



**UNIVERSITAS INDONESIA**

**ANALISA PENGARUH *BIT RATE* TERHADAP *DELAY* DAN  
*PACKET LOSS* PADA JARINGAN IPV6  
DENGAN *TUNNELING 6TO4* DAN ISATAP  
UNTUK APLIKASI *VIDEO STREAMING***

**SKRIPSI**

**ADI PRAYITNO  
07 06 19 89 66**

**DEPARTEMEN TEKNIK ELEKTRO  
FAKULTAS TEKNIK UNIVERSITAS INDONESIA  
DEPOK  
JUNI 2009**



UNIVERSITAS INDONESIA

ANALISA PENGARUH *BIT RATE* TERHADAP *DELAY* DAN  
*PACKET LOSS* PADA JARINGAN IPV6  
DENGAN *TUNNELING 6TO4* DAN ISATAP  
UNTUK APLIKASI *VIDEO STREAMING*

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh gelar  
Sarjana Teknik

ADI PRAYITNO  
07 06 19 89 66

DEPARTEMEN TEKNIK ELEKTRO  
FAKULTAS TEKNIK UNIVERSITAS INDONESIA  
DEPOK  
JUNI 2009

## **PERNYATAAN ORISINALITAS**

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

Nama : Adi Prayitno

NPM : 07 06 19 89 66

Tanda Tangan :

Tanggal : 30 Juni 2009

## PENGESAHAN

Skripsi ini diajukan oleh :  
Nama : Adi Prayitno  
NPM : 0706198966  
Program Studi : Teknik Elektro  
Judul Skripsi : Analisa Pengaruh *Bit Rate* Terhadap *Delay* dan *Packet Loss* pada Jaringan IPv6 dengan *Tunelling* 6to4 dan ISATAP untuk Aplikasi *Video Streaming*

**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. Endang Sriningsih MT., Si ( )  
Penguji : Dr. Ir. Anak Agung Putri Ratna M.Eng ( )  
Penguji : Prima Dewi Purnamasari ST., MT., MSc ( )

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:

Ir. Endang Sriningsih MT. , Si, selaku dosen pembimbing yang telah menyediakan waktu, tenaga, dan pikiran untuk mengarahkan saya dalam penyusunan 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, 30 Juni 2009

Penulis

## HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

---

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

Nama : Adi Prayitno  
NPM : 0706198966  
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 PENGARUH BIT RATE TERHADAP DELAY DAN PACKET LOSS  
PADA JARINGAN IPV6 DENGAN TUNNELING 6T04 DAN ISATAP UNTUK  
APLIKASI VIDEO STREAMING*

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 mempublikasikan 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 : 30 Juni 2009

Yang menyatakan

(.....)

## ABSTRAK

Nama : Adi Prayitno  
Program Studi : Teknik Elektro  
Judul : Analisa Pengaruh *Bit Rate* Terhadap *Delay* dan *Packet Loss* pada Jaringan IPv6 dengan *Tunneling 6to4* dan ISATAP untuk Aplikasi *Video Streaming*

Skripsi ini bertujuan untuk menganalisa dan membandingkan kualitas jaringan IPv4 murni, IPv6 murni, IPv6 dengan *Tunneling 6to4* dan ISATAP, khususnya untuk aplikasi *video streaming*. Analisa didasarkan pada pengaruh *bit rate* terhadap *delay* dan *packet loss* dari *video streaming*.

Rancangan jaringan lokal terdiri dari 2 buah *mobile computer* yang berfungsi sebagai *client* dan *server* dengan platform Windows XP, serta 2 buah Router Cisco 2600 Series sebagai *intermediate device*. Aplikasi yang akan diimplementasikan pada jaringan lokal adalah aplikasi VideoLAN *Client* pada sisi *client* dan *server*. Pengujian dilakukan dengan melakukan streaming file berformat .mpg berdurasi 29 detik, berukuran 9285 KB dan *frame rate* 23,98 fps. *Video streaming* dilakukan sebanyak 10 kali dengan pengaturan *bit rate* yang bervariasi untuk video dan audio.

Hasil pengujian menunjukkan bahwa *tunneling 6to4* dan ISATAP mempunyai delay lebih besar dibanding IPv4 dan lebih kecil dibanding IPv6, serta mempunyai packet loss lebih kecil dibanding IPv4 dan lebih besar dibanding IPv6. *Tunneling ISATAP* mempunyai keunggulan dibanding dengan *tunneling 6to4* dimana *delay* pada ISATAP sebesar 0.9149-0.9523 detik dan 6to4 sebesar 0.9276-0.9549 detik, sedangkan persentase *packet loss* pada ISATAP sebesar 0.08-0.16% dan 6to4 sebesar 0.11-0.18%.

**Kata kunci :** *IPv4, IPv6, Tunneling, 6to4, ISATAP, Video Streaming, Bit Rate, Delay, Packet Loss, VLC*

## ABSTRACT

Name : Adi Prayitno  
Study Program: Electrical Engineering  
Title : Analysis Of *Bit Rate* Influence About *Delay* And *Packet Loss* On IPv6 Network With 6to4 And ISATAP *Tunneling* For *Video Streaming*

This thesis is purposed to analyze and compare the quality of network on IPv4, IPv6, IPv6 with 6to4 and ISATAP tunneling, especially for video streaming application. Analysis is focused on bit rate influence for delay and packet loss on video streaming.

The local network design included 2 mobile computers as client and server with Windows XP platform, and also 2 Router Cisco 2600 Series as intermediate device. The application that implemented is VideoLAN Client at client and server. The test is done by streaming the .mpg format file with 29 seconds duration, sized 9285 KB, and frame rate 23,98 fps. Video streaming is done 10 times with variation of bit rate for video and audio.

The examination result indicate that 6to4 and ISATAP have delay more higher than IPv4 and less than IPV6. And also have packet loss less than IPv4 and more than IPv6. ISATAP tunneling more excellence rather than 6to4 tunneling which delay ISATAP equal to 0.9149-0.9523 seconds and delay 6to4 0.9276-0.9549 seconds. Meanwhile the ISATAP packet loss equal to 0.08-0.16% and 6to4 packet loss 0.11-0.18%.

