [4]. Penerapan otomatisasi VXLAN, Python, dan Ansible, bersama dengan pemanfaatan GitHub untuk manajemen konfigurasi, merupakan perkembangan yang signifikan dalam efektivitas operasional, yang menyoroti peran penting mereka dalam peningkatan dan perlindungan infrastruktur jaringan terkini [4].

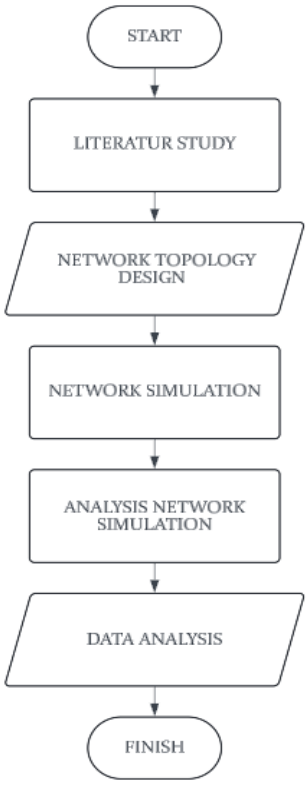
Penelitian sebelumnya menjelaskan bahwa *Virtual Extensible Local Area Network* (VXLAN) adalah salah satu metode yang paling populer untuk mencapai jaringan Cloud Computing [6]. Ini adalah bagian dari skema jaringan dengan overlay Layer 2 di atas Layer 3. Penelitian ini menggunakan Mininet untuk mensimulasikan arsitektur VXLAN berbasis SDN dan menunjukkan hasil penyeimbangan beban yang sukses[6]. Intinya, rancangan yang diusulkan ini memiliki potensi untuk menjadi model untuk jaringan Cloud Computing yang akan datang.

Dengan kata lain, teknologi *overlay* Layer 2 pada Layer 3 pada VXLAN menyediakan cara untuk menghubungkan jaringan secara virtual tanpa dibatasi oleh batasan geografis atau fisik. Selain itu, teknologi ini secara luas diterapkan pada jaringan Cloud Computing. Dengan demikian, VXLAN menawarkan solusi yang tepat untuk masalah konektivitas antar jaringan di lokasi yang berbeda. Perbedaan dari penelitian sebelumnya dengan penelitian yang dilakukan terletak pada objek dan metode yang dipakai. Pada penelitian ini menggunakan metode virtualiasi dengan bantuan software GNS3 dengan VMWARE. Objek yang disimulasikan adalah Universitas Khairun dengan bantuan RouterOS Mikrotik untuk mendukung konfigurasi VXLAN secara simulasi.

Analisis dan Perancangan Virtual Extensible Local Area Network (VXLAN) untuk Interkoneksi Lokasi yang Berbeda di Universitas Khairun bertujuan untuk menciptakan lingkungan jaringan dalam satu koneksi meskipun berada di lokasi yang berbeda. Selain itu, evaluasi kinerja VXLAN saat mengatasi hambatan geografis akan menjadi fokus penelitian, memberikan wawasan yang berguna bagi para pengambil keputusan dalam hal efisiensi dan keamanan. penelitian tentang Analisis dan Perancangan Virtual Extensible Local Area Network (VXLAN) untuk Interkoneksi Lokasi yang Berbeda di Universitas Khairun bertujuan untuk menciptakan lingkungan jaringan dalam satu koneksi meskipun dalam lokasi yang berbeda. Selain itu, evaluasi kinerja VXLAN saat mengatasi hambatan geografis akan menjadi fokus penelitian, memberikan wawasan yang berguna bagi para pengambil keputusan dalam hal efisiensi dan keamanan.

II. METODE

Penelitian ini dimulai dengan melewati beberapa tahapan seperti studi literatur, perancangan topologi jaringan, simulasi jaringan, analisis simulasi jaringan, dan data hasil analisis. Perhatikan Gambar 1 berikut ini.



