Jurnal CESS Medan - Junta Zeniarja

by Jurnal Cess Medan Junta Z

Submission date: 21-May-2020 09:06AM (UTC+0700)
Submission ID: 1328805619
File name: Jurnal_CESS_Medan.pdf (279.21K)
Word count: 3663
Character count: 20126

KOMPARASI PERFORMA METODE 6TO4 DAN KOMBINASI L2TP/IPSEC UNTUK IMPLEMENTASI IPV6 PADA JARINGAN KOMPUTER

Adhitya Nugraha[1], Muhammad Joyo Satrio[2], Junta Zeniarja[3]

[1,2,3] *Universitas Dian Nuswantoro*
Jl. Imam Bonjol No. 207, Semarang, Jawa Tengah
[1]*adhitya@dsn.dinus.ac.id*, [2]*1muhammad.joyosatrio19@gmail.com*, [3]*Junta@dsn.dinus.ac.id*

Abstrak— **Seiring dengan peningkatan pengguna internet, kebutuhan pengalamatan Internet Protocol versi 4 (IPv4) semakin meningkat sehingga dikhawatirkan ketersediaannya akan semakin berkurang dan habis. Kehadiran Internet Protocol versi 6 (IPv6) yang merupakan protokol pengalamatan internet generasi terbaru, ditujukan untuk menggantikan penggunaan IPv4 saat ini. Namun, dalam implementasinya masih terdapat beberapa kendala yang salah satunya adalah kondisi infrastruktur yang saat ini yang belum banyak mendukung implementasi IPv6 sehingga proses migrasi IPv4 ke IPv6 menjadi sangat sulit. Pada akhirnya diterapkanlah metode transisi IPv6 untuk melakukan koneksi terhadap infrastruktur IPv4. Teknik 6to4 dan L2TP/IPSec merupakan metode tunneling yang mampu melakukan transisi dari IPv4 ke IPv6. Dalam penelitian ini, dilakukan komparasi terhadap kedua metode tersebut dengan melakukan pengukuran throughput, delay dan packet loss dengan berbagai skenario koneksi jaringan. Berdasarkan hasil dari percobaan yang dilakukan, diketahui bahwa peneraepan teknik L2TP/IPSec menghasilkan kualitas koneksi yang lebih baik daripada kualitas koneksi penerapan teknik 6to4.**

Kata Kunci— **IPv4, IPv6, transisi, *Tunneling*, 6to4, L2TP/IPSec.**

Abstract— **Along with the increase in internet users, the need for addressing Internet Protocol version 4 (IPv4) is increasing so it is feared that its availability will decrease and run out. The presence of Internet Protocol version 6 (IPv6), which is the latest generation of internet addressing protocols, is intended to replace the current use of IPv4. However, in its implementation there are still several obstacles, one of which is the current condition of infrastructure which does not yet support the implementation of IPv6 so that the process of migrating from IPv4 to IPv6 becomes very difficult. In the end, the IPv6 transition method was applied to connect to the IPv4 infrastructure. The 6to4 and L2TP / IPSec techniques are tunneling methods that are able to make the transition from IPv4 to IPv6. In this study, a comparison of the two methods was carried out by measuring throughput, delay and packet loss with various network connection scenarios. Based on the results of the experiments conducted, it is known that the L2TP / IPSec engineering arrangement produces better connection quality than the connection quality of the 6to4 technique.**

Keywords— **IPv4, IPv6, transisi, Tunneling, 6to4, L2TP/IPSec.**

I. PENDAHULUAN

Perkembangan teknologi, aplikasi internet saat ini telah memberikan dampak kepada penggunaan layanan internet yang semakin hari meningkat setiap waktunya. Penggunaan layanan internet yang besar juga harus diimbangi dengan kebutuhan akan kestabilan, kelancaran dan keamanan saat berkomunikasi.

Internet Protokol atau dikenal sebagai IP merupakan serangkaian nomor unik yang dialokasikan kepada perangkat berbasis komputer yang dimanfaatkan sebagai sistem pengalamatan untuk pada jaringan berbasis protokol TCP/IP. IP versi 4 (IPv4) dikenal sebagai sistem pengalamatan internet yang digunakan saat ini. Namun, seiring pengguna layanan internet yang semakin meningkat, kebutuhan alamat IPv4 juga meningkat setiap waktunya[1]–[3].

