



InComTech: Jurnal Telekomunikasi dan Komputer
vol.11, no.2, Agustus 2021, 85-99
<http://publikasi.mercubuana.ac.id/index.php/Incomtech>
P-ISSN: 2085-4811 E-ISSN: 2579-6089

Analisis Perbandingan Performansi Jaringan IPv4 dan IPv6 pada MPLS VPN Menggunakan *Server IMS Core*

Donny Bayu Dwiartanto, Dadiek Pranindito*, Nanda Iryani

*Teknik Telekomunikasi, Institut Teknologi Telkom Purwokerto
Jl. DI. Panjaitan No. 128 Purwokerto, Indonesia*

* Email Penulis Koresponden: dadiek@ittelkom-pwt.ac.id

Abstrak:

IP *Multimedia Subsystem* (IMS), sebuah teknologi yang menyediakan aplikasi *based on IP* yang memungkinkan pengguna untuk menggunakan layanan *triple play* (*voice, video* dan *data*) dalam waktu yang bersamaan. Penerapan layanan *triple play* yang menggunakan teknologi dari IMS membutuhkan jaringan *backbone* yang memiliki kecepatan pengiriman data yang baik dan handal, maka digunakan sebuah jaringan MPLS. *Multi Protocol Label Switching* (MPLS) merupakan metode *forwarding* data melalui suatu jaringan menggunakan informasi dalam label yang dikaitkan pada IP. MPLS mempunyai komponen utama salah satunya MPLS-VPN yang diharapkan dapat melakukan pengiriman layanan yang beragam melalui jaringan *private* pada *network layer*. Perkembangan menggunakan IPv6 membuat peralihan penggunaan protokol IPv4 ke IPv6 tidak bisa serentak begitu saja dilakukan karena sudah banyaknya infrastruktur jaringan IPv4 yang sudah terpasang. Penelitian ini menggunakan 6VPE sebagai metode untuk translasi dari IPv4 ke IPv6 yang dapat berjalan pada jaringan *backbone* MPLS VPN. Dari hasil simulasi didapatkan *throughput* terbaik pada layanan *voice call* IPv4 sebesar 7488 kbps, *delay* dan *jitter* terbaik pada layanan *text messaging* IPv4 sebesar 0,0206 ms dan 0,0015 ms, *packet loss* terbaik pada layanan *voice call* dan *text messaging* dengan IPv4 dan IPv6 sebesar 0%. Sedangkan, pada layanan *video call* grafik *traffic loss* mengalami penurunan dengan nilai 0,2 %, 0,1 % dan 0,1 %. *Packet loss* pada layanan *video call* masih dapat dikatakan baik dalam standar klasifikasi *packet loss*. Penelitian ini menyimpulkan bahwa *backbone* IPv4 lebih baik daripada *backbone* IPv6 digunakan pada jaringan MPLS VPN menggunakan *server* Open IMS Core.

This is an open access article under the [CC BY-NC](https://creativecommons.org/licenses/by-nc/4.0/) license



Kata Kunci:

IMS;
Triple Play;
MPLS-VPN;
6VPE;
QoS;

Riwayat Artikel:

Diserahkan 23 November 2020
Direvisi 5 Januari 2021
Diterima 23 Mei 2021
Dipublikasi 21 Agustus 2021

DOI:

10.22441/incomtech.v11i2.10195

1. PENDAHULUAN

Perkembangan kemajuan teknologi seperti saat ini, membuat kebutuhan akan kecepatan dan mudahnya layanan komunikasi menuntut tersedianya layanan-layanan baru yang inovatif, tidak hanya menggunakan satu layanan saja tetapi layanan yang terintegrasi seperti suara, video dan data. Hal tersebut yang kemudian melatarbelakangi munculnya *IP Multimedia Subsystem (IMS)*, sebuah teknologi yang memungkinkan pengguna untuk menggunakan layanan *triple play* (suara, video dan data) dalam waktu yang bersamaan [1]. Pada saat ini teknologi komunikasi data yang banyak digunakan oleh *service provider* salah satunya adalah teknologi *Multi Protocol Label Switching (MPLS)*. MPLS merupakan metode *forwarding* data melalui suatu jaringan menggunakan informasi dalam label yang dikaitkan pada IP. Salah satu layanan MPLS adalah kemampuan membentuk *tunnel* atau *virtual circuit* yang melintasi jaringannya sehingga kemampuan ini membuat MPLS berfungsi sebagai *platform* alami untuk membangun *Virtual Private Network (VPN)* [2]. Dinyatakan IPv4 IPsec menunjukkan performansi yang lebih baik dibandingkan dengan IPv6, saat video dan audio ditransmisikan hasil yang diperoleh untuk *delay* video sebesar 9.89 ms bila dibandingkan IPv6 sebesar 10.47 ms dengan trafik pengganggu sebesar 500 kbps dan untuk *delay* audio sebesar 53.67 ms bila dibandingkan IPv6 sebesar 64.33 ms dengan trafik pengganggu sebesar 500 kbps. Migrasi dari IPv4 ke IPv6 memang masih terkendala namun terdapat metode transisi IPv6 untuk melakukan koneksi terhadap infrastruktur IPv4. Diantaranya teknik 6to4 dan L2TP/IPsec merupakan metode *tunneling* yang mampu melakukan transisi dari IPv4 ke IPv6 selain metode 6VPE [3, 17].

Salah satu fitur yang dapat digunakan pada jaringan MPLS adalah *Virtual Private Network (VPN)*, yang sering disebut sebagai MPLS-VPN. VPN dapat terbentuk dengan adanya fasilitas *tunnel* yang dapat melintasi jaringan MPLS. Fasilitas *tunnel* tersebut bisa membangun sebuah jalur sebuah *site* ke *site* lain secara virtual dan mempunyai tingkat keamanan yang cukup baik karena *site to site connection* tersebut hanya dapat diakses oleh *user* yang berada pada salah satu *site (private connection)*. Dikarenakan semakin menipisnya persediaan IPv4 sedangkan kebutuhan IP yang semakin bertambah, menggunakan IPv6 adalah sebuah solusi yang tepat. Namun peralihan penggunaan protokol IPv4 ke IPv6 tidak bisa serentak begitu saja dilakukan karena sudah banyaknya infrastruktur jaringan IPv4 yang sudah terpasang. Maka dibutuhkan suatu metode untuk memadukan IPv4 dengan IPv6 salah satunya dengan menggunakan metode 6 VPN Provider Edge (6VPE). 6VPE memberikan keuntungan bagi provider yaitu tidak diperlukannya perombakan pada jaringan *backbone* berbasis IPv4 [3]. Sehingga pada penelitian ini akan dibahas analisa perbandingan jaringan IPv4 dan IPv6 (6VPE) pada MPLS VPN dengan menggunakan *server IMS Core*.