**Key word : IPv4, IPv6, Tunneling, 6to4, ISATAP, Video Streaming, Bit Rate, Delay, Packet Loss, VLC**



## DAFTAR ISI

HALAMAN JUDUL .....	i
HALAMAN PERNYATAAN ORISINALITAS .....	ii
HALAMAN PENGESAHAN .....	iii
KATA PENGANTAR .....	iv
HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS .....	v
ABSTRAK .....	vi
ABSTRACT .....	vii
DAFTAR ISI .....	viii
DAFTAR GAMBAR .....	x
DAFTAR TABEL .....	xii
DAFTAR PERSAMAAN .....	xiii
DAFTAR LAMPIRAN .....	xiv
DAFTAR SINGKATAN .....	xv
<b>1. PENDAHULUAN .....</b>	<b>1</b>
1.1 Latar Belakang .....	1
1.2 Tujuan Penulisan .....	2
1.3 Metodologi Penelitian .....	2
1.4 Pembatasan Masalah .....	2
1.5 Sistematika Penulisan .....	3
<b>2. ROUTING PROTOCOL IPv6 DAN APLIKASI VIDEO STREAMING .....</b>	<b>4</b>
2.1 Latar Belakang IPv6 .....	4
2.2 Struktur IPv6 .....	5
2.2.1 Fitur-Fitur pada IPv6 .....	5
2.2.2 Format <i>Header</i> IPv6 .....	6
2.2.3 Perbandingan antara IPv6 dengan IPv4 .....	7
2.2.4 Ekivalensi pada IPv6 dengan IPv4 .....	9
2.2.5 Pengalamatan IPv6 .....	10
2.2.5.1 Format Alamat .....	10
2.2.5.2 Penyederhanaan Bentuk Alamat .....	11
2.2.5.3 Format Prefiks .....	12
2.2.5.4 Jenis-Jenis Alamat IPv6 .....	13
2.3 <i>Tunneling</i> .....	13
2.3.1 <i>Tunneling</i> 6to4 .....	14
2.3.2 <i>Intra-Site Automatic Tunnel Addressing Protocol</i> (ISATAP) .....	15
2.4 Aplikasi <i>Video Streaming</i> .....	17
2.4.1 <i>Mode</i> Jaringan <i>Video Streaming</i> .....	17
2.4.2 Performansi Jaringan <i>Video Streaming</i> .....	18
2.4.3 Parameter-Parameter Aplikasi <i>Video Streaming</i> .....	20
2.4.3.1 <i>Bit Rate</i> .....	20

2.4.3.2 <i>Frame Rate</i> .....	20
<b>3. PERANCANGAN JARINGAN DAN RENCANA METODE PENGAMBILAN DATA</b> .....	<b>21</b>
3.1 Topologi Jaringan .....	21
3.2 Konfigurasi Jaringan .....	22
3.2.1 Konfigurasi Jaringan IPv4 Murni .....	22
3.2.2 Konfigurasi Jaringan IPv6 Murni .....	22
3.2.3 Konfigurasi <i>Tunneling</i> 6to4 .....	23
3.2.4 Konfigurasi <i>Tunneling</i> ISATAP .....	24
3.3 <i>Software</i> Pendukung .....	25
3.4 Metode Pengambilan Data .....	25
<b>4. ANALISA</b> .....	<b>28</b>
4.1 Pengambilan Data .....	28
4.2 Dokumentasi Proses Pengambilan Data .....	31
4.2.1 Jaringan IPv4 .....	31
4.2.2 Jaringan IPv6, <i>Tunneling</i> 6to4 dan ISATAP .....	33
4.3 Analisa Konfigurasi Jaringan .....	36
4.3.1 Konfigurasi Jaringan IPv4 .....	36
4.3.2 Konfigurasi Jaringan IPv6 .....	37
4.3.3 Konfigurasi Jaringan <i>Tunneling</i> 6to4 .....	38
4.3.4 Konfigurasi Jaringan <i>Tunneling</i> ISATAP .....	40
4.4 Analisa Pengaruh Bit Rate Terhadap Delay dan Packet Loss ...	42
4.4.1 Analisa Pengaruh <i>Bit Rate</i> Terhadap <i>Packet Loss</i> .....	43
4.4.2 Analisa Pengaruh <i>Bit Rate</i> Terhadap <i>Delay</i> .....	46
4.5 Analisa Perbandingan Kinerja Secara Keseluruhan .....	49
<b>5. KESIMPULAN</b> .....	<b>51</b>
<b>DAFTAR REFERENSI</b> .....	<b>52</b>

## DAFTAR GAMBAR

<b>Gambar 2.1</b>	Struktur dari Paket IPv6 .....	6
<b>Gambar 2.2</b>	Perbandingan Format <i>Header</i> IPv4 dengan IPv6 .....	7
<b>Gambar 2.3</b>	<i>Tunneling</i> IPv6 over IPv4 .....	14
<b>Gambar 2.4</b>	Enkapsulasi Paket pada Proses <i>Tunneling</i> .....	14
<b>Gambar 2.5</b>	Struktur Alamat <i>Tunneling</i> 6to4 .....	15
<b>Gambar 2.6</b>	Contoh Konfigurasi Pengalamatan 6to4 .....	15
<b>Gambar 2.7</b>	Struktur Alamat <i>Tunneling</i> ISATAP .....	16
<b>Gambar 2.8</b>	Contoh Konfigurasi Pengalamatan ISATAP .....	16
<b>Gambar 2.9</b>	<i>Streaming Unicast Mode</i> .....	18
<b>Gambar 2.10</b>	<i>Streaming Multicast Mode</i> .....	18
<b>Gambar 3.1</b>	Topologi Global Jaringan untuk Proses Pengujian .....	21
<b>Gambar 3.2</b>	Topologi Jaringan IPv4 Murni .....	22
<b>Gambar 3.3</b>	Topologi Jaringan IPv6 Murni .....	23
<b>Gambar 3.4</b>	Topologi Jaringan <i>Tunneling</i> 6to4 .....	24
<b>Gambar 3.5</b>	Topologi Jaringan <i>Tunneling</i> ISATAP .....	25
<b>Gambar 4.1</b>	Cara Melakukan <i>Filter Protocol Streaming</i> .....	29
<b>Gambar 4.2</b>	Data Latency Pengiriman File Dari <i>Server</i> ke <i>Client</i> .....	30
<b>Gambar 4.3</b>	Data Jumlah Paket Disisi <i>Server</i> dan <i>Client</i> yang Ditangkap <i>Wireshark</i> .....	30
<b>Gambar 4.4</b>	Pengaturan <i>Server</i> pada VLC untuk Jaringan IPv4 .....	31
<b>Gambar 4.5</b>	Pengaturan <i>Client</i> pada VLC untuk jaringan IPv4 .....	32
<b>Gambar 4.6</b>	Hasil <i>Packet Sniffing</i> IPv4 pada <i>Wireshark</i> Disisi <i>Server</i> .....	33
<b>Gambar 4.7</b>	Hasil <i>Packet Sniffing</i> IPv4 pada <i>Wireshark</i> Disisi <i>Client</i> .....	33
<b>Gambar 4.8</b>	Pengaturan <i>Server</i> pada VLC untuk Jaringan IPv6, 6to4 dan ISATAP .....	34
<b>Gambar 4.9</b>	Pengaturan <i>Client</i> pada VLC untuk Jaringan IPv6, 6to4 dan ISATAP .....	35
<b>Gambar 4.10</b>	Hasil <i>Packet Sniffing</i> IPv6 pada <i>Wireshark</i> Disisi <i>Server</i> .....	35
<b>Gambar 4.11</b>	Hasil <i>Packet Sniffing</i> IPv6 pada <i>Wireshark</i> Disisi <i>Client</i> .....	36
<b>Gambar 4.12</b>	Hasil <i>Traceroute</i> IPv4 .....	37
<b>Gambar 4.13</b>	Hasil <i>Traceroute</i> IPv6 .....	38
<b>Gambar 4.14</b>	Hasil <i>Traceroute Tunneling</i> 6to4 .....	40
<b>Gambar 4.15</b>	Hasil <i>Traceroute Tunneling</i> ISATAP .....	42
<b>Gambar 4.16</b>	Diagram <i>Bit Rate</i> Terhadap <i>Packet Loss</i> untuk Seluruh Konfigurasi Jaringan .....	45
<b>Gambar 4.17</b>	Grafik <i>Bit Rate</i> Terhadap <i>Packet Loss</i> untuk Seluruh Konfigurasi Jaringan .....	45
<b>Gambar 4.18</b>	Grafik <i>Bit Rate</i> Terhadap <i>Packet Loss</i> untuk Konfigurasi IPv6, <i>Tunneling</i> 6to4 dan ISATAP .....	46