Regional Internet Registry (RIR), sebuah organisasi atau lembaga resmi internasional yang mengatur dan mengelola alamat IP publik dunia merilis data bahwa jumlah alamat tersisa dari IPv4 pada tahun 2016 kurang lebih hanya tersisa 2.5 persen dari kapasitas awal atau hanya 43.847.976 alamat IP. Sedangkan untuk regional Asia-Pasifik pada tahun 2020 hanya tersisa 2.798.848 alamat IP[4].

Terkait kondisi tersebut, *Internet Engineering Task Force* (IETF) telah mengembangkan sebuah protokol internet yang diberi nama IP versi 6 (IPv6) yang memungkinkan untuk menampung lebih banyak *host*

yang dapat terhubung dalam jaringan. Secara struktur, fitur dan mekanisme kerja IPv6 sangat berbeda dengan IPv4. Perbedaan ini menimbulkan kesulitan untuk mencoba mengintegrasikan pengalamatan IPv6 kedalam teknologi berbasis IPv4 yang sudah diterapkan kebanyakan pengguna internet. Maka dari itu, banyak penelitian dan percobaan yang dilakukan untuk mengadopsi teknologi IPv6 ini tanpa harus menghilangkan penggunaan IPv4 yang sudah berjalan[5], [6].

Mekanisme transisi merupakan salah satu teknik yang dapat diterapkan untuk memfasilitasi agar *host* IPv6 dapat berkomunikasi dengan *host* IPv4 yang sudah berjalan. Untuk mendukung transisi tersebut, *Internet Engineering Task Force* (IETF) membuat beberapa metode transisi yaitu *Dual IP Stack, Tunneling* dan *Translation*[2], [7], [8].

Tunneling memungkinkan agar paket IPV6 terenkapsulasi kedalam IPV4 dimana hal ini dilakukan dengan memanfaatkan IPV4 sebagai link layer IPV6. Salah satu jenis mekanisme *tunneling* adalah 6to4 yang merupakan sebuah mekanisme *tunneling* yang memungkinkan pengiriman paket IPv6 ke *site* IPv6 lainya melewati infrastuktur *routing* IPv4[5], [9]–[11]. Pada titik awal *tunnel*, paket IPv6 dienkapsulasi atau diringkas menjadi paket IPv4 kemudian saat tiba pada titik akhir *tunnel* paket tersebut didekapsulasi menjadi paket IPv6 kembali. *Dual IP Stack (native dual stack)* merupakan implementasi yang mempersyaratkan dukungan terhadap IPv6 dan IPv4 di perangkat yang sama. Artinya semua perangkat yang terhubung kedalam jaringan harus mendukung untuk implementasi IPV6 sedangkan seperti yang diketahui tidak semua perangkat jaringan yang tersedia memiliki dukungan IPV6[5], [7], [12]. *Translation* digunakan memecahkan masalah ketidaksesuaian antara IPv4 dan IPv6. *Translation* dapat diimplementasikan menggunakan Application Layer Gateway atau dengan menggunakan network layer IPv6 / IPv4. Contoh mekanisme ini adalah *ICMP Translation Algorithm (*SIIT*), Stateful NAT64, DNS64,* dan lain-lain. Kelemahan dari mekanisme ini adalah merusak konektivitas end-to-end, yang dianggap sebagai konsep inti dari Internet[5], [12]–[14].

Mekanisme *tunneling* merupakan solusi terbaik saat ini yang memungkinkan untuk segera diterapkan dengan memanfaatkan infrastruktur IPV4. Namun, adapula teknik yang menerapkan teknik Virtual Private Network (VPN) *native* pada dual stack IPv6.

Penelitian yang dilakukan oleh Sohely Jahaan dkk[15] menggunakan VPN protokol GRE, IPSec, PPTP, dan Layer 2 Tunneling Protocol with IP Security (L2TP/IPSec). Membahas performa VPN protokol dengan parameter *throughput*, RTT, *jitter* dan *security mechanism*. Hasil dari penelitian ini menunjukkan L2TP/IPSec lebih baik daripada PPTP. Hal ini dibuktikan ketika uji *throughput* bahwa L2TP/IPSec secara bertahap meningkat sedangkan *throughput* PPTP mengalami perubahan secara fluktuatif sejalan dengan pertambahan paket.

Penelitian yang dilakukan oleh Shaneel Narayan dkk [16] menggunakan IPv4, IPv6, 4to6, 6to4, PPTP dan IPSec. Penelitian ini membahas tentang perbandingan kinerja 4to6 dan 6to4 ketika melalui atau tanpa melalui VPN protokol. Hasil dari penelitian ini menunjukkan mekanisme transisi 6to4 menunjukan hasil *delay* sangat rendah, tetapi ketika dikonfigurasi dengan IPsec nilai *delay* meningkat menjadi hampir tiga kali lipat dari nilai aslinya.

