



UNIVERSITAS INDONESIA

**ANALISA PERFORMANSI *FILE TRANSFER PROTOCOL*
PADA JARINGAN IPv6
DENGAN TUNNELING 6to4 DAN ISATAP**

SKRIPSI

**MUAMAR PUTRA PERDANA
0706199672**

**FAKULTAS TEKNIK
PROGRAM STUDI TEKNIK ELEKTRO
DEPOK
JUNI 2009**



UNIVERSITAS INDONESIA

**ANALISA PERFORMANSI *FILE TRANSFER PROTOCOL*
PADA JARINGAN IPv6
DENGAN TUNNELING 6to4 DAN ISATAP**

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Teknik

**MUAMAR PUTRA PERDANA
0706199672**

**FAKULTAS TEKNIK
PROGRAM STUDI TEKNIK ELEKTRO
DEPOK
JUNI 2009**

HALAMAN PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya saya sendiri,
dan semua sumber baik yang dikutip maupun dirujuk
telah saya nyatakan dengan benar.

Nama : Muamar Putra Perdana

NPM : 0706199672

Tanda Tangan :

Tanggal : 17 Juni 2009

HALAMAN PENGESAHAN

Skripsi ini diajukan oleh :

Nama : Muamar Putra Perdana

NPM : 0706199672

Program Studi : Teknik Elektro

Judul Skripsi : Analisa Performansi File Transfer Protocol Pada Jaringan IPv6 Dengan Tunneling 6to4 dan ISATAP.

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Teknik pada Program Studi Teknik Elektro, Fakultas Teknik, Universitas Indonesia

DEWAN PENGUJI

Pembimbing : Ir. A Endang Sriningsih MT., Si (.....)
NIP. 130781318

Penguji : Dr. Ir. Anak Agung Putri Ratna M.Eng. (.....)
NIP. 131865234

Penguji : Prima Dewi Purnamasari ST., MT., MSc. (.....)
NIP. 040803035

Ditetapkan di : Depok

Tanggal : 30 Juni 2009

KATA PENGANTAR

Puji syukur saya panjatkan kepada Tuhan Yang Maha Esa, karena atas berkat dan rahmat-Nya, saya dapat menyelesaikan skripsi ini. Penulisan skripsi ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Sarjana Teknik Jurusan Teknik Elektro pada Fakultas Teknik Universitas Indonesia. Saya menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan skripsi ini, sangatlah sulit bagi saya untuk menyelesaikan skripsi ini. Oleh karena itu, saya mengucapkan terima kasih kepada :

1. Ir. A Endang Sriningsih MT. , Si, selaku dosen pembimbing yang telah menyediakan waktu, tenaga, dan pikiran untuk mengarahkan saya dalam penyusunan skripsi ini.
2. Orang tua dan keluarga saya yang telah memberikan bantuan dukungan moral.
3. Sahabat yang telah banyak membantu saya dalam menyelesaikan skripsi ini.

Akhir kata, saya berharap Tuhan Yang Maha Esa berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga skripsi ini membawa manfaat bagi pengembangan ilmu.

Depok, 11 Juni 2009

Penulis

**HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI
TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS**

Sebagai civitas akademik Universitas Indonesia, saya yang bertanda tangan di bawah ini:

Nama : Muamar Putra Perdana
NPM : 0706199672
Program Studi : Teknik Elektro
Departemen : Teknik Elektro
Fakultas : Teknik
Jenis karya : Skripsi

demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Indonesia **Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty-Free Right*)** atas karya ilmiah saya yang berjudul :

ANALISA PERFORMANSI *FILE TRANSFER PROTOCOL* PADA JARINGAN
IPv6 DENGAN TUNNELING 6to4 DAN ISATAP

beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Indonesia berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan memublikasikan skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Depok
Pada tanggal : 16 Juni 1009
Yang menyatakan

(Muamar Putra Perdana)

ABSTRAK

Nama : Muamar Putra Perdana
Program Studi : Teknik Elektro
Judul : Analisa Performansi *File Transfer Protocol* pada Jaringan IPv6 dengan Tunneling 6to4 dan ISATAP.

Dalam perkembangan bidang telekomunikasi khususnya *Internet Protocol* (IP) telah memunculkan jenis protokol internet baru yang dinamakan IPv6. Kemunculan protokol internet baru IPv6 diharapkan memiliki performansi lebih baik daripada pendahulunya yaitu IPv4. Tujuan dari penulisan skripsi ini adalah untuk menganalisa dan membandingkan performa dari jaringan protokol IPv6, IPv4 dan IPv6 menggunakan *tunneling* 6to4 dengan ISATAP yang diterapkan pada aplikasi FTP (*File Transfer Protocol*).

Proses pengambilan data menggunakan jaringan lokal berskala kecil. Dalam pengujian digunakan dua buah *notebook* yang diterapkan sebagai *server* dan *client* serta 2 buah router sebagai jaringan *intermediate*. Pengambilan data dilakukan dengan cara men-*download* file dengan ukuran yang berbeda - beda dari *server* ke *client*. Parameter uji coba yang dibandingkan adalah *delay*, *transfer time* dan *throughput*.

Kesimpulan yang didapatkan bahwa konfigurasi IPv4 murni memiliki nilai *throughput*, *delay* dan *transfer time* paling baik dibandingkan konfigurasi lainnya. Konfigurasi IPv6 murni memiliki nilai *throughput* lebih kecil 73.39% dari konfigurasi IPv4 murni, konfigurasi 6to4 lebih kecil 85.66% dari IPv4 murni, sedangkan konfigurasi ISATAP lebih kecil 85.51% dari IPv4 murni. Untuk parameter *transfer time* dan *delay*, IPv4 murni lebih kecil 73.94% dari IPv6 murni, lebih kecil 85.93% dari 6to4 dan lebih kecil 85.81% dari ISATAP. Konfigurasi ISATAP memiliki nilai *throughput* lebih besar 1.1% dari 6to4. Konfigurasi ISATAP memiliki nilai *delay* dan *transfer time* lebih kecil 0.85% dari 6to4. Perbedaan panjang *header* pada IPv6 dan IPv4 mempengaruhi besarnya nilai *delay*. Proses enkapsulasi dan dekapulasi paket pada ISATAP lebih baik daripada 6to4.

Kata Kunci :

IPv6, *File Transfer Protocol*, *Tunneling*, *throughput*, *delay*, *transfer time*

ABSTRACT

Name : Muamar Putra Perdana
Study Program: Electrical Engineering
Title : Performance Analysis of File Transfer Protocol in IPv6 Network with 6to4 Tunneling and ISATAP Tunneling.

In growth of telecommunications specially Internet Protocol (IP) have developed the new internet protocol named IPv6. Apparition of new internet protocol is expected to have performance better than IPv4. Intention of this last project is to analyse and compare a performance from IPv4 network, IPv6 network, IPv6 use 6to4 tunneling and ISATAP tunneling which applied at FTP (File Transfer Protocol).

Experiment process use the small network. In examination is used two notebook which applied as server and client. It use two router as intermediate network. Experiment which The different size of file is downloaded by client from server. The parameter which is compared delay, transfer time and throughput.

The conclusion that IPv4 network have the value of throughput, delay and transfer time is the best from the other configuration. Configuration IPv6 network have the value of throughput smaller 73.39% than IPv4 network, configuraton of 6to4 smaller 85.66% than IPv4 network and configuration ISATAP smaller 85.51% from IPv4 network. For parameter of transfer time and delay, IPv4 network quicker 73.94% than IPv6 network, quicker 85.93% than 6to4 tunneling and quicker 85.81% than ISATAP tunneling. Configuration ISATAP tunneling have the value of throughput bigger 1.1% than 6to4 tunneling. Configuration ISATAP tunneling have the value of delay and transfer time smaller 0.85% than 6to4 tunneling. Difference of length header at IPv6 and IPv4 influence the value of delay. Encapsulation ans decapsulation process in ISATAP tunneling better than 6to4 tunneling.

Key Words :

IPv6, *File Transfer Protocol, Tunneling, throughput, delay, transfer time*

DAFTAR ISI

HALAMAN JUDUL	i
PERNYATAAN ORISINALITAS	ii
LEMBAR PENGESAHAN	iii
KATA PENGANTAR	iv
HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI	v
ABSTRAK	vi
ABSTRACT	vii
DAFTAR ISI	viii
DAFTAR GAMBAR	x
DAFTAR TABEL	xi
DAFTAR SINGKATAN	xii
1. PENDAHULUAN	1
1.1. Latar Belakang	1
1.2. Tujuan	2
1.3. Pembatasan Masalah	2
1.4. Metodologi Penelitian	2
1.5. Sistematika Penulisan	3
2. IPv6	4
2.1. Defini dan Latar Belakang	4
2.2. Spesifikasi dan Struktur IPv6	4
2.2.1. Struktur IPv6	5
2.2.2. Pengalamatan IPv6	7
2.2.3. Perbedaan IPv6 dan IPv4	9
2.2.4. Fitur – Fitur IPv6	10
2.3. Metode <i>Tunneling</i>	11
2.3.1. <i>Tunneling</i> 6to4	12
2.3.2. <i>Tunneling</i> ISATAP	14
2.4. <i>File Transfer Protocol</i> (FTP)	15
2.4.1. <i>Anonymous</i>	16
2.4.2. <i>User legal (Authenticated User)</i>	16
3. KONFIGURASI JARINGAN DAN METODE PENGAMBILAN DATA	18
3.1. Topologi Jaringan	18
3.2. Perangkat Lunak yang digunakan	19
3.2.1. Perangkat Lunak FTP	19
3.2.2. Wireshark	21
3.3. Konfigurasi Jaringan	21
3.3.1. Konfigurasi IPv4 Murni	21
3.3.2. Konfigurasi IPv6 Murni	22
3.3.3. Konfigurasi <i>Tunneling</i> 6to4	23
3.3.4. Konfigurasi <i>Tunneling</i> ISATAP	24
3.4. Konfigurasi IPv6 pada <i>Server</i> dan <i>Client</i>	25
3.5. Metodologi Pengambilan Data	29

4. ANALISA DATA	31
4.1. Analisa Topologi dan Konfigurasi Jaringan	31
4.1.1. Konfigurasi IPv4 Murni	31
4.1.2. Konfigurasi IPv6 Murni	32
4.1.3. Konfigurasi <i>Tunneling</i> 6to4	32
4.1.4. Konfigurasi <i>Tunneling</i> ISATAP	33
4.2. Analisa Performa Jaringan pada FTP	34
4.2.1. Analisa <i>Throughput</i>	36
4.2.2. Analisa <i>Transfer Time</i>	39
4.2.3. Analisa <i>Delay</i>	43
5. KESIMPULAN	46
DAFTAR REFERENSI	47
DAFTAR LAMPIRAN	48
LAMPIRAN 1. Konfigurasi Router pada Jaringan IPv4 Murni	48
LAMPIRAN 2. Konfigurasi Router pada Jaringan IPv6 Murni	50
LAMPIRAN 3. Konfigurasi Router pada Jaringan Tunneling 6to4	52
LAMPIRAN 4. Konfigurasi Router pada Jaringan Tunneling ISATAP	55
LAMPIRAN 5. Hasil Capture Wireshark Konfigurasi IPv4 Murni	58
LAMPIRAN 6. Hasil Capture Wireshark Konfigurasi IPv6 Murni	59
LAMPIRAN 7. Hasil Capture Wireshark Konfigurasi Tunneling 6to4	60
LAMPIRAN 8. Hasil Capture Wireshark Konfigurasi Tunneling ISATAP ...	61
LAMPIRAN 9. Data Hasil Uji Coba Konfigurasi IPv4 Murni	62
LAMPIRAN 10. Data Hasil Uji Coba Konfigurasi IPv6 Murni	63
LAMPIRAN 11. Data Hasil Uji Coba Konfigurasi <i>Tunneling</i> 6to4	64
LAMPIRAN 12. Data Hasil Uji Coba Konfigurasi <i>Tunneling</i> ISATAP	65

DAFTAR GAMBAR

Gambar 2.1	Struktur IPv6	5
Gambar 2.2	Format Header IPv6	5
Gambar 2.3	Proses Tunneling	12
Gambar 2.4	Contoh Jaringan <i>Tunneling</i> 6to4	13
Gambar 2.5	Format Alamat 6to4	13
Gambar 2.6	Contoh Jaringan <i>Tunneling</i> ISATAP	14
Gambar 2.7	Format Alamat ISATAP	15
Gambar 3.1	Topologi Global	18
Gambar 3.2	Tampilan Xlight FTP server	20
Gambar 3.3	Tampilan FTP client	20
Gambar 3.4	Tampilan Wireshark	21
Gambar 3.5	Konfigurasi IPv4 Murni	22
Gambar 3.6	Konfigurasi IPv6 Murni	23
Gambar 3.7	Konfigurasi <i>Tunneling</i> 6to4	24
Gambar 3.8	Konfigurasi Tunneling ISATAP	25
Gambar 3.9	Tampilan <i>Local Area Connection Properties</i>	26
Gambar 3.10	<i>Install IPv6</i>	26
Gambar 3.11	<i>Local Area Connection Properties</i> sudah ter- <i>install</i> IPv6	27
Gambar 3.12	Tampilan Konfigurasi IPv6 pada setiap <i>Interface</i>	28
Gambar 3.13	Penambahan Alamat IPv6 pada Sistem Operasi Windows	28
Gambar 3.14	<i>Routing Gateway</i>	29
Gambar 4.1	Tampilan <i>Traceroute</i> Jaringan IPv4 Murni	31
Gambar 4.2	Tampilan <i>Traceroute</i> Jaringan IPv6 Murni	32
Gambar 4.3	Tampilan <i>Traceroute</i> Jaringan <i>Tunneling</i> 6to4	33
Gambar 4.4	Tampilan <i>Traceroute</i> Jaringan <i>Tunneling</i> ISATAP	34
Gambar 4.5	Tampilan FTP <i>Client</i> setelah terkoneksi dengan <i>Server</i>	35
Gambar 4.6	<i>Throughput</i> pada <i>Summary</i> Wireshark	36
Gambar 4.7	Diagram Perbandingan Nilai <i>Throughput</i>	38
Gambar 4.8	Grafik Perbandingan Nilai <i>Throughput</i> ISATAP dan 6to4	38
Gambar 4.9	<i>Transfer Time</i> pada <i>Summary</i> Wireshark	39
Gambar 4.10	Diagram Perbandingan <i>Transfer Time</i>	40
Gambar 4.11	Grafik Perbandingan <i>Transfer Time</i> ISATAP dan 6to4 File Size 16MB	41
Gambar 4.12	Grafik Perbandingan <i>Transfer Time</i> ISATAP dan 6to4 File Size 32MB	41
Gambar 4.13	Grafik Perbandingan <i>Transfer Time</i> ISATAP dan 6to4 File Size 64MB	42
Gambar 4.14	Grafik Perbandingan <i>Transfer Time</i> ISATAP dan 6to4 File Size 128MB	42
Gambar 4.15	Grafik Perbandingan <i>Transfer Time</i> ISATAP dan 6to4 File Size 256MB	43
Gambar 4.16	Diagram Perbandingan Nilai <i>Delay</i>	44
Gambar 4.17	Grafik Perbandingan Nilai <i>Delay</i> antara ISATAP dan 6to4	45

DAFTAR TABEL

Tabel 2.1	Perbandingan IPv4 dan IPv6	9
Tabel 2.2	Assigned Port	15
Tabel 4.1	File Uji Coba	35
Tabel 4.2	Data Rata – Rata <i>Throughput</i>	37
Tabel 4.3	Data Rata – Rata <i>TransferTime</i>	39
Tabel 4.4	Data Rata – Rata Perhitungan <i>Delay</i>	43



DAFTAR SINGKATAN

ARP	Address Resolution Protocol
DHCP	Dynamic Host Configuration Protocol
FTP	File Transfer Protocol
IANA	Internet Assign Numbers Authority
ICMPv6	Internet Control Message Protocol version 6
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IPng	Internet Protocol Next Generation
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol
NSAP	Network Service Access Point
MLD	Multicast Listener Discovery
QoS	Quality of Service
RIP	Routing Information Protocol
RIPng	Routing Information Protocol Next Generation
TCP/IP	Transmission Control Protocol / Internet Protocol

BAB 1 PENDAHULUAN

1.1. LATAR BELAKANG

Dalam bidang komunikasi data tidak terlepas dari adanya *internet protocol* atau disingkat dengan IP. *Internet protocol* merupakan protokol lapisan jaringan yang digunakan oleh protokol TCP/IP untuk melakukan pengalamatan dan *routing* paket data antar *host* di jaringan komputer berbasis TCP/IP. *Internet protocol* yang sering digunakan pada saat ini adalah IP versi 4 (IPv4).

Dengan perkembangan teknologi internet yang begitu pesat menyebabkan semakin bertambahnya pengguna internet di seluruh dunia, karena hal ini IP versi 4 (IPv4) diperkirakan tidak mampu untuk memenuhi kebutuhan dari alamat IP, sehingga muncul sistem pengalamatan baru yang dinamakan IP versi 6 (IPv6) yang mempunyai kapasitas lebih banyak dibandingkan dengan IPv4. Tujuan utama pengembangan protokol IPv6 adalah untuk memenuhi kebutuhan alamat IP untuk jangka panjang sekaligus menyempurnakan kekurangan yang terdapat pada protokol IPv4.

Protokol IPv6 yang diluncurkan sejak tahun 1994 kini telah mulai diarahkan untuk menggantikan kedudukan protokol IPv4 sebagai protokol transport di internet. Hal ini dikarenakan alokasi alamat IPv4 yang tersedia di dunia sangat terbatas, sehingga hal ini menjadi hambatan bagi yang ingin terhubung ke internet dengan menggunakan alamat yang unik. IPv6 menyediakan ruang pengalamatan yang sangat besar yaitu 2^{128} (3.4×10^{38}). Didukung oleh spesifikasi IPv6 yang telah terbentuk (dalam bentuk RFC yang dikeluarkan IETF), maka tahap implementasi sangat dimungkinkan, sekaligus ditunjang oleh mulai banyaknya aplikasi yang telah mendukung IPv6.

Kemunculan protokol IPv6 tidak akan membuat keberadaan protokol IPv4 ditinggalkan begitu saja. Mekanisme transisi dari protokol IPv4 ke IPv6 telah dilakukan secara perlahan – lahan tanpa mempengaruhi kinerja jaringan yang telah ada. Salah satu metode transisi IPv6 yang sering diketahui adalah metode transisi *tunneling*. Metode *tunneling* ini dapat menghubungkan jaringan protokol IPv6 dengan jaringan protokol IPv4. Ada bermacam – macam metode *tunneling*

antara lain 6to4, 6over4, teredo dan *Intra-Site Automatic Tunnel Addressing Protocol* (ISATAP). Dengan adanya mekanisme transisi *tunneling*, diharapkan transisi jaringan protokol IPv6 tidak menemui hambatan yang berarti.

1.2. TUJUAN

Penulisan skripsi ini bertujuan untuk menganalisa dan membandingkan performa dari aplikasi *File Transfer Protocol* (FTP) yang diterapkan pada jaringan protokol IPv4 murni, IPv6 murni, IPv6 menggunakan *tunneling* 6to4 dan IPv6 menggunakan *tunneling* ISATAP.

1.3. PEMBATAAN MASALAH

Permasalahan yang akan dibahas dalam skripsi ini adalah menganalisa dan membandingkan performa dari aplikasi *File Transfer Protocol* (FTP) yang diterapkan pada jaringan IPv4 murni, IPv6 murni dan IPv6 menggunakan mekanisme *tunneling*. Mekanisme *tunneling* yang digunakan adalah 6to4 dan ISATAP. Dalam membandingkan performa dari aplikasi FTP dibatasi pada parameter *delay*, *transfer time* dan *throughput*.

1.4. METODOLOGI PENELITIAN

Metode penelitian yang digunakan pada skripsi ini adalah dengan menggunakan jaringan lokal berskala kecil (*test bed*). Dalam pengujian menggunakan dua buah notebook yang diterapkan sebagai *server* dan *client* serta dua buah Router Cisco sebagai jaringan *intermediate* yang dikonfigurasi sebagai jaringan IPv4 murni, IPv6 murni, *tunneling* 6to4 dan ISATAP. Parameter uji coba yang digunakan adalah *delay*, *transfer time* dan *throughput*, sedangkan untuk aplikasi yang digunakan adalah *File Transfer Protocol* (FTP). Proses pengambilan data dilakukan dengan cara sisi *client* melakukan *download* file dari *server* dengan kapasitas file yang berbeda – beda, kemudian dilakukan analisa performansi FTP terhadap ketiga parameter uji coba tersebut.

1.5. SISTEMATIKA PENULISAN

Penulisan skripsi ini dibagi menjadi 5 bab dengan pembagian sebagai berikut. Pada Bab 1 berisi tentang pendahuluan, yang didalamnya meliputi latar belakang, tujuan, metodologi, pembatasan masalah dan sistematika penulisan. Bab 2 berisi tentang penjelasan IPv6 sebagai dasar teori dan referensi penunjang dalam penulisan ini. Bab 3 berisi tentang penjelasan rancangan dari topologi konfigurasi jaringan, metode pengambilan data. Bab 4 berisi tentang analisa dari data yang telah diambil. Bab 5 berisi tentang kesimpulan dari skripsi yang telah dibuat.