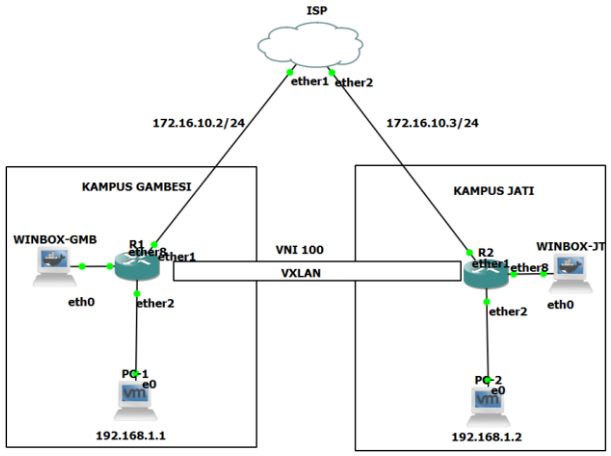
Gambar 1. Flowchart Penelitian

A. *Tahapan Literatur Study*

Pada tahap ini, Peneliti mempelajari berbagai istilah dan alat serta bahan yang akan digunakan dalam penelitian ini. Seperti pengertian VXLAN, GNS3, VMWARE, Mikrotik, dan lain-lain. Peneliti menggunakan situs seperti Google Scholar dan Mendeley yang dapat mempermudah dalam melakukan studi literatur.

B. *Tahapan Network Topology Design*

Pada tahap ini dilakukan perancangan dan desain topologi jaringan yang akan diimplementasikan sesuai dengan rancangan. Perancangan topologi jaringan melalui pemanfaatan aplikasi GNS3. Graphical Network Simulator 3 (GNS3) adalah sebuah program perangkat lunak berbasis antarmuka pengguna yang dirancang untuk mensimulasikan jaringan komputer, mirip dengan Cisco Packet Tracer. Khususnya, GNS3 memungkinkan simulasi jaringan yang rumit dengan memanfaatkan sistem operasi asli dari penyedia peralatan jaringan seperti Cisco dan Juniper. Sehingga kita berada dalam kondisi yang lebih nyata dalam mengkonfigurasi router secara langsung dibandingkan dengan Cisco Packet Tracer [7]. Untuk desain topologi jaringan, lihat Gambar 2.



Gambar 2. Topology Design

C. *Tahapan Network Simulation*

Pada tahap ini dilakukan simulasi jaringan dengan mengimplementasikan VXLAN berdasarkan rancangan topologi jaringan sebelumnya dengan bantuan aplikasi VMWARE dan GNS3. Virtual Extensible LAN (VXLAN) adalah sebuah teknologi virtualisasi jaringan yang memungkinkan terciptanya jaringan Layer 2 yang tervirtualisasi di atas jaringan Layer 3 [5]. VXLAN mencapai hal ini dengan mengenkapsulasi *frame* Ethernet ke dalam datagram UDP, yang memungkinkan perluasan jaringan Layer 2 melalui infrastruktur Layer 3 yang sudah ada [8]. VMWare Workstation memiliki arsitektur *host* untuk virtualisasi I/O, yang memungkinkannya untuk hidup berdampingan dengan sistem operasi *host* yang sudah ada sebelumnya [9]. Virtualisasi adalah teknologi yang memungkinkan kita untuk tidak melihat spesifikasi nyata di dalamnya seperti sistem operasi, penyimpanan data, memori, dan bahkan bandwidth [10].

D. *Tahapan Network Simluation Analysis*

Pada tahap ini dilakukan analisa terhadap simulasi jaringan, analisa dilakukan dengan menggunakan perintah *ping* antar *client* dan *traceroute* melalui *client* yang terintegrasi *system* operasi Ubuntu dan *packet capture* dengan Wireshark. *Ping* dan *traceroute* merupakan perintah yang terkenal untuk mengukur waktu respon dalam bidang jaringan komputer [11]. Perintah *ping* digunakan untuk memeriksa hasil protokol *routing* jaringan [12]. Perintah *traceroute* sering digunakan untuk membantu mendiagnosa ketika pengguna mengalami masalah dengan aplikasi atau layanan Internet [13]. Hal ini menunjukkan bahwa perintah *ping* dan *traceroute* digunakan secara luas pada pengujian dan pemeliharaan jaringan komputer.