<b>Gambar 4.19</b>	Diagram <i>Bit Rate</i> Terhadap <i>Delay</i> untuk Seluruh Konfigurasi Jaringan .....	47
<b>Gambar 4.20</b>	Grafik <i>Bit Rate</i> Terhadap <i>Delay</i> untuk Seluruh Konfigurasi Jaringan .....	48

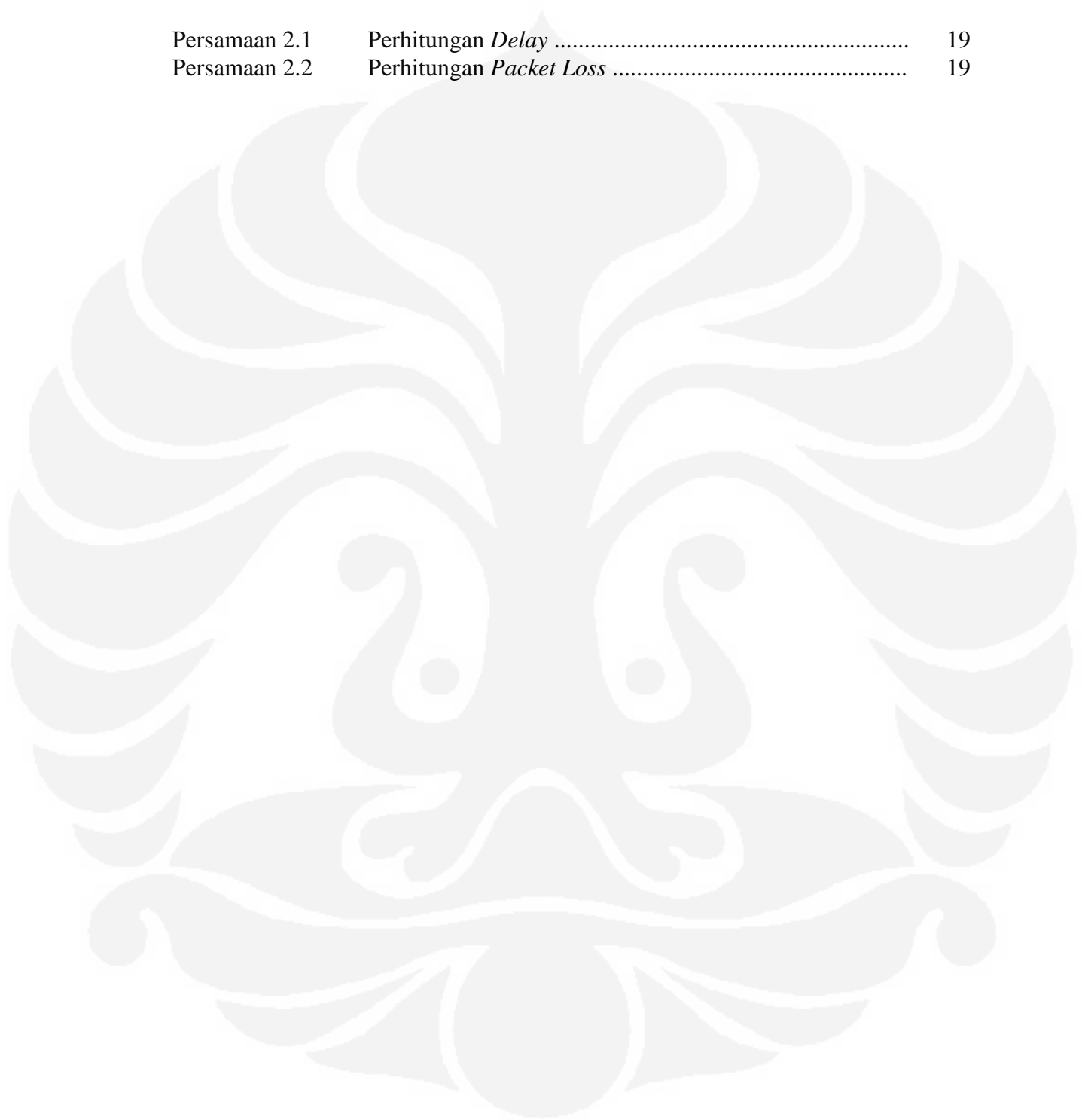


## DAFTAR TABEL

<b>Tabel 2.1</b>	Perbandingan antara IPv4 dengan IPv6 .....	8
<b>Tabel 2.2</b>	Ekivalensi pada IPv6 dan IPv4 .....	9
<b>Tabel 2.3</b>	Penyederhanaan Bentuk Alamat pada IPv6 .....	11
<b>Tabel 4.1</b>	Data <i>Packet Loss</i> untuk Setiap Konfigurasi Jaringan .....	43
<b>Tabel 4.2</b>	Persentase <i>Packet Loss</i> untuk Setiap Konfigurasi Jaringan.....	44
<b>Tabel 4.3</b>	Data <i>Delay</i> untuk Setiap Konfigurasi Jaringan.....	47

## DAFTAR PERSAMAAN

Persamaan 2.1	Perhitungan <i>Delay</i> .....	19
Persamaan 2.2	Perhitungan <i>Packet Loss</i> .....	19



## DAFTAR LAMPIRAN

Lampiran 1	Konfigurasi Router IPv4 Murni .....	53
Lampiran 2	Konfigurasi Router IPv6 Murni .....	55
Lampiran 3	Konfigurasi Router Tunneling 6to4 .....	57
Lampiran 4	Konfigurasi Router Tunneling ISATAP .....	60
Lampiran 5	Data Rata-Rata Packet Loss Konfigurasi Jaringan IPv4..	63
Lampiran 6	Data Rata-Rata Packet Loss Konfigurasi Jaringan IPv6..	64
Lampiran 7	Data Rata-Rata Packet Loss Konfigurasi Jaringan Tunneling 6to4 .....	65
Lampiran 8	Data Rata-Rata Packet Loss Konfigurasi Jaringan Tunneling ISATAP .....	66
Lampiran 9	Data Rata-Rata Delay Konfigurasi Jaringan IPv4 .....	67
Lampiran 10	Data Rata-Rata Delay Konfigurasi Jaringan IPv6 .....	68
Lampiran 11	Data Rata-Rata Delay Konfigurasi Jaringan Tunneling 6to4 .....	69
Lampiran 12	Data Rata-Rata Delay Konfigurasi Jaringan Tunneling ISATAP .....	70