BAB 2

IPv6

2.1. DEFINISI DAN LATAR BELAKANG IPv6

Dengan perkembangan teknologi internet yang begitu pesat menyebabkan semakin bertambahnya pengguna internet di seluruh dunia, karena hal ini IP versi 4 (IPv4) diperkirakan tidak mampu lagi untuk memenuhi kebutuhan dari alamat IP. Hal tersebut mengakibatkan kemunculan sistem pengalamatan baru yang dinamakan IP versi 6 (IPv6) yang mempunyai kapasitas lebih banyak dibandingkan dengan IPv4. Tujuan utama pengembangan protokol IPv6 adalah untuk memenuhi kebutuhan alamat IP untuk jangka panjang sekaligus menyempurnakan kekurangan yang terdapat pada protokol IPv4.

IPv6 merupakan IP generasi berikutnya dari teknologi *packet switching* pada jaringan internet atau disebut juga Internet Protocol Next Generation (IPng). Saat ini yang paling banyak digunakan adalah alamat IPv4, dimana alamat IPv4 diprediksikan tidak dapat memenuhi kebutuhan internet yang semakin meningkat pada saat ini. Pada bulan Desember 1998, *Internet Engineering Task Force* (IETF) mendesain alamat IPv6 yang memiliki keunggulan dari pada IPv4. diharapkan kemunculan dari IPv6 dapat mengatasi tentang kekurangan tersebut.

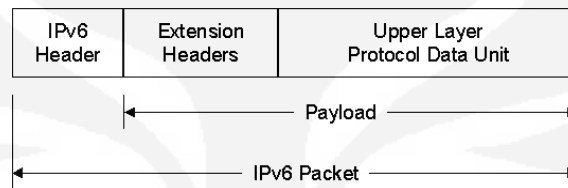
Alamat protokol IPv6 didesain untuk menggantikan alamat IPv4 yang digunakan pada saat ini. Panjang alamat IPv4 adalah 32 bit, sedangkan panjang IPv6 adalah 128 bit. Pada alamat IPv4, alamat yang didapatkan sejumlah 2^{32} atau sekitar $4,294 \times 10^9$. Dengan menggunakan alamat IPv6, alamat yang kita dapatkan sejumlah 2^{128} atau sekitar $3,402 \times 10^{38}$. Dengan kapasitas alamat IPv6 yang sangat banyak maka kebutuhan alamat IP pada jangka panjang akan dapat teratasi.

2.2. SPESIFIKASI DAN STRUKTUR IPv6

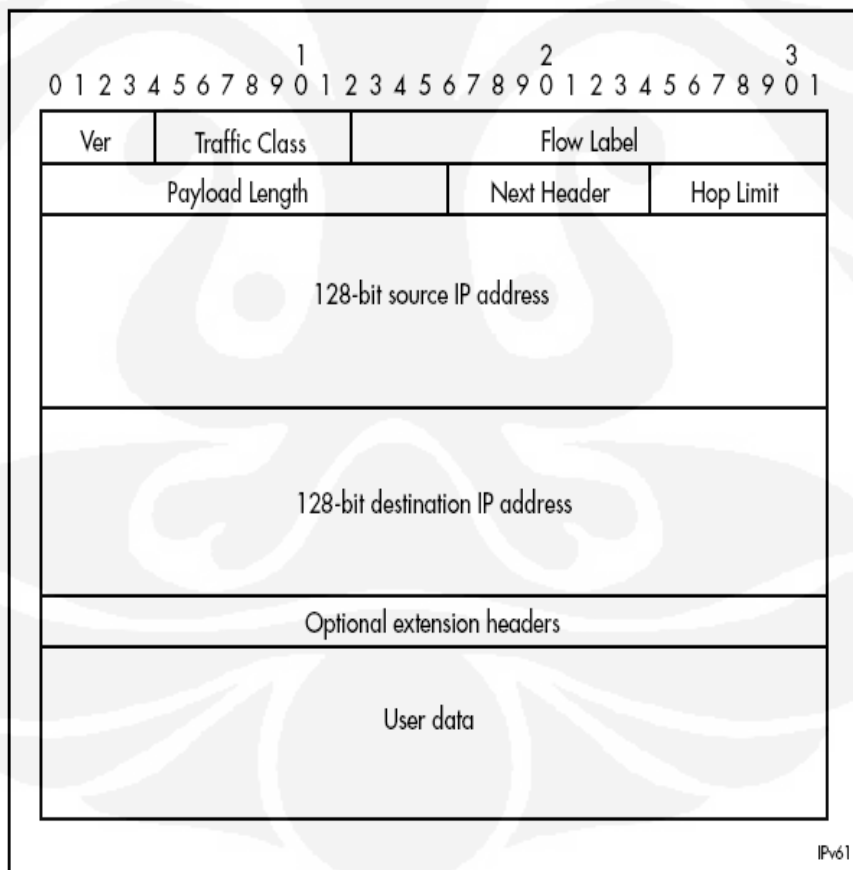
Pada alamat protokol IPv6 memiliki struktur dan spesifikasi yang berbeda dengan alamat protokol IPv4. Protokol IPv6 memiliki panjang 128 bit dan penulisannya menggunakan bilangan hexadecimal, serta memiliki header yang panjangnya 40 bytes.

2.2.1. Struktur IPv6

Protokol IPv6 mempunyai struktur seperti Gambar 2.1 yang terdiri dari IPv6 header, extension headers dan upper layer protocol data unit. IPv6 header mempunyai kapasitas sebesar 40 bytes. Bagian header dapat dilihat pada Gambar 2.2. Untuk bagian *payload* yang terdiri dari *extension header* dan *upper layer protocol data unit* berisi tentang *header* tambahan dan pesan – pesan tambahan seperti *ICMPv6 message*.



Gambar 2.1 Struktur IPv6 [1]



Gambar 2.2 Format header IPv6 [2]

Gambar 2.2 merupakan bentuk header dari protokol IPv6. Berikut penjelasan untuk masing – masing bagiannya :

- Version
Merupakan 4 bit *field* yang menunjukkan versi dari suatu protokol IP dimana untuk paket IPv6 diinisialisasi dengan nilai 6.
- Traffic Class
Merupakan 8 bit *field* yang mengindikasikan skala prioritas pada paket atau mengidentifikasi paket – paket yang membutuhkan penanganan khusus.
- Flow Label
Bagian yang terdiri dari 20 bit yang berfungsi mengidentifikasi paket – paket real time yang dianggap memiliki alur data yang sama.
- Payload Length
Merupakan 16 bit *field* yang berfungsi untuk menunjukkan panjang bit data yang dibawa pada paket IPv6.
- Next Header
Merupakan 8 bit *field* yang menunjukkan jenis protokol dari paket IPv6 yang dikirimkan tersebut. Selain itu, bisa berfungsi untuk identifikasi adanya *extension header* pada paket IPv6.
- Hop Limit
Merupakan 8 bit *field* yang menunjukkan jumlah hop yang akan dilewati oleh suatu paket IPv6 yang dikirimkan.
- Source Address
Merupakan 128 bit *field* yang menunjukkan alamat pengirim atau sumber dari paket IPv6 yang telah dikirimkan.
- Destination Address
Merupakan 128 bit *field* yang menunjukkan alamat penerima dari paket IPv6 yang telah dikirimkan.
- Optional Extension Headers
Merupakan header tambahan yang berfungsi sebagai informasi tambahan.

2.2.2. Pengalamatan IPv6

Dalam arsitektur pengalamatannya alamat IPv6 mempunyai ukuran 128 bits yang artinya berjumlah 2^{128} atau $3,4 \times 10^{38}$ alamat. Namun perhitungan teori ini tidaklah sepenuhnya akurat karena adanya hirarki routing dan kenyataan bahwa pada akhirnya nanti sebuah alamat akan didelegasikan sebagai blok yang bersambung dan bukan sebagai tiap-tiap satuan alamat.

Alamat ini bisa direpresentasikan menjadi 8 segmen bilangan 16 bit dalam bilangan heksa antara 0x0000 s.d 0xffff misal: 2001:d30:3:242:0000:0000:0000:1 Untuk penyederhanaan bisa dituliskan sebagai berikut : 2001:d30:3:242:0:0:0:1 atau 2001:d30:3:242::1.

Alamat IPv6 ini dapat diklasifikasikan menjadi 3 yaitu :

1. Alamat *Unicast*

Alamat *unicast* digunakan pada komunikasi *single interface* atau dinamakan *one to one communication*. Alamat ini yang memiliki sifat global dan unik sehingga bisa dirutekan di Internet. Selain *global unicast*, IPv6 juga mempunyai alamat *local unicast* dengan area terbatas pada link lokal. Beberapa tipe alamat *unicast* IPv6 ini antara lain :

○ *Aggregatable global unicast addresses*

Sering disebut sebagai alamat global, mirip dengan alamat publik pada IPv4 dan alamat ini ditandai dengan prefix 001. Alamat ini bisa dirutekan dan dijangkau secara global dari alamat IPv6 di Internet. Dinamakan *aggregatable* karena memang didesain untuk bisa diaggregasi dan diringkas (*aggregation* dan *summarization*) untuk menghasilkan infrastruktur routing yang efisien. IANA telah mulai mengalokasikan blok alamat pertama untuk alamat global ini yaitu 2001::/16. Menurut kebijakan IANA setiap *end-site* seharusnya diberikan blok alamat IPv6 dengan panjang prefix /48 [1].

○ *Link-local addresses*

Alamat ini digunakan untuk berkomunikasi dalam area link lokal yaitu pada link yang sama (misal jaringan flat tanpa router). Router tidak akan melewatkan trafik dari alamat-alamat ini keluar link. Alamat ini ditandai dengan prefix 1111 1110 10 atau FE80::/10. Alamat ini akan

selalu diawali FE80 dan menggunakan prefix FE80::/64 dengan 64 bit selanjutnya adalah *interface id*. Alamat link local ini dikonfigurasi melalui IPv6 *autoconfiguration* [1].

- *Site-local addresses*

Alamat ini mirip dengan alamat private pada IPv4 yang dalam teknologi IPv6 digunakan dalam lingkup site dan ditandai dengan prefix 1111 1110 11 atau FEC0::/10. Alamat ini akan selalu diawali dengan FEC0. Karena sifatnya yang ambigu dan sulitnya pendefinisian baku dari lingkup site maka alamat ini dihapuskan penggunaannya [1].

- *Special addresses*

Ada dua jenis alamat spesial pada IPv6 yaitu :

- a) *Unspecified address*, sering disebut *all-zeros-address* karena memang bernilai 0:0:0:0:0:0:0 atau bisa dituliskan ::. Alamat ini sama dengan 0.0.0.0 di alamat IPv4. Alamat ini tidak boleh dikonfigurasi pada interface dan tidak boleh menjadi tujuan rute [1].

- b) *Loopback Addresses*, jika alamat loopback pada IPv4 adalah 127.0.0.1 maka pada IPv6 adalah 0:0:0:0:0:0:0:1 atau bisa diringkas menjadi ::1. Alamat ini tidak boleh dikonfigurasi pada *interface* [1].

- *Compatibility addresses*

Alamat ini dibuat untuk mempermudah migrasi dan masa transisi dari IPv4 ke IPv6. Beberapa alamat ini antara lain, alamat IPv4-compatible, alamat IPv4-mapped, alamat 6over4, alamat 6to4 dan alamat ISATAP [1].

- *NSAP addresses*

Adalah alamat yang digunakan untuk penterjemahan alamat Open System Interconnect (OSI) NSAP ke alamat IPv6. Alamat IPv6 ini ditandai dengan prefix 0000001 dan 121 sisanya adalah alamat NSAP [1].

2. Alamat Anycast

Alamat *anycast* mengidentifikasi komunikasi *multiple interface*. Alamat ini digunakan pada sistem *one to one of many communication*. Alamat *anycast* sama seperti alamat *unicast* IPv6 biasa (telah ditentukan dalam standar) dengan tambahan fitur bahwa router akan selalu merutekan ke tujuan yang terdekat atau lebih tepatnya terbaik sesuai yang telah dikonfigurasi [1].

3. Alamat Multicast

Alamat *multicast* digunakan pada sistem *one to many communication*. Seperti halnya pada IPv4 pada IPv6 alamat ini menunjukkan sekumpulan piranti dalam grup *multicast*. Jadi alamat ini hanya akan muncul sebagai alamat tujuan, tidak akan pernah sebagai alamat asal. Jika paket dikirimkan ke alamat ini maka semua anggota grup akan memprosesnya [1].

2.2.3. Perbedaan IPv4 dan IPv6

Berikut ini adalah perbandingan utama antara IPv4 dan IPv6 :

Tabel 2.1 Perbandingan IPv4 dan IPv6 [1]

IPv4	IPv6
Panjang alamat 32 bit (4 bytes)	Panjang alamat 128 bit (16 bytes)
Dikonfigurasi secara manual atau DHCP IPv4	Tidak harus dikonfigurasi secara manual, bisa menggunakan <i>address autoconfiguration</i> .
Dukungan terhadap IPSec opsional	Dukungan terhadap IPSec dibutuhkan
Fragmentasi dilakukan oleh pengirim dan pada router, menurunkan kinerja router.	Fragmentasi dilakukan hanya oleh pengirim.
Tidak mensyaratkan ukuran paket pada link-layer dan harus bisa	Paket link-layer harus mendukung ukuran paket 1280 byte dan harus bisa menyusun

menyusun kembali paket berukuran 576 byte.	kembali paket berukuran 1500 byte.
Checksum termasuk pada <i>header</i> .	Cheksum tidak masuk dalam <i>header</i> .
Header mengandung <i>option</i> .	Data opsional dimasukkan seluruhnya ke dalam <i>extensions header</i> .
Menggunakan ARP Request secara broadcast untuk menterjemahkan alamat IPv4 ke alamat link-layer.	ARP Request telah digantikan oleh Neighbor Solitcitation secara multicast.
Untuk mengelola keanggotaan grup pada subnet lokal digunakan Internet Group Management Protocol (IGMP).	IGMP telah digantikan fungsinya oleh Multicast Listener Discovery (MLD).

2.2.4. Fitur – fitur IPv6

Sebagai teknologi penerus atau bisa disebut sebagai pengganti IPv4, dalam standarnya IPv6 mempunyai berbagai fitur baru yang selain mengatasi berbagai keterbatasan pengalaman menggunakan IPv4 juga menambah beberapa kemampuan baru. Beberapa fitur IPv6 ini adalah sebagai berikut :

- Format header baru
Header baru IPv6 lebih efisien daripada header pada IPv4 (karena memiliki overhead yang lebih kecil). Hal ini diperoleh dengan menghilangkan beberapa bagian yang tidak penting atau opsional.
- Jumlah alamat yang jauh lebih besar
Dengan spesifikasi bit untuk alamat standar sebanyak 128-bit memiliki arti IPv6 akan mampu menyediakan 2^{128} kemungkinan alamat unik. Walaupun tidak semuanya akan dialokasikan namun sudah cukup untuk keperluan masa mendatang.
- Infrastruktur routing dan addressing yang efisien dan hirarkis.
Arsitektur pengalaman IPv6 yang hirarkis membuat infrastruktur routing menjadi efisien dan hirarkis juga. Adanya konsep wilayah atau area juga memudahkan dalam manajemen pengalaman untuk berbagai mode teknologi transmisi.

- Kemampuan *Plug-and-play* melalui *stateless* maupun *statefull address auto-configuration*.

Pada teknologi IPv6, sebuah node yang memerlukan alamat bisa secara otomatis mendapatkannya (alamat global) dari router IPv6 ataupun cukup dengan mengkonfigurasi dirinya sendiri dengan alamat IPv6 tertentu (alamat link local) tanpa perlu adanya DHCP server seperti pada IPv4. Hal ini juga akan memudahkan konfigurasi. Hal ini penting bagi kesuksesan teknologi pengalamatan masa depan karena di internet masa depan nanti akan semakin banyak node yang akan terkoneksi. Perangkat rumah tangga dan bahkan manusia pun bisa saja akan memiliki alamat IP. Tentu saja ini mensyaratkan kesederhanaan dalam konfigurasinya. Mekanisme konfigurasi otomatis pada IPv6 ini akan memudahkan tiap host untuk mendapatkan alamat.

- Keamanan yang sudah menjadi standar built-in.

Jika pada IPv4 fitur IPsec hanya bersifat opsional maka pada IPv6 fitur IPsec ini menjadi spesifikasi standar. Paket IPv6 sudah bisa secara langsung diamankan pada layer network.

- Dukungan yang lebih bagus untuk QoS

Adanya bagian (*field*) baru pada header IPv6 untuk mengidentifikasi trafik (*Flow Label*) dan Traffic Class untuk prioritas trafik membuat QoS yang lebih terjamin bisa diperoleh.

- Berbagai protokol baru untuk keperluan interaksi antar node
Adanya protokol baru misalnya *Network Discovery* dengan komunikasi *multicast* dan *unicast* yang efisien bisa menggantikan komunikasi broadcast ARP untuk menemukan neighbor dalam jaringan.

- Ekstensibilitas.

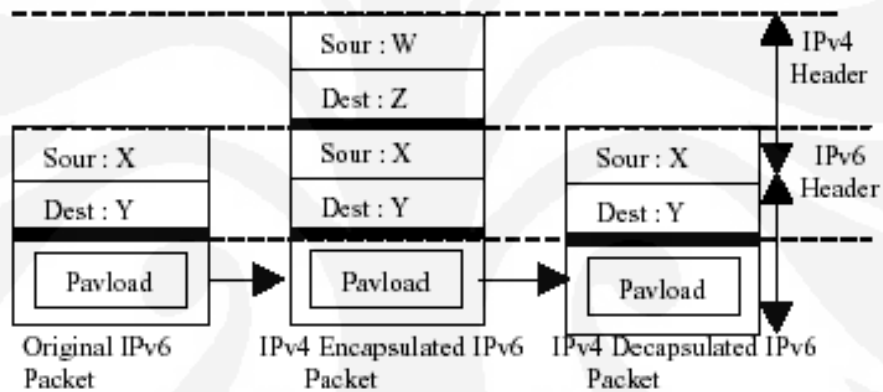
Di masa depan IPv6 dapat dikembangkan lagi fitur-fiturnya dengan menambahkannya pada *extension header*.

2.3. METODE TUNNELING

Pada alamat protokol IPv6 memiliki format alamat dan header yang berbeda dengan alamat protokol IPv4, sehingga secara langsung IPv6 tidak bisa

terkoneksi dengan jaringan IPv4. Karena hal ini, dapat menimbulkan masalah pada penerapan jaringan IPv6 terhadap jaringan IPv4 yang telah ada. Mekanisme transisi digunakan untuk interkoneksi jaringan IPv6 dan IPv4. Salah satu contoh mekanisme transisi adalah *tunneling*.

Tunneling adalah sebuah mekanisme enkapsulasi dan dekapsulasi suatu protokol dengan protokol lainnya untuk dapat melewati jaringan yang belum dapat dilewati protokol tersebut secara langsung. Mekanisme *tunneling* mempunyai prinsip kerja mengenkapsulasi paket IPv6 dengan header IPv4, kemudian paket tersebut langsung dikirim melalui jaringan IPv4. Gambaran dari proses *tunneling* dapat dilihat pada Gambar 2.3.

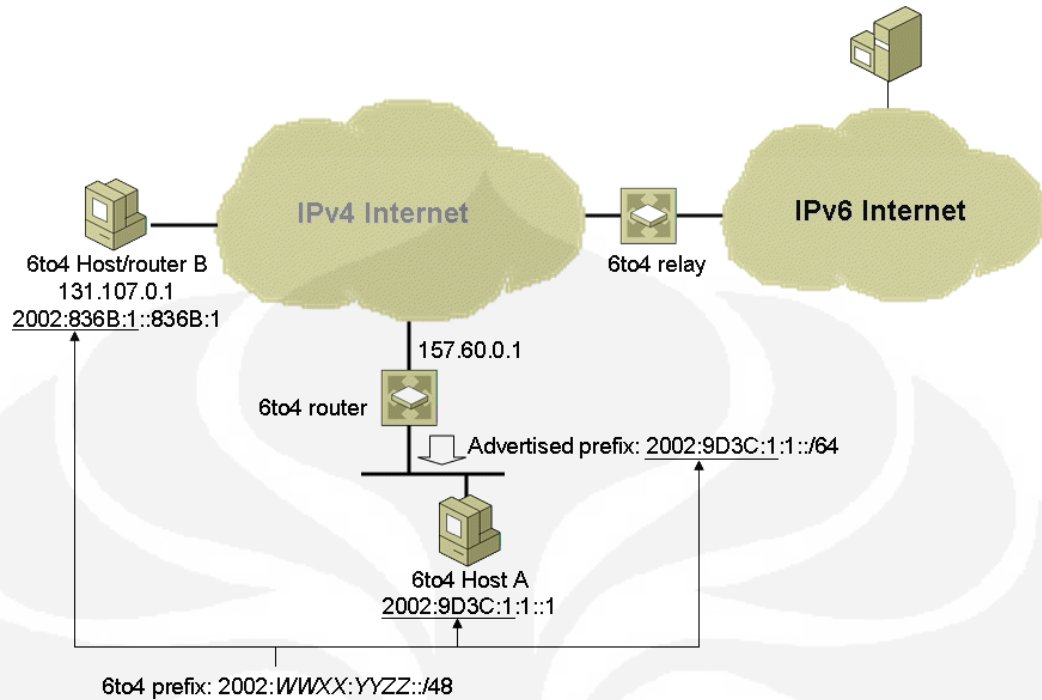


Gambar 2.3 Proses Tunneling [3]

Dalam metode transisi *tunneling* terdapat bermacam – macam tipe, yaitu 6to4 dan *Intra-Site Automatic Tunnel Addressing Protocol* (ISATAP).