Packet capture adalah metode standar yang digunakan selama analisis jaringan [14], *packet capture* adalah teknik penting dalam analisis dan keamanan jaringan. Teknik ini melibatkan penangkapan seluruh aliran paket, termasuk paket jaringan yang masuk dan keluar selama periode waktu tertentu [15]. Wireshark adalah penganalisis protokol jaringan serbaguna yang banyak digunakan untuk analisis lalu lintas jaringan, deteksi intrusi, forensik jaringan, dan penilaian keamanan [16], [17], [18].

E. *Tahapan Data Analysis*

Pada tahap ini, data dari hasil simulasi menggunakan *ping*, *traceroute* dan *packet capture* dikumpulkan dan dibuat kesimpulan. Sehingga mendapatkan hasil yang sesuai dengan tujuan penelitian.

III. HASIL DAN PEMBAHASAN

A. *Pengujian Ping*

Pengujian *ping* dilakukan dengan menggunakan perintah *ping* antar *client* ke ISP dan *client* ke *client*. Pengujian ini bertujuan untuk mengetahui terhubung atau tidaknya suatu koneksi.

```
jati@gambesi:~$ ping 172.16.10.1
PING 172.16.10.1 (172.16.10.1) 56(84) bytes of data.
From 192.168.1.1 icmp_seq=1 Destination Host Unreachable
From 192.168.1.1 icmp_seq=2 Destination Host Unreachable
From 192.168.1.1 icmp_seq=3 Destination Host Unreachable
From 192.168.1.1 icmp_seq=4 Destination Host Unreachable
From 192.168.1.1 icmp_seq=5 Destination Host Unreachable
From 192.168.1.1 icmp_seq=6 Destination Host Unreachable
From 192.168.1.1 icmp_seq=7 Destination Host Unreachable
From 192.168.1.1 icmp_seq=8 Destination Host Unreachable
From 192.168.1.1 icmp_seq=9 Destination Host Unreachable
^C
--- 172.16.10.1 ping statistics ---
11 packets transmitted, 0 received, +9 errors, 100% packet loss, time 10244ms
pipe 4
jati@gambesi:~$
```

Gambar 3. Pengujian ping *client* Gambesi ke ISP

Dari gambar 3 menunjukkan saat melakukan *ping* ke ISP terdapat pesan *destination host unreachable* yang berarti bahwa koneksi dari *client* Gambesi ke ISP tidak terhubung, dengan data dari 11 *packet* yang di transmisi semuanya mengalami *packet loss*.

```
jati@jati:~$ ping 172.16.10.1
PING 172.16.10.1 (172.16.10.1) 56(84) bytes of data.
^C
--- 172.16.10.1 ping statistics ---
8 packets transmitted, 0 received, 100% packet loss, time 7151ms

jati@jati:~$ _
```

Gambar 4.Pengujian ping *client* Jati ke ISP

Dari gambar 4 hal yang sama juga terjadi pada *client* Jati saat melakukan *ping* ke ISP. Dengan data dari 8 packet yang di transmisis, semuanya mengalami *packet loss*.

```
jati@gambesi:~$ ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=64 time=8.03 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=64 time=11.9 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=64 time=20.6 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=64 time=9.55 ms
64 bytes from 192.168.1.2: icmp_seq=5 ttl=64 time=10.1 ms
64 bytes from 192.168.1.2: icmp_seq=6 ttl=64 time=9.72 ms
64 bytes from 192.168.1.2: icmp_seq=7 ttl=64 time=6.97 ms
64 bytes from 192.168.1.2: icmp_seq=8 ttl=64 time=15.5 ms
64 bytes from 192.168.1.2: icmp_seq=9 ttl=64 time=8.32 ms
64 bytes from 192.168.1.2: icmp_seq=10 ttl=64 time=8.97 ms
^C
--- 192.168.1.2 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9018ms
rtt min/avg/max/mdev = 6.974/10.966/20.626/3.938 ms
jati@gambesi:~$ _
```