## DAFTAR SINGKATAN

DHCP	Dynamic Host Configuration Protocol
HTTP	Hiper Text Transfer Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPng	Internet Protocol Next Generation
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol
MPEG TS	Moving Picture Experts Group Transport Stream
QoS	Quality of Service
RTP	Real Time Protocol
TCP	Transmission Control Protocol
UDP	Unit Datagram Protocol
VLC	VideoLAN Client



# BAB 1

## PENDAHULUAN

### 1.1 Latar Belakang

IPv6 adalah kependekan dari *Internet Protocol Version 6*, protokol generasi baru yang didesain oleh *Internet Engineering Task Force* (IETF) untuk menggantikan protokol internet saat ini, yaitu IPv4. Aplikasi internet saat ini kebanyakan menggunakan IPv4, yang berumur hampir 20 tahun. IPv4 mulai mengalami beberapa masalah dan masalah yang paling penting adalah mulai menipisnya alamat pada IPv4 yang dibutuhkan oleh perangkat-perangkat untuk terhubung ke internet. Alamat IPv4 pada dasarnya menggunakan metode pengalamatan berbasis 32 bit, yang berarti mampu mengakomodasi jumlah pengalamatan sampai dengan  $2^{32}$  atau sekitar  $4,294 \times 10^9$ . Seiring dengan berjalannya waktu dan perkembangan internet yang semakin pesat menyebabkan kebutuhan akan jumlah pengalamatan yang lebih banyak juga semakin besar. Karena alasan itulah, dimunculkan suatu *routing protocol* baru IPv6 yang menggunakan metode pengalamatan berbasis 128 bit, yang berarti mampu mengakomodasi jumlah pengalamatan sampai dengan  $2^{128}$  atau sekitar  $3,402 \times 10^{38}$ . Jika dibandingkan panjangnya, IPv4 sepanjang 1 inci, sedangkan IPv6 sepanjang diameter galaksi.

IPv6 (*Internet Protocol version 6*) merupakan IP generasi berikutnya atau disebut juga *Internet Protocol Next Generation* (IPng). IPv6 didesain untuk menggantikan IPv4 (*Internet Protocol version 4*) yang dipergunakan sekarang ini. IPv6 dirancang sedemikian rupa agar memiliki kinerja yang lebih handal bila dibandingkan dengan IPv4 seperti dalam pengiriman paket, *security*, *authentication* dan QoS (*Quality Of Service*). Selain itu diharapkan IPv6 juga mampu memberikan fitur-fitur lain yang lebih kompleks yang akan dikembangkan lagi.

Sampai saat ini, secara umum jaringan masih menggunakan IPv4 sehingga implementasi jaringan IPv6 dilakukan secara bertahap dan diusahakan tidak akan mengganggu jaringan IPv4 yang sudah ada saat ini. Oleh karena itu, diperlukan suatu mekanisme transisi untuk mengganti penggunaan jaringan IPv4 menjadi

jaringan IPv6 secara keseluruhan. Untuk melakukan proses transisi dari IPv4 ke IPv6 maka diperlukan suatu metode yang mampu menunjang mekanisme transisi tersebut. Beberapa metode telah diteliti dan diantaranya yaitu metode *Dual Stack*, *Tunneling* dan *Translation*. Metode *Tunneling* yang digunakan dalam mekanisme transisi dari IPv4 ke IPv6 ada beberapa macam, diantaranya adalah *Tunneling 6to4*, *ISATAP*, *Teredo* dan sebagainya.

*Video streaming* merupakan salah satu aplikasi yang dapat diimplementasikan untuk menguji kehandalan jaringan pada jaringan IPv6 maupun pada proses transisi dari IPv4 ke IPv6 dengan menggunakan metode *Tunneling*.

## 1.2 Tujuan Penulisan

Skripsi ini ditulis bertujuan untuk menganalisa dan membandingkan kualitas jaringan IPv4 murni, IPv6 murni, IPv6 dengan *Tunneling 6to4* dan *ISATAP*, khususnya untuk aplikasi *video streaming*. Analisa didasarkan pada pengaruh perubahan *bit rate* terhadap *delay* dan *packet loss* dari data video yang ditranmisikan.

## 1.3 Metodologi Penelitian

Metode yang akan digunakan dalam skripsi ini adalah membangun jaringan lokal berskala kecil (*test bed*) dengan beberapa konfigurasi jaringan. Dengan melakukan perubahan *bit rate* dalam suatu *file* video kemudian akan dianalisa pengaruhnya terhadap *delay* dan *packet loss* selama proses *video streaming*.

## 1.4 Pembatasan Masalah

Pengujian dilakukan menggunakan jaringan *test bed* yang difokuskan pada aplikasi *video streaming* dan diterapkan pada konfigurasi jaringan IPv4 murni, jaringan IPv6 murni, jaringan IPv6 dengan *Tunneling 6to4* dan *Tunneling ISATAP*.

Rancangan *test bed* yang digunakan adalah jaringan lokal yang terdiri dari 2 buah *mobile computer* yang berfungsi sebagai *client* dan *server* dengan *platform*

Windows XP, serta 2 buah router Cisco 2621 sebagai *intermediate device* yang menghubungkan *client* dan *server*.

Aplikasi yang akan diimplementasikan pada jaringan *test bed* adalah aplikasi VideoLAN *Client* pada sisi *client* dan *server*.

Parameter-parameter yang akan dianalisa untuk menguji kualitas jaringan meliputi *bit rate*, *delay* dan *packet loss*.

## 1.5 Sistematika Penulisan

Sistematika skripsi ini tersusun atas 5 bab. Bab 1 merupakan pendahuluan yang berisi tentang latar belakang pemilihan tema, tujuan penulisan, metodologi penelitian, pembatasan masalah dan sistematika penulisan. Bab 2 berisi tentang teori-teori yang berkaitan tentang IPv6, metode transisi jaringan IPv4 ke IPv6, dan *video streaming*. Bab 3 berisi tentang rancangan untuk implementasi jaringan IPv6 dimana akan dibangun sebuah *server* dan *client* yang terhubung pada jaringan baik jaringan IPv4 murni, IPv6 murni maupun melalui proses transisi dari IPv6 menjadi IPv4 dengan *Tunneling 6to4* dan ISATAP, serta metode pengujian yang akan dilakukan. Bab 4 berisi tentang pengambilan data dan analisa data pengujian untuk menunjukkan kualitas video streaming pada jaringan *Tunneling 6to4*, *Tunneling ISATAP*, IPv6 murni dan IPv4 murni. Bab 5 berisi tentang kesimpulan dari keseluruhan isi skripsi.

