Analisis Perbandingan Performansi Tunneling ISATAP dan Tunneling 6to4 pada Jaringan File Transfer Protocol (FTP)

Reza Ardy Wibowo
Program Studi Teknik Informatika –S1, Fakultas Ilmu Komputer
Universitas Dian Nuswantoro (Udinus) Semarang
URL : http://dinus.ac.id/
Email : ihate4ll@gmail.com

Abstrak

Jaringan komputer saat ini sangat dibutuhkan untuk menghubungkan berbagai instansi pemerintahan, kampus, dan bisnis. Sering kali terjadi permasalahan pada IP version 4 (IPv4) karena pengalamatannya yang semakin terbatas. Salah satu untuk mengatasi kekurangan IP tersebut adalah IP version 6 (IPv6). Yaitu untuk meminimalisir permasalahan kekurangan pengalamtan host. Namun IPv4 dan IPv6 tidak dapat terhubung secara langsung. Dengan adanya perbedaan IPv4 dan IPv6 maka akan diuji protocol *tunneling* untuk membandingkan performasi antara *tunneling* ISATAP dengan *tunneling* 6to4 serta menggunakan FTP sebagai media uji coba. Akan tetapi dari kedua metode tersebut belum diketahui manakah yang lebih optimal. Maka akan diuji untuk menganalisa perbandingan perfoma antara *tunneling* ISATAP dengan *tunneling* 6to4 pada server FTP dalam jaringan Local Area Network (LAN). Setelah diujikan *tunneling* 6to4 lebih optimal dibandingkan *tunneling* ISATAP dikarenakan nilai throughtput pada *tunneling* 6to4 lebih tinggi dibandingkan *tunneling* ISATAP.

Kata kunci : Tunneling, ISATAP, 6to4

I. PENDAHULUAN

1.1. Latar Belakang Masalah

Seiring dengan pertumbuhan industri Internet di Indonesia, baik disadari maupun tidak, kebutuhan akan alamat *Internet Protocol* (IP) juga akan meningkat. Jaringan Internet sangat dibutuhkan untuk menghubungkan berbagai instansi pemerintahan, kampus, dan bahkan untuk bisnis dimana banyak sekali perusahaan yang memerlukan informasi dan data-data dari kantor-kantor lainnya dan dari rekan kerja, afiliasi bisnis, dan konsumen. Dengan meningkatnya perkembangan teknologi komunikasi terutama pada komunikasi berbasis IP saat ini dimungkinkan banyak pengguna IP *version* 4 (IPv4) yang saat ini banyak digunakan oleh pengguna IP mengalami masalah karena pengalamatannya yang semakin terbatas.

Salah satu solusi untuk mengatasi kekurangan alamat IP tersebut ialah penggunaan *Network Address Translation* (NAT) dan *Classless Inter-Domain Routing* (CIDR). Keduanya digunakan dalam rangka penghematan dan efisiensi alamat IP. Namun solusi seperti NAT tidak menyelesaikan persoalan secara utuh. Ada beberapa hambatan jika menggunakan NAT, seperti kesulitan pada aplikasi *Voice over* IP (VoIP), kesulitan pada aplikasi IPSec, lalu lintas Multicast yang tidak dapat melewati NAT dimana jika mesin penyedia NAT rusak maka semua koneksi client dengan internet menjadi terputus. Untuk mengatasi hal tersebut, dikembangkanlah protokol IP versi baru

yaitu IP *version* 6 (IPv6) atau juga disebut IP *Next Generation* (IPng). Keberhasilan IPv4 (protokol IP yang digunakan saat ini) sebagai protokol standar dalam dunia Internet merupakan salah satu dasar pengembangan IPv6. (Kusniyati, 2004)

IPv6 merupakan suatu langkah baru untuk meminimalisir permasalahan kekurangan pengalamatan host yang terjadi karena dengan jumlah tersebut lebih dari cukup untuk menyelesaikan masalah persediaan alamat IP untuk waktu yang sangat panjang. Versi IP baru ini dirancang untuk suatu tindakan *evolusioner* dari IPv4. Secara langsung IPv4 dengan IPv6 tidak dapat dihubungkan, dibutuhkan suatu sistem *tunneling* untuk menghubungkan keduanya.

Selain itu pada IPv6 juga dirancang sedimikan rupa agar memiliki kinerja yang lebih baik dan handal bila dibandingkan dengan IPv4 seperti dalam pengiriman paket data, keamanan, *authentication* dan *Quality of Service* (QoS) yang menjadikan IPv6 terlihat istimewa. Akan tetapi evaluasi kinerja IPv4 dan IPv6 dalam jaringan berbasis *Ethernet* menunjukan bahwa kinerja IPv4 sedikit lebih baik dibandingkan IPv6, dimana IPv4 memiliki *throughput* yang lebih baik dan *One-Way Delay* (OWD) yang lebih rendah. (Gamess, Morales, 2011)

Implementasian IPv6 dilakukan secara bertahap agar mampu atau dapat terhubung dengan IPv4 yang sudah ada tanpa mengganggu jaringan IPv4. Oleh karena itu dipergunakanlah metode transisi dari IPv4 ke IPv6 dengan metode *Dual Stack*, *Tunneling* dan *Translation*. *Tunneling* sendiri merupakan mekanisme proses enkapsulasi suatu *network* yang disebut *payload protocol* kedalam *delivery protocol* yang berbeda. Sedangkan ISATAP dan 6to4 adalah mekanisme yang bertujuan mengirimkan paket IPv6 pada jaringan IPv4.