Gambar 5. Pengujian ping *client* Gambesi ke Jati

Dari gambar 5 menunjukkan bahwa saat melakukan *ping* dari *client* Gambesi ke Jati terdapat pesan *reply from* 192.168.1.2 yang dimana ini adalah IP *address* dari *client* Jati, dengan data dari 10 *packet* yang di transmisikan semuanya tidak mengalami *packet loss*. Ini menunjukkan bahwa *client* Gambesi terhubung ke *client* Jati dengan baik walaupun tidak terkoneksi ke ISP.

```
jati@jati:~$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=15.2 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=49.6 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=18.5 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=27.6 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=64 time=19.7 ms
64 bytes from 192.168.1.1: icmp_seq=6 ttl=64 time=42.5 ms
64 bytes from 192.168.1.1: icmp_seq=7 ttl=64 time=13.2 ms
64 bytes from 192.168.1.1: icmp_seq=8 ttl=64 time=34.2 ms
64 bytes from 192.168.1.1: icmp_seq=9 ttl=64 time=53.5 ms
64 bytes from 192.168.1.1: icmp_seq=10 ttl=64 time=24.6 ms
^C
--- 192.168.1.1 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9025ms
rtt min/avg/max/mdev = 13.150/29.854/53.523/13.726 ms
jati@jati:~$ _
```

Gambar 6. Pengujian ping *client* Jati ke Gambesi

Dari gambar 6 menunjukkan bahwa saat melakukan *ping* sebaliknya dari *client* Jati ke *client* Gambesi terjadi koneksi yang baik dilihat dari pesan *reply from* 192.168.1.1. Dengan data dari 10 *packet* yang di transmisikan semuanya tidak mengalami *packet loss*.

B. *Pengujian Traceroute*

Pengujian *traceroute* dilakukan dengan menggunakan perintah *traceroute* antar *client* Gambesi ke *client* Jati dan sebaliknya. Pengujian ini bertujuan untuk mengetahui jalur yang dilewati *client* menggunakan metode VXLAN.

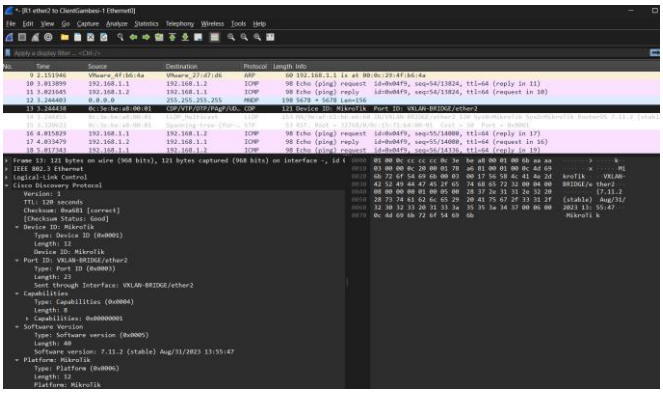
```
jati@gambesi:~$ traceroute 192.168.1.2
traceroute to 192.168.1.2 (192.168.1.2), 30 hops max, 60 byte packets
 1  192.168.1.2 (192.168.1.2)  9.538 ms  10.497 ms  10.536 ms
jati@gambesi:~$ _
```

Gambar 7. Pengujian Traceroute

Dari gambar 7 terlihat bahwa koneksi dari *client* Gambesi menuju *client* Jati terjadi secara *direct* atau langsung. Tidak terlihat tanda bahwa dari *client* Jati harus melewati *hope* dari ISP maupun server lainnya, namun ini terjadi langsung.