2. METODE

2.1 Open IMS Core

IP Multimedia Subsystem (IMS) adalah sebuah arsitektur *framework* yang digunakan untuk mengirimkan layanan *internet protocol multimedia*. Arsitektur

dirancang sesuai dengan standar *wireless* oleh *3rd Generation Partnership Project* (3GPP), yang merupakan bagian visi untuk berkembang diluar GSM [4]. IMS menggunakan protokol *Session Initiation Protocol* (SIP) untuk kemudahan dalam mengintegrasikan layanan IMS dengan internet. Layanan IMS mempunyai jangkauan yang luas karena keunggulan protokol SIP dalam hal fleksibilitas yang digunakan pada jaringan. IMS mendukung *multiple application server* yang memberi layanan telepon PSTN dan *non* telepon [5]. IMS mempunyai beberapa kemampuan sebagai lapisan jaringan *packet switched* dan *circuit switched existing*, antara lain:

1. Memberikan dukungan multimedia berbasis IP dengan dukungan *Quality of Service*.
2. Pensinyalan berdasarkan protokol SIP.
3. Dapat berintegrasi dengan *Public Service Telephone Network* (PSTN).

IMS Core berfungsi untuk menerima permintaan dari *client*, memeriksa apakah *client* tersebut sudah terdaftar dan mempunyai hak untuk mengakses layanan yang diminta atau tidak, meneruskan permintaan dari *client* ke *Application Server* (AS) dan selanjutnya mengembalikan jawaban dari AS ke *client*.

2.2 Teknologi 6VPE

Teknologi 6VPE adalah ekstensi IPv6 berdasarkan pada teknologi MPLS VPN. Teknologi 6VPE menggunakan prinsip kerja BGP MPLS-VPN, yang bertujuan untuk mewujudkan transisi IPv4 ke IPv6. IPv4 dan IPv6 memiliki trafik yang cepat apabila masing-masing *interface* IPv4 dan IPv6 masih dalam *VPN Routing and Forwarding Table* (VRF) yang sesuai [6]. Pada sistem VRF, setiap *router* PE akan mempertahankan tabel *routing* dan *forwarding* ke sirkuit PE/CE dan biasanya sirkuit PE/CE dikaitkan dengan satu tabel VRF. Ketika paket IP tiba di sirkuit terlampir tertentu, alamat IP tujuannya terlihat di tabel terkait untuk menentukan *hop* selanjutnya dari paket itu. Jika paket IP tiba di atas rangkaian lampiran yang tidak terkait dengan VRF apapun, maka alamat tujuan paket adalah mencari di tabel *default forwarding* dan paketnya dialihkan dan diteruskan sesuai dengan tabel *standard forwarding* termasuk paket dari tetangga P atau *router* PE, serta paket dari pelanggan sirkuit lampiran yang belum dikaitkan dengan VRF [7]. Pertukaran pada informasi 6VPE ini dengan cara *reachability* 6VPE yang lain pada MPLS *domain* dengan menggunakan *Multiprotocol* BGP, IPv4 (OSPF atau IS-IS) yang terbagi dengan perangkat P dan PE lainnya dalam *domain*. Tabel *routing* yang dipisah, ditahan untuk penumpukan IPv4 dan IPv6 kemudian hirarki label MPLS ini masuk pada paket pelanggan IPv6 di *edge* LSR. Label luar atau IGP untuk iBGP *next hop* yang didistribusikan oleh LDP, kemudian label bagian dalam atau label VPN untuk awalan IPv6 didistribusikan oleh MP-BGP [8]. Pada Paket pelanggan IPv6 yang masuk dalam *interface* VRF 6VPE ini diteruskan dengan tidak terlihat dalam inti *provider*, inti IPv4 ini berdasarkan pada label MPLS.

2.3 Internet Protocol version 6 (IPv6)

Teknologi IPv6 adalah protokol untuk *next generation Internet*. IPv6 didesain sedemikian rupa untuk jauh melampaui kemampuan IPv4 yang umum digunakan sekarang ini. Alamat IPv6 merupakan sebuah jenis pengalamatan jaringan yang

digunakan di dalam protokol jaringan TCP/IP yang menggunakan protokol IPv6 [9]. Panjang totalnya adalah 128-bit dan secara teoritis dapat mengalami hingga $2^{128} = 3,4 \times 10^{38}$ host komputer di seluruh dunia. Contoh IPv6 adalah 21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A [10]. Seperti halnya IPv4 yang menggunakan *bit-bit* pada tingkat tinggi (*high-order-bit*) sebagai alamat jaringan sementara *bit-bit* pada tingkat rendah (*low-order-bit*) sebagai alamat *host*, dalam IPv6 juga terjadi hal serupa [11]. Dalam IPv6, *bit-bit* pada tingkat tinggi akan digunakan sebagai tanda pengenal jenis alamat IPv6, yang disebut dengan *Format Prefix* (FP). IPv6 tidak memiliki *subnet mask*, namun hanya memiliki *Format Prefix*. Implementasi migrasi IPv4 ke IPv6 saat ini terkendala oleh kesiapan Network engineering (admin jaringan lokal), yang merasa alasan untuk implementasi belum cukup kuat, karena stock IPv4 Publik yang dimiliki masih ada.

2.4 MPLS VPN

MPLS VPN merupakan jaringan VPN berbasis MPLS dimana komunikasi antar pengguna menjadi lebih aman meskipun menggunakan jaringan publik [12]. Beberapa istilah penting pada jaringan MPLS-VPN yaitu CE adalah *Customer Edge, router* di sisi pelanggan, menjalankan *routing* biasa atau *routing* lokal milik perusahaan yang menggunakan VPN. PE adalah *Provider Edge, router* di sisi ISP yang membatasi sisi pelanggan dengan jaringan *core* atau *backbone* milik ISP dan menerapkan MP-BGP dan VRF pada MPLS di *interface* menuju *core*. *Core* adalah *router* milik ISP yang menjadikan *router* di jaringan *core* dengan menerapkan IGP lokal ISP atau OSPF pada semua *interface* MPLS. VRF adalah *Virtual Route Forwarding* yang merupakan tempat mengartikan anggota VPN dengan menggunakan RD yang menjadi *instance* untuk meneruskan *routing* dan *packet* dengan melalui MP-BGP. *Route Distinguisher* (RD), merupakan angka pembeda antara VPN satu dengan VPN lainnya, dengan Format [ASn:nn] atau [ASn:IPadd] *Autonomous System:number number*. *RD Export* adalah RD yang harus di-*export* agar dapat menerima dan digunakan oleh PE yang dituju untuk membentuk jalur VPN yang diinginkan. *RD Import* yaitu untuk menegaskan bahwa RD tertentu digunakan oleh PE tertentu untuk membentuk jalur dari pengekspor ke PE pengimpor.