Dalam perkembangan penggunaan internet juga digunakan salah satu aplikasi *File Transfer Protoco*l (FTP) yang digunakan server untuk mengunggah dan mengunduh konten-konten data melalui jaringan TCP/IP.

Dengan adanya perbedaan IPv4 dan IPv6 ini maka akan di uji *protocol Tunneling* untuk membandingkan performansi antara *Tunneling* ISATAP dengan *Tunneling* 6to4 serta menggunakan aplikasi FTP sebagai media uji coba.

1.2. Rumusan Masalah

Dengan adanya perbedaan dalam pengalamatan IP serta adanya transisi dari IPv4 ke IPv6 maka dapat dirumuskan permasalahan bagaimana perbandingan perfoma antara *tunneling* ISATAP dengan *tunneling* 6to4 pada server FTP dalam jaringan *Local Area Network* (LAN).

1.3. Batasan Masalah

Untuk menghindari penyimpangan dari judul dan tujuan yang sebenarnya serta keterbatasan pengetahuan yang dimiliki penulis, maka penulis membuat ruang lingkup dan batasan masalah :

a. Pengujian dilakukan dalam jaringan sederhanan yang terfokus pada FTP yang menerapkan konfigurasi *tunneling* ISATAP dan *tunneling* 6to4.
b. Pengujian menggunkan rancang jaringan sederhana dengan menggunakan aplikasi GNS3 sebagai *emulator router* serta

percobaan menggunakan media *wired*.

c. Aplikasi tolak ukur dalam percobaan menggunakan aplikasi Wireshark dengan parameter ukur *throughput*, *transfer time*, dan *delay*.

1.4. Tujuan Penelitian

Tujuan dalam penelitian ini adalah untuk menganalisis perbandingan perfoma antara *tunneling* ISATAP dengan *tunneling* 6to4 pada server FTP dalam jaringan *Local Area Network* (LAN).

1.5. Manfaat Penelitian

Adapun manfaat yang didapat diperoleh dengan perbandingan perfomansi *Internet Protcol* ini :

a. Membantu mengetahui implemtasi IP yang optimal untuk diterapkan dalam infrastruktur jaringan yang akan digunakan.
b. Membantu mengukur kualitas jaringan yang dihasilkan dari tiap-tiap konfigurasi.

II. Tinjauan Pustaka

2.1 Penelitian Terkait

Internet telah menghadapi masalah serius dalam beberapa tahun terakhir karena kurangnya ruang alamat IPv4 yang memadai. LACNIC 1 (Latin American and Caribbean Internet Addresses Registry) telah mengumumkan kelelahan alamat IPv4 yang diharapkan pada tahun 2011. Untuk menghadapi masalah ini, beberapa proposal telah dikembangkan dan diimplementasikan. Sebuah solusi parsial dan populer adalah NAT (*Network Address Translation*) yang terdiri dari jaringan dengan menyembunyikan alamat pribadi IPv4 di belakang router NAT - *enabled* dengan beberapa alamat IPv4 publik. NAT memiliki kelemahan karena host di belakang router NAT -*enabled* tidak memiliki konektivitas *end-to -end* yang benar dan tidak dapat berpartisipasi dalam beberapa protokol *internet*.

Solusi lain untuk masalah kekurangan alamat IPv4 publik yang menghadapi *internet* terdiri untuk bermigrasi ke versi baru dari protokol Internet (IPv6), atau koeksistensi antara kedua protokol (IPv4 dan IPv6). IPv6 memperbaiki sejumlah masalah dalam IPv4, seperti keterbatasan jumlah alamat IPv4. IPv6 memiliki alamat 128-bit sedangkan IPv4 memiliki alamat 32-bit. IPv6 juga menambahkan banyak perbaikan ke IPv4 di berbagai bidang seperti kualitas layanan, *routing*, dan jaringan konfigurasi otomatis.

Untuk IPv6 untuk mendapatkan penerimaan, adalah penting bahwa kinerja jaringan aplikasi pengguna tidak mengalami degradasi terlihat. Beberapa karya telah diusulkan untuk membandingkan kinerja IPv4 dan IPv6 dan sebagian besar dari mereka menyimpulkan bahwa kinerja IPv4 adalah sedikit lebih baik daripada yang ditunjukkan oleh IPv6, tetapi perbedaannya tidak signifikan.