2.3.1. Tunneling 6to4

Tunneling 6to4 merupakan salah satu jenis sistem *tunneling* yang memperbolehkan paket dari IPv6 lewat pada jaringan protokol 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 [4]. Contoh dari topologi dan konfigurasi *tunneling* 6to4 dapat dilihat pada Gambar 2.4.

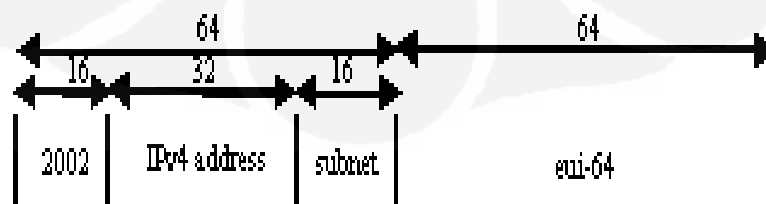


Gambar 2.4 Contoh Jaringan *Tunnelling* 6to4 [1]

Tunneling 6to4 melakukan tiga fungsi utama, yaitu :

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

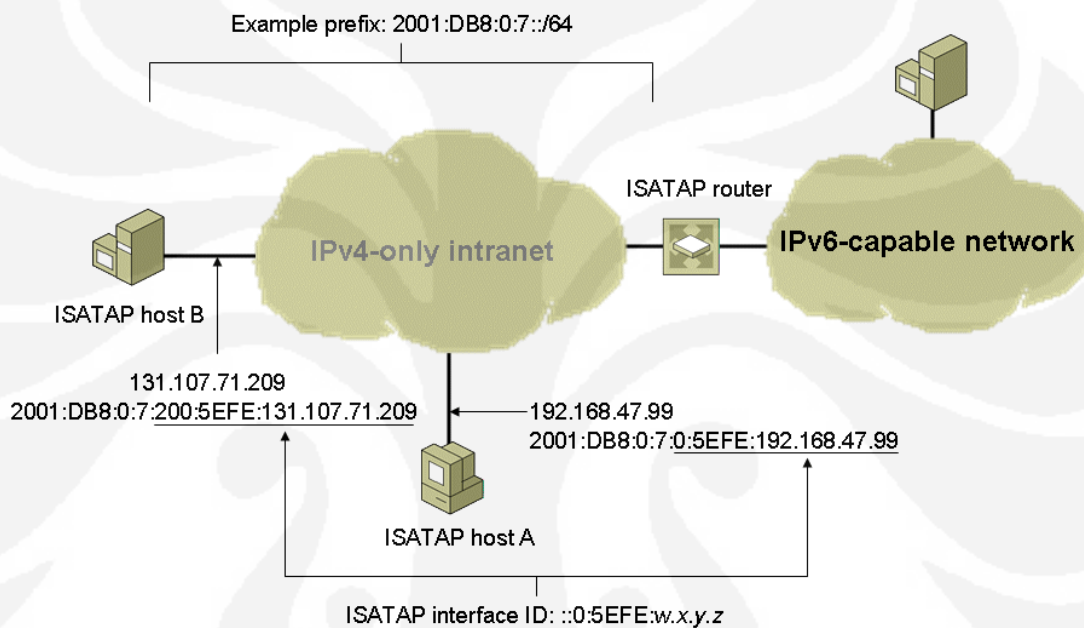
Alokasi alamat blok IPv6 pada 6to4 *tunnels* diawali dengan alamat 2002 (hex) dan diikuti oleh alamat IPv4 suatu *host* yang sudah diubah menjadi bilangan hexadecimal. Contohnya, jika terdapat suatu *host* yang memiliki alamat IPv4 192.1.2.3 maka untuk konfigurasi dari alamat 6to4 *prefix* adalah 2002:C001:0203::/48. Format dari alamat *tunneling* 6to4 dapat dilihat pada Gambar 2.5 dibawah ini.



Gambar 2.5 Format alamat 6to4 [5]

2.3.2. Tunneling ISATAP

ISATAP merupakan kepanjangan dari *Intra-Site Automatic Tunnel Addressing Protocol*. ISATAP adalah pengalamatan yang digunakan pada *host to host*, *host to router* dan *router to host* yang menggunakan teknologi *automatic tunneling*. ISATAP digunakan untuk menyediakan koneksi *unicast* IPv6 diantara *host* IPv6/IPv4 yang melewati IPv4 *intranet* [1]. Contoh *tunneling* ISATAP dari sebuah network dapat dilihat pada Gambar 2.6.



Gambar 2.6 Contoh Jaringan *Tunnelling* ISATAP [1]

Untuk format pengalamatan pada ISATAP dapat dilihat pada Gambar 2.7. Pada 64 bit awal merupakan *link local* atau *ISATAP assigned prefix*. Kemudian untuk 32 bit berikutnya diinisialisasi dengan alamat IPv6 00:00:5E:FE. Untuk 32 bit yang terakhir merupakan alamat dari IPv4 yang telah diubah menjadi bentuk bilangan hexadecimal. Sebagai contoh, jika pada suatu ISATAP terdapat suatu prefix 2001:0DB8:1234:5678::/64 dan alamat IPv4 10.173.129.8. Jika alamat IPv4 diubah ke bentuk bilangan hexadecimal menjadi 0AAD:8108. Sehingga format alamat ISATAP menjadi 2001:0DB8:1234:5678::5EFE:0AAD:8108 [6].



Gambar 2.7 Format alamat ISATAP [5]

2.4. 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 *downloading* melalui jaringan TCP/IP.

Tabel 2.2 Assigned Port [7]

Port	Protocol	Use
21	FTP	File Transfer
23	Telnet	Remote Login
25	SMTP	Email
69	TFTP	Trivial file transfer protocol
79	Finger	Lookup Information about a user
80	HTTP	World Wide Web
110	POP-3	Remote email Acces
119	NNTP	USENET news

Protokol FTP merupakan sebuah protokol yang digunakan untuk melakukan pemindahan satu atau lebih file dari suatu *local host* menuju *remote host* atau host tujuan. Dapat dilihat pada Tabel 2.2, Protokol FTP ditempatkan pada port 21. 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 system 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).

Ketika menggunakan FTP sebagai user terdapat dua macam cara yang dapat dilakukan yaitu sebagai berikut :

2.4.1. Anonymous

Sistem FTP *anonymous* dibuat dengan tujuan agar setiap orang yang terkoneksi ke dalam dunia internet dapat saling berbagi file dengan orang lain yang belum memiliki *account* dalam *server*. Dengan sistem ini setiap orang dapat menggunakan sebuah *account* yang umum (*public account*) berupa *anonymous*.

Melihat kondisi diatas yang menggunakan *public account*, hak yang dimiliki seorang pengguna sangat terbatas kepada aturan-aturan yang dimiliki oleh pemilik server (*remote host*).

Keterbatasan yang dimiliki ketika pengguna menggunakan jenis FTP *anonymous* biasanya meliputi keterbatasan dalam proses akses directory dan file yang tersedia dalam server yang dituju. Selain itu, pengguna yang menggunakan sistem ini tidak dapat melakukan *uploading data* terhadap *server* yang dituju. Namun sebaliknya ia hanya memiliki kemampuan dalam *downloading*, baca file tertentu dan pindah *directory* yang diizinkan oleh pemilik *server*.

2.4.2. User Legal (Authenticated User)

Sistem FTP *User Legal* adalah sebuah cara lain yang digunakan oleh pengguna internet dalam mengakses sebuah *server* dengan menggunakan FTP. Untuk dapat mengakses *remote host*, cara *user legal (authenticated user)* menuntut kita untuk memiliki sebuah *account* khusus yang dimiliki secara pribadi.

Untuk dapat memiliki *account* khusus ini, seorang pengguna harus mendaftarkan diri terlebih dahulu kepada pemilik *remote host* tersebut. Terdapat banyak server yang memberikan fasilitas *account* FTP secara gratis, selain server lain yang mengharuskan pengguna untuk membeli sebuah *account* yang tentunya

dengan fasilitas yang lebih banyak dibandingkan dengan sebuah account yang dimiliki secara free.

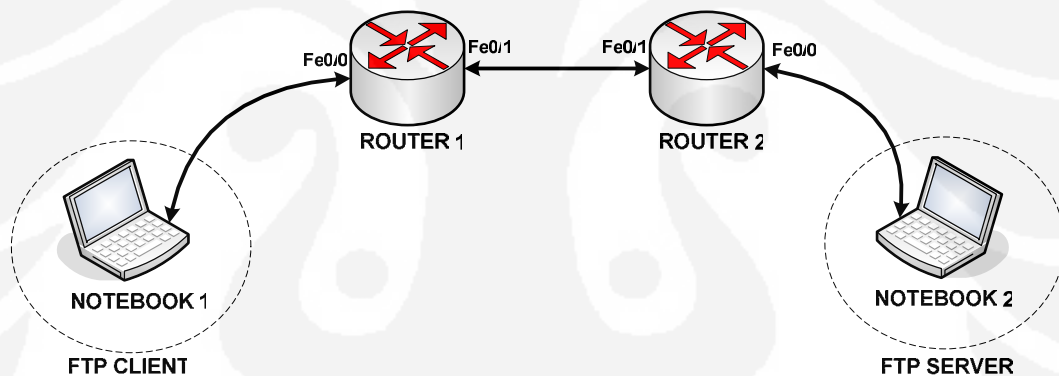
Dengan menggunakan account ini, seorang pengguna memiliki hak akses yang jauh berbeda dengan seorang pengguna jenis *anonymous*. Selain kemampuan yang dimiliki oleh pengguna *anonymous*, seperti download dan berpindah dari satu directory ke directory lain serta kemampuan baca file tertentu, uploading, membuat sebuah directory, menghapus file dan directory. Hak yang dimiliki adalah hak seorang pemilik bukan seorang pengunjung biasa.



BAB 3 KONFIGURASI JARINGAN DAN METODE PENGAMBILAN DATA

3.1. TOPOLOGI JARINGAN

Skripsi ini menggunakan jaringan berskala kecil sebagai sarana pengujian. Jaringan terdiri dari dua buah Notebook dan dua buah Router Cisco. Notebook 1 menggunakan sistem operasi Windows XP service pack 3 dan untuk Notebook 2 menggunakan sistem operasi Windows XP service pack 2. Sedangkan dua buah Router yang digunakan adalah Router Cisco seri 2600. Pada sisi *server* di-install suatu program FTP *server* yaitu Xlight sedangkan pada sisi *client* menggunakan perintah pada command prompt untuk mengakses FTP server. Secara global, topologi jaringan dapat dilihat pada Gambar 3.1 dibawah ini.



Gambar 3.1 Topologi Global

Untuk spesifikasi detail dari seluruh perangkat adalah sebagai berikut :

- *Server*
 - Processor : Intel Core Duo 1.86 GHz
 - Memory : 1G RAM
 - Ethernet : 100Mbps
 - Operating System : Windows XP service pack 3
- *Client*
 - Processor : Intel Core Duo 2 GHz
 - Memory : 1G RAM
 - Ethernet : 100Mbps

Operating System : Windows XP service pack 2

- Router

Jenis : Router CISCO 2600.

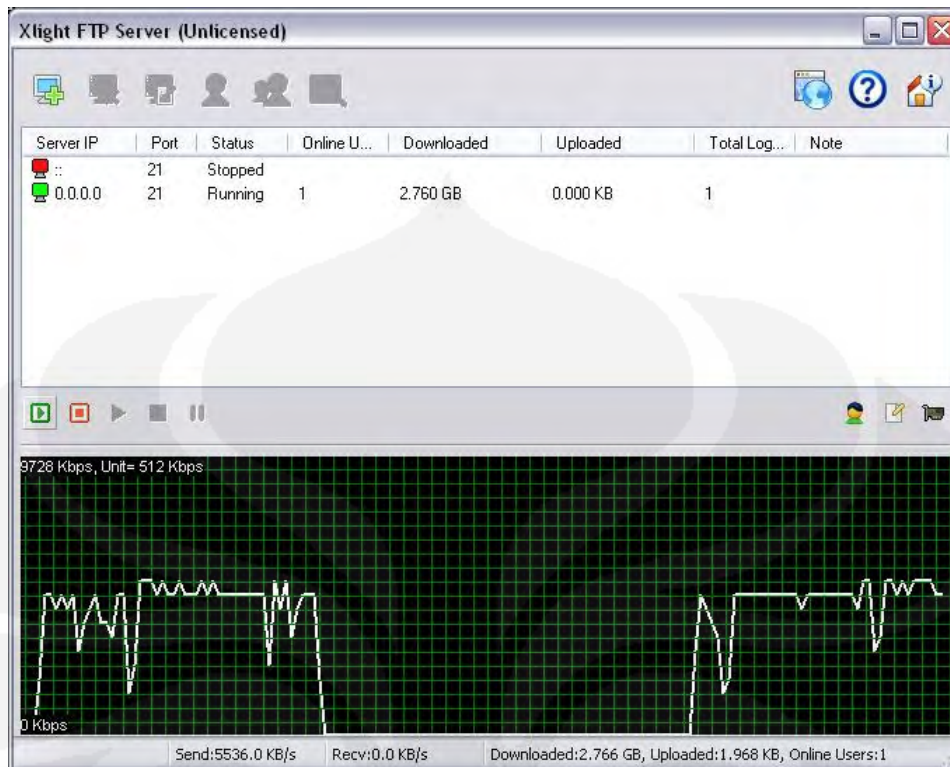
Jumlah : 2 buah.

3.2. PERANGKAT LUNAK YANG DIGUNAKAN

Dalam konfigurasi ini digunakan sistem operasi Windows XP service pack 3 pada sisi FTP server, sedangkan untuk FTP client menggunakan sistem operasi Windows XP service pack 2. Pertimbangan digunakan sistem operasi *Windows* karena sistem operasi ini paling banyak digunakan oleh kebanyakan *user* serta memiliki aplikasi – aplikasi IPv6 yang lebih *friendly user* daripada sistem operasi lainnya. Untuk FTP server menggunakan aplikasi yang bernama Xlight FTP server, sedangkan di sisi client menggunakan perintah FTP dari command prompt. Selain aplikasi yang berhubungan dengan FTP, digunakan juga aplikasi yang berfungsi untuk menangkap paket – paket yang lewat, yaitu Wireshark.

3.2.1. Perangkat Lunak FTP

Xlight FTP merupakan perangkat lunak yang berfungsi sebagai server FTP. Perangkat lunak ini di-*install* pada sisi notebook yang difungsikan sebagai *server*. FTP server berisi file – file yang akan di-*download* oleh FTP client. Perangkat lunak Xlight FTP bekerja pada *platforms* Windows, telah mendukung IPv6, dan *user friendly*. Untuk tampilan dari perangkat lunak Xlight FTP dapat dilihat pada Gambar 3.2. Sedangkan pada sisi *client* digunakan perintah – perintah dari command prompt. Untuk tampilan sisi client dapat dilihat pada Gambar 3.3.



Gambar 3.2 Tampilan Xlight FTP server

```

Command Prompt - ftp 2001:0:0:b::2
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

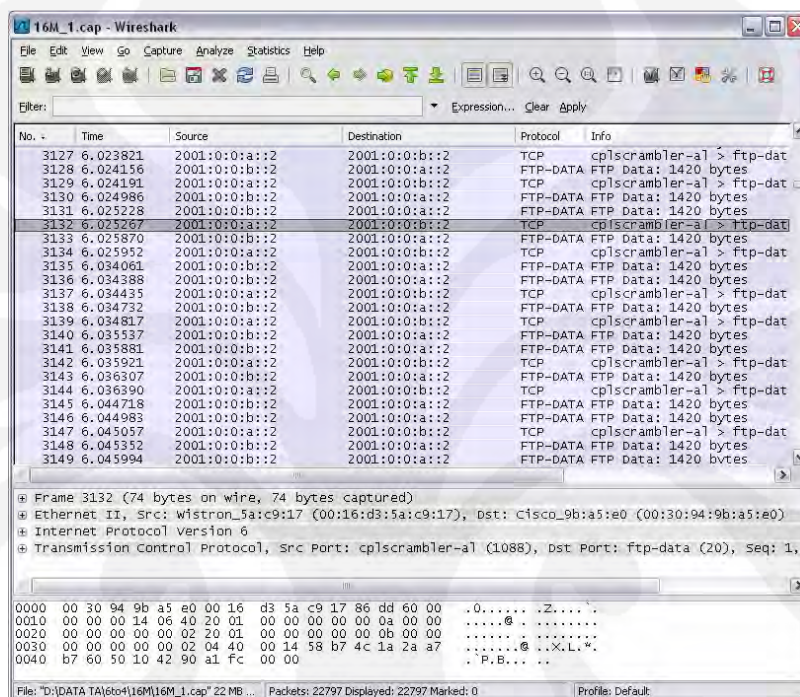
C:\Documents and Settings\Administrator>ftp 2001:0:0:b::2
Connected to 2001:0:0:b::2.
220 Xlight FTP Server 3.1 ready...
User (2001:0:0:b::2:(none)): anonymous
331 Anonymous login OK, send your e-mail as password
Password:
230 Login OK
ftp> bin
200 Type set to I.
ftp>

```

Gambar 3.3 Tampilan FTP client

3.2.2. Wireshark

Wireshark merupakan perangkat lunak yang digunakan untuk mengamati paket – paket yang lewat pada *interface* tertentu. Wireshark dapat berjalan baik pada *platforms* Windows, telah mendukung IPv6, dan *user friendly*. Tampilan dari Wireshark dapat dilihat pada Gambar 3.4.



Gambar 3.4 Tampilan Wireshark

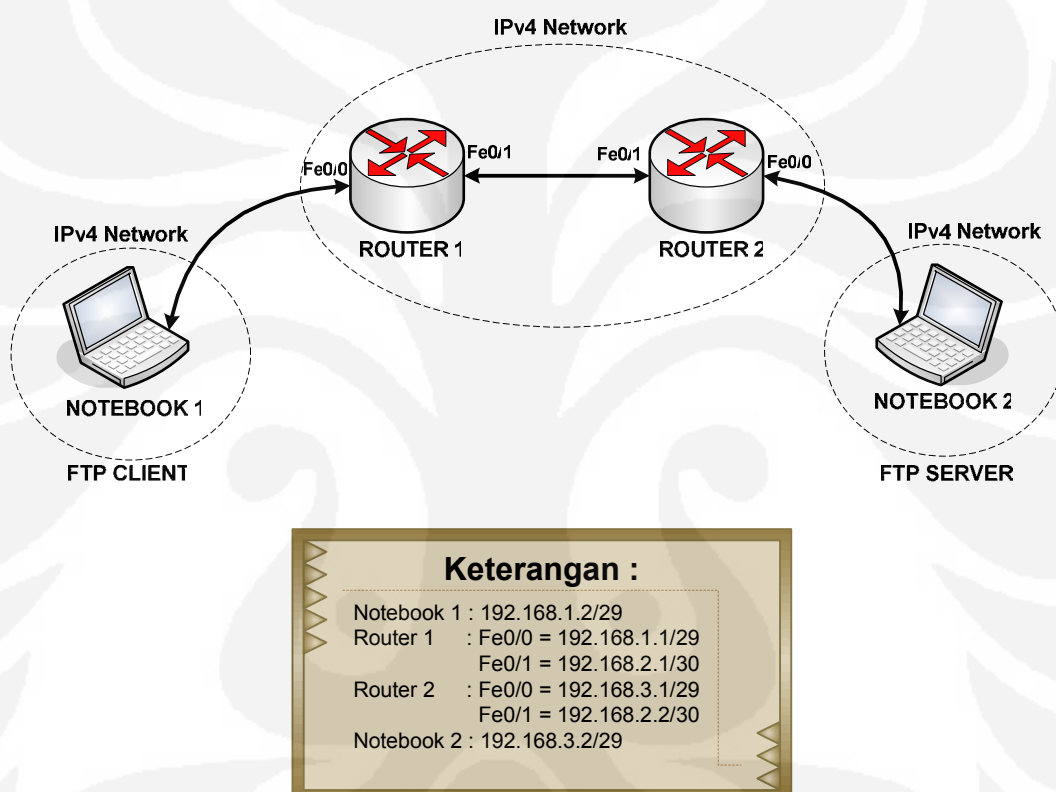
3.3. KONFIGURASI JARINGAN

Dari gambar topologi global, jaringan *test-bed* dibagi menjadi 4 konfigurasi yaitu jaringan IPv4 murni, IPv6 murni, *tunneling* 6to4 dan *tunneling* ISATAP.

3.3.1. Konfigurasi IPv4 murni

Konfigurasi ini terdiri dari dua buah Notebook dan dua buah Router yang masing – masing perangkat diberi pengalamatan IPv4 secara manual. Pada sisi *client* diberi alamat IP 192.168.1.2 dengan subnet mask 255.255.255.248, sedangkan pada sisi *server* diberi alamat IP 192.168.3.2 dengan subnet mask 255.255.255.248. Begitu juga pada sisi router, untuk Router 1 dan Router 2 pada sisi Fe0/0 dan Fe0/1 diberikan alamat IPv4 secara manual. Pada Router 1 untuk *interface* Fe0/0 diberikan alamat IP 192.168.1.1

subnet mask 255.255.255.248 sedangkan untuk *interface* Fe0/1 diberikan alamat IP 192.168.2.1 subnet mask 255.255.255.252. Pada Router 2 untuk *interface* Fe0/0 diberikan alamat IP 192.168.3.1 subnet mask 255.255.255.248, sedangkan pada *interface* Fe0/1 diberikan alamat IP 192.168.2.2 subnet mask 255.255.255.252. Pada Router 1 dan Router 2 perlu ditambahkan suatu *static route* untuk menghubungkan jaringan IPv4 yang satu dengan yang lainnya. Konfigurasi jaringan dapat dilihat pada Gambar 3.5.