Berdasarkan latar belakang tersebut, penulis menyimpulkan bahwa beberapa teknik VPN dapat diterapkan untuk mentransmisikan paket IPv6. Diantara protokol VPN tersebut, L2TP lebih *firewall friendly* dibandingkan jenis VPN yang lainnya seperti PPTP, GRE dan lainnya. Namun L2TP tidak memiliki fitur enkripsi sehingga perlu dipadukan dengan IPSec untuk mendapatkan keamanan yang lebih tinggi. Terakhir, penulis bermaksud melakukan komparasi antara mekanisme transisi *tunneling* (teknik 6to4) dengan teknik VPN (L2TP/IPSec) IPv6 untuk membandingkan hasil performa *throughput, delay* dan *packet loss* berdasarkan skenario pengujian yang telah disiapkan.

II. METODOLOGI

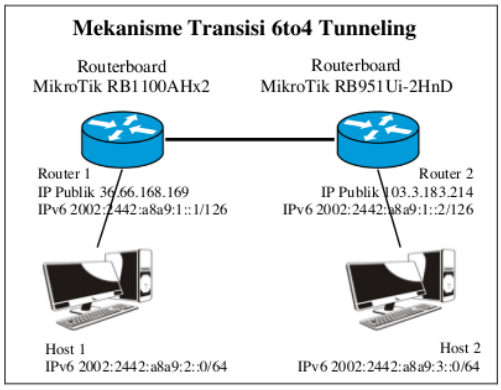
A. Persiapan Peralatan Jaringan

Penelitian ini dilakukan melalui uji coba lapangan dengan menggunakan perangkat jaringan yang telah dikonfigurasikan. Adapun perangkat *software* dan *hardware* yang dipersiapkan adalah sebagai berikut.

- Routerboard MikroTik RB951Ui-2HnD
- Routerboard MikroTik RB1100AHx2
- 2 PC klien
- Wireshark
- Winbox

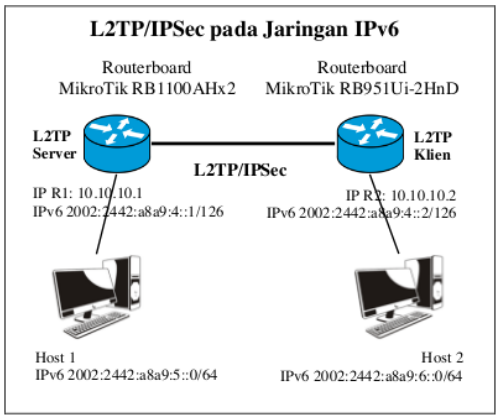
B. Perancangan Infrastruktur Jaringan

Pada mekanisme tunneling 6to4, jaringan lokal di *host* 1 dan *host* 2 akan dikonfigurasikan menggunakan IPv6 yang kemudian akan saling berkomunikasi menggunakan layanan IP publik IPv4. Hal tersebut dapat dilakukan dikarenakan paket IPv6 dari *host* 1 akan dienkapsulasikan pada *router* 1 menjadi paket IPv4 yang nantinya akan melewati *tunnel* transmisi dan akan didekapsulasikan apabila paket telah sampai pada *router* 2 yang kemudian diteruskan ke *host* 2. Gbr. 1 menunjukan konfigurasi infrastruksur jaringan yang dilakukan untuk metode transisi 6to4.



Gbr. 1 Rancangan desain jaringan mekanisme transisi 6to4

Sedangkan pada mekanisme L2TP/IPSec, *router* 1 bertindak sebagai L2TP server sedangkan *router* 2 bertindak sebagai L2TP client. Paket L2TP akan dienkapsulasi bersama dengan paket IPSec saat *router* 1 mengirim data atau berkomunikasi ke *router* 2. Jaringan LAN pada *host* 1 dan *host* 2 menggunakan IPv6. Gbr. 2 menunjukan konfigurasi infrastruksur jaringan yang dilakukan untuk mekanisme L2TP/IPSec.