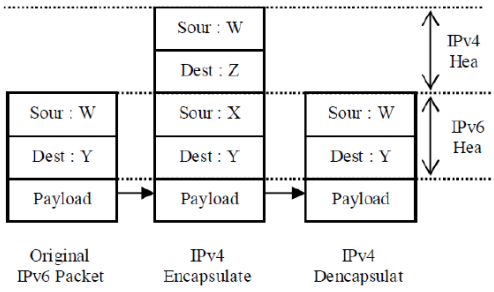
Percobaan kami dan model kami menunjukkan bahwa kinerja IPv4 adalah sedikit lebih baik yang setara dalam IPv6 (IPv4 memiliki throughput yang lebih baik dan OWD rendah). Hal ini disebabkan perbedaan dalam header IP (20 *byte* untuk IPv4 dan 40 *byte* untuk IPv6), bahkan jika IPv4 harus menghitung *checksum* yang tersingkir di IPv6. Dengan menyederhanakan model kami (kasus ideal), kami menyimpulkan kinerja terbaik daripada yang bisa diarsipkan dalam jaringan *Ethernet* untuk koneksi *end-to-end* (koneksi antara komputer dipisahkan oleh beberapa perangkat lapisan-engkau *intermediate*). Jadi model kami memberikan peneliti dan *administrator* jaringan wawasan kinerja terbaik yang dapat diarsipkan dengan jaringan

Ethernet, yang merupakan jaringan dengan sedikit beban. Hasil ini dapat digunakan untuk memodelkan suatu batas atas dari kinerja jaringan dari aplikasi. (Gamess, Morales, 2011)

2.2 Mekanisme *Tunneling*

IPv6 mempunyai format alamat dan *header* yang berbeda dengan IPv4 sehingga tidak bisa melakukan interkoneksi dengan IPv4 secara langsung. Oleh karena itu, diperlukan suatu mekanisme transisi IPv6 agar paket IPv6 dapat dilewatkan pada jaringan IPv4 yang telah ada ataupun sebaliknya. Salah satu contoh mekanisme transisi adalah metode *Tunneling*.

Tunneling protocol merupakan mekasnisme proses enskapsulasi suatu *network protocol* yang disebut *payload protocol* kedalam *delivery protocol* yang berbeda. *Tunneling* IPv6 *over* IPv4 merupakan proses enkapsulasi paket IPv6 dengan *header* IPv4 sehingga paket IPv6 dapat dikirim melalui jaringa IPv4. Selama proses *Tunneling* IPv6 pada IPv4 berlangsung maka akan terjadi proses enkapsulasi dan dekapsulasi paket IPv6 oleh IPv4.



Gambar 2.1 Proses enkapsulasi pada mekanisme transisi *Tunneling*

2.3 *Tunneling* Manual

Tunneling manual dapat didefinisikan sebagai suatu teknik *tunneling* dimana ujung – ujung *interface tunnel* dikonfigurasi secara eksplisit, baik oleh manusia (administrasi jaringan) maupun melalui sebuah layanan otomatis yang disebut *tunnel broker*.

Tunneling manual merupakan suatu teknik *tunneling* yang menggunakan enkapsulasi UDP (*User Datagram Protocol*). Teknik *tunneling manual* dapat dilakukan dengan cara mengatur *dual address* pada tiap-tiap *endpoints route* (*dual stack*). Artinya *router* mampu meneruskan paket baik paket IPv4 ataupun paket IPv6.

Tunneling manual mudah untuk diimplementasikan pada suatu jaringan namun keterbatasannya terdapat pada keamanannya. Selain itu pada teknik *tunneling manual* sangat bergantung pada peran administrator untuk mengkonfigurasinya ketika terjadi perubahan topologi jaringan.

2.4 *Tunneling* Otomatis

Pada *tunneling* otomatis tiap-tiap *interface tunnel* memperoleh alamat atau *prefix* IPv6 berdasarkan format alamat IPv4 yang telah sesuai dengan konfigurasi networknya. Artinya *prefix* alamat IPv6 merupakan identitas unik yang dapat diperoleh dengan cara pengintegrasian alamat IPv4 dengan cara perubahan format bilangan dari *biner* menjadi *hexadecimal.*

Koneksi *tunneling* terjadi secara efektif karena proses *tunneling* hanya bekerja saat dibutuhkan. Artinya ketika paket-paket dengan alamat IPv6 memerlukan jalur untuk mencapai alamat tujuan melalui jaringan IPv4 maka disaat inilah proses *tunneling* secara otomatis akan berjalan dan berakhir saat tidak dibutuhkan. Contoh *tunneling* otomatis yang biasa digunakan adalah *tunneling* 6to4, ISATAP, Teredo dll. (Somad, 2003)

2.5 *Tunneling* ISATAP

ISATAP (*Intra-Site Automatic Tunnel Addressing Protocol*) adalah mekanisme transisi yang bertujuan

mengirimkan paket IPv6 di antara *node dual stack* pada jaringan IPv4. ISATAP menggunakan IPv4 sebagai sebuah *virtual nonbroadcast multiple-access network* (NBMA) data *link layer*, jadi tidak lagi membutuhkan infrastruktur jaringan IPV4 yang mendukung *multicast.* ISATAP mendefenisikan metode untuk membangun *link-local* IPv6 *address* dari sebuah IPv4 *address* dan mekanisme untuk menampilkan *Neighbor Discovery* pada jaringan IPv4. Contoh penerapannya adalah semua *host* yang ingin menggunakan ISATAP pada jaringan IPv4 dapat mengeset virtual IPv6 *network interface.* Alamat *link local* dideskripsikan dengan fe80:0000:0000:0000:0000:5efe: dan diubah ke 32 bit alamat IPv4.