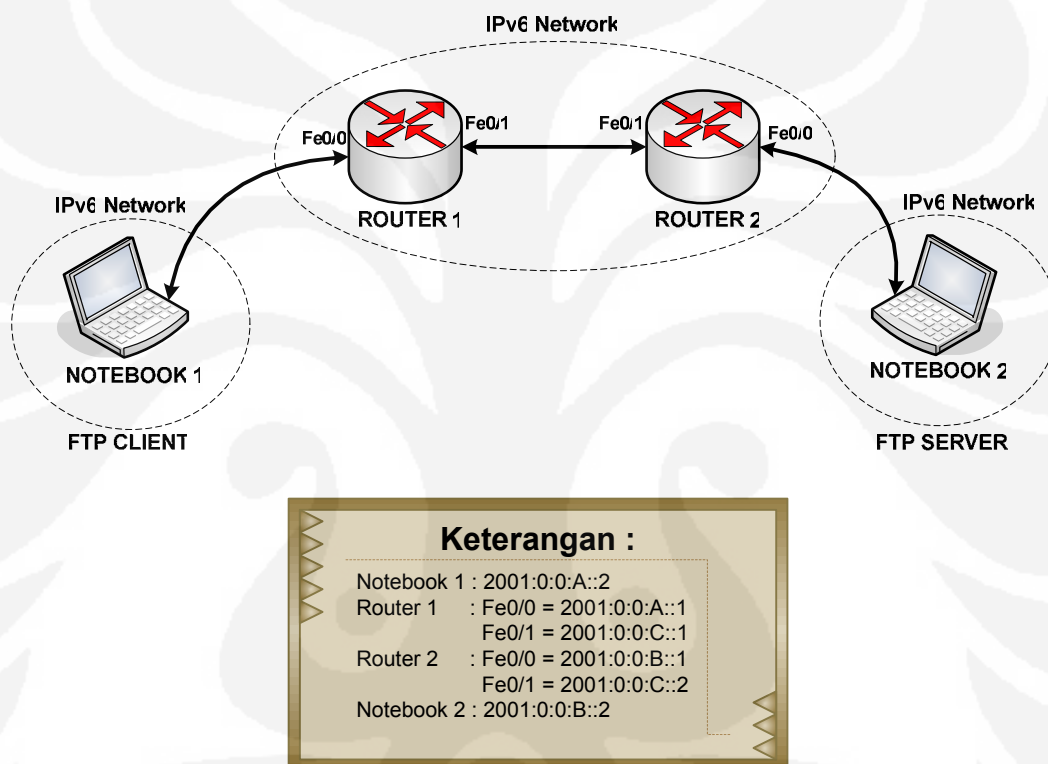


Gambar 3.5 Konfigurasi IPv4 Murni

3.3.2. Konfigurasi IPv6 murni

Konfigurasi ini terdiri dari dua buah Notebook dan dua buah Router yang masing – masing perangkat diberikan pengalamatan IPv6 secara manual. Untuk metode pengalamatan pada IPv6 berbeda dengan IPv4, sehingga pada konfigurasi ini digunakan metode pengalamatan IPv6 jenis *unicast* baik itu disisi *server*, sisi *client*, maupun Router. Pada sisi *server* diberi alamat IPv6 2001:0:0:B::2/64, sedangkan di sisi *client* diberi alamat IPv6

2001:0:0:A::2/64. Pada Router 1 untuk bagian Fe0/0 diberikan alamat IPv6 2001:0:0:A::1/64, sedangkan bagian Fe0/1 diberikan alamat IPv6 2001:0:0:C::1/64. Pada Router 2 untuk bagian Fe0/0 diberikan alamat IPv6 2001:0:0:B::1/64, sedangkan bagian Fe0/1 diberikan alamat IPv6 2001:0:0:C::2/64. Pada sisi Router ditambahkan suatu *static route* IPv6 untuk menghubungkan antar jaringan IPv6. Topologi dan konfigurasi jaringan dapat dilihat pada Gambar 3.6.

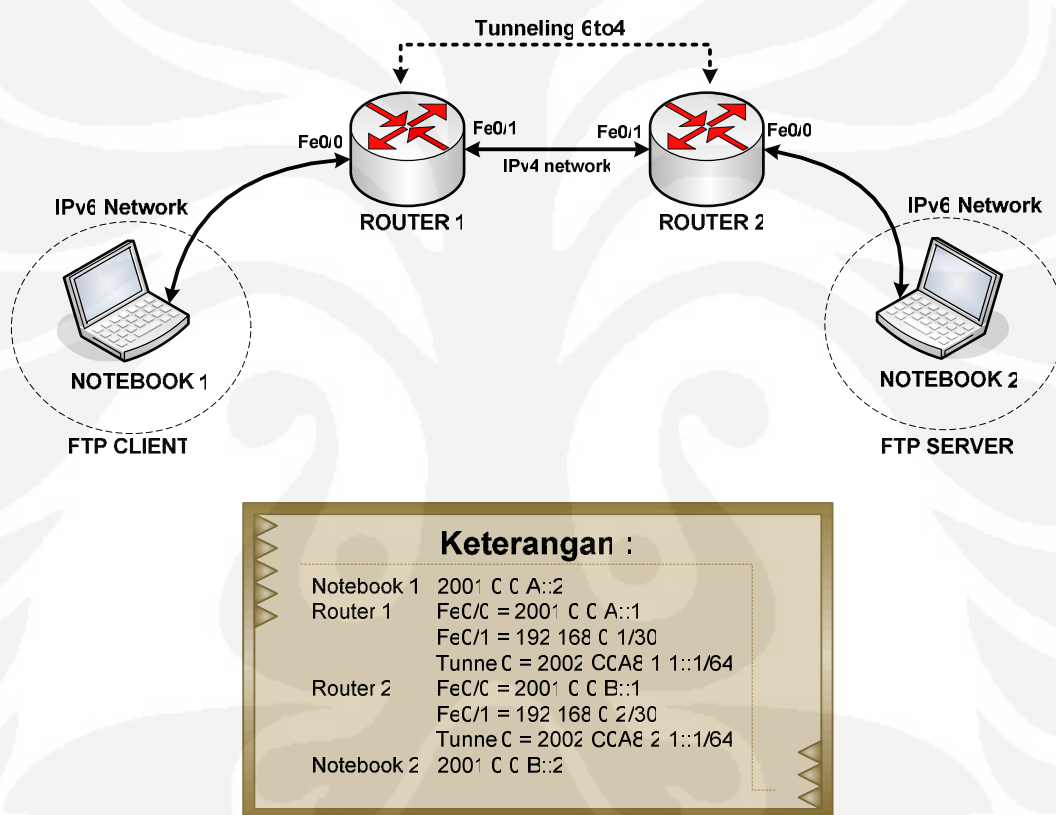


Gambar 3.6 Konfigurasi IPv6 Murni

3.3.3. Konfigurasi *Tunneling 6to4*

Konfigurasi ini terdiri dari dua buah Notebook dan dua buah Router yang diberikan alamat IPv4 pada jaringan antar Router dan alamat IPv6 pada sisi *server* dan *client*. Pada sisi server, Router 1 *interface* Fe0/0, client dan Router 2 *interface* Fe0/0 diberikan alamat IPv6 dengan jenis pengalamatan *unicast*. Pada sisi server diberikan alamat IPv6 2001:0:0:B::2/64, sedangkan pada sisi client diberikan alamat IPv6 2001:0:0:A::2/64. Pada Router 1 bagian Fe0/0 diberikan alamat IPv6 2001:0:0:A::1/64, sedangkan untuk Router 2

bagian Fe0/0 diberikan alamat IPv6 2001:0:0:B::1/64. Jaringan *intermediate* yang menghubungkan antara Router 1 dan Router 2 diberikan alamat IPv4. Pada Router 1 bagian Fe0/1 diberikan alamat 192.168.0.1 subnet mask 255.255.255.252, sedangkan pada Router 2 bagian Fe0/1 diberikan alamat 192.168.0.2 subnet mask 255.255.255.252. Selain itu, pada Router 1 dan Router 2 ditambahkan suatu IP *tunneling* 6to4 pada *interface* Tunnel 0 sebagai jalur dari *tunneling* 6to4. Protokol *routing* yang digunakan adalah RIP versi 2 dan RIPng. Topologi dan konfigurasi dapat dilihat pada Gambar 3.7.

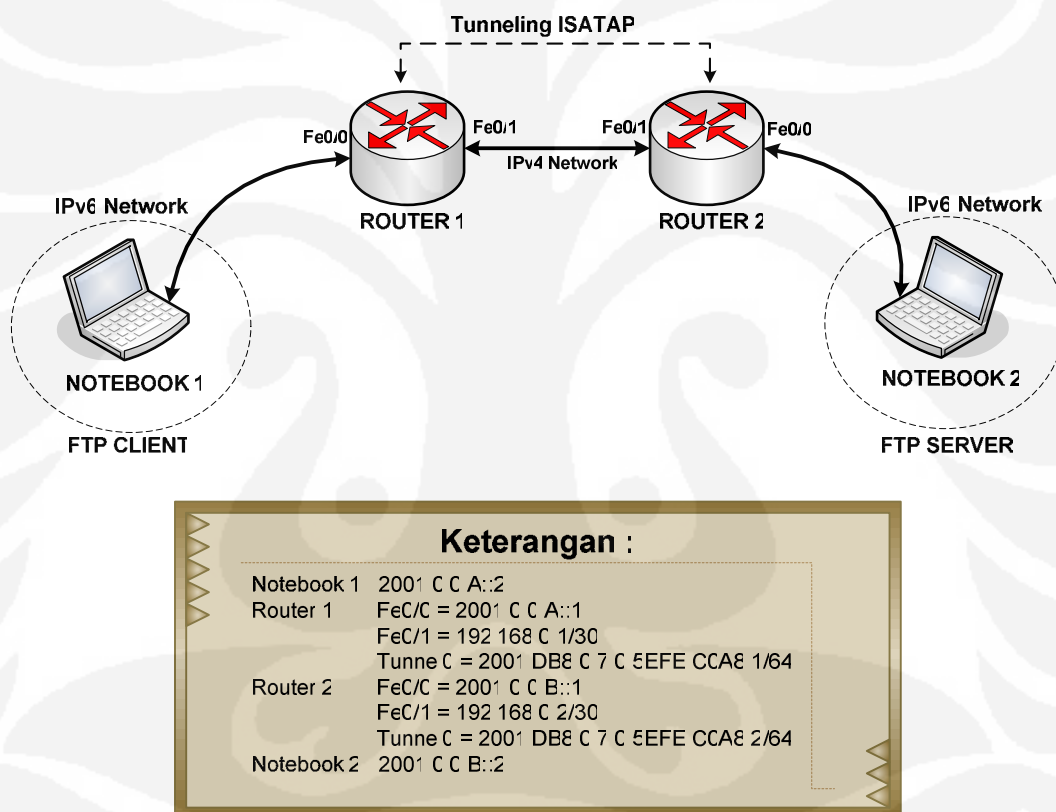


Gambar 3.7 Konfigurasi *Tunneling* 6to4

3.3.4. Konfigurasi *Tunneling* ISATAP

Konfigurasi ini terdiri dari dua buah Notebook dan dua buah Router yang diberikan alamat IPv4 pada jaringan antar Router dan alamat IPv6 pada sisi *server* dan *client*. Pada sisi server, Router 1 *interface* Fe0/0, client dan Router 2 *interface* Fe0/0 diberikan alamat IPv6 dengan jenis pengalamatan *unicast*. Pada sisi server diberikan alamat IPv6 2001:0:0:B::2/64, sedangkan pada sisi client diberikan alamat IPv6 2001:0:0:A::2/64. Pada Router 1 bagian

Fe0/0 diberikan alamat IPv6 2001:0:0:A::1/64, sedangkan untuk Router 2 bagian Fe0/0 diberikan alamat IPv6 2001:0:0:B::1/64. Jaringan *intermediate* yang menghubungkan antara Router 1 dan Router 2 diberikan alamat IPv4. Pada Router 1 bagian Fe0/1 diberikan alamat 192.168.0.1/30, sedangkan pada Router 2 bagian Fe0/1 diberikan alamat 192.168.0.2/30. Selain itu, pada Router 1 dan Router 2 ditambahkan suatu IP *tunneling* ISATAP pada *interface* Tunnel 0 sebagai jalur dari *tunneling* ISATAP. Protokol *routing* yang digunakan adalah RIP versi 2 dan RIPng. Topologi dan konfigurasi dapat dilihat pada Gambar 3.8.



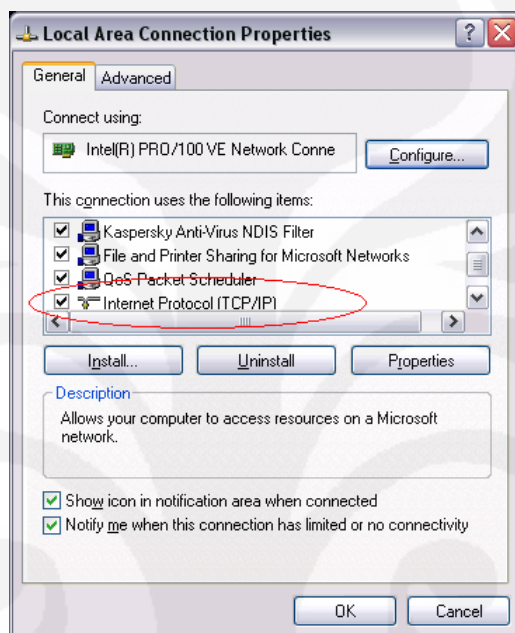
Gambar 3.8 Konfigurasi *Tunneling* ISATAP

3.4. KONFIGURASI IPv6 PADA *SERVER* DAN *CLIENT*

Pada sisi *server* dan *client* menggunakan notebook yang memiliki sistem operasi Windows XP *service pack* 3 dan *service pack* 2. Notebook harus dipastikan terlebih dahulu konfigurasi dari IPv6, jika pada notebook belum

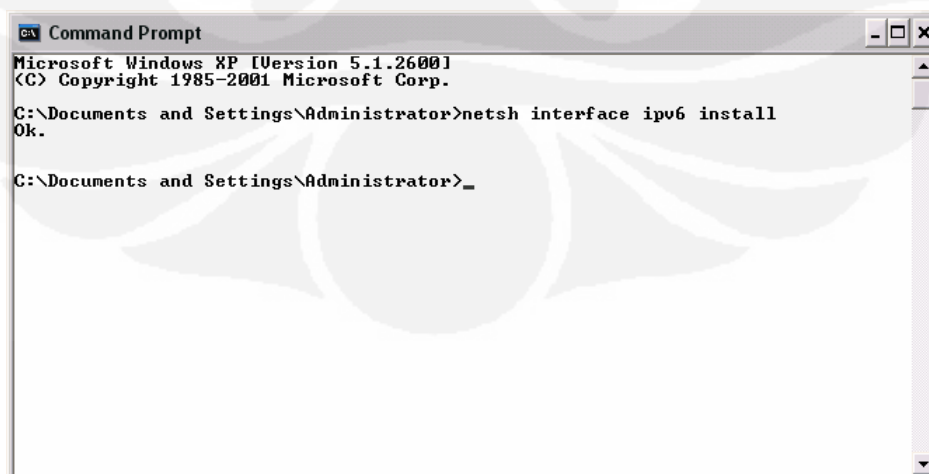
terkonfigurasi protokol IPv6 maka harus dilakukan instalasi terlebih dahulu. Langkah – langkah instalasi IPv6 pada Windows XP adalah sebagai berikut :

- a. Lihat *setting* TCP/IP pada *Local Area Connection properties*. Pastikan menu Microsoft TCP/IP version 6 sudah ada pada *Local Area Connection properties*. Jika belum, ikuti langkah selanjutnya. Ilustrasi dapat dilihat pada Gambar 3.9



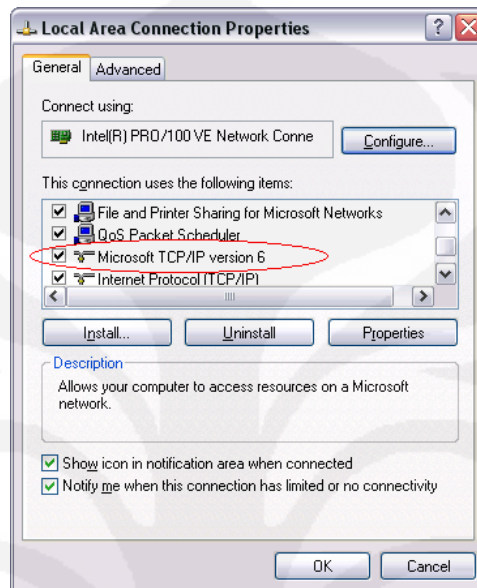
Gambar 3.9 Tampilan *Local Area Connection properties*

- b. Kemudian lakukan instalasi IPv6 dengan menjalankan menu *command prompt*. Setelah itu, ketik `netsh interface ipv6 install` untuk memulai *install* IPv6 dan tunggu sampai muncul ok. Ilustrasi dapat dilihat pada Gambar 3.10.



Gambar 3.10 *Install IPv6*

- c. Pastikan kembali pada menu *Local Area Connection properties* sudah terdapat menu Microsoft TCP/IP version 6. Ini menunjukkan IPv6 sudah terkonfigurasi pada notebook *server* dan *client*.



Gambar 3.11 *Local Area Connection Properties* sudah ter-install IPv6

Setelah dilakukan instalasi jaringan IPv6 pada *server* dan *client*, langkah berikutnya yaitu menambahkan alamat *unicast* IPv6 dan *routing gateway* pada *server* dan *client*. Sebelumnya, agar dilihat terlebih dahulu konfigurasi IPv6 pada setiap *interface*. Perintah `ipv6 if` pada layar *command prompt* digunakan untuk melihat konfigurasi IPv6 pada setiap *interface*. Dikarenakan menggunakan *ethernet* maka digunakan *interface* 4. Ilustrasi dilihat pada Gambar 3.12.


```

Select Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Muamar>ipconfig /all
Interface 6: Teredo Tunneling Pseudo-Interface
    Guid {EDFD00FD-A810-4B31-AFF7-BDA27EBFB4C1}
    zones: link 6 site 3
    cable unplugged
    uses Neighbor Discovery
    uses Router Discovery
    routing preference 2
    link-layer address: 0.0.0.0
    preferred link-local fe80::ffff:ffff:ffff, life infinite
    multicast interface-local ff01::1, 1 refs, not reportable
    multicast link-local ff02::1, 1 refs, not reportable
    link MTU 1280 (true link MTU 1280)
    current hop limit 128
    reachable time 44000ms (base 30000ms)
    retransmission interval 1000ms
    DAD transmits 0
    default site prefix length 48
Interface 5: Ethernet: Wireless Network Connection
    Guid {06ADE841-05C9-4EE9-82E3-319BF0E50250}
    cable unplugged
    uses Neighbor Discovery
    uses Router Discovery
    link-layer address: 00-19-d2-bd-7e-03
    tentative link-local fe80::219:d2ff:febd:7e03, life infinite
    multicast interface-local ff01::1, 1 refs, not reportable
    multicast link-local ff02::1, 1 refs, not reportable
    link MTU 1500 (true link MTU 1500)
    current hop limit 128
    reachable time 31000ms (base 30000ms)
    retransmission interval 1000ms
    DAD transmits 1
    default site prefix length 48
Interface 4: Ethernet: Local Area Connection
    Guid {F002237F-0E28-4C43-9C89-2F2FA1B746D8}
    zones: link 4 site 2
    uses Neighbor Discovery
    uses Router Discovery
    link-layer address: 00-02-3f-ec-d9-3b
    preferred global 2001:0:0:b::2, life infinite (manual)
    preferred link-local fe80::202:3fff:feec:d93b, life infinite
    multicast interface-local ff01::1, 1 refs, not reportable
    multicast link-local ff02::1, 1 refs, not reportable
    multicast link-local ff02::1:ffec:d93b, 1 refs, last reporter
    multicast link-local ff02::1:ff00:2, 1 refs, last reporter
    link MTU 1500 (true link MTU 1500)
    current hop limit 128
    reachable time 16500ms (base 30000ms)
    retransmission interval 1000ms
    DAD transmits 1
  
```

Gambar 3.12 Tampilan konfigurasi IPv6 pada setiap *interface*

Untuk mengkonfigurasi *interface 4* digunakan perintah netsh interface ipv6 add address interface=4 address=2001:0:0:a::2. Pada bagian interface=4 menunjukkan bagian *interface* yang dilakukan konfigurasi dan untuk bagian address=2001:0:0:a::2 menunjukkan alamat IPv6 yang dikonfigurasi secara manual. Ilustrasi dapat dilihat pada Gambar 3.13.

```

Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Muamar>netsh interface ipv6 add address interface=4 address=2001:0:0:a::2
Ok.

C:\Documents and Settings\Muamar>
  
```

Gambar 3.13 Penambahan Alamat IPv6 Pada Sistem Operasi Windows

Setelah mengkonfigurasi alamat IPv6 pada *interface* 4, langkah berikutnya adalah menambahkan *routing gateway*. Penambahan *routing gateway* dilakukan dengan perintah `netsh interface ipv6 add route ::/0 interface=4 2001:0:0:b::1`. Alamat *gateway* ditunjukkan oleh alamat `2001:0:0:b::1`. Setelah mengkonfigurasi *routing gateway*, tabel *routing* dapat dilihat dengan perintah `netsh interface ipv6 show route`. Ilustrasi dapat dilihat pada Gambar 3.14.

```

Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Muamar>netsh interface ipv6 add route ::/0 interface=4
2001:0:0:b::1
Ok.

C:\Documents and Settings\Muamar>netsh interface ipv6 show route
Querying active state...

Publish  Type      Met  Prefix                               Idx  Gateway/Interface Name
-----  -
no       Manual    0    ::/0                               4    2001:0:0:b::1

C:\Documents and Settings\Muamar>

```

Gambar 3.14 *Routing Gateway*

3.5. METODE PENGAMBILAN DATA

Pengambilan data bertujuan untuk dipakai sebagai materi yang akan digunakan untuk membandingkan performa FTP pada konfigurasi antara IPv4 murni, IPv6 murni, IPv6 menggunakan *tunneling* 6to4 dan IPv6 menggunakan *tunneling* ISATAP. Dari perbandingan tersebut dapat ditentukan konfigurasi yang memiliki kualitas lebih baik jika dilalui paket – paket dari aplikasi FTP berdasarkan parameter uji coba. Parameter uji coba yang digunakan adalah *delay*, *throughput* dan *transfer time*.