Gbr. 2 Rancangan desain jaringan mekanisme L2TP/IPSec

C. *Proses Konfigurasi Jaringan*

Pada proses ini, router dikonfigurasikan lewat host menggunakan aplikasi winbox. Pada skema 6to4 tunnel, diperlukan 2 alamat IPv4 sebagai alamat IP publik untuk dapat saling terkoneksi. Alamat IP yang digunakan pada router 1 dan router 2 yaitu 2002:2442:a8a9:1::0 dengan prefix /126. Untuk alamat IP pada network host 1 menggunakan alamat 2002:2442:a8a9:2::0/64. Sedangkan untuk alamat IP pada network host 2 menggunakan alamat IP 02002:2442:a8a9:3::0/64.

Pada Skema metode L2TP dapat berjalan jika router yang bertindak sebagai server mempunyai IP Public. Alamat IPv4 yang digunakan untuk koneksi pada router 1 dan router 2 yaitu 10.10.10.0/30 dan 2002:2442:a8a9:4::0/126 untuk alamat IPv6 nya. Untuk alamat IP pada jaringan host 1 menggunakan alamat IPv6 2002:2442:a8a9:5::0/64. Untuk alamat IP pada jaringan host 2 menggunakan alamat IPv6 2002:2442:a8a9:6::0/64. Pada router 1 menggunakan alamat IP Public 36.66.168.169 sebagai "Remote Address" yang nanti akan digunakan sebagai akses "Dial Out" pada router 2.

D. *Melakukan Pengujian*

Skenario pengujian koneksi dilakukan dengan menggunakan *perintah ping, send file dan video streaming* yang nanti paket akan dicapture menggunakan aplikasi wireshark. Perintah *ping* dijalankan selama 60 detik setelah dilakukannya instalasi dan konfigurasi pada kedua metode. Hal ini dilakukan untuk memeriksa koneksi dari host pada router 1 menuju ke host pada router 2. Pengujian berikutnya yaitu *send file* yang dilakukan dengan menggunakan aplikasi VNC Server dan VNC Viewer yang sudah diinstal sebelumnya di *host* pada jaringan *router* 1 dan *host* di jaringan *router* 2. Saat mengirim berkas berlangsung, paket yang dikirim akan di capture pada aplikasi *wireshark* dengan ukuran berkas sebesar 167 MB. Pengujian selanjutnya *video streaming*, yaitu memutar video selama 60 detik di host router 2 yang diakses melalui jaringan dengan host router 1 sebagai server penyedia video. Semua skenario pengujian tersebut dilakukan sebanyak 5 kali untuk dapat melihat rata-rata dari setiap percobaan.

III. HASIL DAN PEMBAHASAN

A. *Hasil Pengujian pada Skenario Mekanisme 6to4*

TABEL I
HASIL UJI PING MEKANISME 6TO4

Uji ke	Throughput (kbps)	Delay (ms)	Packet loss (%)
1	1,671	48	0
2	1,671	51	0
3	1,601	44	0
4	1,668	48	0
5	1,667	42	0

Pada uji coba ping dimetode 6to4, hasil pertama menunjukkan throughput sebesar 1,671 kbps, delay sebesar 48 ms dan packet loss 0%. Saat tes kedua menunjukkan throughput sebesar 1,671 kbps, delay sebesar 51 ms dan packet loss 0%. Untuk tes ketiga, nilai throughput sebesar 1,601 kbps, delay sebesar 44 ms dan packet loss 0%. Pada tes keempat hasilnya menunjukkan throughput sebesar 1,668 kbps, delay sebesar 48 ms dan packet loss 0%. Sedangkan tes kelima hasilnya menunjukkan throughput sebesar 1,667 kbps, delay sebesar 42 ms dan packet loss 0%.

TABEL II
HASIL UJI PENGIRIMAN FILE PADA MEKANISME 6TO4

Uji ke	Throughput (kbps)	Delay (ms)	Packet loss (%)
1	3571	1,14	0

2	2646	1,84	0
3	3419	1,43	0
4	3372	1,45	0
5	2967	1,64	0

Pada uji coba pengiriman file dimetode 6to4, hasil pertama menunjukkan throughput sebesar 3571 kbps, delay sebesar 1,14 ms dan packet loss 0%. Saat tes kedua menunjukkan throughput hanya sebesar 2646 kbps, delay sebesar 1,84 ms dan packet loss 0%. Untuk tes ketiga, nilai throughput menjadi 3419 kbps, delay sebesar 1,43 ms dan packet loss 0%. Pada tes keempat hasilnya throughput sebesar 3372 kbps, delay sebesar 1,45 ms dan packet loss 0%. Sedangkan tes kelima nilai throughput turun sebesar 2967 kbps, delay sebesar 1,64 ms dan packet loss 0%.