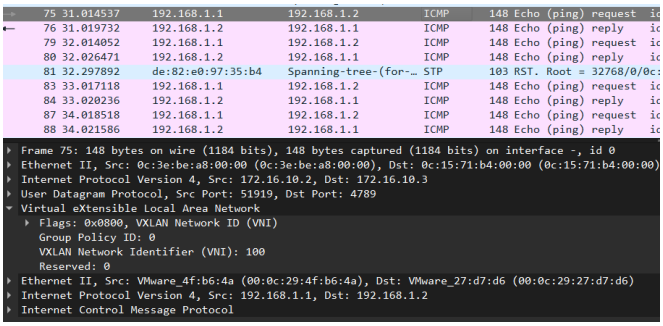
C. *Packet Capture dengan Wireshark*

Packet capture dengan Wireshark dilakukan untuk mengetahui *packet* apa saja yang di bawah saat melakukan koneksi antar *client*.



Gambar 8. Packet capture dari *client* Gambesi ke router Gambesi

Dari gambar 8 menunjukkan bahwa disaat *client* melakukan *ping* muncul sebuah protokol *Cisco Discovery Protocol* (CDP). *Cisco Discovery Protocol* (CDP) adalah protokol manajemen jaringan layer 2 milik perusahaan Cisco yang tertanam pada perangkat Cisco [19]. *Header protocol* CDP sendiri memuat informasi terkait perangkat dan Port ID. Pada Gambar 7 terlihat *Device* ID : Mikrotik dan Port ID : VXLAN-BRIDGE dimana ini sama dengan perangkat dan *port* yang dilakukan konfigurasi VXLAN sebelumnya.

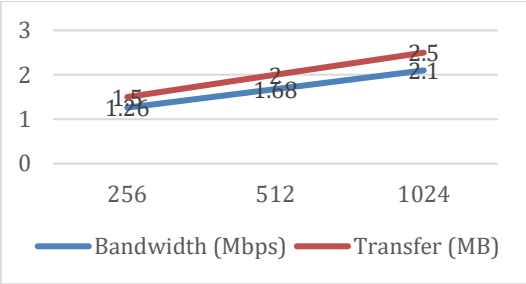


Gambar 9. Packet Capture dari *Client* Gambesi ke *Client* Gambesi

Pada gambar 9 saat melakukan *packet capture* antara *client* Gambesi dan *client* Jati terdapat *protocol Internet Control Massage Protocol* (ICMP). Protokol ini digunakan oleh perintah *ping*. Dari *protocol* dapat lihat bahwa terdapat *header Virtual Extensible LAN* (VXLAN) yang dibawa oleh paket ICMP. Di dalam *header* tersebut terdapat informasi terkait VXLAN *Network Identifier* (VNI) bernilai 100.

D. *Pengujian Throughput*

Pengujian *throughput* dilakukan untuk mengetahui seberapa sukses metode VXLAN dapat mengirimkan data dan menerima data. *Throughput* merujuk pada besar data yang dibawa oleh trafik jaringan. *Throughput* diukur dengan cara menghitung *bytes* yang dikirim selama rentang waktu tertentu [20]. Pengujian *throughput* dilakukan dengan menjalankan selama 10 detik pengiriman *buffer size* sesuai yang di inginkan.



Gambar 10. Hasil Pengujian *Throughput*

- Pengujian dengan *buffer size* 256 KB, ukuran *buffer* yang lebih kecil (256) menghasilkan transfer data sebesar 1.5 MB dengan *bandwidth* sekitar 1.26 Mbps. Ukuran *buffer* yang lebih kecil biasanya membatasi kemampuan jaringan menangani jumlah data yang ditransfer, yang pada akhirnya membatasi *throughput*.
- Pengujian dengan *buffer size* 512 KB. Dengan ukuran *buffer* yang sedang (512), transfer data meningkat menjadi 2 MB, dan bandwidth meningkat menjadi sekitar 1.68 Mbps. Ukuran *buffer* yang lebih besar memungkinkan lebih banyak data disimpan dalam *buffer* sementara sebelum dikirimkan, yang dapat meningkatkan *throughput*.
- Pengujian dengan *buffer* size 1024 KB.dengan ukuran *buffer* yang lebih besar (1024), transfer data bertambah menjadi 2.5 MB, dan *bandwidth* meningkat lagi menjadi sekitar 2.1 Mbps. Ukuran *buffer* yang lebih besar memberikan lebih banyak ruang untuk menyimpan data sebelum dikirimkan, yang dapat meningkatkan kemampuan jaringan untuk mentransfer data dengan *throughput* yang lebih tinggi.