2.5 Parameter *Quality of Service*

Pada penelitian ini menggunakan parameter pengukuran *Quality of Service* (QoS). *Quality of Service* adalah parameter-parameter yang mempengaruhi kualitas layanan jaringan yang berbasis paket [13]. Parameter-parameter dalam QoS antara lain:

a) *Throughput*

Throughput merupakan kecepatan (rate) transfer data efektif, yang diukur dalam *bit per second* (bps). *Throughput* merupakan jumlah total kedatangan paket yang sukses yang diamati pada tujuan selama interval waktu tertentu dibagi oleh durasi interval waktu tersebut. *Throughput* merupakan kemampuan sebenarnya suatu jaringan dalam melakukan pengiriman data [14].

b) *Delay*

Delay adalah waktu tunda suatu paket yang diakibatkan oleh proses transmisi dari suatu *node* ke *node* lain yang menjadi tujuannya. waktu yang dibutuhkan data untuk menempuh jarak dari asal ke tujuan. *Delay* dapat dipengaruhi oleh jarak, media fisik, kongesti atau juga waktu proses yang lama.

c) *Jitter*

Jitter merupakan variasi *delay* antar paket yang terjadi pada jaringan komputer. *Jitter* menunjukkan banyaknya variasi *delay* pada transmisi data di jaringan. *Delay* antrian pada *router* dan *switch* dapat menyebabkan *jitter*. Besarnya nilai *jitter* akan sangat dipengaruhi oleh variasi beban trafik dan besarnya tumbukan antar paket (*congestion*) yang ada dalam jaringan. Semakin besar nilai *jitter* akan mengakibatkan nilai QoS akan semakin turun. Untuk mendapatkan nilai QoS jaringan yang baik, nilai *jitter* harus dijaga seminimum mungkin [15].

d) *Packet Loss*

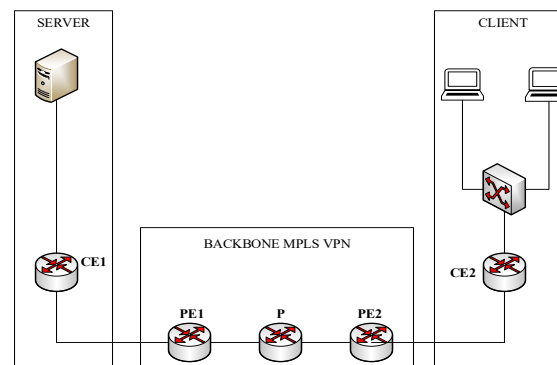
Packet loss didefinisikan sebagai kegagalan transmisi paket mencapai tujuannya. *Packet loss* merupakan suatu parameter yang menggambarkan suatu kondisi yang menunjukkan jumlah total paket yang hilang, dapat terjadi karena *collision* dan *congestion* pada jaringan dan hal ini berpengaruh pada semua aplikasi karena retransmisi akan mengurangi efisiensi jaringan secara keseluruhan meskipun jumlah *bandwidth* cukup tersedia.

2.6 Perancangan dan Pengujian Sistem

Tahapan pertama pada penelitian ini adalah membuat *backbone* MPLS VPN, tahapan kedua membuat *server Open IMS Core* kemudian perancangan sistem untuk menganalisis kebutuhan yang diperlukan seperti mendapatkan QoS.

1) Topologi Jaringan

Topologi jaringan dapat dilihat pada [Gambar 1](#) sebagai berikut.



Gambar 1. Topologi Jaringan

Keterangan:

p = *Provider Router*

pe = *Provider Edge Router*

ce = *Customer Edge Router*

Pada [Gambar 1](#) di atas menjelaskan mengenai proses dan implementasi pengujian layanan *triple play* yang penulis lakukan pada saat simulasi yang mempunyai tiga komponen penting yaitu *Open IMS Core*, *GNS3* dan *Client*.

Pengoperasian GNS3 bertindak sebagai jaringan *backbone* atau *emulator* MPLS VPN, sedangkan *Open IMS Core* akan bertindak sebagai *database user* serta mengatur atau melayani sesi komunikasi yang diminta *user*. *Client* menggunakan bantuan aplikasi *Boghe IMS Client* untuk dapat mengakses sesi komunikasi menggunakan *Open IMS Core*. Pada *Boghe IMS Client* yang menyediakan aplikasi komunikasi *triple play* yang meliputi *voice call*, *video call*, dan *text messaging*. *Boghe IMS Client* juga dapat mengirimkan *file* serta dapat memungkinkan dua komunikasi dijalankan dalam satu waktu. Salah satunya adalah sesi *video call* yang dijalankan bersama dengan *text messaging*.

2) Proses Pengambilan Data

Dari hasil simulasi yang telah disesuaikan dengan skenario dan topologi. Pengujian bertujuan untuk mengetahui performansi dari implementasi server *Open IMS Core* pada jaringan *backbone* MPLS VPN menggunakan GNS3. Adapun parameter - parameter yang akan diukur untuk dianalisis adalah *throughput*, *delay*, *jitter* dan *packet loss*. Pada proses pengambilan data menggunakan aplikasi *wireshark* sebagai aplikasi *network analyzer* di sisi *client* selama sesi komunikasi video, suara dan *text messaging* berlangsung. Proses pengambilan data tersebut untuk mengetahui kualitas jaringan yang didapatkan pada sisi penerima *client*.

Skenario pengambilan data dilakukan dua kali, yang pertama dilakukan dengan semua perangkat hanya memiliki alamat IPv4 dan belum dikonfigurasi 6VPE dengan menggunakan beban trafik yang telah ditentukan. Dan skenario yang kedua, perangkat *client* dan perangkat yang dikonfigurasi 6VPE memiliki alamat IPv6 dengan menggunakan beban trafik yang telah ditentukan. Layanan dan parameter yang diukur untuk kedua skenario sama. Setelah hasil data QoS telah diperoleh, selanjutnya penulis membandingkan dan menganalisis antara skenario pertama dan kedua.