TABEL III
HASIL UJI VIDEO STREAMING PADA MEKANISME 6TO4

Uji ke	Throughput (kbps)	Delay (ms)	Packet loss (%)
1	3507	1,97	7,1
2	468	15,02	7,3
3	967	7,16	7
4	5224	1,31	6,8
5	4421	1,58	6,9

Pada uji coba video streaming dimetode 6to4, hasil pertama menunjukkan *throughput* sebesar 3507 kbps, *delay* sebesar 1,97 ms dan *packet loss* 7,1 %. Saat tes kedua menunjukkan nilai *throughput* turun menjadi sebesar 468 kbps, *delay* meningkat sebesar 15,02 ms dan *packet loss* 7,3 %. Untuk tes ketiga, nilai *throughput* naik menjadi sebesar 967 kbps, *delay* sebesar 7,16 ms dan *packet loss* 4,5 %. Pada tes keempat hasilnya *throughput* naik drastis menjadi sebesar 5224 kbps, *delay* sebesar 1,31 ms dan *packet loss* 6,8 %. Sedangkan tes kelima menunjukkan *throughput* sebesar 4421 kbps, *delay* sebesar 1,58 ms dan *packet loss* 6,9 %

B. Hasil Pengujian pada Skenario Mekanisme L2TP/IPSec

TABEL IV
HASIL UJI PING L2TP/IPSEC

Uji ke	Throughput (kbps)	Delay (ms)	Packet loss (%)
1	1,858	21	0
2	1,685	20	0
3	1,677	20	0
4	1,633	20	0
5	1,602	20	0

Pada uji coba ping dimetode L2TP/IPSec, hasil pertama menunjukkan throughput sebesar 1,858 kbps, delay sebesar 21 ms dan packet loss 0%. Saat tes kedua menunjukkan throughput sebesar 1,685 kbps, delay sebesar 20 ms dan packet loss 0%. Untuk tes ketiga, nilai throughput sebesar 1,677 kbps, delay sebesar 20 ms dan packet loss 0%. Pada tes keempat hasilnya menunjukkan throughput sebesar 1,633 kbps, delay sebesar 20 ms dan packet loss 0%. Sedangkan tes kelima hasilnya menunjukkan *throughput* sebesar 1,602 kbps, delay sebesar 22 ms dan packet loss 0%.

TABEL V
HASIL UJI PENGIRIMAN FILE PADA L2TP/IPSEC

Uji ke	Throughput (kbps)	Delay (ms)	Packet loss (%)
1	4342	1,12	0
2	4416	1,06	0
3	4428	1,06	0
4	4450	1,06	0
5	4402	1,07	0

Pada uji coba pengiriman file dimetode L2TP/IPSec, hasil pertama menunjukkan throughput sebesar 4342 kbps, delay sebesar 1,12 ms dan packet loss 0%. Saat tes kedua menunjukkan throughput sebesar 4416 kbps, delay sebesar 1,06 ms dan packet loss 0%. Untuk tes ketiga, nilai throughput menjadi 4428 kbps, delay sebesar 1,06 ms dan packet loss 0%. Pada tes keempat hasilnya throughput sebesar 4450 kbps, nilai delay tetap sama sebesar 1,06 ms dan packet loss 0%. Sedangkan tes kelima menunjukkan throughput sebesar 4402 kbps, delay sebesar 1.07 ms dan packet loss 0%.

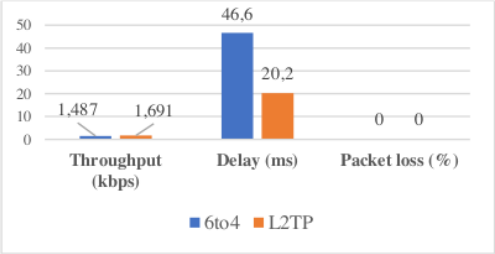
TABEL VI
HASIL UJI VIDEO STREAMING L2TP/IPSEC

Uji ke	Throughput (kbps)	Delay (ms)	Packet loss (%)
1	4441	1,77	5
2	4517	1,79	5,3
3	4711	1,73	5,4
4	4751	1,65	4,8
5	4700	1,65	4,4

Pada uji coba video streaming dimetode L2TP/IPSec, hasil pertama menunjukkan throughput sebesar 4441 kbps, delay sebesar 1,77 ms dan packet loss 5 %. Saat tes kedua menunjukkan throughput sebesar 4517 kbps, delay sebesar 1,79 ms dan packet loss 5,3 %. Untuk tes ketiga, nilai throughput naik sebesar 4711 kbps, delay sebesar 1,73 ms dan packet loss 5,4 %. Pada tes keempat hasilnya throughput sebesar 4751 kbps, delay sebesar 1,65 ms dan packet loss 4,8 %. Sedangkan tes kelima menunjukkan throughput sebesar 4700 kbps, delay sebesar 1,65 ms dan packet loss 4,4 %.