## BAB 2

### ROUTING PROTOCOL IPV6

### DAN APLIKASI VIDEO STREAMING

#### 2.1 Latar Belakang IPv6

Aplikasi internet saat ini kebanyakan masih menggunakan *Internet Protocol version 4* (IPv4) yang menggunakan metode pengalamatan berbasis 32 bit, yang berarti mampu mengakomodasi jumlah pengalamatan sampai dengan  $2^{32}$  atau sekitar  $4,294 \times 10^9$ . *Internet Protocol version 4* (IPv4) yang dijadikan standar *routing protocol* pada tahun 1981 (RFC 791) sebenarnya telah terbukti tangguh, mudah diimplementasikan dan dioperasikan, dan telah berhasil melalui tes skalabilitas dalam jaringan internet secara global sampai saat ini. Namun design dari IPv4 tidak mengantisipasi dampak yang mungkin ditimbulkan akibat perkembangan jaringan internet yang semakin pesat, diantaranya :

- a. Membutuhkan jumlah pengalamatan yang lebih banyak untuk mendukung kebutuhan perkembangan jaringan internet dimasa yang akan datang.
- b. Membutuhkan kemampuan dari *router backbone* internet dalam mengelola tabel *routing* yang besar.
- c. Membutuhkan konfigurasi yang lebih sederhana.
- d. Membutuhkan keamanan pada level IP (*Internet Protocol*).
- e. Membutuhkan dukungan yang lebih baik untuk pengiriman data secara *real-time*, disebut juga dengan *Quality Of Service* (QoS).

Untuk mengantisipasi hal tersebut diatas, maka sebuah organisasi yang bernama *Internet Engineering Task Force* (IETF) telah mengembangkan suatu standar protokol baru yang bernama *Internet Protocol version 6* (IPv6) yang sebelumnya disebut *IP-The Next Generation* (IPng). IPv6 ini diharapkan mampu menyempurnakan kekurangan-kekurangan yang ada pada IPv4 dengan fitur-fitur yang ada didalamnya. [1]

Sampai saat ini, secara umum jaringan internet masih menggunakan IPv4 sehingga implementasi jaringan IPv6 dilakukan secara bertahap dan diusahakan tidak akan mengganggu jaringan IPv4 yang sudah ada saat ini. Oleh karena itu, diperlukan suatu mekanisme transisi untuk mengganti penggunaan jaringan IPv4

menjadi jaringan IPv6 secara keseluruhan. Untuk melakukan proses transisi dari IPv4 ke IPv6 maka diperlukan suatu metode yang mampu menunjang mekanisme transisi tersebut. Beberapa metode telah diteliti dan diantaranya yaitu metode *Dual Stack*, *Tunneling* dan *Translation*. Metode *Tunneling* yang digunakan dalam mekanisme transisi dari IPv4 ke IPv6 ada beberapa macam, diantaranya adalah *Tunneling 6to4*, *ISATAP*, *Teredo* dan sebagainya.

## 2.2 Struktur IPv6

Pengembangan IPv6 diharapkan mampu mengatasi kekurangan-kekurangan yang ada pada IPv4 dengan fitur-fitur yang ada didalamnya.

### 2.2.1 Fitur-Fitur pada IPv6

IPv6 didukung oleh fitur-fitur yang diharapkan dapat mengatasi kekurangan-kekurangan yang ada pada *routing protocol* IPv4, beberapa diantaranya :

- a. Format *header* yang baru  
*Header* IPv6 dua kali lebih besar dari *header* IPv4, sedangkan pengalamatan IPv6 empat kali lebih besar dari pengalamatan IPv4. Walaupun demikian, format *header* IPv6 justru mengalami penyederhanaan dimana ada beberapa *field* yang dihilangkan karena dianggap tidak efisien. Sebagai gantinya ditambahkan *header* tambahan yang disebut *extension header*.
- b. Perluasan format pengalamatan  
 IPv6 mempunyai format pengalamatan 128-bit (16-byte) yang berarti mampu mengakomodasi jumlah pengalamatan sampai dengan  $2^{128}$  atau sekitar  $3,402 \times 10^{38}$ .
- c. Infrastruktur *routing* dan pengalamatan yang lebih efisien dan berbentuk hierarki.
- d. Konfigurasi alamat *stateless* dan *stateful*  
 Sama seperti halnya IPv4, pada IPv6 juga mengizinkan adanya DHCP *server* sebagai pengatur alamat otomatis. Jika dalam IPv4 terdapat *dynamic address* dan *static address*, maka dalam IPv6, konfigurasi alamat

dengan menggunakan DHCP *server* dinamakan dengan *stateful address configuration*, sementara jika konfigurasi alamat IPv6 tanpa DHCP *server* dinamakan dengan *stateless address configuration*.

- e. Keamanan yang lebih baik

IPv6 telah dirancang untuk mendukung IPsec sehingga bisa dikatakan IPv6 memiliki keamanan yang lebih baik bila dibandingkan dengan IPv4.

- f. Mendukung Quality of Services (QoS)

*Field* baru yang berada pada IPv6 *header* mendefinisikan bagaimana trafik khusus ditangani dan diidentifikasi. Identifikasi trafik yang memerlukan penanganan khusus menggunakan *field flow table*.

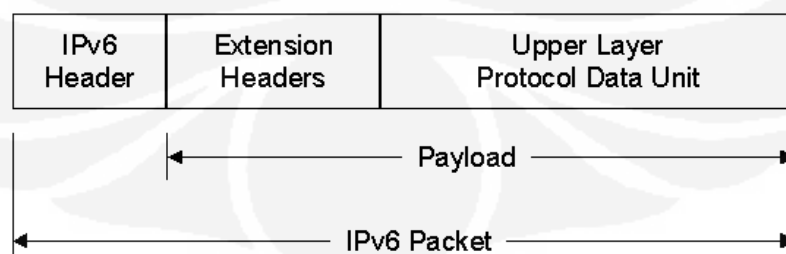
- g. Ekstensibilitas

IPv6 dapat dengan mudah memperluas fitur baru dengan menambahkan *extension header* setelah IPv6 *header*. [1]

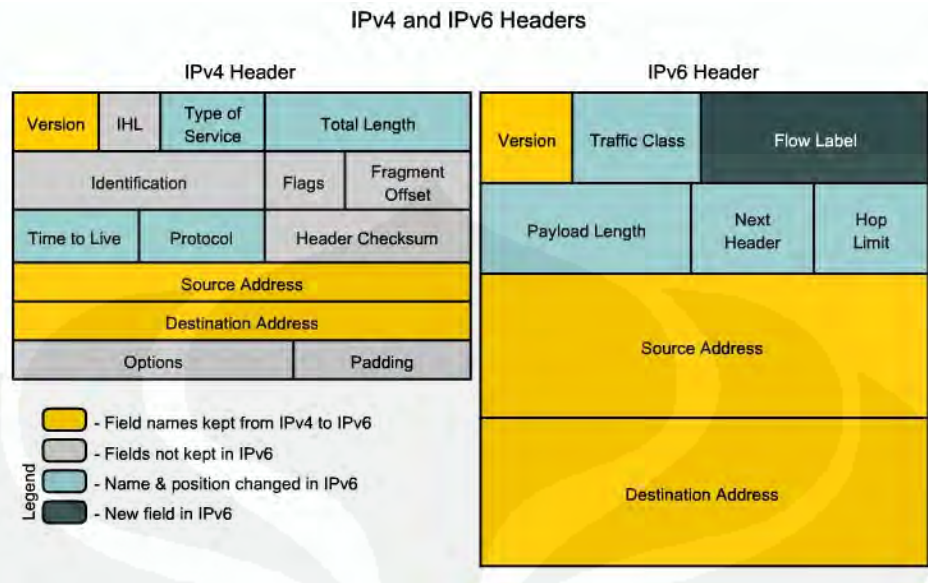
Fitur-fitur diatas hanya sedikit contoh dari fitur-fitur yang dimiliki oleh IPv6 yang mampu mendukung IPv6 agar dapat menjadi sebuah *routing protocol* yang handal dimasa yang akan datang.