Misalkan *host* 192.0.2.143 akan diubah menjadi alamat IPv6 maka berubah menjadi fe80:0000:0000:0000:0000:5efe:c000:028f sebagai alamat *link local* IPv6 karena IP 192.0.2.143 adalah c000028f dalam notasi *hexadecimal*. Notasi penyederhanaannya adalah fe80::5efe:c000:28f. Karena ISATAP menggunakan IPv4 sebagai sebuah *non multicast/broadcast-capable* atau tidak seperti *Ethernet link layer* maka ICMPv6 Neighbor Discovery tidak bisa dilakukan seperti jaringan pada umumnya. Itulah alasan mengapa ISATAP sedikit lebih kompleks bila dibandingkan dengan 6over4.

2.6 *Tunneling* 6to4

Tunneling 6to4 merupakan salah satu jenis sistem *tunneling* yang memperbolehkan paket dari IPv6 lewat pada jaringan *protocol* IPv4 dengan melakukan proses enkapsulasi dan dekapsulasi paket. Jenis *tunneling* ini dapat digunakan pada *individual host* ataupun *local* IPv6 *network.* Ketika digunakan pada *individual host*, *host* tersebut harus memiliki koneksi ke jaringan IPv4 dan alamat IPv4. *Host* tersebut bertanggung jawab dalam enkapsulasi paket IPv6 yang keluar dan dekapsulasi paket dari 6to4 yang masuk.

Tunneling 6to4 melakukan tiga fungsi utama, yaitu :

a. Menentukan blok dari tempat alamat IPv6 pada *host* atau jaringan yang mempunyai alamat global IPv4.
b. Enkapsulasi paket IPv6 didalam paket IPv4 untuk dikirim melalui jaringan IPv4
c. Mengirimkan trafik data diantara 6to4 dan jaringan IPv6.

2.7 GNS3

GNS3 adalah *software* simulasi jaringan komputer berbasis GUI yang mirip dengan *Cisco Packet Tracer*. Namun pada GNS3 memungkinkan simulasi jaringan yang komplek, karena menggunakan *operating system* asli dari perangkat jaringan seperti cisco dan juniper. Sehingga kita berada kondisi lebih nyata dalam mengkonfigurasi *router* langsung daripada di *Cisco Packet Tracer*. GNS3 adalah alat pelengkap yang sangat baik untuk laboratorium nyata bagi *network engineer*, *administrator* dan orang-orang yang ingin belajar untuk sertifikasi seperti Cisco CCNA, CCNP, CCIP dan CCIE serta Juniper JNCIA, JNCIS dan JNCIE.

Fitur utama dari GNS3 adalah :

a. Desain kualitas tinggi dan topologi jaringan yang kompleks.
b. Mendukung banyak platform Cisco IOS router, IPS, PIX dan ASA firewall, JUNOS.
c. Simulasi *Ethernet* sederhana, ATM dan *Frame Relay switch*.
d. Koneksi jaringan simulasi ke dunia nyata.
e. *Packet capture* menggunakan Wireshark. (Dewannanta, 2013)

2.8 *File Transfer Protocol* (FTP)

Semakin berkembangnya pengguna internet di seluruh dunia menyebabkan semakin berkembang juga aplikasi – aplikasi baru. Salah satu aplikasi yang sering digunakan adalah FTP yang merupakan kepanjangan dari *File Transfer Protocol*. Aplikasi FTP pada internet diterapkan pada jenis – jenis file server seperti *rapidshare*, megaupload, *mediafire*, dan sebagainya. Domain – domain tersebut merupakan *File Server* yang bekerja dengan menggunakan *File Transfer Protocol* (FTP) untuk *uploading* dan *downloading* data. FTP digunakan dalam proses pengiriman data baik *uploading* maupun *dowloading* melalui jaringan TCP/IP.

Protocol FTP merupakan sebuah *protocol* yang digunakan untuk melakukan pemindahan satu atau lebih *file* dari suatu *local host* menuju *remote host* atau *host* tujuan.

FTP memiliki kemampuan yang tidak terbatas pada pemindahan *file* saja, namun juga sangat memungkinkan pengguna untuk dapat melakukan *remote* (pengendalian) secara jarak jauh. Kemampuan transfer data dari satu komputer ke komputer yang dengan sistem operasi yang berbeda merupakan kemampuan lain yang dimiliki oleh FTP. Sebagai contoh, sebuah *local host* yang menggunakan sistem operasi *windows* XP (sistem *file* NTFS) menghubungkan diri dengan sebuah *remote host* yang menggunakan sistem operasi linux Ubuntu (dengan file sistem ex2fs).

Dua hal yang penting dalam FTP adalah FTP Server dan FTP Client :

1. FTP *server* adalah suatu *server* yang menjalankan *software* yang berfungsi untuk memberikan layanan tukar menukar *file* dimana *server* tersebut selalu siap memberikan layanan FTP apabila mendapat permintaan (*request*) dari FTP *client*.
2. FTP *client* adalah komputer yang me-*request* koneksi ke FTP *server* untuk tujuan tukar menukar *file*. Setelah terhubung dengan FTP *server*, maka *client* dapat men-*download*, meng-*upload*, me-*rename*, men-*delete*, dll sesuai dengan *permission* yang diberikan oleh FTP *server*.