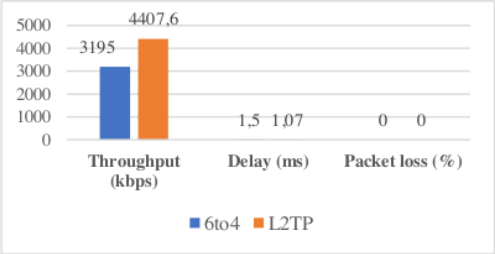
C. Hasil Pengamatan

Berdasarkan percobaan yang dilakukan, peneliti telah mendapatkan data atas 3 skenario yang telah dibuat yaitu menggunakan perintah ping, pengiriman file dan video streaming untuk diambil penilaian pengukuran atas parameter *throughput, delay* dan *packet loss*. Adapun hasil dari percobaan dapat dilihat pada Gbr. 3 menunjukan perbandingan kualitas 6to4 dan L2TP/IPSec pada skenario ping, Gbr. 4 menunjukan perbandingan kualitas 6to4 dan L2TP/IPSec pada skenario pengiriman file, Gbr. 5 menunjukan perbandingan kualitas 6to4 dan L2TP/IPSec pada skenario video streaming.



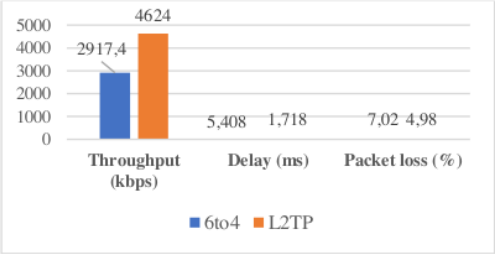
Gbr. 3 Kualitas 6to4 dan L2TP/IPSec pada skenario ping

Hasil rata-rata pengujian ping pada L2TP/IPSec adalah nilai *throughput* sebesar 1,691 kbps, *delay* sebesar 20,2 ms dan *packet loss* sebesar 0%. Hasil itu cukup baik jika dibandingkan dengan metode 6to4 yang mempunyai nilai *throughput* sebesar 1,487 kbps, *delay* sebesar 46,6 ms dan *packet loss* 0%.



Gbr. 4 Kualitas 6to4 dan L2TP/IPSec pada skenario pengiriman file

Untuk pengujian pengiriman file, metode L2TP/IPSec memiliki nilai rata rata *throughput* sebesar 4407,6 kbps, *delay* hanya 1,5 ms dan *packet loss* 0% merupakan hasil lebih baik daripada metode 6to4 dengan nilai rata rata *throughput* sebesar 3195 kbps, *delay* 1,5 ms dan *packet loss* 0%.



Gbr. 5 kualitas 6to4 dan L2TP/IPSec pada skenario video streaming

Sedangkan pada tes *video streaming*, nilai rata rata pada metode L2TP/IPSec yaitu sebesar 4624 kbps, *delay* sebesar 1,608 ms dan *packet loss* hanya 7,02% yang memiliki hasil lebih baik daripada metode 6to4 yang mempunyai nilai rata rata *throughput* sebesar 2917,4 kbps, *delay* sebesar 5,408 ms dan *packet loss* 7,02%.

Data-data di atas menunjukan bahwa metode L2TP/IPSec menghasilkan nilai rata-rata *throughput* pada ketiga skenario lebih baik daripada mekanisme 6to4. Dengan nilai *throughput* lebih besar berarti pengiriman paket dapat dilakukan lebih cepat. Berikutnya L2TP/IPSec menghasilkan nilai rata-rata *delay* pada ketiga skenario lebih sedikit daripada mekanisme 6to4 yang artinya lebih baik. Dimana *delay* merupakan proses tunda dalam pengiriman paket sehingga semakin sedikit nilai *delay* maka pengiriman semakin cepat. *Packet loss* hanya terjadi pada skenario video streaming, hal ini wajar dikarenakan jenis paket yang dikirimkan adalah datagram yang bekerja pada protokol UDP. Namun secara hasil kualitas yang didapatkan pada percobaan menunjukan L2TP/IPSec menghasilkan nilai rata-rata *packet loss* lebih sedikit daripada mekanisme 6to4.