3. HASIL DAN PEMBAHASAN

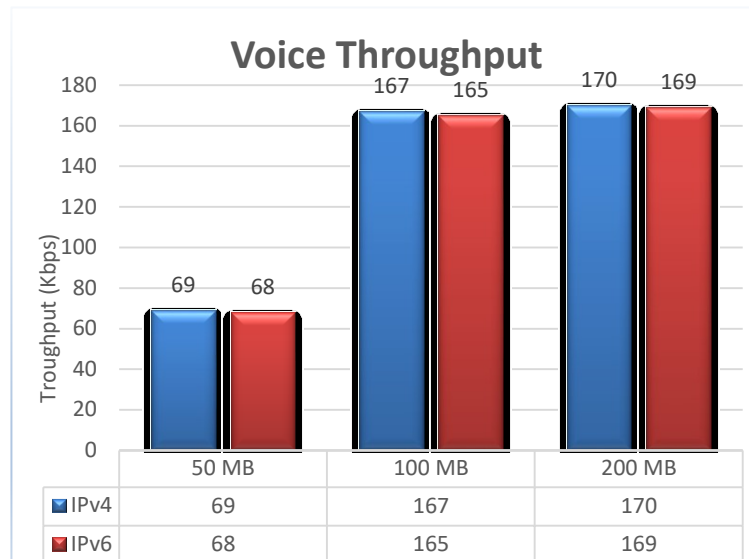
Uji coba yang dilakukan dengan tujuan untuk mengetahui nilai QoS dari simulasi. Apakah nilai QoS masih termasuk kedalam standar ITU-T REC G.1010 atau tidak.

3.1 Analisis *Throughput*

Throughput adalah kecepatan transfer data efektif yang diukur dalam bps (*bit per second*). Namun, dalam penulisan skripsi ini dikonversi menjadi Kbps karena untuk meminimalkan penulisan besar *throughput* yang dihasilkan. Faktor yang menentukan *throughput* adalah besarnya data yang ditransfer, topologi jaringan yang dipakai, jumlah *user* yang aktif serta kualitas perangkat jaringannya. Nilai *throughput* pada layanan *voice call*, *video call* dan *text messaging* ditunjukkan dengan grafik pada [Gambar 2](#), [Gambar 3](#) dan [Gambar 4](#).

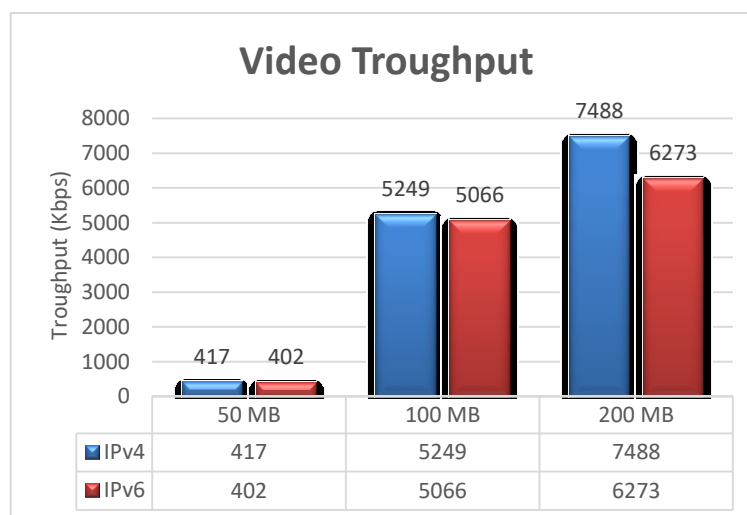
Dapat dilihat pada [Gambar 2](#) bahwa nilai *throughput* IPv4 pada setiap beban lebih besar dibandingkan nilai *throughput* IPv6, hal ini dikarenakan *backbone* IPv4 tidak mengalami proses enkapsulasi dan dekapsulasi terlalu lama

dibandingkan *backbone* IPv6. Jadi performa yang dimiliki *backbone* IPv4 lebih baik daripada *backbone* IPv6.



Gambar 2. Throughput pada Voice Call

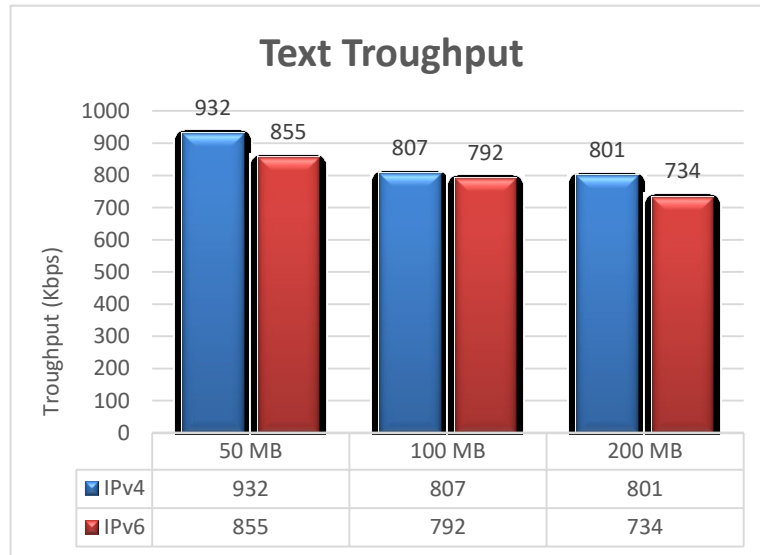
Persamaan layanan *video call* dengan layanan *voice call* yaitu nilai *throughput* yang lebih besar terdapat pada skenario pertama dengan *backbone* IPv4. Jadi pada layanan *video call* performa yang dimiliki *backbone* IPv4 lebih baik daripada *backbone* IPv6. Nilai *throughput* pada layanan *video call* dapat dilihat pada Gambar 3.



Gambar 3. Throughput pada Video Call

Menariknya grafik pada layanan *text messaging* (Gambar 4), dari beban pertama ke beban yang terakhir mempunyai grafik yang menurun pada kedua skenarionya. Hal ini dikarenakan intensitas dalam pengiriman teksnya dan banyaknya karakter dalam satu kali pengiriman teksnya berpengaruh pada besarnya nilai *throughput*. Walaupun beban trafik yang semakin meningkat

namun intensitas dalam pengiriman teksnya sedikit bisa mengakibatkan besar nilai *throughput*-nya menjadi lebih kecil dari sebelumnya.