IV. KESIMPULAN

Temuan penelitian menunjukkan bahwa meskipun berlokasi di wilayah geografis yang berbeda, klien Gambesi dan Jati berbagi *subnet* IP yang sama, sehingga memungkinkan konektivitas tanpa batas seolah-olah mereka berada dalam jarak yang berdekatan. Melalui analisis simulasi, diamati bahwa teknologi VXLAN memfasilitasi komunikasi yang fleksibel dan andal antara klien yang terisolasi dalam jaringan yang sama, bahkan ketika akses ke ISP dibatasi. VXLAN memanfaatkan berbagai protokol Layer 2, termasuk *Cisco Discovery Protocol* (CDP), untuk meningkatkan kinerja jaringan dan memberikan wawasan tentang fungsinya. Uji kinerja yang dilakukan dengan berbagai ukuran *buffer* menunjukkan peningkatan kecepatan transfer data dan kapasitas *bandwidth*, yang menunjukkan efisiensi VXLAN dalam transmisi data. Dengan memanfaatkan perangkat lunak GNS3 dan virtualisasi VMWare *Workstation*, para peneliti dapat memperoleh pemahaman komprehensif tentang pengoperasian VXLAN, melakukan eksperimen, dan mengembangkan skenario tanpa mengganggu infrastruktur jaringan sebenarnya.

UCAPAN TERIMA KASIH

Saya dengan tulus berterima kasih kepada Jurusan Prodi Informatika, Fakultas Teknik, Universitas Khairun serta para peneliti atas semua dukungan dan bantuan yang diberikan..

REFERENSI

[1] H. Suryantoro, A. Sopian, and D. Dartono, "Penerapan Teknologi Fortigate Dalam Pembangunan Jaringan Vpn-Ip Berbasis Ipsec," *Jeis J. Elektro Dan Inform. Swadharma*, vol. 1, no. 1, pp. 1–7, 2021, doi: 10.56486/jeis.vol1no1.64.

[2] S. Do Abdullah, A. W. Nur, H. K. Siradjuddin, Rosihan, and A. Ibrahim, "Analysis and Design of Cisco Packet Tracer Interconnections Between Autonomous Systems (AS) Using the Border Gateway Protocol at Campus 3 Khairun University," *Tech. Rom. J. Appl. Sci. Technol.*, 2023, doi: 10.47577/technium.v17i.10075.

[3] A. Adam, A. Fuad, H. Kurniadi Siradjuddin, and S. N Kapita, "Sistem Pendukung Keputusan Pemilihan Dosen Berprestasi Di Universitas Khairun Ternate Menggunakan Metode Multi- Attribute Utility Theory," *JIKO (Jurnal Inform. dan Komputer)*, 2020, doi: 10.33387/jiko.v3i3.2246.

[4] Arfan Efendi, Diyanatul Husna, and I Gde Dharma Nugraha, "Advancing Network Infrastructure: Integrating VXLAN Technology with Automated Circuit Operations and NOS Configurations," *Int. J. Electr. Comput. Biomed. Eng.*, 2023, doi: 10.62146/ijecbe.v1i2.30.

[5] M. Mahalingam *et al.*, "Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks," Request for Comments.

[6] Z. Zhao, F. Hong, and R. Li, "SDN Based VxLAN Optimization in Cloud Computing Networks," *IEEE Access*, 2017, doi: 10.1109/ACCESS.2017.2762362.

[7] P. Fitriani, U. Dani, and A. Prayogi, "Implementasi Jaringan internet dan Konfigurasi Mikrotik dengan simulasi GNS3 Pada Perusahaan Intelligent Komputer," *J. Inf. Komput. Log.*, vol. 2, pp. 1–3, 2021.