IV. KESIMPULAN

Berdasarkan hasil uji percobaan menunjukkan bahwa L2TP/IPSec memiliki kualitas yang baik dibandingkan metode transisi 6to4 dimana hasil throughput untuk rata-rata ketiga skenario pengujian pengiriman file adalah sebesar 4407,6 kbps yang lebih baik daripada metode 6to4 yang hanya sebesar 3195 kbps. Nilai rata rata packet loss pada skenario tes video streaming pada L2TP/IPSec yaitu sebesar 4,98 % yang lebih baik daripada metode 6to4 yaitu 7,02. Hasil delay pada skenario pengujian ping pada metode L2TP yaitu 20,2 ms lebih baik daripada hasil metode 6to4 yaitu 46,6 ms. Sebagai kesimpulan bahwa pengukuran QoS dengan parameter throughput, delay dan packet loss pada metode L2TP/IPSec memiliki hasil yang lebih baik daripada hasil yang diperoleh pada metode 6to4.

Penelitian selanjutnya dapat mempertimbangkan untuk menganalisa skenario pengujian yang berbeda, dapat pula melakukan perbandingan dengan metode yang berbeda seperti metode GRE Tunnel maupun Dual Stack.

REFERENSI

[1] S. Wardoyo, T. Ryadi, and R. Fahrizal, "Analisis Performa File Transport Protocol Pada Perbandingan Metode IPv4 Murni, IPv6 Murni dan Tunneling 6to4 Berbasis Router Mikrotik," J. Nas. Tek. Elektro, vol. 3, no. 2, p. 106, 2014.

[2] I. Marzuki, "Mekanisme Transisi IPv4 dan IPv6 Menggunakan Metode Automatic Tunneling Pada Jaringan Client Server Berbasis Linux," J. Teknol. Inf. Indones., vol. 3, no. 2, pp. 68–73, 2019.

[3] A. Hamarsheh and Y. Abdalaziz, "Transition to IPv6 Protocol, Where We Are?," 2019 Int. Conf. Comput. Inf. Sci. ICCIS 2019, no. July 2017, pp. 1–6, 2019.

[4] LACNICLabs, "IPV4 Stats - IPV4 Available Space," 2020. [Online]. Available: http://opendata.labs.lacnic.net/ipv4stats/graphs/ipv4avail.html. [Accessed: 10-Mar-2020].

[5] Y. Sookun and V. Bassoo, "Performance analysis of IPv4/IPv6 transition techniques," 2016 IEEE Int. Conf. Emerg. Technol.

Innov. Bus. Pract. Transform. Soc. EmergiTech 2016, pp. 188–193, 2016.

[6] F. L. Budiono and R. Azmi, "Kondisi Migrasi Internet Protocol Version 6 (IPV6) DI INDONESIA," Bul. Pos dan Telekomun., vol. 9, no. 2, pp. 149–162, 2011.

[7] A. R. Mukti and Ferdiansyah, "Studi Performa Migrasi Ipv4 Ke Ipv6 Pada Metode Tunneling," J. Sist. Inf. Musirawas, vol. 2, no. 1, pp. 28–34, 2017.

[8] S. T. Telekomunikasi, F. Teknik, and I. T. Telkom, "Analisa Performansi Metode Transisi IPv6 Tunneling 6to4 Pada Jaringan MPLS," in Proceedings on Conference on Electrical Engineering, Telematics, Industrial Technology, and Creative Media, 2018, pp. 240–244.

[9] F. Siddika, M. A. Hossen, and S. Saha, "Transition from IPv4 to IPv6 in Bangladesh: The competent and enhanced way to follow," Proc. 2017 Int. Conf. Networking, Syst. Secur. NSysS 2017, pp. 174–179, 2017.

[10] J. M. V. Ruiz, C. S. Cardenas, and J. L. M. Tapia, "Implementation and testing of IPv6 transition mechanisms," 2017 IEEE 9th Latin-American Conf. Commun. LATINCOM 2017, vol. 2017-January, pp. 1–6, 2017.

[11] M. S. Ali and T. A. Yahiya, "Performance Analysis of Native Ipv4/Ipv6 Networks Compared to 6to4 Tunnelling Mechanism," ICOASE 2018 - Int. Conf. Adv. Sci. Eng., pp. 250–255, 2018.