Gambar 4. *Throughput* pada *Text Messaging*

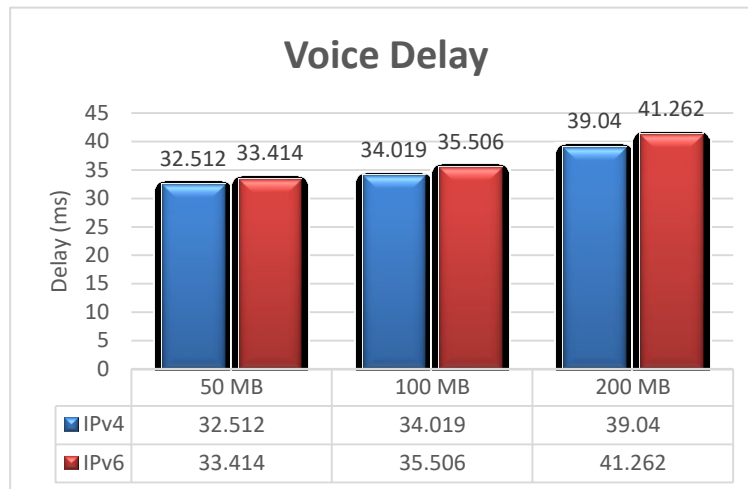
3.2 Analisis *Delay*

Parameter *delay* merupakan banyaknya waktu yang diperlukan sebuah paket untuk melakukan perjalanan dari sumber ke tujuan. *Delay* dapat dipengaruhi oleh jarak, media fisik, dan proses waktu yang lama. Klasifikasi dapat dilihat pada Tabel 1.

Tabel 1. Klasifikasi *Delay* berdasarkan ITU-T REC G.1010

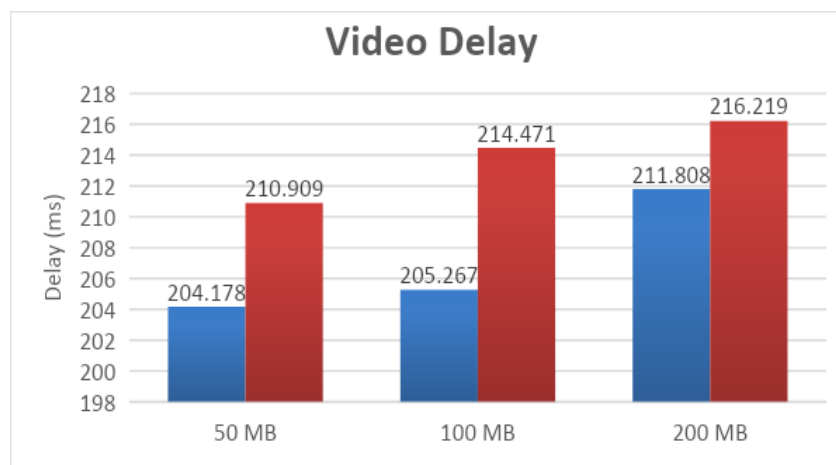
Medium	Application	Delay(ms)
Audio	Conversation Voice	<150 ms preferred <400 ms limit
Video	Videophone	<150 ms preferred <400 ms limit
Data	Bulk Data Transfer/Retrieval	Preferred <15 s Acceptable < 60 s

Nilai *delay* pada *voice call* dapat dilihat pada Gambar 5. Dari hasil data tersebut menunjukkan jika skenario pertama yaitu dengan *backbone* IPv4 lebih baik dibandingkan dengan skenario kedua. Hal ini dikarenakan perbedaan jumlah bit pada IPv4 dan IPv6. IPv4 memiliki 32 bit sedangkan IPv6 mempunyai 128 bit. Semakin banyak jumlah bit semakin lama dalam proses enkapsulasi dan dekapsulasi paket pada saat pengiriman data. Maka paket lebih dahulu sampai pada jumlah bit yang sedikit sehingga nilai *delay*-nya kecil.



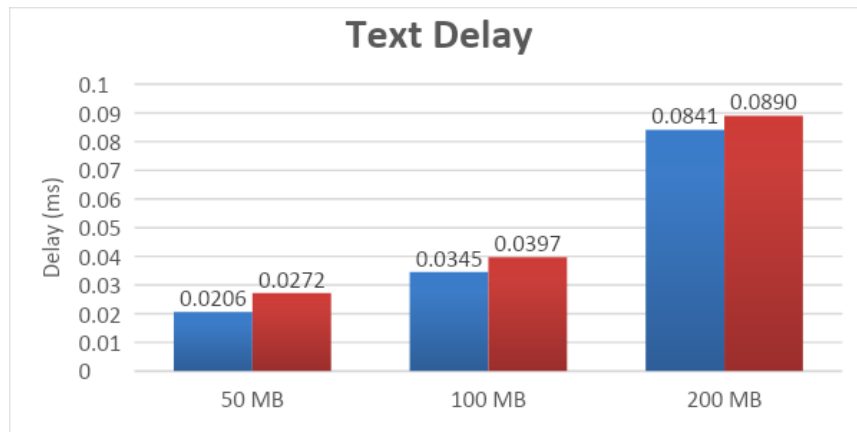
Gambar 5. Delay pada Voice Call

Sama seperti layanan *voice call* pada layanan *video call* (Gambar 6), pada skenario pertama dengan *backbone* IPv4 menghasilkan nilai *delay* yang lebih baik dibandingkan skenario kedua dengan *backbone* IPv6, karena pada *backbone* IPv6 proses enkapsulasi dan dekapsulasinya yang lama sehingga mempunyai nilai *delay* yang lebih tinggi. Hanya saja pada layanan *video call* ini mempunyai nilai *delay* yang cukup besar hingga diatas 200 ms, hal ini dikarenakan ada penambahan beban trafik yang digunakan pada penelitian ini.



Gambar 6 Delay pada Video Call

Gambar 7 merupakan grafik nilai *delay* pada *text messaging*. Selisih antara skenario pertama dan skenario kedua pada setiap beban trafik mempunyai selisih nilai yang tidak jauh, hal ini dikarenakan jumlah karakter dalam teks yang dikirimkan dan intensitas pengiriman teks yang dilakukan hampir sama. Karena banyaknya karakter dalam teks dan intensitas dalam pengiriman teks berpengaruh ke hasil *delay*.