### 2.2.2 Format Header IPv6

Format *header* IPv6 terbagi menjadi 2 bagian, yaitu *header standart (default)* dan *header tambahan (extension)*. *Header standart (default)* merupakan *field-field* yang selalu ada dalam setiap paket IPv6, sedangkan *header tambahan (extension)* merupakan *field-field* yang ditambahkan hanya apabila dibutuhkan saja, terletak diantara *header standart* IPv6 dengan *upper-layer header*. Pada Gambar 2.1 berikut ini ditunjukkan struktur dari paket IPv6.



**Gambar 2.1** Struktur dari Paket IPv6 [1]



**Gambar 2.2** Perbandingan Format *Header* IPv4 dengan IPv6 [3]

Dari Gambar 2.2 ditunjukkan bahwa *header* IPv6 mempunyai ukuran yang lebih besar bila dibandingkan dengan *header* IPv4 sehingga mampu mendukung jumlah pengalamatan sampai dengan 128 bit. Meskipun demikian, format *header* IPv6 lebih sederhana bila dibandingkan dengan format *header* IPv4 karena ada beberapa *field* pada *header* IPv4 yang dihilangkan pada *header* IPv6. *Field-field* yang dihilangkan yaitu *Internet Header Length (IHL)*, *Identification*, *Flags*, *Fragment Offset*, *Header Checksum*, *Option* dan *Padding*. Ada beberapa *field* yang masih dipertahankan pada *header* IPv6 yaitu *Version*, *Source Address* dan *Destination Address*. Disamping itu, pada *header* IPv6 juga ditambahkan *field* tambahan bernama *Flow Label* yang berfungsi mengidentifikasi paket-paket *real-time* yang membutuhkan perlakuan yang sama atau dianggap mempunyai alur data yang sama.

### 2.2.3 Perbandingan antara IPv4 dengan IPv6

Dengan adanya *routing protocol* baru IPv6 diharapkan mampu mengatasi kekurangan-kekurangan yang ada pada IPv4. Secara garis besar, perbandingan yang mendasar antara IPv4 dengan IPv6 ditunjukkan pada Tabel 2.1 berikut ini.

**Tabel 2.1** Perbandingan antara IPv4 dengan IPv6 [1]

<b>IPv4</b>	<b>IPv6</b>
Format pengalamatan 32 bit (4 byte).	Format pengalamatan 128 bit (16 byte).
Dukungan IPsec merupakan pilihan.	Mendukung IPsec.
Tidak ada identifikasi aliran paket untuk penanganan QoS oleh <i>router</i> yang dimasukkan ke dalam <i>header</i> IPv4.	Identifikasi aliran paket untuk penanganan QoS oleh <i>router</i> dimasukkan ke dalam <i>header</i> IPv6 menggunakan <i>Flow Label field</i> .
Fragmentasi dilakukan oleh kedua <i>router</i> dan <i>host</i> pengirim.	Fragmentasi tidak dilakukan oleh <i>router</i> , hanya oleh <i>host</i> pengirim.
<i>Header</i> mengandung <i>checksum</i> .	<i>Header</i> tidak mengandung <i>checksum</i> .
<i>Header</i> mengandung <i>options</i> .	Semua <i>options</i> dipindahkan ke <i>extension headers</i> .
<i>Address Resolution Protocol</i> (ARP) menggunakan <i>frame Broadcast ARP Request</i> untuk mengubah alamat IPv4 menjadi alamat <i>link layer</i> .	ARP diganti dengan <i>Multicast Neighbor Solicitation messages</i> .
<i>Internet Group Management Protocol</i> (IGMP) digunakan untuk mengatur kumpulan <i>local subnet group</i> .	IGMP diganti dengan <i>Multicast Listener Discovery</i> (MLD) <i>messages</i> .
ICMP <i>Router Discovery</i> digunakan untuk mencari <i>default gateway</i> yang terbaik dan hal ini merupakan pilihan	ICMP <i>Router Discovery</i> diganti dengan ICMPv6 <i>Router Solicitation</i> dan <i>Router Advertisement messages</i> , dan hal ini memang dibutuhkan.
Terdapat alamat <i>broadcast</i> .	Tidak ada alamat <i>broadcast</i> .
Harus dikonfigurasi secara manual ataupun melalui DHCP.	Tidak membutuhkan konfigurasi secara manual maupun DHCP.



Menggunakan alamat <i>host</i> (A) yang tercatat pada <i>Domain Name System</i> (DNS) untuk memetakan <i>hostname</i> pada alamat IPv4.	Menggunakan alamat <i>host</i> (AAAA) yang tercatat pada <i>Domain Name System</i> (DNS) untuk memetakan <i>hostname</i> pada alamat IPv6.
Menggunakan <i>pointer</i> (PTR) yang tercatat pada <i>domain</i> IN-ADDR.ARPA DNS untuk memetakan alamat IPv4 ke <i>hostname</i> .	Menggunakan <i>pointer</i> (PTR) yang tercatat pada <i>domain</i> IP6.ARPA DNS untuk memetakan alamat IPv6 ke <i>hostname</i> .
Mendukung sampai 576-byte ukuran paket.	Mendukung sampai 1280-byte ukuran paket.

#### 2.2.4 Ekivalensi pada IPv6 dan IPv4

Walaupun ada perbedaan antara IPv6 dengan IPv4, namun ada beberapa konsep pengalamatan yang masih mempunyai kesamaan diantara keduanya. Beberapa hal yang ekivalen antara IPv6 dengan IPv4 ditunjukkan pada Tabel 2.2 berikut ini.

**Tabel 2.2** Ekivalensi pada IPv6 dengan IPv4 [1]

IPv4 Address	IPv6 Address
<i>Internet address classes</i> (Class A, B, C, D, E)	Dihilangkan pada IPv6
<i>Multicast addresses</i> (224.0.0.0/4)	<i>Multicast addresses</i> (FF00::/8)
<i>Broadcast addresses</i>	Tidak digunakan pada IPv6
<i>Unspecified address</i> (0.0.0.0)	<i>Unspecified address</i> (::)
<i>Loopback address</i> (127.0.0.1)	<i>Loopback address</i> (::1)
<i>Public IP addresses</i>	<i>Global unicast addresses</i>
<i>Private IP addresses</i> (10.0.0.0/8, 172.16.0.0/12, dan 192.168.0.0/16)	<i>Site-local addresses</i> (FEC0::/10)

<i>Autoconfigured addresses</i> (169.254.0.0/16)	<i>Link-local addresses</i> (FE80::/64)
Penulisan IP menggunakan <i>format dotted decimal</i> (.)	Penulisan IP menggunakan <i>format colon hexadecimal</i> (:)
Penulisan <i>subnet mask</i> menggunakan <i>format dotted decimal</i> atau <i>prefix length</i>	Penulisan <i>subnet mask</i> hanya menggunakan <i>format prefix length</i>