[12] Komal, "Performance Evaluation of Tunneling Mechanisms in IPv6 Transition: A Detailed Review," Proc. - 2015 2nd IEEE Int. Conf. Adv. Comput. Commun. Eng. ICACCE 2015, pp. 144–149, 2015.

[13] X. Yu, J. Cheng, S. Wu, and W. Song, "A framework of timestamp replantation for panorama video surveillance," Multimed. Tools Appl., vol. 75, no. 17, pp. 10357–10381, 2016.

[14] M. A. Hossain and B. Song, "Efficient Resource Management for Cloud-enabled Video Surveillance over Next Generation Network," Mob. Networks Appl., vol. 21, no. 5, pp. 806–821, 2016.

[15] S. Jahan, M. S. Rahman, and S. Saha, "Application specific tunneling protocol selection for Virtual Private Networks," Proc. 2017 Int. Conf. Networking, Syst. Secur. NSysS 2017, pp. 39–44, 2017.

[16] S. Narayan, S. Ishrar, A. Kumar, R. Gupta, and Z. Khan, "Performance analysis of 4to6 and 6to4 transition mechanisms over point to point and IPSec VPN protocols," IFIP Int. Conf. Wirel. Opt. Commun. Networks, WOCN, vol. 2016-November, pp. 0–6, 2016.

Jurnal CESS Medan - Junta Zeniarja

ORIGINALITY REPORT

15%	9%	10%	12%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Universitas Dian Nuswantoro Student Paper	3%
2	Submitted to Universidad Pontificia Bolivariana Student Paper	3%
3	Firmansyah, Mochamad Wahyudi, Rachmat Adi Purnama, Lise Pujiastuti. "Performance Analysis of Routing Enhanced Interior Gateway Routing Protocol Load Balancing for IPv6", 2019 Fourth International Conference on Informatics and Computing (ICIC), 2019 Publication	2%
4	Yongquan Yang, Zhiqiang Wei, Bowei Hong. "Research on IPv6 Transition Technology for Digital Ocean", 2018 IEEE 4th International Conference on Computer and Communications (ICCC), 2018 Publication	1%
5	Thattapon Surasak, Scott C.-H Huang. "Enhancing VoIP Security and Efficiency using VPN", 2019 International Conference on	1%

	Computing, Networking and Communications (ICNC), 2019 Publication	
6	Imam Marzuki. "Mekanisme Transisi IPv4 dan IPv6 Menggunakan Metode Automatic Tunneling Pada Jaringan Client Server Berbasis Linux", Jurnal Teknologi Informasi Indonesia (JTII), 2019 Publication	1%
7	Submitted to Glasgow Caledonian University Student Paper	1%
8	www.ukh.edu.krd Internet Source	<1%
9	Submitted to Sriwijaya University Student Paper	<1%
10	thisismybreath.blogspot.com Internet Source	<1%
11	Submitted to Multimedia University Student Paper	<1%
12	AYMAN AL-ANI, MOHAMMED ANBAR, AHMED K AL-ANI, IZNAN HUSAINY HASBULLAH. "DHCPv6Auth: a mechanism to improve DHCPv6 authentication and privacy", Sādhanā, 2020 Publication	<1%

13	jurnal.untirta.ac.id Internet Source	<1%
14	A. Ezaz Mohammed AL-Dahasi, B. Nazar Abbas Saqib. "Attack tree Model for Potential Attacks Against the SCADA System", 2019 27th Telecommunications Forum (TELFOR), 2019 Publication	<1%
15	fachryclp.blogspot.com Internet Source	<1%
16	primadonal.blogspot.com Internet Source	<1%
17	www.pttz.org Internet Source	<1%
18	Submitted to Universitas Nasional Student Paper	<1%
19	Submitted to University of Hertfordshire Student Paper	<1%
20	www.koreascience.or.kr Internet Source	<1%
21	docplayer.info Internet Source	<1%
22	jurnal.fkip.uns.ac.id Internet Source	<1%
	Submitted to Universitas Brawijaya	

23	Student Paper	<1%
24	ishandayani.blogspot.com Internet Source	<1%
25	Submitted to Universitas Gunadarma Student Paper	<1%
26	Submitted to Universiti Malaysia Pahang Student Paper	<1%
27	Submitted to UC, Irvine Student Paper	<1%
28	Submitted to Universitas Islam Indonesia Student Paper	<1%
29	Submitted to Ayrshire Regional College Student Paper	<1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	Off		