Pengujian performa dari *File Trasfer Protocol* (FTP) dilakukan dengan cara melakukan *download* file dari *server* ke *client* pada konfigurasi jaringan yang berbeda – beda yaitu IPv4 murni, IPv6 murni, *tunneling* 6to4 dan *tunneling* ISATAP. Kemudian dilakukan penangkapan paket – paket yang lewat pada *interface ethernet* di sisi *client* menggunakan aplikasi Wireshark. Parameter –

parameter yang diambil dan dianalisa dari pengujian ini adalah *delay*, *transfer time* dan *throughput*. File yang di-*download* dari FTP server dibedakan dalam bermacam – macam ukuran, yaitu 16 Mbytes, 32 Mbytes, 64 Mbytes, 128 Mbytes dan 256 Mbytes. Perbedaan ukuran file ini bertujuan untuk mengamati hubungan antara ukuran file dengan parameter – parameter uji.

Pengambilan data pada masing - masing parameter uji coba dilakukan sebanyak 10 kali untuk setiap kapasitas file pada masing – masing konfigurasi jaringan. Pada setiap konfigurasi jaringan dilakukan pengambilan data sebanyak 150 kali. Jadi total pengambilan data secara keseluruhan dalam skripsi ini dilakukan sebanyak 600 kali. Pengambilan data dilakukan dengan kondisi jaringan *test-bed* semirip mungkin dengan jaringan pada umumnya. Hal ini penting untuk dilakukan agar dapat diperoleh kesimpulan yang tepat. Untuk itu pada waktu pengambilan data dilakukan *ping* dengan beban 64Kbytes dari *server* ke *client*.

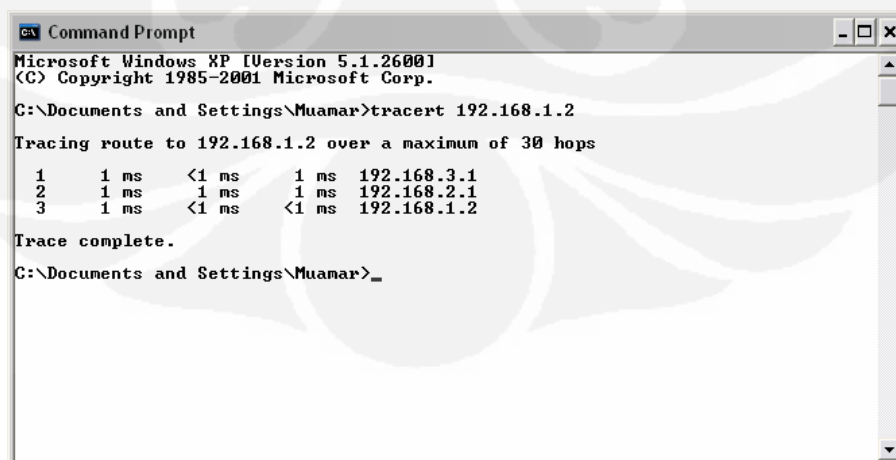
BAB 4 ANALISA DATA

4.1. ANALISA TOPOLOGI DAN KONFIGURASI JARINGAN

Pengambilan data dilakukan dengan menggunakan jaringan berskala kecil untuk setiap konfigurasi jaringan yang diujikan. Secara keseluruhan untuk topologi yang digunakan sama, yaitu menggunakan dua buah Notebook dan dua buah Router. Notebook 1 difungsikan sebagai *client*, sedangkan untuk Notebook 2 difungsikan sebagai *server*. Untuk menghubungkan antar perangkat baik itu Notebook dengan Router dan Router dengan Router digunakan kabel UTP yang mempunyai tipe *cross-over*. Konfigurasi yang digunakan dalam penelitian ini ada 4 macam, yaitu konfigurasi jaringan IPv4 murni, IPv6 murni, IPv6 dengan menggunakan *tunneling* 6to4 dan IPv6 dengan menggunakan *tunneling* ISATAP.

4.1.1. Konfigurasi IPv4 Murni

Pada konfigurasi jaringan IPv4 murni seluruh perangkat baik itu Router maupun Notebook diberikan alamat IPv4. Dalam konfigurasi ini, pada sisi Router memegang peranan penting dalam proses *routing*. Jenis *routing* yang digunakan pada konfigurasi adalah *static routing*, dikarenakan semua konfigurasi menggunakan alamat IPv4 maka proses transmisi data yang terjadi pada saat melalui Router hanya *routing* dan *forwarding* paket seperti jaringan pada umumnya. Hasil *traceroute* pada Gambar 4.1 dilakukan dari *server* ke *client*. Pada hasil *traceroute* tersebut terlihat bahwa seluruh hop yang dilewati merupakan alamat IPv4.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Muamar>tracert 192.168.1.2

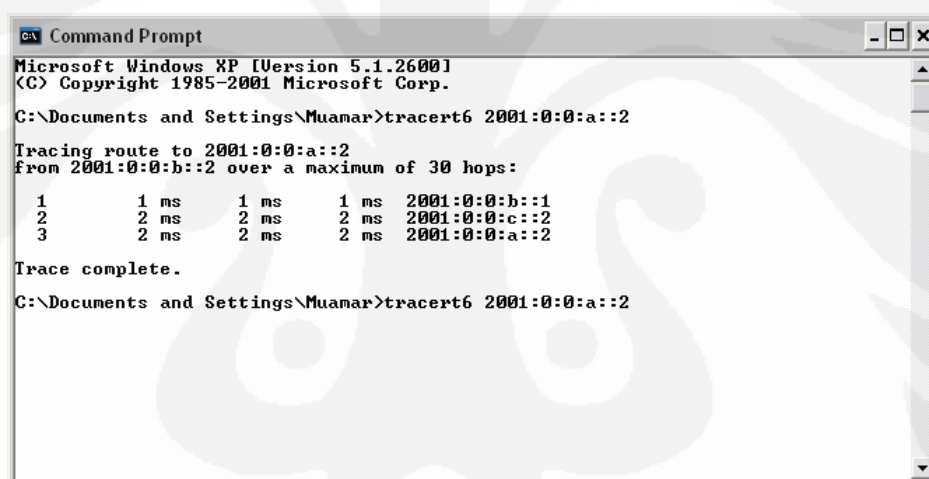
Tracing route to 192.168.1.2 over a maximum of 30 hops:
  0  1 ms  <1 ms    1 ms  192.168.3.1
  1  1 ms  1 ms     1 ms  192.168.2.1
  2  1 ms  <1 ms   <1 ms  192.168.1.2
Trace complete.

C:\Documents and Settings\Muamar>_
```

Gambar 4.1 Tampilan *Traceroute* Jaringan IPv4 Murni

4.1.2. Konfigurasi IPv6 Murni

Pada konfigurasi jaringan IPv6 murni juga memiliki topologi yang sama dengan topologi IPv4 murni sehingga tidak ada perbedaan jumlah hop. Perbedaannya terletak pada konfigurasi alamat IP yang diberikan adalah menggunakan alamat IPv6. Dalam konfigurasi ini fungsi Router juga tidak berbeda dengan IPv4 murni yaitu hanya *routing* dan *forwarding* paket seperti jaringan pada umumnya. Jenis *routing* yang digunakan pada konfigurasi ini yaitu *static routing*. Mekanisme *tunneling* belum digunakan pada konfigurasi jaringan ini. Hasil *traceroute* pada Gambar 4.2 merupakan hasil *traceroute* dari *server* ke *client*. Dari hasil *traceroute* tersebut dapat diketahui hop yang dilewati oleh data. Hasil *traceroute* menunjukkan bahwa seluruh hop yang dilewati merupakan alamat IPv6.



```

Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Muamar>tracert6 2001:0:0:a::2

Tracing route to 2001:0:0:a::2
over a maximum of 30 hops:
  0  0 ms  0 ms  0 ms  2001:0:0:b::1
  1  1 ms  1 ms  1 ms  2001:0:0:c::2
  2  2 ms  2 ms  2 ms  2001:0:0:a::2
  3  2 ms  2 ms  2 ms  2001:0:0:a::2

Trace complete.

C:\Documents and Settings\Muamar>tracert6 2001:0:0:a::2

```

Gambar 4.2 Tampilan *Traceroute* Jaringan IPv6 Murni

4.1.3. Konfigurasi *Tunneling* 6to4

Pada konfigurasi jaringan *tunneling* 6to4 juga memiliki topologi sama dengan jaringan IPv4 murni dan IPv6 murni sehingga tidak ada perbedaan jumlah hop. Pada konfigurasi ini menggunakan mekanisme *tunneling* jenis 6to4 sehingga pada sisi Router perlu ditambahkan *interface tunnel* yang di-*setting* menjadi *mode* 6to4. Peran Router pada konfigurasi ini selain *routing*, juga berfungsi untuk proses enkapsulasi dan deenkapsulasi paket. Paket IPv6 yang dikirimkan dari *server* akan dienkapsulasi dengan paket IPv4 pada

Router 2 melalui proses mekanisme *tunneling* 6to4 sehingga paket yang terkirim ke Router 1 sudah menjadi paket IPv4. Proses dekapsulasi IPv4 juga melalui proses mekanisme *tunneling* 6to4 yang terjadi pada Router 1 sehingga paket yang terkirim ke *client* sudah dalam paket IPv6 seperti semula. Hasil *traceroute* pada Gambar 4.3 dilakukan dari sisi *server* ke *client*. Dapat dilihat pada hasil *traceroute* bahwa pada hop kedua terdapat alamat IPv6 2002:C0A8:1:1::1. Alamat IPv6 pada hop kedua tersebut menunjukkan alamat *identifiser* dari *tunneling* 6to4 sehingga bisa dipastikan bahwa data yang dikirim dari *server* ke *client* melalui mekanisme *tunneling* 6to4 terlebih dahulu.

```

Select Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Muamar>tracert6 2001:0:0:a::2
Tracing route to 2001:0:0:a::2
from 2001:0:0:b::2 over a maximum of 30 hops:
  1      <1 ms    <1 ms    <1 ms    2001:0:0:b::1
  2       4 ms     4 ms     4 ms     2002:c0a8:1:1::1
  3       4 ms     4 ms     4 ms     2001:0:0:a::2
Trace complete.
C:\Documents and Settings\Muamar>_

```

Gambar 4.3 Tampilan *Traceroute* Jaringan *Tunneling* 6to4

4.1.4. Konfigurasi *Tunneling* ISATAP

Pada konfigurasi jaringan *tunneling* ISATAP juga memiliki topologi yang sama dengan konfigurasi lainnya sehingga tidak terdapat perbedaan jumlah hop. Pada konfigurasi ini menggunakan mekanisme *tunneling* jenis ISATAP (*Intra-Site Automatic Tunnel Addressing Protocol*) sehingga untuk *interface tunnel* pada sisi Router di-*setting* dengan *mode* isatap. Pada konfigurasi ini, Router berfungsi sebagai *routing*, enkapsulasi dan dekapsulasi paket yang dikirimkan. Paket IPv6 yang dikirim dari sisi *server* akan dienkapsulasi pada sisi Router 2 melalui proses mekanisme *tunneling* ISATAP sehingga paket yang terkirim ke Router 1 sudah dalam bentuk paket IPv4.

Pada Router 1 akan terjadi proses dekapsulasi paket IPv4 menjadi paket IPv6 yang dikirimkan ke sisi *client*. Hasil *traceroute* pada Gambar 4.4 dilakukan dari *server* ke *client*. Dilihat pada hasil *traceroute* tersebut pada hop kedua terdapat alamat IPv6 2001:db8:0:7:0:5EFE:192.168.0.1. Alamat ini merupakan alamat *identifier* dari mekanisme *tunneling* ISATAP sehingga bisa dipastikan bahwa data yang dikirim dari *server* akan melewati mekanisme *tunneling* ISATAP terlebih dahulu sebelum sampai pada *client*.

```

Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Muamar>tracert6 2001:0:0:a::2
Tracing route to 2001:0:0:a::2
from 2001:0:0:b::2 over a maximum of 30 hops:
  1      1 ms    1 ms    1 ms    2001:0:0:b::1
  2      4 ms    4 ms    4 ms    2001:db8:0:7:0:5efe:192.168.0.1
  3      4 ms    4 ms    4 ms    2001:0:0:a::2
Trace complete.

C:\Documents and Settings\Muamar>tracert 2001:0:0:a::2
Tracing route to 2001:0:0:a::2 over a maximum of 30 hops
  1      1 ms    <1 ms  <1 ms  2001:0:0:b::1
  2      4 ms    3 ms   4 ms   2001:db8:0:7:0:5efe:192.168.0.1
  3      4 ms    4 ms   4 ms   2001:0:0:a::2
Trace complete.

C:\Documents and Settings\Muamar>

```

Gambar 4.4 Tampilan *Traceroute* Jaringan *Tunneling* ISATAP

4.2. ANALISA PERFORMA JARINGAN PADA FTP

File Transfer Protocol (FTP) merupakan suatu aplikasi yang digunakan untuk memindahkan suatu file data dari suatu *server* ke *client* atau sebaliknya. FTP merupakan suatu jenis protokol yang bekerja dengan memanfaatkan protokol TCP/IP yang pada umumnya menggunakan port 21. FTP *server* merupakan tempat untuk menyimpan file- file yang akan didownload oleh *client*. FTP *client* berfungsi untuk melakukan *download* file dari *server*. Pertama kali, notebook yang berfungsi sebagai *client* akan melakukan permintaan koneksi FTP yang ditujukan pada FTP *server*. Proses *requesting* ini diawali dengan *three way handshaking* yang merupakan ciri khas dari protokol TCP/IP. Setelah *server* dan *client* terkoneksi, maka selanjutnya akan diminta *username* dan *password* oleh FTP *server*. Dalam pengujian ini digunakan modus *anonymous* sehingga tidak

perlu mendaftarkan *account* terlebih dahulu pada *server*. Proses *autentification* pada *username* dan *password* yang dimasukkan *client* akan dilakukan oleh *server*. Setelah dinyatakan tersambung oleh *server* maka *client* sudah mendapatkan layanan FTP dengan modus *anonymous*. Gambaran proses koneksi FTP *client* dan *server* dapat dilihat pada Gambar 4.5.