Tujuan dari FTP *server* adalah sebagai berikut :

a. Untuk tujuan *sharing* data
b. Untuk menyediakan *indirect* atau *implicit remote computer*
c. Untuk menyediakan tempat penyimpanan bagi *user*
d. Untuk menyediakan *transfer* data yang *reliable* dan *efisien*

III. Metode Penelitian

3.1. Perencanaan

Pada tahap ini penelitian dimulai dari penentuan kebutuhan-kebutuhan dari untuk melakukan analisa perbandingan performansi IP.

a. Prosedur pengambilan atau pengumpulan data.

Dalam pengumpulan data pada penelitian ini dengan menggunakan beberapa metode, yaitu :

1. Eksperimen

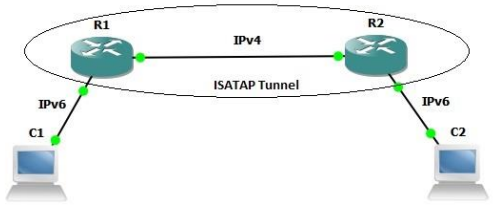
   Merupakan metode pengumpulan data yang diperoleh dengan cara mengambil atau mencatat langsung dari percobaan atau pengukuran berulang-ulang dengan *wireshark*
2. Studi Pustaka

   Studi pustaka merupakan metode pengumpulan data dengan cara mencari informasi melalui buku-buku, jurnal, internet, koran, majalah, dan *literature-literature* lainnya.

3.2. Desain Eksperimen

Pada bagian ini dijelaskan menganai kebutuhan perangkat dan rencana topologi yang akan digunakan dalam eksperimen. Topologi tersebut meliputi jaringan *Tunneling* ISATAP dan *Tunneling* 6to4.

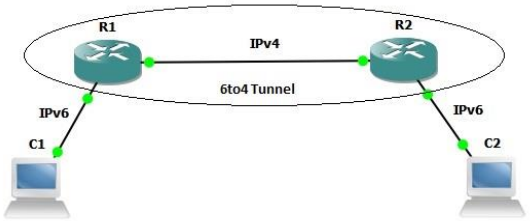
a. Jaringan IPv6 *Tunnel* ISATAP



Gambar 3.1 Konsep Jaringan ISATAP

Pada gambar 3.1 merupakan gambaran konfigurasi ISATAP. Pada C1 yang betugas sebagai PC *server* dengan R1 dan R2 dengan C2 yang bertugas sebagai PC client dihubungkan dengan IPv6, sedangkan pada R1 dan R2 dihubungkan dengan konfigurasi IPv4. Dengan demikian PC *server* tidak dapat melakukan komunikasi data dengan PC *client* karena kedua PC tersebut terpisahkan oleh R1 dan R2 yang memiliki konfigurasi yang berbeda. Oleh sebab itu pada R1 dan R2 perlu menerapkan ISATAP agar komunikasi IPv6 dan IPv4 dapat terjadi.

b. Jaringan IPv6 Tunnel 6to4



Gambar 3.2 Konsep Jaringan 6to4

Pada gambar 3.2 merupakan gambaran konfigurasi 6to4. Pada C1 yang betugas sebagai PC *server* dengan R1 dan R2 dengan C2 yang bertugas sebagai PC *client* dihubungkan dengan IPv6, sedangkan pada R1 dan R2 dihubungkan dengan konfigurasi IPv4. Sama halnya dengan ISATAP PC *server* tidak dapat melakukan komunikasi data dengan PC client karena kedua PC tersebut terpisahkan oleh R1 dan R2 yang memiliki konfigurasi yang berbeda.

3.3. Eksperimen

Eksperimen dilakukan untuk mendapatkan data yang diharapkan, dalam eksperiman ini data ukur diperoleh dengan cara melihat paket data yang melalui jaringan tersebut pada sisi PC *client* dengan menggunakan aplikasi *Wireshark.* Dalam pengujian terdapat 3 paramater uji yang akan digunakan dalam pengambilan data yaitu :

a. Besar *throughput* pada masing – masing konfigurasi.
b. *Transfer time* pada masing – masing konfigurasi.
c. *Delay* pada masing – masing konfigurasi.

Pada uji parameter tersebut, data yang ditampilkan pada wireshark difilter terlebih dahulu sehingga didapatkan data yang diingikan. Tampilan untuk melihat hasil uji coba terdapat label *Packet*, Between first and last packet, Avg. Packet/sec, Avg. Packet size, Bytes, Avg. Bytes/sec, Avg.Mbit/sec. Untuk mendapatkan hasil uji parameter dilihat pada label AVG.Bytes/sec kemudian dikalikan 8, untuk hasil uji parameter transfer time dapat dilihat pada label “Between first and last packet” (Dani, 2013), sedangkan nilai delay diperoleh dari rumus

$$delay\ (\text{sec}) = \frac{Transfer\ Time\ (sec)}{\text{jumlah bit}}$$

Sedangkan *file* yang akan diunduh dari PC *server* memiliki besaran yang berbeda – beda antara 5MB, 10MB, 15MB, dan 20MB untuk mengamati hubungan antara besarnya data dengan parameter uji.