Gambar 7. Delay pada Text Messaging

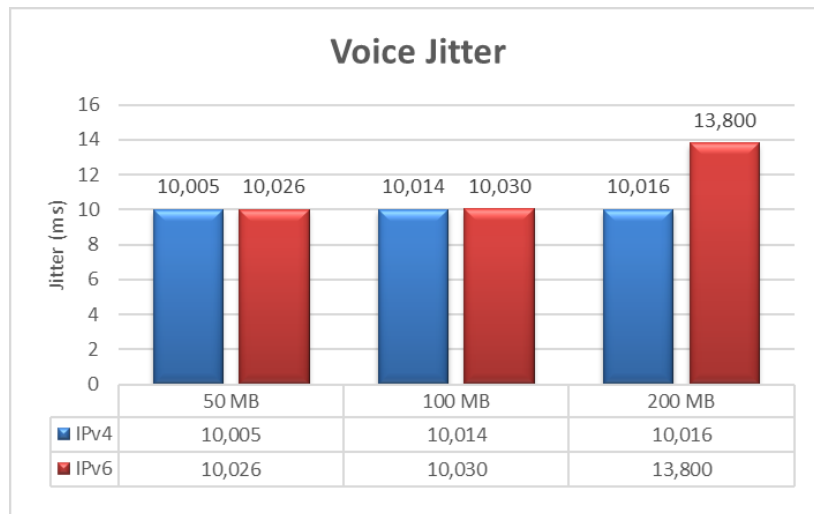
3.3 Analisis Jitter

Hasil pengujian ketiga skenario layanan *triple play* berbasis *Open IMS Core* yaitu pengukuran *jitter* yang bertujuan untuk menganalisis *jitter* yang terjadi pada komunikasi antar *client*. Apabila besarnya nilai *jitter* akan sangat dipengaruhi oleh variasi beban trafik dan besarnya tumbukan antar paket (*congestion*) yang ada dalam jaringan IP. Semakin besar beban trafik di dalam jaringan akan menyebabkan semakin besar pula peluang terjadinya *congestion* dengan demikian nilai *jitter*-nya akan semakin besar. *Jitter* adalah variasi *delay* yang terjadi karena adanya ketidakstabilan pada kondisi jaringan, sehingga pada waktu penerimaan paket di penerima akan mendapatkan hasil yang berbeda – beda. *Jitter* diamati untuk mengetahui performansi QoS dari *server Open IMS Core* yang berjalan pada MPLS – VPN yang berada di GNS3. Pengukuran *jitter* dilakukan dengan melakukan komunikasi layanan *triple play* dengan waktu yang telah ditentukan sesuai skenario. Dalam pengambilan data parameter *jitter* tidak berbeda dengan pengambilan data pada parameter *delay* dimana terdapat pada *stream analyzer rtp* yang kemudian di buka dalam bentuk *file excel*. Hasil data yang telah diamati dapat dilihat klasifikasi *jitter* berdasarkan standarisasi seperti pada Tabel 2.

Tabel 2. Klasifikasi Standar *Jitter* berdasarkan ITU-T REC G.1010

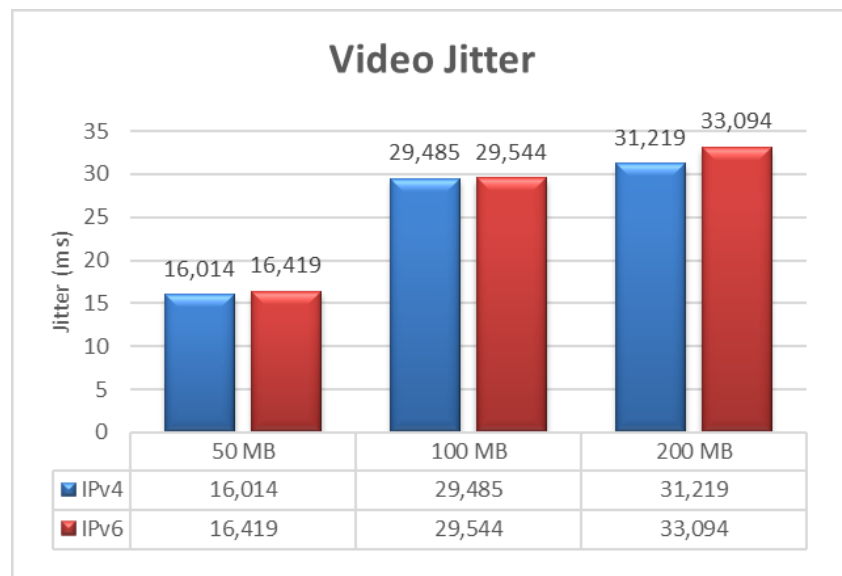
Medium	Application	Jitter (ms)
Audio	Conversion voice	<1 ms
Video	Videophone	<1 ms
Data	Bulk data transfer/retrieval	N.A

Sama halnya dengan *delay*, skenario pertama pada *voice call* memiliki *jitter* yang lebih baik daripada skenario kedua (Gambar 8). Hal ini dikarenakan nilai *jitter* biasanya lebih kecil daripada nilai *delay*. Sehingga nilai *jitter* mengikuti besar nilai *delay* pada parameter sebelumnya. Nilai *jitter* yang didapat termasuk lumayan besar dikarenakan adanya penambahan beban trafik untuk menguji keandalan jaringan.



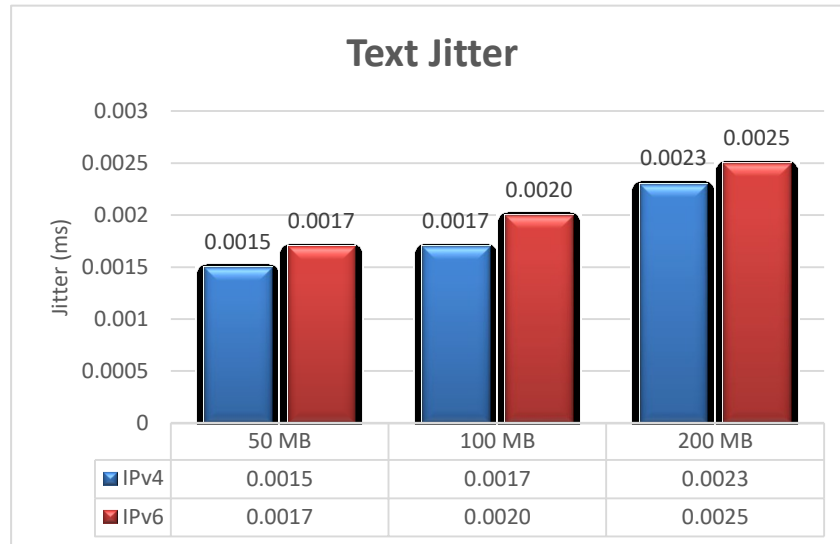
Gambar 8. Jitter pada Voice Call

Seperti halnya *jitter* pada *voice call* selisih antara nilai *jitter* skenario pertama dan skenario kedua tidak terlalu jauh kecuali pada beban 200 MB yang lumayan jauh selisihnya, hal ini dikarenakan pada beban trafik 200 MB dengan *backbone* IPv6 mempunyai bit yang lebih banyak daripada *backbone* IPv4 yang menyebabkan proses enkapsulasi dan dekapsulasi pengiriman paket berlangsung lebih lama sehingga menghasilkan nilai *jitter* yang tinggi. Nilai *jitter* pada video call diperlihatkan pada Gambar 9.