```

C:\Documents and Settings\Administrator>ftp 2001:0:0:b::2
Connected to 2001:0:0:b::2.
220 Xlight FTP Server 3.1 ready...
User (2001:0:0:b::2:(none)): anonymous
331 Anonymous login OK, send your e-mail as password
Password:
230 Login OK
ftp> bin
200 Type set to I.
ftp> ls
200 PORT command successful
150 Opening ASCII mode data connection for NLIST (77 bytes).
file1_16M.rar
file2_32M.rar
file3_64M.rar
file4_128M.rar
file5_256M.rar
226 Transfer complete (0.478 KB/s).
ftp: 77 bytes received in 0.01Seconds 7.70Kbytes/sec.
ftp>

```

Gambar 4.5 Tampilan FTP *client* setelah terkoneksi dengan *server*

Proses *download* file dari *server* dilakukan oleh *client* dengan ukuran file yang berbeda - beda. Ukuran file dibedakan menjadi lima macam, yaitu 16 MB, 32 MB, 64 MB, 128 MB dan 256 MB. Semua tipe file dibuat sama dalam bentuk rar untuk memudahkan *client* melakukan *download* dari *server* dan menghindari pengaruh perbedaan tipe file pada performa FTP. File – file yang diujikan dapat dilihat pada Tabel 4.1.

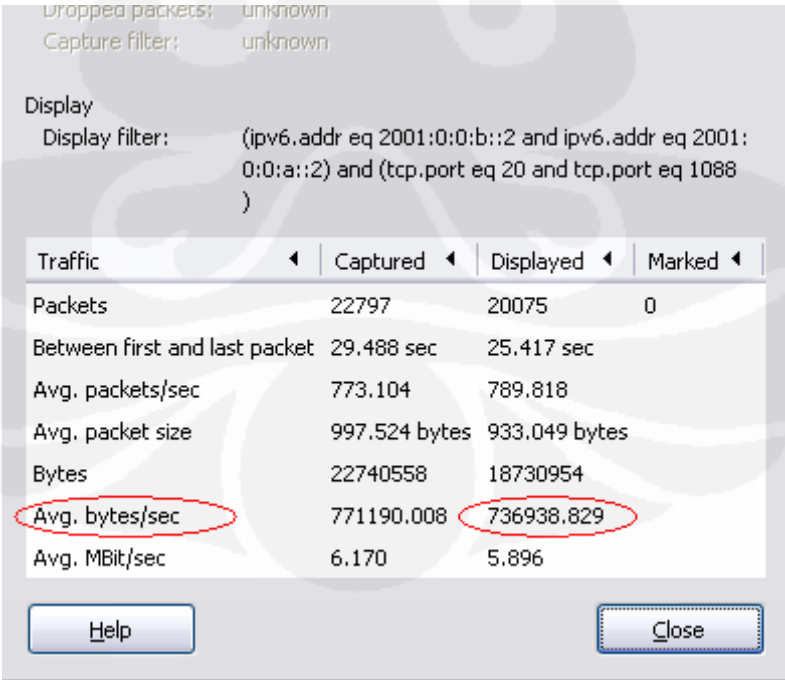
Tabel 4.1 File Uji Coba

Nama File	Ukuran File (bytes)
file1_16M.rar	17245396
file2_32M.rar	32976505
file3_64M.rar	65775243
file4_128M.rar	131228435
file5_256M.rar	262071864

Terdapat tiga parameter yang diambil dalam pengambilan data, yaitu *throughput*, *delay* dan *transfer time*. Parameter tersebut dianggap sudah dapat mewakili unjuk kerja dari FTP dalam melakukan proses *download* data. Jika dilihat dari ketiga parameter tersebut memiliki keterkaitan satu sama lain. Untuk analisa data tentang ketiga parameter tersebut dijelaskan pada bagian berikut ini.

4.2.1. Analisa Throughput

Throughput merupakan kecepatan transfer data yang berarti besarnya data rata – rata yang mampu ditransfer melewati jaringan per detik pada umumnya menggunakan satuan *bit per second* (bps). Pengambilan parameter *throughput* dilakukan dengan cara sisi *client* melakukan *download* file dari *server* dan pada saat itu juga di sisi *client* melakukan penangkapan paket – paket yang masuk melalui *interface ethernet* dengan aplikasi Wireshark. Seluruh paket yang masuk akan ditangkap oleh Wireshark bukan hanya paket FTP. Untuk mendapatkan paket – paket FTP dilakukan *filtering* terlebih dahulu pada hasil *capture* Wireshark. Dari paket – paket FTP yang sudah dilakukan *filtering* tersebut bisa dilihat pada bagian *summary* untuk menentukan besarnya *throughput* pada paket- paket FTP. Dapat dilihat pada Gambar 4.6.



Dropped packets: unknown
Capture filter: unknown

Display filter: (ipv6.addr eq 2001:0:0:b::2 and ipv6.addr eq 2001:0:0:a::2) and (tcp.port eq 20 and tcp.port eq 1088)

Traffic	Captured	Displayed	Marked
Packets	22797	20075	0
Between first and last packet	29.488 sec	25.417 sec	
Avg. packets/sec	773.104	789.818	
Avg. packet size	997.524 bytes	933.049 bytes	
Bytes	22740558	18730954	
Avg. bytes/sec	771190.008	736938.829	
Avg. MBit/sec	6.170	5.896	

Buttons: Help, Close

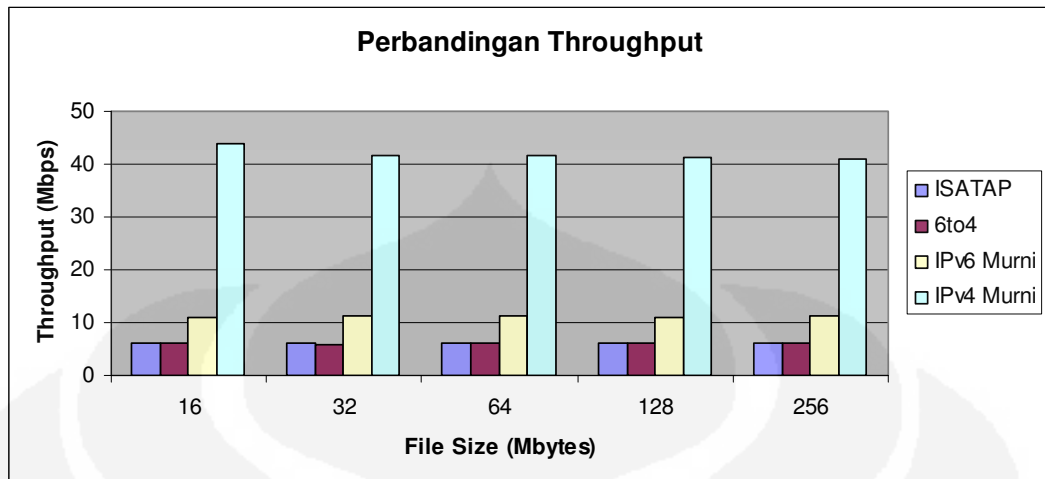
Gambar 4.6 Throughput pada Summary Wireshark

Data yang tertangkap di Wireshark masih dalam satuan *bytes per second* sehingga perlu diubah menjadi satuan *bit per second* dengan mengalikan delapan dari data yang diambil dari Wireshark. Data keseluruhan hasil pengujian didapatkan nilai rata – rata parameter *throughput* yang ditunjukkan pada Tabel 4.2, sedangkan untuk data secara keseluruhan dapat dilihat pada Lampiran 9 – Lampiran 12.

Tabel 4.2 Data Rata – Rata *Throughput*

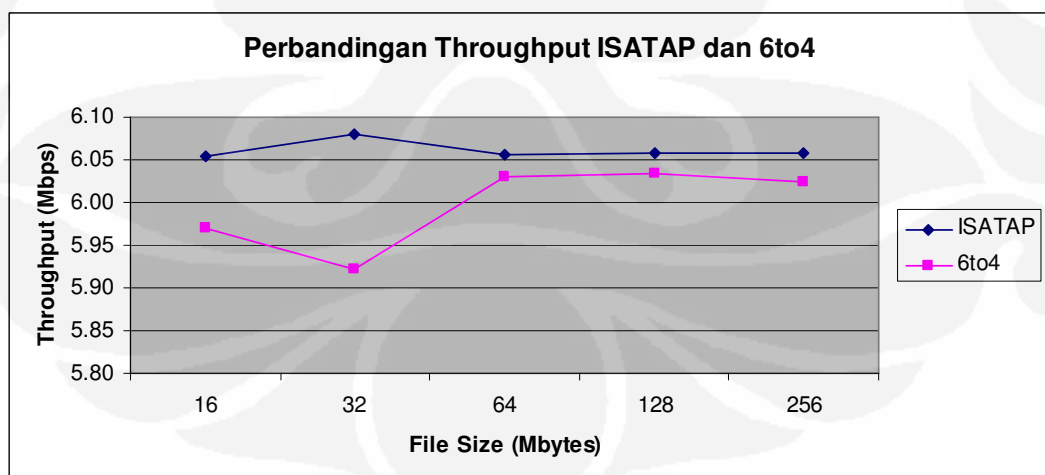
File Size (MBytes)	Throughput (Mbps)			
	IPv4 Murni	IPv6 Murni	6to4	ISATAP
16	43.7426	11.0231	5.9709	6.0547
32	41.7557	11.1471	5.9211	6.0793
64	41.6926	11.1836	6.0294	6.0570
128	41.2227	11.1145	6.0333	6.0586
256	40.8342	11.1721	6.0250	6.0589

Dari Tabel 4.2, dapat dilihat pada waktu ukuran file semakin besar nilai *throughput* tidak mengalami perubahan yang signifikan dan cenderung stabil sehingga perbedaan kapasitas ukuran file tidak mempengaruhi pada besarnya nilai *throughput*. Jika dibandingkan pada masing - masing konfigurasi maka nilai *throughput* yang paling besar terjadi pada konfigurasi IPv4 murni sedangkan nilai *throughput* yang paling kecil terjadi pada konfigurasi yang menggunakan *tunneling*. Secara persentase rata – rata, nilai *throughput* IPv6 murni lebih kecil 73.39% dari nilai *throughput* IPv4 murni. Jika dibandingkan dengan mekanisme *tunneling*, maka nilai *throughput* untuk konfigurasi *tunneling* 6to4 lebih kecil 85.66% dari IPv4 murni, sedangkan untuk konfigurasi *tunneling* ISATAP lebih kecil 85.51% dari IPv4 murni. Konfigurasi IPv6 murni juga memiliki nilai *throughput* lebih besar 84.59% dari konfigurasi 6to4 dan ISATAP. Hal ini dikarenakan pada mekanisme *tunneling* terjadi proses enkapsulasi dan dekapsulasi paket dari IPv6 ke IPv4. Pada Gambar 4.7 merupakan diagram perbandingan nilai *throughput* dari empat macam konfigurasi.



Gambar 4.7 Diagram Perbandingan Nilai *Throughput*

Perbandingan antara konfigurasi ISATAP dan 6to4 pada Gambar 4.7 tidak dapat dilihat dengan begitu jelas sehingga perlu dilakukan perbandingan khusus. Perbandingan antara kedua mekanisme *tunneling* dapat dilihat pada Gambar 4.8. Dari grafik yang terdapat pada Gambar 4.8, menunjukkan bahwa konfigurasi ISATAP memiliki nilai *throughput* lebih besar dari 6to4. Konfigurasi ISATAP memiliki nilai *throughput* lebih besar 1.1% dari konfigurasi 6to4. Ini menunjukkan bahwa proses enkapsulasi dan dekapsulasi pada konfigurasi ISATAP lebih baik daripada 6to4.



Gambar 4.8 Grafik Perbandingan Nilai *Throughput* ISATAP dan 6to4

4.2.2. Analisa Transfer Time

Transfer Time adalah jumlah waktu yang dibutuhkan untuk mengirimkan seluruh paket dari *server* ke *client*. Parameter *transfer time* diambil dari hasil *capture* Wireshark yang sudah dilakukan *filtering* terlebih dahulu sehingga hanya muncul paket – paket FTP saja. Data *transfer time* diambil dari perbedaan rentang waktu antara paket pertama sampai dengan paket terakhir. Pengambilan nilai *transfer time* pada *summary* Wireshark dapat dilihat pada Gambar 4.9.

Traffic	Captured	Displayed	Marked
Packets	22797	20075	0
Between first and last packet	29.488 sec	25.417 sec	
Avg. packets/sec	773.104	789.818	
Avg. packet size	997.524 bytes	933.049 bytes	
Bytes	22740558	18730954	
Avg. bytes/sec	771190.008	736938.829	
Avg. MBit/sec	6.170	5.896	

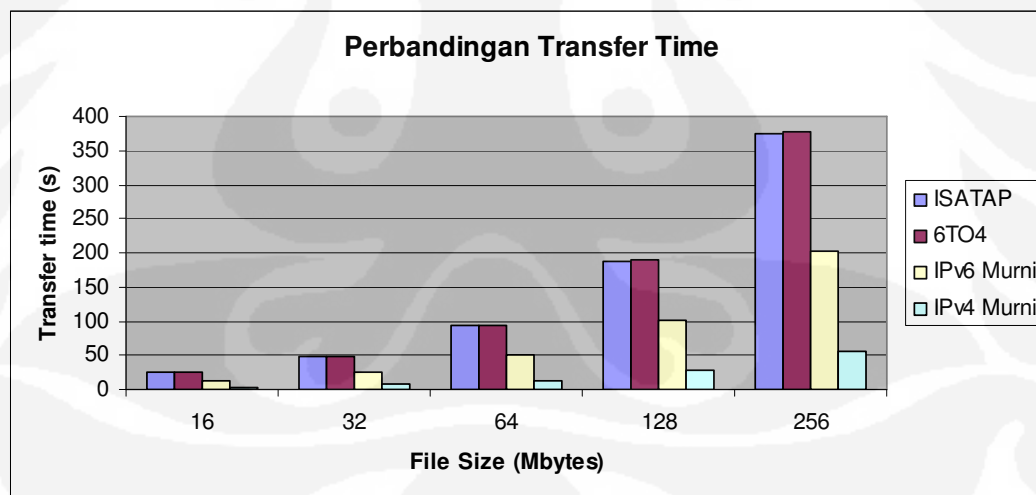
Gambar 4.9 *Transfer Time* pada *Summary* Wireshark

Dari pengujian data yang dilakukan sebanyak 10 kali pada masing – masing file dan masing – masing konfigurasi didapat data rata – rata dari nilai *transfer time* seperti pada Tabel 4.3.

Tabel 4.3 Data Rata – Rata *TransferTime*

File Size (MBytes)	Transfer Time (s)			
	IPv4 Murni	IPv6 Murni	6to4	ISATAP
16	3.2999	13.5779	25.1226	24.7021
32	6.7586	25.6723	47.6399	47.1153
64	13.4030	51.0382	94.7924	94.3174
128	27.1058	102.4862	188.9949	188.2111
256	54.9167	203.5639	377.9535	375.8524

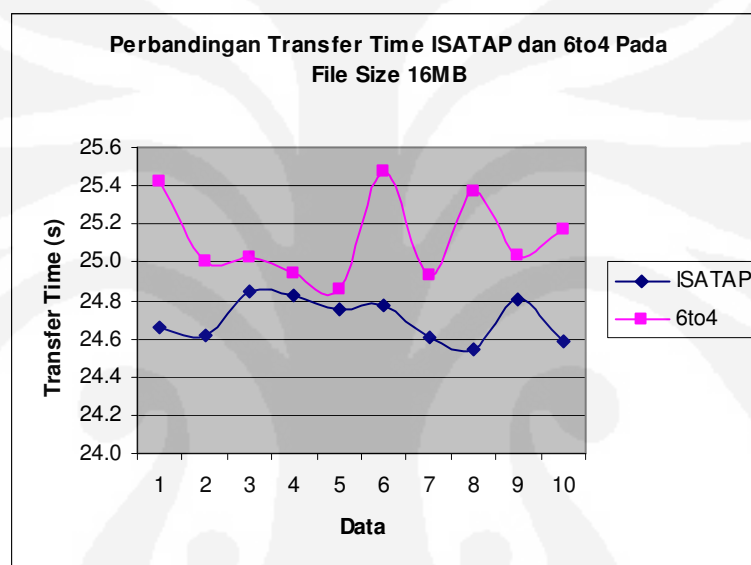
Berdasarkan hasil rata - rata pada Tabel 4.3, didapatkan bahwa ukuran dari kapasitas file mempunyai pengaruh terhadap nilai *transfer time*. Semakin besar kapasitas data maka semakin besar pula nilai dari *transfer time*. Jika dibandingkan antar jenis konfigurasi, maka konfigurasi IPv4 murni memiliki nilai *transfer time* lebih kecil dibandingkan dengan konfigurasi lainnya. Secara persentase rata – rata, konfigurasi IPv4 murni memiliki nilai *transfer time* lebih kecil 73.94% dari konfigurasi IPv6 murni. Jika dibandingkan dengan konfigurasi yang menggunakan *tunneling*, maka nilai *transfer time* IPv4 murni juga lebih kecil 85.93% dari konfigurasi *tunneling* 6to4 dan lebih kecil 85.81% dari konfigurasi ISATAP. Pada konfigurasi IPv6 murni juga memiliki nilai *transfer time* lebih kecil 45.8% dari konfigurasi *tunneling* 6to4 dan ISATAP. Hal ini dikarenakan adanya proses enkapsulasi dan dekapsulasi paket pada mekanisme *tunneling*. Selain *routing*, proses enkapsulasi dan dekapsulasi juga dapat menambah waktu *transfer* suatu file. Diagram perbandingan nilai *transfer time* dari empat konfigurasi dapat dilihat pada Gambar 4.10.



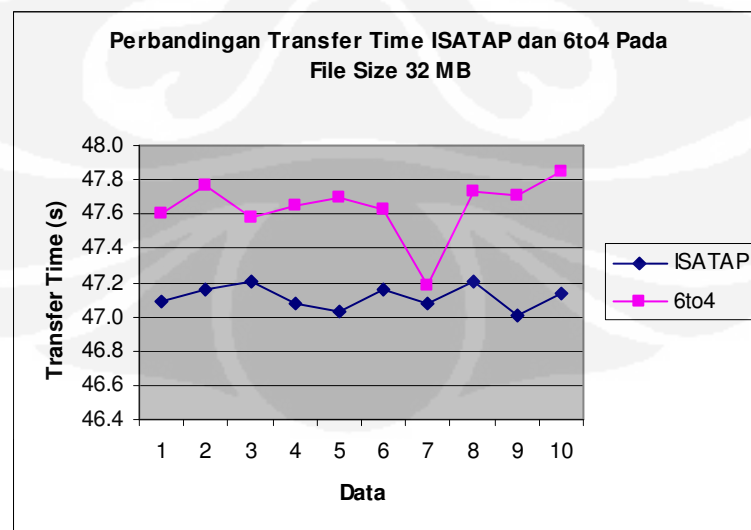
Gambar 4.10 Diagram Perbandingan *Transfer Time*

Jika dibandingkan antara konfigurasi ISATAP dan 6to4, maka nilai *transfer time* paling kecil terjadi pada konfigurasi ISATAP. Secara persentase rata – rata, konfigurasi ISATAP memiliki nilai *transfer time* lebih kecil 0.85% dari konfigurasi 6to4. Ini menunjukkan bahwa *tunneling* ISATAP dalam

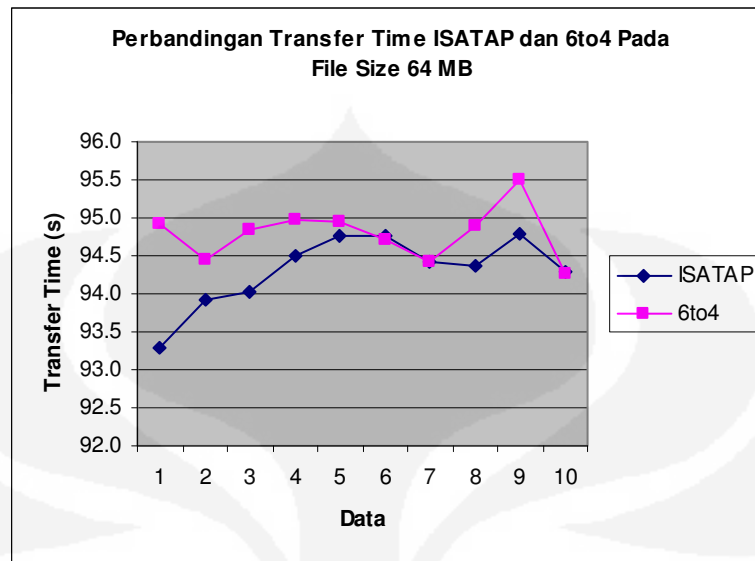
melakukan proses enkapsulasi dan dekapsulasi lebih cepat daripada 6to4. Selain itu, dilihat pada konfigurasi router untuk proses *routing*, konfigurasi 6to4 memiliki proses *routing* lebih banyak dari pada konfigurasi ISATAP. Proses *routing* ini akan menambah waktu pemrosesan paket pada router sehingga apabila jumlah *routing* semakin banyak waktu prosesnya juga semakin lama. Grafik perbedaan antara konfigurasi ISATAP dan 6to4 dapat dilihat pada Gambar 4.10 – Gambar 4.15. Grafik pada Gambar 4.10 – Gambar 4.15 diambil dari data pada Lampiran 9 – Lampiran 12.



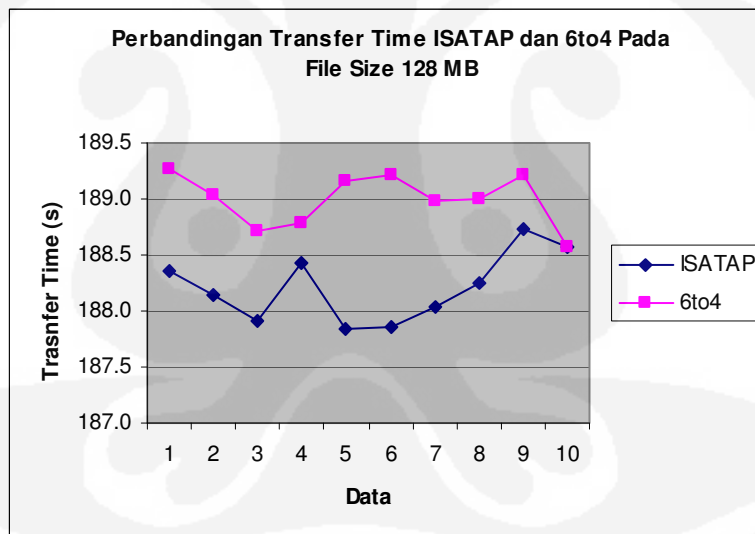
Gambar 4.11 Grafik Perbandingan *Transfer Time* ISATAP dan 6to4 File Size 16MB



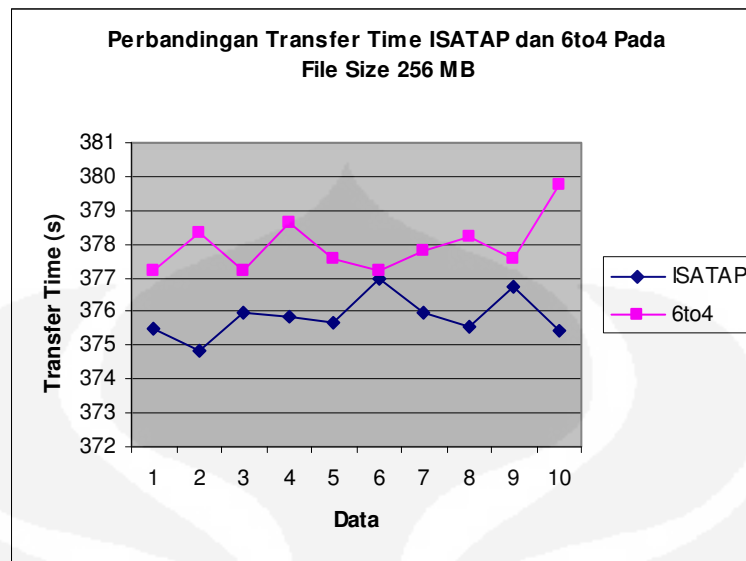
Gambar 4.12 Grafik Perbandingan *Transfer Time* ISATAP dan 6to4 File Size 32MB



Gambar 4.13 Grafik Perbandingan *Transfer Time* ISATAP dan 6to4 File Size 64MB



Gambar 4.14 Grafik Perbandingan *Transfer Time* ISATAP dan 6to4 File Size 128MB



Gambar 4.15 Grafik Perbandingan *Transfer Time* ISATAP dan 6to4 File Size 256MB

4.2.3. Analisa Delay

Delay adalah waktu yang dibutuhkan untuk setiap bit data dalam melewati jaringan dari terminal sumber ke terminal tujuan [9]. Parameter *delay* dihitung dengan cara membagi nilai *transfer time* dengan jumlah bit data. Ditunjukkan pada rumus dibawah ini :

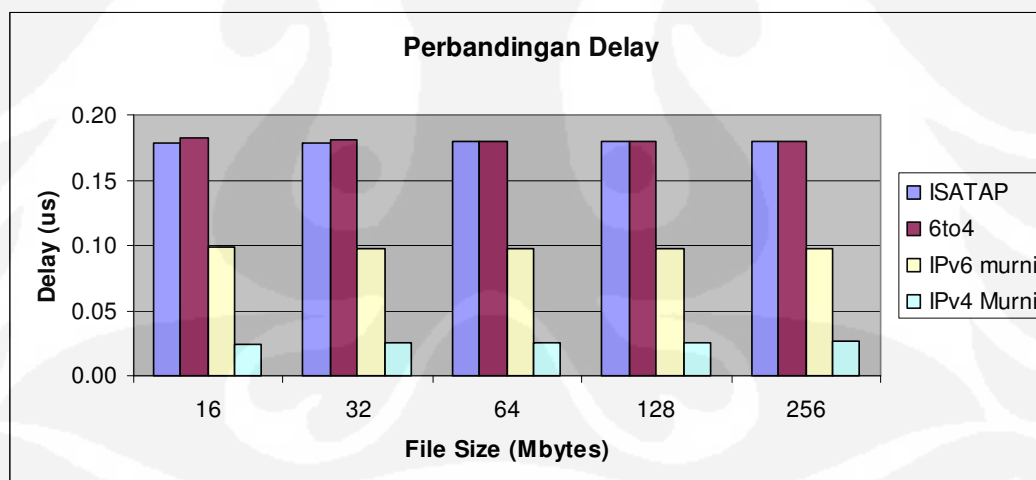
$$delay \text{ (sec)} = \frac{transfer \text{ time (sec)}}{jumlah \text{ bit}} \quad \dots\dots\dots [4.1]$$

Hasil pengambilan data secara keseluruhan untuk parameter *delay* dapat dilihat pada bagian Lampiran sedangkan untuk hasil rata – rata dari perhitungan *delay* dapat dilihat pada Tabel 4.3 dibawah ini.

Tabel 4.4 Data Rata – Rata Perhitungan *Delay*

File Size (MBytes)	Delay (µs)			
	IPv4 Murni	IPv6 Murni	6to4	ISATAP
16	0.02392	0.09842	0.18210	0.17905
32	0.02562	0.09731	0.18058	0.17859
64	0.02547	0.09699	0.18014	0.17924
128	0.02582	0.09762	0.18002	0.17928
256	0.02619	0.09709	0.18027	0.17927

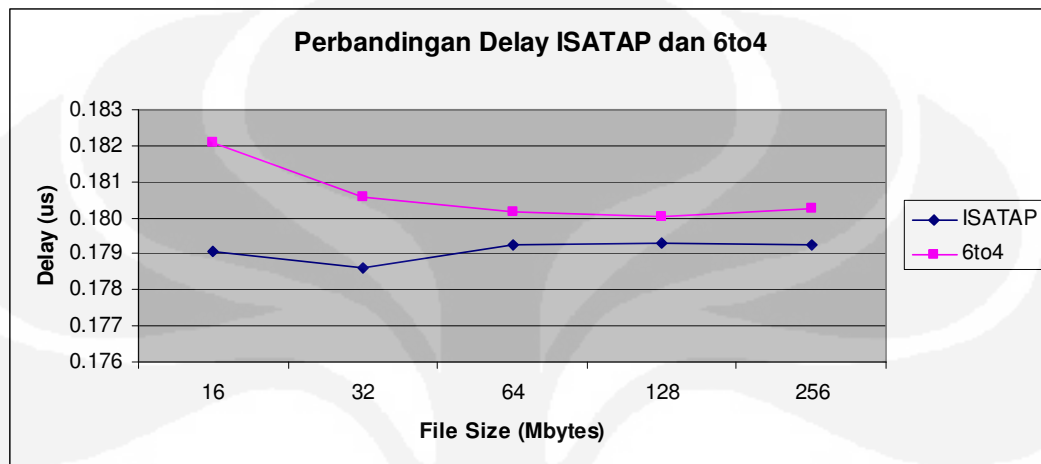
Dari hasil perhitungan rata – rata delay pada Tabel 4.4, dapat diamati bahwa diantara keempat konfigurasi tersebut yang memiliki nilai *delay* paling kecil adalah konfigurasi IPv4 murni. Secara persentase rata – rata, konfigurasi IPv4 murni memiliki nilai *delay* lebih kecil 73.94% dari konfigurasi IPv6 murni. Ini disebabkan karena besar kapasitas *header* IPv6 dua kali lebih besar daripada IPv4. Panjang *header* pada IPv6 40 bytes, sedangkan panjang *header* pada IPv4 20 bytes. Jika dibandingkan dengan konfigurasi *tunneling*, secara persentase rata – rata konfigurasi IPv4 murni memiliki *delay* lebih kecil 85.93% dari konfigurasi 6to4 dan lebih kecil 85.81% dari konfigurasi ISATAP. Untuk *delay* dari konfigurasi IPv6 murni lebih kecil 45.8% dari konfigurasi yang menggunakan *tunneling* 6to4 dan ISATAP. Ini menunjukkan bahwa selain proses *routing*, proses *tunneling* juga dapat menambah *delay* jaringan. Proses *tunneling* merupakan proses enkapsulasi dan dekapsulasi paket – paket yang masuk. Untuk diagram perbandingan nilai *delay* pada keempat konfigurasi dapat dilihat pada Gambar 4.16.



Gambar 4.16 Diagram Perbandingan Nilai *Delay*

Jika dibandingkan antara konfigurasi yang sama-sama menggunakan *tunneling* maka *delay* paling kecil terjadi pada *tunneling* ISATAP. Secara persentase rata – rata, konfigurasi ISATAP memiliki nilai *delay* lebih kecil 0.85% dari konfigurasi 6to4. Ini menunjukkan proses enkapsulasi dan dekapsulasi yang terjadi pada *tunneling* ISATAP lebih baik daripada 6to4.

Selain itu, dilihat pada konfigurasi proses *routing*, konfigurasi 6to4 memiliki proses *routing* lebih banyak daripada *tunneling* ISATAP. Ini menunjukkan jumlah proses *routing* dapat menambah delay pada jaringan. Untuk grafik perbandingan antara ISATAP dan 6to4 dapat dilihat pada Gambar 4.17.



Gambar 4.17 Grafik Perbandingan Nilai *Delay* antara ISATAP dan 6to4

BAB 5 KESIMPULAN

Berdasarkan hasil pengambilan data pada konfigurasi jaringan yang telah dilakukan, untuk penelitian ini didapatkan kesimpulan sebagai berikut :

1. Berdasarkan parameter *throughput*, konfigurasi IPv6 murni memiliki nilai *throughput* lebih kecil 73.39% dari konfigurasi IPv4 murni, konfigurasi 6to4 lebih kecil 85.66% dari IPv4 murni, sedangkan konfigurasi ISATAP lebih kecil 85.51% dari IPv4 murni.
2. Konfigurasi *tunneling* ISATAP memiliki nilai *throughput* lebih besar 1.1% dari konfigurasi *tunneling* 6to4.
3. Berdasarkan parameter *transfer time*, konfigurasi IPv4 murni memiliki nilai *transfer time* lebih kecil 73.94% dari IPv6 murni, IPv4 murni juga lebih kecil 85.93% dari *tunneling* 6to4 dan lebih kecil 85.81% dari *tunneling* ISATAP.
4. Konfigurasi ISATAP memiliki nilai *transfer time* lebih kecil 0.85% dari konfigurasi 6to4.
5. Dilihat pada parameter *delay*, konfigurasi IPv4 murni memiliki nilai *delay* lebih kecil 73.94% dari konfigurasi IPv6 murni, IPv4 murni juga lebih kecil 85.93% dari *tunneling* 6to4 dan lebih kecil 85.81% dari *tunneling* ISATAP.
6. Konfigurasi *tunneling* ISATAP memiliki nilai *delay* lebih kecil 0.85% dari konfigurasi *tunneling* 6to4.
7. Perbedaan panjang *header* pada IPv6 dan IPv4 mempengaruhi besarnya nilai *delay*.
8. Proses enkapsulasi dan dekapsulasi paket pada *tunneling* ISATAP lebih baik daripada *tunneling* 6to4.

DAFTAR REFERENSI

- [1]. Microsoft corporation, "*Introduction to IP version 6*", September 2003.
- [2]. Allied Telesyn International, "*Chapter 14: Internet Protocol version 6 (IPv6)*", Copyright (c) 1992-2003.
- [3]. Somad, Wahidi. "Interkoneksi IPv6 dan IPv4 dengan Mekanisme Automatic Tunneling", IlmuKomputer.com, 2003.
- [4]. Wikipedia, "6to4", *Last Modified* 18 Januari 2009. Diakses 21 Januari 2009 dari Wikipedia.
<<http://en.wikipedia.org/wiki/6to4>>
- [5]. Tremblay, Jean Francois. Lind, Mikael. "IPv6 Tunneling Techniques", Hexago Inc., September, 2006.
- [6]. www.cisco.com, "*Implementing tunneling for IPv6*", Diakses 3 Maret 2009.
<<http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-tunnel.html>>
- [7]. Tanenbaum, Andrew S. "*Computer Networks, Fourth Edition*". Prentice Hall. March 17, 2003.
- [8]. Isa, Mohammad. "Komparasi Unjuk Kerja File Transfer Protocol Pada Jaringan Test-Bed IPv6 VPN terhadap Teredo dan IPv4 Murni". Departemen Teknik Elektro, Universitas Indonesia, 2007-2008.
- [9]. "Network delay." Wikipedia. 2 Juni 2009.
<http://en.wikipedia.org/wiki/Network_delay>
- [10]. "Transmission Delay." Wikipedia. 15 April 2009.
<http://en.wikipedia.org/wiki/Transmission_delay>

LAMPIRAN 1 : Konfigurasi Router pada Jaringan IPv4 Murni