3.4. Hasil Eksperimen

Setelah data dari tiap-tiap konfigurasi dikumpulkan, kemudian akan dilakukan perbangingan antara tunneling ISATAP dan tunneling 6to4.

3.5. Evaluasi

Evaluasi berdasarkan hasil yang didapat dari penelitian melalui parameter yang sudah ditetapkan sebelumnya.

IV. Pembahasan

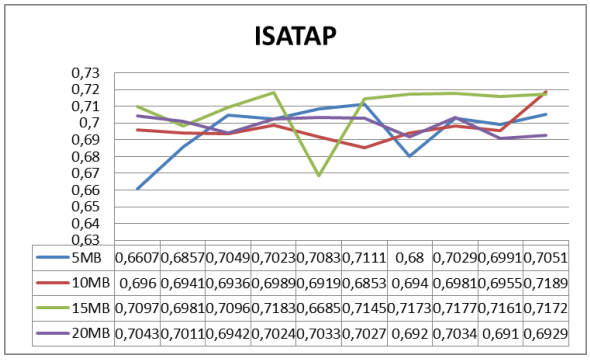
4.1. Analisis *Throughput*

Throughput merupakan kecepatan transfer rata-rata dari suksesnya paket yang dikirim per detiknya, pada umumnya menggunkana satuan bit per second (bps). Pengambilan parameter dilakukan dengan cara men-download file dari sever ke client. Kemudian disaat yang bersamaan pada sisi client melakukan capture data atau penangkapan paket yang masuk melalui interface Ethernet dengan aplikasi wireshark.

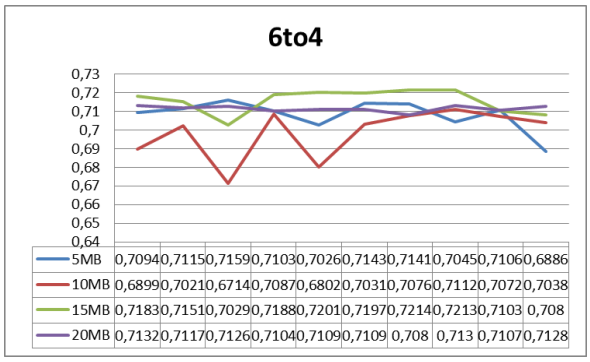
Dikarenakan pada *Ethernet* tidak hanya *file* FTP yang masuk pada *interface*, maka pada aplikasi *wireshark* dilakukan *filtering* agar yang ditampilkan pada aplikasi tersebut hanya bagian-bagian yang diinginkan saja.

4.1.1. Analisis Throughput ISATAP dan 6to4

Dalam pengujian *throughput* ini dilakukan pengambilan data sebanyak 10 kali pada tiap-tiap besaran *file* dan pada masing – masing konfigurasi,kemudian diambil rata-ratanya yang dilakukan pada sisi *client.*



Gambar 4.1 Hasil uji coba *througput* ISATAP



Gambar 4.2 Hasil uji coba *througput* 6to4

Berdasarkan Gambar 4.1 dan 4.2 besarnya *throughput file* dengan kapasitas 5MB pada *tunneling* ISATAP lebih kecil 1,72% dari pada *tunneling* 6to4. Pada besarnya *file* 10MB *tunnel* ISATAP nilai *throughput* lebih kecil 0,31% dari pada *tunnel* 6to4, dan pada besaran *file* besar 15MB dan 20MB nilai *throughput tunnel* ISATAP lebih kecil 0,96% dan 1,78% dari *tunnel* 6to4. Akan tetapi, ketika melihat tabel percobaan *throughput* kedua konfigurasi *tunnel* tersebut ketika ukuran *file* semakin besar, nilai *throughput* tidak mengalami perubahan

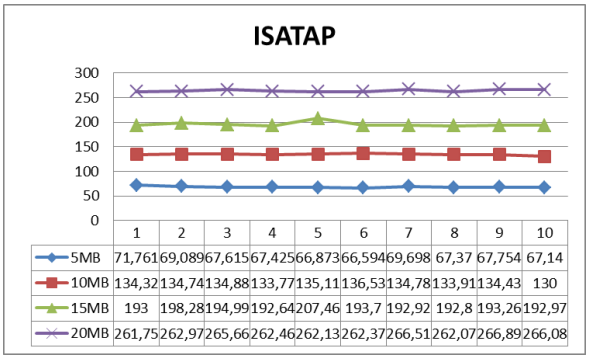
yang signifikan dan cenderung stabil, sehingga besarnya ukuran *file* tidak mempengaruhi pada besarnya nilai *throughput*. Apabila membandingkan kedua jenis konfigurasi, maka dapat disimpulkan bahwa konfigurasi 6to4 memiliki nilai *throughput* yang lebih besar dibandingkan nilai *throughput* pada konfigurasi ISATAP. Hal ini memperlihatkan bahwa jaringan *tunnel* 6to4 lebih baik untuk nilai *throughput* dibangkan dengan ISATAP.