Gambar 9. Jitter pada Video Call

Berbeda pada layanan *voice call* dan *video call*, layanan *text messaging* mempunyai nilai *jitter* yang sangat kecil, hal ini dikarenakan nilai *delay* yang diperoleh pada layanan ini juga kecil. Gambar 10 memperlihatkan nilai *jitter* pada *text messaging*.



Gambar 10. *Jitter* pada *Text Messaging*

3.4 Analisis *Packet Loss*

Hasil pengambilan data pada ketiga layanan *triple play* berbasis *Open IMS Core* adalah *packet loss*. *Packet loss* bertujuan untuk menganalisis paket yang hilang saat komunikasi antar *client*. Jika paket yang dikirim hilang akan menjadi masalah *packet loss*. Hasil data yang telah dihitung dapat diamati dan dilihat pada klasifikasi *packet loss* berdasarkan standarisasi pada Tabel 3.

Tabel 3. Klasifikasi Standar *Packet Loss* berdasarkan ITU-T REC G.1010

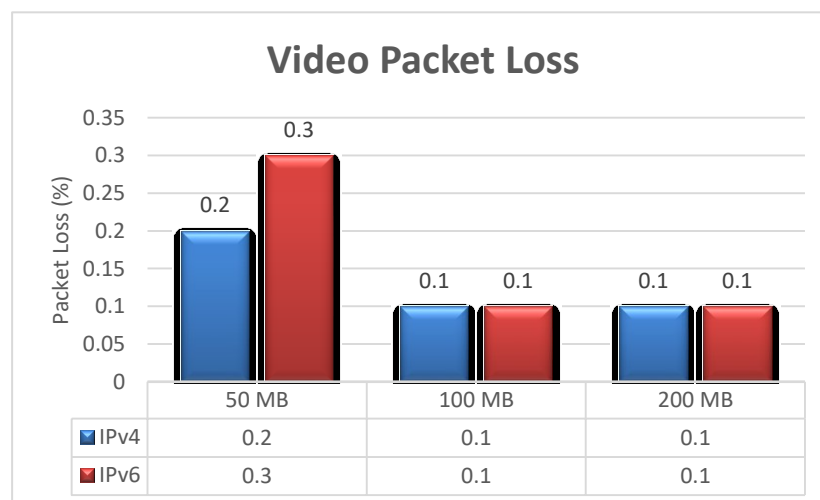
Medium	Application	Packet Loss (%)
Audio	Conversation voice	< 3%
Video	Videophone	< 3%
Data	Bulk data transfer/retrieval	0%

Tabel 4 berikut ini merupakan hasil dari pengambilan data layanan *voice call* menggunakan skenario pertama dan kedua. Pada proses pengambilan data layanan *voice call* selama 1 menit dan sebanyak 3 kali pada setiap beban trafik yang ditentukan, didapatkan hasil rata-rata dari *packet loss* sebesar 0% pada setiap beban trafik dan kedua skenario. Hasil *packet loss* dari kedua skenario mempunyai nilai sebesar 0% menandakan tidak ada paket yang hilang saat komunikasi berlangsung. Pada keterangan standar klasifikasi *packet loss* sendiri dikategorikan sangat baik untuk hasil yang didapat pada penelitian ini.

Tabel 4. Hasil *Packet Loss* pada *Voice Call*

Beban Trafik	IPv4	IPv6
50 MB	0 %	0 %
100 MB	0 %	0 %
200 MB	0 %	0 %

Tidak seperti *packet loss* pada layanan *voice call* yang mempunyai *packet loss* 0%, layanan *video call* sendiri mempunyai nilai *packet loss* pada masing-masing skenario dan beban trafik yang ditentukan. Gambar 11 merupakan grafik nilai *packet loss* pada *video call*. Pada skenario pertama dengan beban 50 MB, 100 MB dan 200 MB berturut-turut mempunyai nilai *packet loss* sebesar 0,2 %, 0,1 % dan 0,1 %. Sedangkan pada skenario kedua dengan beban 50 MB, 100 MB dan 200 MB berturut-turut mempunyai nilai sebesar 0,3 %, 0,1 % dan 0,1 %. Pada setiap skenario mempunyai grafik yang menurun pada setiap beban trafiknya, artinya pada setiap skenario mempunyai kondisi yang membaik pada beban trafik berikutnya. *Packet loss* pada layanan *video call* masih dapat dikatakan baik dalam standar klasifikasi *packet loss* pada Tabel 3.

Gambar 11. *Packet Loss* pada *Video Call*

Layanan *text messaging* dilakukan pengiriman teks antar *client* dengan durasi 1 menit pada kedua skenario dan dengan beban yang telah ditentukan. Sesuai dengan yang ditunjukkan pada Tabel 5 seluruh nilai pada kedua skenario parameter *packet loss* mempunyai nilai sebesar 0 % disetiap beban trafiknya. Berarti pada layanan *text messaging* tidak ada data teks yang hilang dan tidak terkirim pada setiap pengiriman antar *client*-nya. Sehingga *packet loss* dikatakan sangat baik pada standar klasifikasi dalam Tabel 3.

Tabel 5. Hasil *Packet Loss* pada *Video Call*

Beban Trafik	IPv4	IPv6
50 MB	0%	0%
100 MB	0%	0%
200 MB	0%	0%

Keseluruhan perbandingan dapat dilihat pada [Tabel 6](#) untuk nilai QoS pada semua layanan mulai dari teks, *voice* dan *video call*.