[8] J. Miguel-Alonso, "A Research Review of OpenFlow for Datacenter Networking," *IEEE Access*, 2023, doi: 10.1109/ACCESS.2022.3233466.

[9] R. A. Nuryadin, T. A. Ramadhani, J. Karaman, and M. Reza, "Analisis Perbandingan Performa Virtualisasi Server Menggunakan Vmware Esxi, Oracle Virtual Box, Vmware Workstation 16 Dan Proxmox," *METHOMIKA J. Manaj. Inform. dan Komputerisasi Akunt.*, 2023, doi: 10.46880/jmika.vol7no2.pp175-180.

[10] D. Marta, M. A. E. Putra, and G. Barovih, "Analisis Perbandingan Performa Virtualisasi Server Sebagai Basis Layanan Infrastructure As A Service Pada Jaringan Cloud," *MATRIK J. Manajemen, Tek. Inform. dan Rekayasa Komput.*, 2019, doi: 10.30812/matrik.v19i1.433.

[11] A. Shakarami, A. Shahidinejad, and M. Ghobaei-Arani, "A review on the computation offloading approaches in mobile edge computing: A game-theoretic perspective," *Softw. - Pract. Exp.*, 2020, doi: 10.1002/spe.2839.

[12] M. A. Hossain and M. S. Akter, "Study and Optimized Simulation of OSPFv3 Routing Protocol in IPv6 Network," *Glob. J. Comput. Sci. Technol.*,

2019, doi: 10.34257/gjcstevol19is2pg11.

[13] I. Morandi, F. Bronzino, R. Teixeira, and S. Sundaresan, “Service Traceroute: Tracing Paths of Application Flows,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2019. doi: 10.1007/978-3-030-15986-3_8.

[14] J. Uhlar, M. Holkovic, and V. Rusnak, “PCAPFunnel: A Tool for Rapid Exploration of Packet Capture Files,” in *Proceedings of the International Conference on Information Visualisation*, 2021. doi: 10.1109/IV53921.2021.00021.

[15] D. Spiekermann and J. Keller, “Encapcap: Transforming Network Traces to Virtual Networks,” in *Proceedings of the 2021 IEEE Conference on Network Softwarization: Accelerating Network Softwarization in the Cognitive Age, NetSoft 2021*, 2021. doi: 10.1109/NetSoft51509.2021.9492602.

[16] R. Alkanhel, A. Ali, F. Jamil, M. Nawaz, F. Mehmood, and A. Muthanna, “Intelligent transmission control for efficient operations in SDN,” *Comput. Mater. Contin.*, 2022, doi: 10.32604/cmc.2022.019766.

[17] R. Umar, I. Riadi, and B. F. Muthohirin, “Live forensics of tools on android devices for email forensics,” *Telkomnika (Telecommunication Comput. Electron. Control.*, 2019, doi: 10.12928/TELKOMNIKA.v17i4.11748.

[18] S. R. Hashim, R. A. Enad, A. M. Al-Khafagi, and N. K. Abdalhameed, “The facilities of detection by using a tool of Wireshark,” *Indones. J. Electr. Eng. Comput. Sci.*, 2023, doi: 10.11591/ijeecs.v31.i1.pp329-336.

[19] M. Oche, M. K. Nasir, A. B. Tambawal, and R. M. Noor, “Securing VoIP network: An overview of applied approaches and analysis,” in *2013 Pan African International Conference on Information Science, Computing and Telecommunications, PACT 2013*, 2013. doi: 10.1109/SCAT.2013.7055097.

[20] Vanny Andini, Lipur Sugiyanta, and Bachren Zaini, “Analisis Kinerja Parameter Throughput Dan Delay Akses Inetrnet Di Smk Karyaguna Jakarta Selatan,” *PINTER J. Pendidik. Tek. Inform. dan Komput.*, 2020, doi: 10.21009/pinter.4.2.8.