4.2. Analisis *Transfer Time*

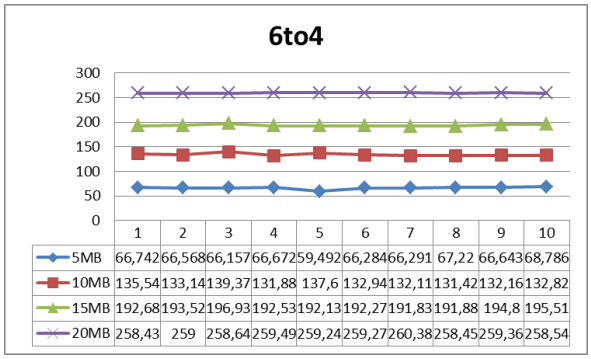
Transfer Time adalah jumlah waktu yang dibutuhkan untuk mengirimkan paket dari *server* ke *client* yang dinyatakan dalam *second.* Pengambilan parameter *transfer time* dilakukan dengan cara *download file* dari *server* ke *client.* Pada saat bersamaan, pada sisi *client* melakukan *capture* data melalui *interface ethernet* dengan aplikasi Wireshark. Dikarenakan pada *Ethernet* tidak hanya *file* FTP yang masuk pada *interface*, maka pada aplikasi wireshark dilakukan *filtering* agar yang ditampilkan pada aplikasi tersebut hanya bagian-bagian yang diingingkan saja.

4.2.1. Analisa *Transfer Time* ISATAP dan 6to4

Dalam pengujian *throughput* ini dilakukan pengambilan data sebanyak 10 kali pada tiap-tiap besaran *file* dan pada masing – masing konfigurasi,kemudian diambil rata-ratanya yang dilakukan pada sisi *client.*



Gambar 4.3 Hasil uji coba *transfer time* ISATAP



Gambar 4.4 Hasil uji coba *transfer time* 6to4

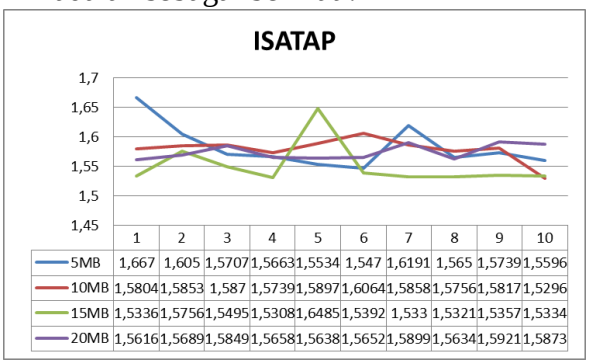
Pada Gambar 4.3 dan 4.4 besarnya nilai transfer time *file* dengan kapasitas 5MB pada *tunnel* 6to4 lebih cepat 3% dari pada nilai *transfer time* pada *tunnel* ISATAP, berbeda dengan *file* berkapasitas 10MB, nilai *transfer time tunnel* 6to4 lebih kecil 0,26% daripada *tunnel* ISATAP. Sedangkan pada *file* berkapsitas 15MB dan 20MB *tunne*l 6to4 lebih cepat 0,91% dan 1,82% dibandingan dengan *tunnel* ISATAP. Apabila kita melihat tabel rata – rata percobaan *transfer time* kedua konfigurasi *tunnel* tersebut terdapat pengaruh kapasitas data terhadap nilai *transfer time*. Semakin besar kapasitas *file*, semakin besar pula nilai dari *transfer time*. Apabila membandingkan kedua jenis konfigurasi, maka dapat disimpulkan bahwa konfigurasi 6to4 memiliki nilai *transfer time* yang lebih kecil dibandingkan nilai *transfer time* pada konfigurasi ISATAP. Hal ini memperlihatkan bahwa jaringan tunnel

6to4 lebih baik untuk nilai *transfer time* dibangkan dengan ISATAP.

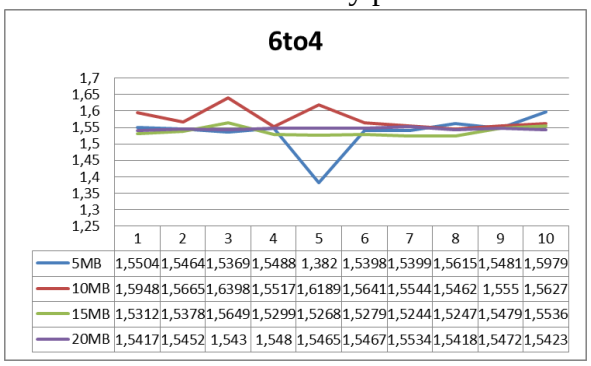
4.3. Analisis Delay

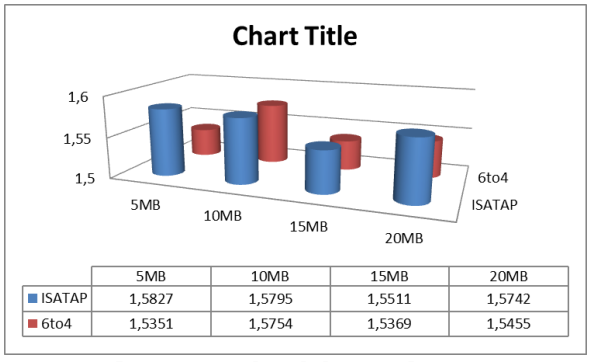
Delay adalah waktu tunda dari waktu yang sebenarnya dari suksesnya seluruh paket yang diterima. Parameter *delay* dihitung dengan cara membagi nilai *transfer time* dengan jumlah bit data.