```
1. ROUTER_1#sh run
Building configuration...

Current configuration : 775 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ROUTER_1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$KiQA$Rk75mM3dd7vJOfrkd7.Sh1
!
no aaa new-model
ip subnet-zero
!
!
ip cef
!
!
interface FastEthernet0/0
description LAN to Server
ip address 192.168.1.1 255.255.255.248
duplex auto
speed auto
!
interface FastEthernet0/1
description WAN to ROUTER_2
ip address 192.168.2.1 255.255.255.252
duplex auto
speed auto
!
no ip http server
ip classless
ip route 192.168.3.0 255.255.255.248 192.168.2.2
!
!
dial-peer cor custom
!
!
line con 0
line aux 0
line vty 0 3
password cisco
login
line vty 4
login
!
!
End
```

LANJUTAN

```
2. ROUTER_2#sh run
Building configuration...
Current configuration : 795 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ROUTER_2
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$jmlF$OdXyoeUTQgs8GkTpLyt9t.
!
memory-size iomem 15
no aaa new-model
ip subnet-zero
!
!
no ip domain lookup
!
ip cef
!
interface FastEthernet0/0
description LAN to Client
ip address 192.168.3.1 255.255.255.248
duplex auto
speed auto
!
interface FastEthernet0/1
description WAN to ROUTER_1
ip address 192.168.2.2 255.255.255.252
duplex auto
speed auto
!
no ip http server
ip classless
ip route 192.168.1.0 255.255.255.248 192.168.2.1
!
!
dial-peer cor custom
!
!
line con 0
line aux 0
line vty 0 3
password cisco
login
line vty 4
login
!
!
end
```

LAMPIRAN 2 : Konfigurasi Router pada Jaringan IPv6 Murni

```
1. ROUTER_1#sh run
Building configuration...

Current configuration : 1154 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ROUTER_1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$KiQA$Rk75mM3dd7vJOfkrkd7.Sh1
!
no aaa new-model
ip subnet-zero
!
ip cef
ipv6 unicast-routing
!
!
interface FastEthernet0/0
description LAN to Server
no ip address
duplex auto
speed auto
ipv6 address 2001:0:0:A::1/64
ipv6 enable
!
interface FastEthernet0/1
description WAN to ROUTER_2
no ip address
duplex auto
speed auto
ipv6 address 2001:0:0:C::2/64
ipv6 enable
!
no ip http server
ip classless
!
ipv6 route ::/0 2001:0:0:C::1
!
dial-peer cor custom
!
line con 0
line aux 0
line vty 0 3
password cisco
login
line vty 4
login
!
End
```

LANJUTAN

```
2. ROUTER_2#sh run
Building configuration...
Current configuration : 835 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ROUTER_2
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$jmlF$OdXyoeUTQgs8GkTpLyt9t.
!
memory-size iomem 15
no aaa new-model
ip subnet-zero
!
no ip domain lookup
!
ip cef
ipv6 unicast-routing
!
interface FastEthernet0/0
description LAN to Client
no ip address
duplex auto
speed auto
ipv6 address 2001:0:0:B::1/64
ipv6 enable
!
interface FastEthernet0/1
description WAN to ROUTER_1
no ip address
duplex auto
speed auto
ipv6 address 2001:0:0:C::1/64
ipv6 enable
!
no ip http server
ip classless
!
ipv6 route ::/0 2001:0:0:C::2
!
dial-peer cor custom
!
line con 0
line aux 0
line vty 0 3
password cisco
login
line vty 4
login
!
end
```


LAMPIRAN 3 : Konfigurasi Router pada Jaringan Tunneling 6to4

```
1. ROUTER_1#sh run
Building configuration...

Current configuration : 1138 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname C2600-ROUTER1
!
boot-start-marker
boot-end-marker
!
no logging buffered
enable secret 5 $1$jmlF$OdXyoeUTQgs8GkTpLyt9t.
!
memory-size iomem 15
no aaa new-model
ip subnet-zero
!
!
no ip domain lookup
!
ip cef
ipv6 unicast-routing
!
!
interface Tunnel0
no ip address
no ip redirects
ipv6 address 2002:C0A8:1:1::1/64
ipv6 enable
tunnel source FastEthernet0/1
tunnel mode ipv6ip 6to4
!
interface FastEthernet0/0
description LAN-to-Server
no ip address
duplex auto
speed auto
ipv6 address 2001:0:0:A::1/64
ipv6 enable
ipv6 rip process1 enable
!
interface FastEthernet0/1
description WAN-to-ROUTER2
ip address 192.168.0.1 255.255.255.252
duplex auto
speed auto
!
router rip
version 2
network 192.168.0.0
```

LANJUTAN

```
no ip http server
ip classless
!
!
ipv6 route 2002::/16 Tunnel0
ipv6 route ::/0 2002:C0A8:2:1::1
ipv6 router rip process1
!
!
dial-peer cor custom
!
!
line con 0
line aux 0
line vty 0 3
  password cisco
  login
line vty 4
  login
!
!
end
```

2. ROUTER_2#sh run
Building configuration...

```
Current configuration : 1117 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname C2600-ROUTER2
!
boot-start-marker
boot-end-marker
!
no logging buffered
enable secret 5 $1$KiQA$Rk75mM3dd7vJOfrkd7.Sh1
!
no aaa new-model
ip subnet-zero
!
!
no ip domain lookup
!
ip cef
ipv6 unicast-routing
!
!
interface Tunnel0
  no ip address
  no ip redirects
  ipv6 address 2002:C0A8:2:1::1/64
  ipv6 enable
```

LANJUTAN

```
tunnel source FastEthernet0/1
  tunnel mode ipv6ip 6to4
!
interface FastEthernet0/0
  description LAN-to-Client
  no ip address
  duplex auto
  speed auto
  ipv6 address 2001:0:0:B::1/64
  ipv6 enable
  ipv6 rip process1 enable
!
interface FastEthernet0/1
  description WAN-to-ROUTER1
  ip address 192.168.0.2 255.255.255.252
  duplex auto
  speed auto
!
router rip
  version 2
  network 192.168.0.0
!
no ip http server
ip classless
!
!
ipv6 route 2002::/16 Tunnel0
ipv6 route ::/0 2002:C0A8:1:1::1
ipv6 router rip process1
!
!
dial-peer cor custom
!
!
line con 0
line aux 0
line vty 0 3
  password cisco
  login
line vty 4
  login
!
!
end
```

LAMPIRAN 4 : Konfigurasi Router pada Jaringan Tunneling ISATAP

```
1. ROUTER_1#sh run
Building configuration...

Current configuration : 1119 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname C2600-ROUTER1
!
boot-start-marker
boot-end-marker
!
no logging buffered
enable secret 5 $1$jmlF$OdXyoeUTQgs8GkTpLyt9t.
!
memory-size iomem 15
no aaa new-model
ip subnet-zero
!
!
no ip domain lookup
!
ip cef
ipv6 unicast-routing
!
!
interface Tunnel0
no ip address
no ip redirects
ipv6 address 2001:DB8:0:7:0:5EFE:C0A8:1/64
ipv6 enable
tunnel source FastEthernet0/1
tunnel mode ipv6ip isatap
!
interface FastEthernet0/0
description LAN to Server
no ip address
duplex auto
speed auto
ipv6 address 2001:0:0:A::1/64
ipv6 enable
ipv6 rip process1 enable
!
interface FastEthernet0/1
description WAN to ROUTER_2
ip address 192.168.0.1 255.255.255.252
duplex auto
speed auto
!
router rip
version 2
```

LANJUTAN

```
network 192.168.0.0
!
no ip http server
ip classless
!
!
ipv6 route ::/0 2001:DB8:0:7:0:5EFE:C0A8:2
ipv6 router rip process1
!
!
dial-peer cor custom
!
!
line con 0
line aux 0
line vty 0 3
password cisco
login
line vty 4
login
!
!
end
```

2. ROUTER_2#sh run
Building configuration...

```
Current configuration : 1097 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname C2600-ROUTER2
!
boot-start-marker
boot-end-marker
!
no logging buffered
enable secret 5 $1$KiQA$Rk75mM3dd7vJOfrkd7.Sh1
!
no aaa new-model
ip subnet-zero
!
!
no ip domain lookup
!
ip cef
ipv6 unicast-routing
!
!
interface Tunnel0
no ip address
no ip redirects
ipv6 address 2001:DB8:0:7:0:5EFE:C0A8:2/64
```

LANJUTAN

```
ipv6 enable
tunnel source FastEthernet0/1
tunnel mode ipv6ip isatap
!
interface FastEthernet0/0
description LAN to Client
no ip address
duplex auto
speed auto
ipv6 address 2001:0:0:B::1/64
ipv6 enable
ipv6 rip process1 enable
!
interface FastEthernet0/1
description WAN-to-ROUTER1
ip address 192.168.0.2 255.255.255.252
duplex auto
speed auto
!
router rip
version 2
network 192.168.0.0
!
no ip http server
ip classless
!
!
ipv6 route ::/0 2001:DB8:0:7:0:5EFE:C0A8:1
ipv6 router rip process1
!
!
dial-peer cor custom
!
!
line con 0
line aux 0
line vty 0 3
password cisco
login
line vty 4
login
!
!
end
```

LAMPIRAN 5 : Hasil Capture Wireshark Konfigurasi IPv4 Murni

The screenshot displays the Wireshark interface with a capture filter: `(ip.addr eq 192.168.3.2 and ip.addr eq 192.168.1.2) and (tcp.port eq 20 and ...)`. The packet list shows alternating TCP and FTP-DATA packets. Packet 2418 is selected, and its details are shown in the lower pane:

- Frame 2418 (1514 bytes on wire, 1514 bytes captured)
- Ethernet II, Src: Cisco_9b:a5:e0 (00:30:94:9b:a5:e0), Dst: wistron_5a:c9:17 (00:16:d3:5a:c9:17)
- Internet Protocol, Src: 192.168.3.2 (192.168.3.2), Dst: 192.168.1.2 (192.168.1.2)
- Transmission Control Protocol, Src Port: ftp-data (20), Dst Port: es-elmd (1822), Seq: 247221, ...
- FTP Data

The raw data pane shows the hex and ASCII representation of the packet bytes:

```

0000 00 16 d3 5a c9 17 00 30 94 9b a5 e0 08 00 45 00  ...Z...0 .....E.
0010 05 dc 99 5c 40 00 7e 06 d8 6a c0 a8 03 02 c0 a8  ...@...~. .j.....
0020 01 02 00 14 07 1e a8 d8 55 6f 75 02 b3 a3 50 10  .....Uou...P.
0030 80 00 c5 d8 00 00 11 78 a6 9c 14 89 31 9b 5e 39  .....x .....1.^9
0040 6a 85 c0 45 f2 36 a8 a7 de 0c b2 a3 e2 75 f5 54  j..E.6.. .....u.T
0050 cd 22 bf 59 39 85 08 0a 57 33 25 d6 d1 10 d8 08  ."Y9... w3%....
  
```

LAMPIRAN 6 : Hasil Capture Wireshark Konfigurasi IPv6 Murni

The screenshot shows a Wireshark capture of network traffic. The main pane displays a list of packets, with packet 3003 selected. The packet list shows alternating FTP-DATA and TCP packets between source IP 2001:0:0:b::2 and destination IP 2001:0:0:a::2. Packet 3003 is an FTP-DATA packet of 1440 bytes.

No.	Time	Source	Destination	Protocol	Info
2990	3.308964	2001:0:0:b::2	2001:0:0:a::2	FTP-DATA	FTP Data: 1440 bytes
2991	3.309006	2001:0:0:a::2	2001:0:0:b::2	TCP	1028 > ftp-data [ACK] S
2992	3.309306	2001:0:0:b::2	2001:0:0:a::2	FTP-DATA	FTP Data: 1440 bytes
2993	3.309381	2001:0:0:a::2	2001:0:0:b::2	TCP	1028 > ftp-data [ACK] S
2994	3.312088	2001:0:0:b::2	2001:0:0:a::2	FTP-DATA	FTP Data: 1440 bytes
2995	3.313296	2001:0:0:b::2	2001:0:0:a::2	FTP-DATA	FTP Data: 1440 bytes
2996	3.313362	2001:0:0:a::2	2001:0:0:b::2	TCP	1028 > ftp-data [ACK] S
2997	3.314207	2001:0:0:b::2	2001:0:0:a::2	FTP-DATA	FTP Data: 1440 bytes
2998	3.314490	2001:0:0:b::2	2001:0:0:a::2	FTP-DATA	FTP Data: 1440 bytes
2999	3.314531	2001:0:0:a::2	2001:0:0:b::2	TCP	1028 > ftp-data [ACK] S
3000	3.314866	2001:0:0:b::2	2001:0:0:a::2	FTP-DATA	FTP Data: 1440 bytes
3001	3.314947	2001:0:0:a::2	2001:0:0:b::2	TCP	1028 > ftp-data [ACK] S
3002	3.315700	2001:0:0:b::2	2001:0:0:a::2	FTP-DATA	FTP Data: 1440 bytes
3003	3.318818	2001:0:0:b::2	2001:0:0:a::2	FTP-DATA	FTP Data: 1440 bytes
3004	3.318864	2001:0:0:a::2	2001:0:0:b::2	TCP	1028 > ftp-data [ACK] S
3005	3.319198	2001:0:0:b::2	2001:0:0:a::2	FTP-DATA	FTP Data: 1440 bytes
3006	3.319233	2001:0:0:a::2	2001:0:0:b::2	TCP	1028 > ftp-data [ACK] S
3007	3.320830	2001:0:0:b::2	2001:0:0:a::2	FTP-DATA	FTP Data: 1440 bytes
3008	3.321299	2001:0:0:b::2	2001:0:0:a::2	FTP-DATA	FTP Data: 1440 bytes
3009	3.321341	2001:0:0:a::2	2001:0:0:b::2	TCP	1028 > ftp-data [ACK] S
3010	3.322521	2001:0:0:b::2	2001:0:0:a::2	FTP-DATA	FTP Data: 1440 bytes
3011	3.322604	2001:0:0:a::2	2001:0:0:b::2	TCP	1028 > ftp-data [ACK] S
3012	3.322790	2001:0:0:b::2	2001:0:0:a::2	FTP-DATA	FTP Data: 1440 bytes

Packet 3003 details:

- Frame 3003 (1514 bytes on wire, 1514 bytes captured)
- Ethernet II, Src: Cisco_9b:a5:e0 (00:30:94:9b:a5:e0), Dst: wistron_5a:c9:17 (00:16:d3:5a:c9:17)
- Internet Protocol version 6
- Transmission Control Protocol, Src Port: ftp-data (20), Dst Port: 1028 (1028), Seq: 2291457, Ack: 1028
- FTP Data

Hex dump of packet 3003:

```

0000 00 16 d3 5a c9 17 00 30 94 9b a5 e0 86 dd 60 00  ...Z...0 .....
0010 00 00 05 b4 06 3e 20 01 00 00 00 00 00 0b 00 00  .....> .....
0020 00 00 00 00 00 02 20 01 00 00 00 00 00 0a 00 00  .....
0030 00 00 00 00 00 02 00 14 04 04 08 c3 37 9a 21 62  .....7.!b
0040 e7 2d 50 10 80 00 f7 fd 00 00 a7 47 03 6a fb 73  -P.....G.j.s
0050 69 e7 0e f9 6f 0c 3d 2c e7 44 8d 3e 59 b5 d2 60  i...o.=, .D.>Y...
    