Tabel 6. Hasil QoS Pada Semua Layanan

IP		QoS								
		Throughput			Delay			Jitter		
		50 MB	100 MB	200 MB	50 MB	100 MB	200 MB	50 MB	100 MB	200 MB
IPv4	<i>Text</i>	932	807	801	0,0206	0,0345	0,0841	0,0015	0,0017	0,0023
	<i>Voice</i>	69	167	170	32,512	34,019	39,04	10,005	10,014	10,016
	<i>Video</i>	417	5249	7488	204,178	205,267	211,808	16,014	29,485	31,219
IPv6	<i>Text</i>	855	792	734	0,0272	0,0397	0,0890	0,0017	0,0020	0,0025
	<i>Voice</i>	68	165	169	33,414	35,506	41,262	10,026	10,030	13,800
	<i>Video</i>	402	5066	6273	210,909	214,471	216,219	16,419	29,544	33,094

4. KESIMPULAN

Berdasarkan hasil implementasi dan analisis *Open IMS Core* pada jaringan MPLS-VPN maka dapat diperoleh kesimpulan sebagai berikut:

1. Hasil simulasi didapatkan *throughput* terbaik pada layanan *voice call* IPv4 sebesar 7488 kbps, *delay* dan *jitter* terbaik pada layanan *text messaging* IPv4 sebesar 0,0206 ms dan 0,0015 ms, *packet loss* terbaik pada layanan *voice call* dan *text messaging* dengan IPv4 dan IPv6 sebesar 0%. Sedangkan, pada layanan *video call* grafik trafik loss mengalami penurunan dengan nilai 0,2 %, 0,1 % dan 0,1 %.
2. Secara keseluruhan pada penelitian ini, simulasi menggunakan *backbone* IPv4 lebih baik dibandingkan *backbone* IPv6 dari segi hasil data QoS yang diperoleh. Dikarenakan jumlah bit IPv4 lebih sedikit sehingga proses enkapsulasi dan dekapsulasi lebih cepat, dan akhirnya menghasilkan QoS yang lebih baik.

REFERENSI

- [1] Pranindito, Dadiek, Levana Rizki Daenira, and Eko Fajar Cahyadi. "Perancangan NGN Berbasis Open IMS Core Pada Jaringan MPLS VPN." *Seminar Nasional Multi Disiplin Ilmu Unisbank 2017, Semarang, Indonesia, July 2017*. Stikubank University, 2017.
- [2] Daud Billy, S, "Simulasi Dan Analisis Variasi Jumlah Router Bgp Pada Jaringan Mpls-Vpn," Universitas Telkom, 2013.
- [3] A. Dumka, H. L. Mandoria, K. Dumka and A. Anand, "MPLS VPN using IPv4 and IPv6 protocol," 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom), 2015, pp. 1051-1055.
- [4] A. Adilah, "Virtualisasi Jaringan Dengan IP Multimedia Subsystem", Lampung: Universitas Bandar Lampung, 2016.
- [5] E. Cahyadi, R. Cahyani, and A. Hikmaturokhan, "Analisa Karakteristik Teori Antrian pada Jaringan IP Multimedia Subsystem (IMS) Menggunakan OPNET Modeler 14.5", *INFOTEL*, vol. 7, no. 1, pp. 15-22, May 2015, doi: 10.20895/infotel.v7i1.24
- [6] S. Salih, A. Abdalrahman and K. Elsharif, "Performance Evaluation of IPv6 VPN Provider Edge Router," 2017 9th IEEE-GCC Conference and Exhibition (GCCCE), 2017, pp. 1-4, doi: 10.1109/IEEEGCC.2017.8448146
- [7] Li, Jing, Ting Rui Li, and Lin Zhang. "The Practice and Evolution Research of the Enterprise Data Communications Network to IPv6 Technology." In *Advanced Materials Research*, vol. 1079, pp. 802-806. Trans Tech Publications Ltd, 2015.
- [8] Amarullah, Ilham, and Adityas Widjajarto. "Perancangan Jaringan Multiprotocol Label Switching Menggunakan Metode NDLC Untuk Layanan File Transfer Protocol Dan Web Service Universitas Telkom." *eProceedings of Engineering* 4, no. 2, 2017.
- [9] Budiyanto, Setyo, and Ahmad Suhendi Prasetyo. "Studi Analisis Performansi Protokol Routing IS-IS Dan OSPFv3 Pada IPv6 Untuk Layanan Video Streaming." *Jurnal Teknologi Elektro, Universitas Mercu Buana* 5, no. 1, pp. 18-32, 2014, doi: 10.22441/jte.v5i1.759
- [10] G. T. Mahardhika, Analisis Unjuk Kerja Mekanisme Transisi IPv4 ke IPv6, Universitas Sanata Dharma Yogyakarta, 2016.
- [11] Afrizal, A, and Fitriani, F. "Penerapan IPV4 dan IPV6 pada Jaringan yang Terhubung." *Jurnal JTIK (Jurnal Teknologi Informasi dan Komunikasi)* 3, no. 1, pp.13-17, 2019, doi: 10.35870/jtik.v3i1.78
- [12] M. Faiz, "Analisis Transfer Data Menggunakan Metode 6VPE Pada Jaringan MPLS VPN", IT Telkom Purwokerto, 2019.
- [13] M. Rusdan, "Analisis Quality of Service (QoS) Pada Jaringan Wireless (Studi Kasus: Universitas Widyatama)", *Jurnal Sistemik*, 2017.
- [14] Novianti, Triuli, and Anang Widiantoro. "Analisa QOS (Quality of Services) pada Implementasi IPV4 dan IPV6 dengan Teknik Tunneling." *Rekayasa* 9, no. 2, pp. 76-83, 2016, doi: 10.21107/rys.v9i2.3343
- [15] Altoberi, Rafki, Giva Andriana Mutiara, and Muh Fahru Rizal. "Implementasi IMS (IP Multimedia Subsystem) Menggunakan Protokol SIP (Session Initiation Protocol) Pada Jaringan Fakultas Ilmu Terapan." *Jurnal Teknologi Informasi* 2, no. 1, 2014.
- [16] Syafrizal, Melwin, Syamsul Qamar, and Damawan Bayu Aji. "Implementasi Migrasi IPv4 ke IPv6." *Data Manajemen dan Teknologi Informasi (DASI)* 14, no. 1, pp.44-50, 2013.
- [17] P. Ika, Hafidudin dan M. Asep, "Analisis dan Implementasi Perbandingan IPsec IPv4 dengan Ipv6 pada Voip", Universitas Telkom, 2008.