Hasil pengambilan data secara keseluruhan untuk parameter *delay* adalah sebagai berikut :



Gambar 4.5 Nilai delay pada ISATAP





Gambar 4.6 Nilai delay pada 6to4

Gambar 4.7 Perbandingan rata – rata ISATAP dan 6to4

Dari Grafik 4.9 dan Grafik 4.10 dapat dilihat bahwa semakin tinggi ukuran *file* tidak memperngaruhi perubahan *delay* yang signifikan, dan cenderung stabil sehingga perbedaan ukuran *file* tidak mempengaruhi besarnya nilai *delay*. Dari Grafik 4.11 juga dapat dilihat perbedaan nilai *delay* pada *file* berkapsitas 5MB pada *tunnel* ISATAP lebih besar 3% dibandingkan dengan *tunnel* 6to4, dan pada *file* berkapasitas 10MB, nilai *delay tunnel* ISATAP hanya terpaut 0,28%. Sedangkan pada *file* berkapasitas 15MB dan 20MB nilai *delay tunnel* 6to4 lebih kecil 0,91% dan 0,82%. Secara keseluruhan nilai *delay* terkecil dimiliki oleh *tunnel* 6to4.

V. Kesimpulan & Saran

5.1. Kesimpulan

Setelah dilakukan percobaan terhadap konfigurasi *tunnel* ISATAP dan *tunnel* 6to4, maka dapat disimpulkan bahwa :

1. Parameter *througput* pada *tunnel* ISATAP dan *tunnel* 6to4 diketahui bahwa *throughput* 6to4 lebih besar 1,19% dari *throughput* ISATAP.
2. Parametet *transfer time* pada *tunnel* ISATAP dan *tunnel* 6to4 deketahui bahwa nilai *transfer time* pada ISATAP lebih tinggi 1,36% dari nilai *transfer time* 6to4.
3. Parameter *delay* pada *tunnel* ISATAP dan *tunnel* 6to4 diketahui bahwa *tunnel* 6to4 memiliki nilai delay lebih kecil 1,50% dari *delay* ISATAP.
4. Pemanfaatan *tunneling* memperlama proses pengiriman data dari *server* ke *client* yang dapat dilihat dari besarnya nilai *delay* pada hasil uji coba dikarenakan proses enkapsulasi dan dekapsulasi.

5.2. Saran

Hal – hal yang dapat dilakukan selanjutnya untuk leboh menyempurnakan penelitian dalam tugas akhir ini adalah :

1. Penggunaan *router* yang sebenarnya dalam penerapan sistem *tunneling*, agar dapat dihasilkan nilai yang optimal.
2. Penambahan sistem manajemen *bandwidth* untuk mengetahui seberapa besar pengaruh manajemen *bandwidth* pada sistem *tunneling*.
3. Pengujian sistem *tunneling* dapat dilakukan pada jaringan yang lebih besar dan meiliki struktur yang lebih kompleks agar dapat dilakukan penelitian lebih lanjut.
4. Menggunakan sistem *tunnel* yang lain sebagai perbandingan yang lebih jelas pada masing – masing sistem *tunneling*.

Daftar Pusataka

[1] Sopandi, Dede. (2008). Instalasi dan Konfigurasi Jaringan Komputer. Bandung:Informatika.

[2] Linto Herlambang, M., (2009). Membangun Sharing Koneksi Internet di Windows,Mikrotik, Linux, dan OpenBSD. Yogyakarta : Andi

[3] Sofana, Iwan. (2011). Teori dan Modul Praktikum Jaringan Komputer. Bandung : Modula

[4] Introduction to IP Version 6, Microsoft Corporation’s, February 2008.

[5] Somad, Wahidi. (2003). Interkoneksi IPv6 dan IPv4 dengan Mekanisme Automatic Tunneling, IlmuKomputer.com

[6] Wiryawan, I Made. (2007). File Transfer Protokol

[7] Harnu Kusniyati. 2004. Mekanisme Transisi IPv4 ke IPv6 Dengan Menggunakan Automatic Tunneling. Jurnal STEKOM

[8] Mardianto Basuki, Jusak, Anjik Sukmaaji. (2012). Implementasi Integrasi Jaringan IPv4 dan Jaringan IPv6 Pada Local Area Network (LAN) dengan Sistem Tunneling. Jurnal Universitas Mercu Buana

[9] Eric Gamess, Neudith Morales. (2011). Modeling IPv4 and IPv6 Performance in Ethernet Networks. International Jurnal of Computer and Electrical Enginering

[10] Dewannanta, Didha. (2013). Mengenal Software Simulator Jaringan Komputer GNS3. IlmuKomputer.com

[11] Dani, Mohamad. (2013). Modul Pengukuran QoS Jaringan Nirkabel. Bandung : Politeknik Telkom Bandung