```


LAMPIRAN 7: Hasil Capture Wireshark Konfigurasi Tunneling 6to4

16M_1.cap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filtre: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
2308	5.109465	2001:0:0:a::2	2001:0:0:b::2	TCP	cp1scrambler-a1 > ftp-c
2309	5.110223	2001:0:0:b::2	2001:0:0:a::2	FTP-DATA	FTP Data: 1420 bytes
2310	5.110496	2001:0:0:b::2	2001:0:0:a::2	FTP-DATA	FTP Data: 1420 bytes
2311	5.110538	2001:0:0:a::2	2001:0:0:b::2	TCP	cp1scrambler-a1 > ftp-c
2312	5.110900	2001:0:0:b::2	2001:0:0:a::2	FTP-DATA	FTP Data: 1420 bytes
2313	5.110997	2001:0:0:a::2	2001:0:0:b::2	TCP	cp1scrambler-a1 > ftp-c
2314	5.119347	2001:0:0:b::2	2001:0:0:a::2	FTP-DATA	FTP Data: 1420 bytes
2315	5.119547	2001:0:0:b::2	2001:0:0:a::2	FTP-DATA	FTP Data: 1420 bytes
2316	5.119591	2001:0:0:a::2	2001:0:0:b::2	TCP	cp1scrambler-a1 > ftp-c
2317	5.120294	2001:0:0:b::2	2001:0:0:a::2	FTP-DATA	FTP Data: 1420 bytes
2318	5.120384	2001:0:0:a::2	2001:0:0:b::2	TCP	cp1scrambler-a1 > ftp-c
2319	5.120633	2001:0:0:b::2	2001:0:0:a::2	FTP-DATA	FTP Data: 1420 bytes
2320	5.121245	2001:0:0:b::2	2001:0:0:a::2	FTP-DATA	FTP Data: 1420 bytes
2321	5.121288	2001:0:0:a::2	2001:0:0:b::2	TCP	cp1scrambler-a1 > ftp-c
2322	5.121471	2001:0:0:b::2	2001:0:0:a::2	FTP-DATA	FTP Data: 1420 bytes
2323	5.121563	2001:0:0:a::2	2001:0:0:b::2	TCP	cp1scrambler-a1 > ftp-c
2324	5.130146	2001:0:0:b::2	2001:0:0:a::2	FTP-DATA	FTP Data: 1420 bytes
2325	5.130471	2001:0:0:b::2	2001:0:0:a::2	FTP-DATA	FTP Data: 1420 bytes
2326	5.130523	2001:0:0:a::2	2001:0:0:b::2	TCP	cp1scrambler-a1 > ftp-c
2327	5.130821	2001:0:0:b::2	2001:0:0:a::2	FTP-DATA	FTP Data: 1420 bytes
2328	5.130906	2001:0:0:a::2	2001:0:0:b::2	TCP	cp1scrambler-a1 > ftp-c
2329	5.131631	2001:0:0:b::2	2001:0:0:a::2	FTP-DATA	FTP Data: 1420 bytes
2330	5.131964	2001:0:0:b::2	2001:0:0:a::2	FTP-DATA	FTP Data: 1420 bytes

Frame 10 (1494 bytes on wire, 1494 bytes captured)

- Ethernet II, Src: Cisco_9b:a5:e0 (00:30:94:9b:a5:e0), Dst: wistron_5a:c9:17 (00:16:d3:5a:c9:17)
- Internet Protocol version 6
- Data (1432 bytes)

```
0000 00 16 d3 5a c9 17 00 30 94 9b a5 e0 86 dd 60 00  ...Z...0 .....
0010 00 00 05 a0 2c 3e 20 01 00 00 00 00 00 0b 00 00  .....> . .....
0020 00 00 00 00 00 02 20 01 00 00 00 00 00 0a 00 00  .....
0030 00 00 00 00 00 00 02 3a 00 27 29 00 00 19 72 6c 6d  .....: )...rlm
0040 6e 6f 70 71 72 73 74 75 76 77 61 62 63 64 65 66  nopqrstu vwabcdef
0050 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmn opqrstuv
```

File: "D:\DATA TAI6to4\16M\16M_1.cap" 22 MB ... Packets: 22797 Displayed: 22797 Marked: 0 Profile: Default

LAMPIRAN 8: Hasil Capture Wireshark Konfigurasi Tunneling ISATAP

The screenshot displays the Wireshark interface for a capture file named '1.cap'. The main packet list pane shows the following data:

No.	Time	Source	Destination	Protocol	Info
8009	9.789663	2001:0:0:a::2	2001:0:0:b::2	TCP	cognex-insight > ftp-da
8010	9.789678	2001:0:0:b::2	2001:0:0:a::2	FTP-DATA	FTP Data: 1420 bytes
8011	9.789769	2001:0:0:a::2	2001:0:0:b::2	TCP	cognex-insight > ftp-da
8012	9.790527	2001:0:0:b::2	2001:0:0:a::2	FTP-DATA	FTP Data: 1420 bytes
8013	9.790864	2001:0:0:b::2	2001:0:0:a::2	FTP-DATA	FTP Data: 1420 bytes
8014	9.790910	2001:0:0:a::2	2001:0:0:b::2	TCP	cognex-insight > ftp-da
8015	9.791248	2001:0:0:b::2	2001:0:0:a::2	FTP-DATA	FTP Data: 1420 bytes
8016	9.791337	2001:0:0:a::2	2001:0:0:b::2	TCP	cognex-insight > ftp-da
8017	9.799649	2001:0:0:b::2	2001:0:0:a::2	FTP-DATA	FTP Data: 1420 bytes
8018	9.799833	2001:0:0:b::2	2001:0:0:a::2	FTP-DATA	FTP Data: 1420 bytes
8019	9.799881	2001:0:0:a::2	2001:0:0:b::2	TCP	cognex-insight > ftp-da
8020	9.800843	2001:0:0:b::2	2001:0:0:a::2	FTP-DATA	FTP Data: 1420 bytes
8021	9.800893	2001:0:0:a::2	2001:0:0:b::2	TCP	cognex-insight > ftp-da
8022	9.800901	2001:0:0:b::2	2001:0:0:a::2	FTP-DATA	FTP Data: 1420 bytes
8023	9.801419	2001:0:0:b::2	2001:0:0:a::2	FTP-DATA	FTP Data: 1420 bytes
8024	9.801468	2001:0:0:a::2	2001:0:0:b::2	TCP	cognex-insight > ftp-da
8025	9.802079	2001:0:0:b::2	2001:0:0:a::2	FTP-DATA	FTP Data: 1420 bytes
8026	9.802120	2001:0:0:a::2	2001:0:0:b::2	TCP	cognex-insight > ftp-da
8027	9.810251	2001:0:0:b::2	2001:0:0:a::2	FTP-DATA	FTP Data: 1420 bytes
8028	9.810519	2001:0:0:b::2	2001:0:0:a::2	FTP-DATA	FTP Data: 1420 bytes
8029	9.810551	2001:0:0:a::2	2001:0:0:b::2	TCP	cognex-insight > ftp-da
8030	9.810968	2001:0:0:b::2	2001:0:0:a::2	FTP-DATA	FTP Data: 1420 bytes
8031	9.811596	2001:0:0:b::2	2001:0:0:a::2	FTP-DATA	FTP Data: 1420 bytes

The packet details pane for packet 8013 shows the following structure:

- Frame 8013 (1494 bytes on wire, 1494 bytes captured)
- Ethernet II, Src: Cisco_9b:a5:e0 (00:30:94:9b:a5:e0), Dst: wistron_5a:c9:17 (00:16:d3:5a:c9:17)
- Internet Protocol Version 6
- Transmission Control Protocol, Src Port: ftp-data (20), Dst Port: cognex-insight (1069), Seq: 6
- FTP Data

The packet bytes pane shows the following hex and ASCII data:

```

0000 00 16 d3 5a c9 17 00 30 94 9b a5 e0 86 dd 60 00  ...Z...0 .....`.
0010 00 00 05 a0 06 3e 20 01 00 00 00 00 00 0b 00 00  .....> . .....
0020 00 00 00 00 00 02 20 01 00 00 00 00 00 0a 00 00  .....
0030 00 00 00 00 00 02 00 14 04 2d 2a 26 6e 3e 5b 01  .....-*&n>[.
0040 32 e7 50 10 80 00 c8 da 00 00 a3 41 48 21 f7 96  2.P.....AH!..
0050 21 eb 1e 90 c3 5b 59 3f d6 bf 9f 6f 69 8e 37 86  !....[Y? ...oi.7.

```

LAMPIRAN 9 : Data Hasil Uji Coba Konfigurasi IPv4 Murni

File	Delay (μ sec)										Rata - rata
	1	2	3	4	5	6	7	8	9	10	
16M (17245396 bytes)	0.02813	0.02303	0.02286	0.02335	0.02286	0.02413	0.02296	0.02411	0.02366	0.02411	0.02392
32M (32976505 bytes)	0.02523	0.02347	0.02325	0.02912	0.02355	0.03122	0.03026	0.02304	0.02368	0.02336	0.02562
64M (65775243 bytes)	0.02521	0.02473	0.02809	0.02324	0.02648	0.02406	0.02688	0.02837	0.02419	0.02345	0.02547
128M (131228435 bytes)	0.02356	0.02972	0.02381	0.02594	0.02565	0.02586	0.02465	0.03000	0.02602	0.02296	0.02582
256M (262071864 bytes)	0.02383	0.02382	0.02296	0.02473	0.02762	0.02803	0.02315	0.02413	0.03356	0.03011	0.02619
File	Transfer Time (sec)										Rata - rata
	1	2	3	4	5	6	7	8	9	10	
16M (17245396 bytes)	3.8810	3.1770	3.1540	3.2210	3.1540	3.3290	3.1670	3.3260	3.2640	3.3260	3.2999
32M (32976505 bytes)	6.6550	6.1910	6.1340	7.6830	6.2140	8.2370	7.9840	6.0780	6.2470	6.1630	6.7586
64M (65775243 bytes)	13.2680	13.0130	14.7820	12.2310	13.9350	12.6580	14.1460	14.9260	12.7290	12.3420	13.4030
128M (131228435 bytes)	24.7360	31.2050	24.9990	27.2370	26.9320	27.1480	25.8800	31.4940	27.3200	24.1070	27.1058
256M (262071864 bytes)	49.9580	49.9320	48.1390	51.8390	57.8990	58.7770	48.5430	50.5890	70.3550	63.1360	54.9167
File	Throughput (Mbps)										Rata - rata
	1	2	3	4	5	6	7	8	9	10	
16M (17245396 bytes)	34.3387	43.3734	45.9994	45.3708	45.6798	43.8901	46.1385	43.9403	44.7642	43.9311	43.7426
32M (32976505 bytes)	41.8221	44.3645	45.5594	36.3701	44.9709	33.9234	34.4998	45.9760	44.7288	45.3420	41.7557
64M (65775243 bytes)	41.7794	42.8312	37.7038	45.5722	39.9618	43.9596	39.1520	37.0176	43.7871	45.1615	41.6926
128M (131228435 bytes)	44.7456	35.4721	44.4837	40.5944	41.2226	40.9173	42.9673	35.1436	40.5739	46.1065	41.2227
256M (262071864 bytes)	44.4495	44.2943	46.0680	42.6833	37.8114	37.4509	45.5494	43.5245	31.5048	35.0063	40.8342

LAMPIRAN 10 : Data Hasil Uji Coba Konfigurasi IPv6 Murni

File	Delay (µs)										Rata - rata
	1	2	3	4	5	6	7	8	9	10	
16M (17245396 bytes)	0.0995	0.0999	0.0980	0.0981	0.0971	0.0979	0.0998	0.0971	0.0990	0.0978	0.0984
32M (32976505 bytes)	0.0974	0.0981	0.0970	0.0979	0.0972	0.0970	0.0973	0.0970	0.0971	0.0972	0.0973
64M (65775243 bytes)	0.0970	0.0969	0.0967	0.0970	0.0969	0.0969	0.0969	0.0967	0.0972	0.0977	0.0970
128M (131228435 bytes)	0.0972	0.1002	0.1016	0.0970	0.0965	0.0970	0.0967	0.0964	0.0968	0.0969	0.0976
256M (262071864 bytes)	0.0966	0.0967	0.0967	0.0967	0.0972	0.0973	0.0973	0.0970	0.0975	0.0979	0.0971
File	Transfer Time (sec)										Rata - rata
	1	2	3	4	5	6	7	8	9	10	
16M (17245396 bytes)	13.7270	13.7810	13.5140	13.5400	13.3970	13.5080	13.7700	13.3960	13.6580	13.4880	13.5779
32M (32976505 bytes)	25.6880	25.8890	25.5800	25.8280	25.6520	25.5810	25.6730	25.5850	25.6080	25.6390	25.6723
64M (65775243 bytes)	51.0360	51.0000	50.8790	51.0660	50.9700	50.9880	51.0020	50.9080	51.1280	51.4050	51.0382
128M (131228435 bytes)	102.0160	105.1480	106.6340	101.8390	101.2970	101.8110	101.5580	101.2330	101.6500	101.6760	102.4862
256M (262071864 bytes)	202.5110	202.8420	202.8090	202.7310	203.8700	204.0350	203.9530	203.2850	204.3550	205.2480	203.5639
File	Throughput (Mbps)										Rata - rata
	1	2	3	4	5	6	7	8	9	10	
16M (17245396 bytes)	10.9025	10.8597	11.0735	11.0533	11.1707	11.0787	10.8680	11.1715	10.9577	11.0956	11.0231
32M (32976505 bytes)	11.1402	11.0536	11.1871	11.0795	11.1556	11.1866	11.1465	11.1850	11.1750	11.1615	11.1471
64M (65775243 bytes)	11.1839	11.1921	11.2185	11.1774	11.1985	11.1943	11.1914	11.2119	11.1640	11.1036	11.1836
128M (131228435 bytes)	11.1625	10.8303	10.6795	11.1818	11.2416	11.1851	11.2129	11.2487	11.2026	11.2000	11.1145
256M (262071864 bytes)	11.2297	11.2114	11.2133	11.2179	11.1552	11.1463	11.1506	11.1873	11.1288	11.0803	11.1721

LAMPIRAN 11 : Data Hasil Uji Coba Konfigurasi Tunneling 6to4

File	Delay (μ s)										Rata - rata
	1	2	3	4	5	6	7	8	9	10	
16M (17245396 bytes)	0.1842	0.1812	0.1814	0.1808	0.1802	0.1847	0.1807	0.1839	0.1815	0.1824	0.1821
32M (32976505 bytes)	0.1805	0.1811	0.1804	0.1806	0.1808	0.1805	0.1788	0.1809	0.1809	0.1814	0.1806
64M (65775243 bytes)	0.1804	0.1795	0.1802	0.1805	0.1804	0.1800	0.1795	0.1804	0.1815	0.1791	0.1801
128M (131228435 bytes)	0.1803	0.1801	0.1798	0.1798	0.1802	0.1802	0.1800	0.1800	0.1802	0.1796	0.1800
256M (262071864 bytes)	0.1799	0.1805	0.1799	0.1806	0.1801	0.1799	0.1802	0.1804	0.1801	0.1811	0.1803
File	Transfer Time (sec)										Rata - rata
	1	2	3	4	5	6	7	8	9	10	
16M (17245396 bytes)	25.4170	25.0020	25.0230	24.9410	24.8570	25.4750	24.9330	25.3710	25.0400	25.1670	25.1226
32M (32976505 bytes)	47.6060	47.7720	47.5810	47.6490	47.6960	47.6250	47.1810	47.7290	47.7110	47.8490	47.6399
64M (65775243 bytes)	94.9310	94.4430	94.8420	94.9620	94.9490	94.7120	94.4300	94.9060	95.4900	94.2590	94.7924
128M (131228435 bytes)	189.2600	189.0350	188.7190	188.7910	189.1580	189.2170	188.9860	188.9940	189.2130	188.5760	188.9949
256M (262071864 bytes)	377.2110	378.3510	377.2200	378.6310	377.5650	377.2370	377.8080	378.1890	377.5910	379.7320	377.9535
File	Throughput (Mbps)										Rata - rata
	1	2	3	4	5	6	7	8	9	10	
16M (17245396 bytes)	5.8955	5.9935	5.9887	6.0085	6.0288	5.8827	6.0104	5.9065	6.0058	5.9885	5.9709
32M (32976505 bytes)	6.0192	5.9983	6.0224	6.0136	6.0078	6.0165	6.0733	6.0034	5.5358	5.5213	5.9211
64M (65775243 bytes)	6.0206	6.0517	6.0262	6.0186	6.0192	6.0342	6.0524	6.0221	5.9853	6.0633	6.0294
128M (131228435 bytes)	6.0247	6.0318	6.0419	6.0399	6.0282	6.0264	6.0338	6.0334	6.0265	6.0468	6.0333
256M (262071864 bytes)	6.0368	6.0188	6.0369	6.0144	6.0313	6.0366	6.0271	6.0210	6.0306	5.9964	6.0250

LAMPIRAN 12 : Data Hasil Uji Coba Konfigurasi *Tunneling* ISATAP

File	Delay (μ s)										Rata - rata
	1	2	3	4	5	6	7	8	9	10	
16M (17245396 bytes)	0.17874	0.17845	0.18010	0.17995	0.17940	0.17956	0.17836	0.17790	0.17981	0.17821	0.17905
32M (32976505 bytes)	0.17850	0.17874	0.17892	0.17847	0.17828	0.17876	0.17847	0.17895	0.17820	0.17865	0.17859
64M (65775243 bytes)	0.17730	0.17851	0.17870	0.17958	0.18009	0.18011	0.17943	0.17933	0.18016	0.17920	0.17924
128M (131228435 bytes)	0.17941	0.17921	0.17899	0.17949	0.17893	0.17894	0.17911	0.17932	0.17977	0.17962	0.17928
256M (262071864 bytes)	0.17909	0.17880	0.17932	0.17928	0.17920	0.17982	0.17933	0.17911	0.17969	0.17906	0.17927
File	Transfer Time (sec)										Rata - rata
	1	2	3	4	5	6	7	8	9	10	
16M (17245396 bytes)	24.6600	24.6200	24.8470	24.8270	24.7510	24.7730	24.6070	24.5430	24.8070	24.5860	24.7021
32M (32976505 bytes)	47.0892	47.1540	47.2014	47.0832	47.0319	47.1600	47.0831	47.2080	47.0108	47.1313	47.1153
64M (65775243 bytes)	93.2972	93.9321	94.0314	94.4966	94.7611	94.7760	94.4184	94.3645	94.8010	94.2957	94.3174
128M (131228435 bytes)	188.3542	188.1425	187.9041	188.4307	187.8448	187.8540	188.0360	188.2530	188.7240	188.5680	188.2111
256M (262071864 bytes)	375.4800	374.8660	375.9480	375.8690	375.6990	376.9980	375.9710	375.5270	376.7430	375.4230	375.8524
File	Throughput (Mbps)										Rata - rata
	1	2	3	4	5	6	7	8	9	10	
16M (17245396 bytes)	6.0748	6.0846	5.9329	6.0341	6.0526	6.0477	6.0874	6.1032	6.0386	6.0911	6.0547
32M (32976505 bytes)	6.0831	6.0744	6.0672	6.0831	6.0893	6.0742	6.0838	6.0682	6.0923	6.0771	6.0793
64M (65775243 bytes)	6.1233	6.0829	6.0763	6.0483	6.0314	6.0306	6.0534	6.0335	6.0287	6.0612	6.0570
128M (131228435 bytes)	6.0538	6.0608	6.0685	6.0514	6.0704	6.0701	6.0642	6.0573	6.0421	6.0471	6.0586
256M (262071864 bytes)	6.0648	6.0748	6.0574	6.0586	6.0614	6.0407	6.0570	6.0642	6.0443	6.0656	6.0589