### 2.2.5 Pengalamatan IPv6

Alamat IP versi 6 (sering disebut sebagai alamat IPv6) adalah sebuah jenis pengalamatan jaringan yang digunakan di dalam protokol jaringan TCP/IP yang menggunakan protokol IP versi 6. Berbeda dengan IPv4 yang hanya memiliki panjang 32-bit (jumlah total alamat yang dapat dicapainya mencapai 4,294,967,296 alamat), alamat IPv6 memiliki panjang 128-bit. IPv4, meskipun total alamatnya mencapai 4 miliar, pada kenyataannya tidak sampai 4 miliar alamat, karena ada beberapa limitasi, sehingga implementasinya saat ini hanya mencapai beberapa ratus juta saja. IPv6, yang memiliki panjang 128-bit, memiliki total alamat yang mungkin hingga  $2^{128} = 3,4 \times 10^{38}$  alamat. Total alamat yang sangat besar ini bertujuan untuk menyediakan ruang alamat yang tidak akan habis (hingga beberapa masa ke depan), dan membentuk infrastruktur *routing* yang disusun secara hierarkis, sehingga mengurangi kompleksitas proses *routing* dan *tabel routing*. [1]

#### 2.2.5.1 Format Alamat

Dalam IPv6, alamat 128-bit akan dibagi ke dalam 8 blok berukuran 16-bit, yang dapat dikonversikan ke dalam bilangan heksadesimal berukuran 4-digit. Setiap blok bilangan heksadesimal tersebut akan dipisahkan dengan tanda titik dua (:). Karenanya, format notasi yang digunakan oleh IPv6 juga sering disebut dengan *colon-hexadecimal format*, berbeda dengan IPv4 yang menggunakan *dotted-decimal format*.

Berikut ini adalah contoh alamat IPv6 dalam bentuk bilangan biner:

```
0010000111011010000000001101001100000000000000001011110011101100
00001010101010100000000011111111111111110001010001001110001011010
```

Untuk menerjemahkannya ke dalam bentuk notasi *colon-hexadecimal format*, angka-angka biner di atas harus dibagi ke dalam 8 buah blok berukuran 16-bit:

```
0010000111011010 0000000011010011 0000000000000000 0010111100111011
0000001010101010 0000000011111111 1111111000101000 1001110001011010
```

Lalu, setiap blok berukuran 16-bit tersebut harus dikonversikan ke dalam bilangan heksadesimal dan setiap bilangan heksadesimal tersebut dipisahkan dengan menggunakan tanda titik dua. Hasil konversinya adalah sebagai berikut:

```
21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A [1]
```

#### 2.2.5.2 Penyederhanaan Bentuk Alamat

Alamat di atas juga dapat disederhanakan lagi dengan membuang angka 0 pada awal setiap blok yang berukuran 16-bit di atas, dengan menyisakan satu digit terakhir. Dengan membuang angka 0, alamat di atas disederhanakan menjadi:

```
21DA:D3:0:2F3B:2AA:FF:FE28:9C5A
```

**Tabel 2.3** Penyederhanaan Bentuk Alamat pada IPv6 [1]

Alamat asli	Alamat asli yang disederhanakan	Alamat setelah dikompres
FE80:0000:0000:0000:02AA:00FF:FE9A:4CA2	FE80:0:0:0:2AA:FF:FE9A:4CA2	FE80::2AA:FF:FE9A:4CA2
FF02:0000:0000:0000:0000:0000:0000:0002	FF02:0:0:0:0:0:0:2	FF02::2

Konvensi pengalamatan IPv6 juga mengizinkan penyederhanaan alamat lebih jauh lagi, yakni dengan membuang banyak karakter 0, pada sebuah alamat yang banyak angka 0-nya. Jika sebuah alamat IPv6 yang direpresentasikan dalam notasi *colon-hexadecimal format* mengandung beberapa blok 16-bit dengan angka 0, maka alamat tersebut dapat disederhanakan dengan menggunakan tanda dua buah

titik dua (::). Untuk menghindari kebingungan, penyederhanaan alamat IPv6 dengan cara ini sebaiknya hanya digunakan sekali saja di dalam satu alamat, karena kemungkinan nantinya pengguna tidak dapat menentukan berapa banyak bit 0 yang direpresentasikan oleh setiap tanda dua titik dua (::) yang terdapat dalam alamat tersebut. Tabel 2.3 berikut mengilustrasikan cara penggunaan hal ini.

Untuk menentukan berapa banyak bit bernilai 0 yang dibuang (dan digantikan dengan tanda dua titik dua) dalam sebuah alamat IPv6, dapat dilakukan dengan menghitung berapa banyak blok yang tersedia dalam alamat tersebut, yang kemudian dikurangkan dengan angka 8, dan angka tersebut dikalikan dengan 16. Sebagai contoh, alamat FF02::2 hanya mengandung dua blok alamat (blok FF02 dan blok 2). Maka, jumlah bit yang dibuang adalah  $(8-2) \times 16 = 96$  buah bit. [1]

### 2.2.5.3 Format Prefiks

Dalam IPv4, sebuah alamat dalam notasi *dotted-decimal format* dapat direpresentasikan dengan menggunakan angka prefiks yang merujuk kepada *subnet mask*. IPv6 juga memiliki angka prefiks, tapi tidak digunakan untuk merujuk kepada *subnet mask*, karena memang IPv6 tidak mendukung *subnet mask*.

Prefiks adalah sebuah bagian dari alamat IP, di mana bit-bit memiliki nilai-nilai yang tetap atau bit-bit tersebut merupakan bagian dari sebuah *route* atau *subnet identifier*. Prefiks dalam IPv6 direpresentasikan dengan cara yang sama seperti halnya prefiks alamat IPv4, yaitu [**alamat**]/[**angka panjang prefiks**]. Panjang prefiks menentukan jumlah bit terbesar paling kiri yang membuat prefiks *subnet*. Sebagai contoh, prefiks sebuah alamat IPv6 dapat direpresentasikan sebagai berikut:

3FFE:2900:D005:F28B::/64

Pada contoh di atas, 64 bit pertama dari alamat tersebut dianggap sebagai prefiks alamat, sementara 64 bit sisanya dianggap sebagai *interface ID*. [1]

#### 2.2.5.4 Jenis-Jenis Alamat IPv6

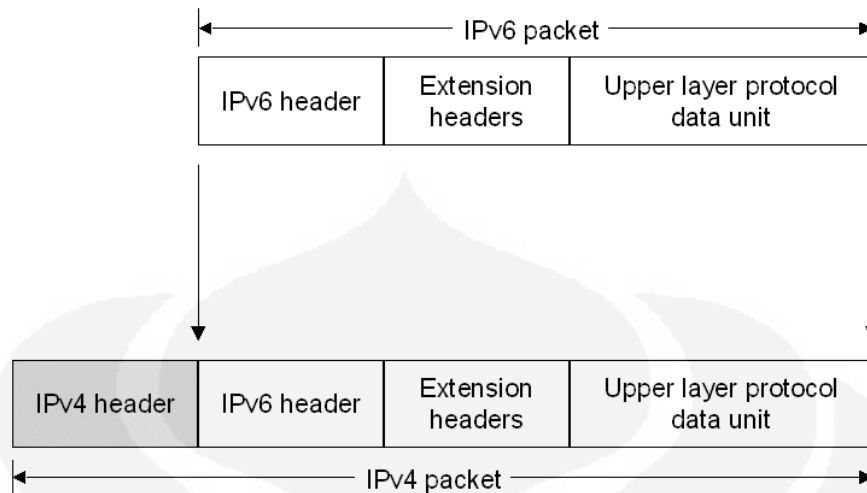
IPv6 mendukung beberapa jenis format prefix, yaitu sebagai berikut:

- a. Alamat *Unicast*, yang menyediakan komunikasi secara *point-to-point*, secara langsung antara dua *host* dalam sebuah jaringan.
- b. Alamat *Multicast*, yang menyediakan metode untuk mengirimkan sebuah paket data ke banyak *host* yang berada dalam *group* yang sama. Alamat ini digunakan dalam komunikasi *one-to-many*.
- c. Alamat *Anycast*, yang menyediakan metode penyampaian paket data kepada anggota terdekat dari sebuah *group*. Alamat ini digunakan dalam komunikasi *one-to-one-of-many*. Alamat ini juga digunakan hanya sebagai alamat tujuan (*destination address*) dan diberikan hanya kepada *router*, bukan kepada *host-host* biasa. [1]

### 2.3 Tunneling

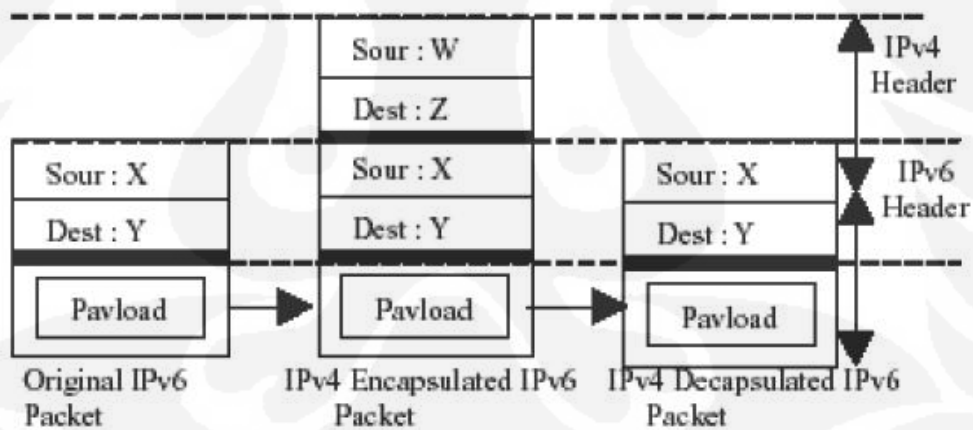
IPv6 mempunyai format alamat dan *header* yang berbeda dengan IPv4 sehingga tidak bisa melakukan interkoneksi dengan IPv4 secara langsung. Oleh karena itu, diperlukan suatu mekanisme transisi IPv6 agar paket IPv6 dapat dilewatkan pada jaringan IPv4 yang telah ada ataupun sebaliknya. Salah satu contoh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

*Tunneling protocol* merupakan mekanisme proses enkapsulasi suatu *network protocol* yang disebut *payload protocol* kedalam *delivery protocol* yang berbeda. [6] *Tunneling IPv6 over IPv4* merupakan suatu proses enkapsulasi paket IPv6 dengan header IPv4 sehingga paket IPv6 dapat dikirim melalui jaringan IPv4. [2] Struktur *tunneling* IPv6 pada IPv4 ditunjukkan pada Gambar 2.3 berikut ini.



**Gambar 2.3** *Tunneling IPv6 over IPv4* [2]

Selama proses *tunneling* IPv6 pada IPv4 berlangsung maka akan terjadi proses enkapsulasi dan dekapsulasi paket IPv6 oleh IPv4. Proses enkapsulasi dan dekapsulasi paket IPv6 ditunjukkan pada Gambar 2.4 berikut ini.



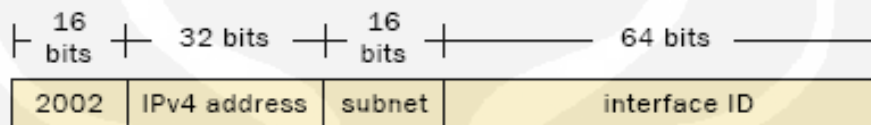
**Gambar 2.4** Enkapsulasi Paket pada Proses *Tunneling* [4]

### 2.3.1 *Tunneling 6to4*

*Tunneling 6to4* memungkinkan melewati paket IPv6 melalui jaringan IPv4 tanpa melakukan konfigurasi *explicit tunnel*. [7] *Tunneling 6to4* merupakan suatu *tunneling* yang digunakan untuk menyediakan konektifitas IPv6 *unicast*

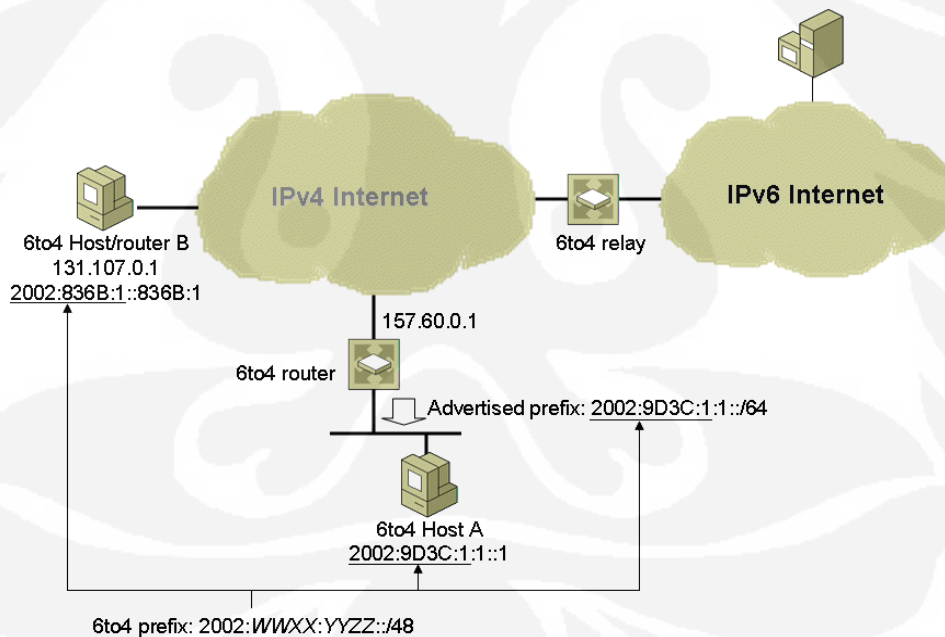
diantara IPv6 *site* dan *host* melalui jaringan internet IPv4. *Tunneling* 6to4 menganggap keseluruhan jaringan IPv4 sebagai *single link*. [2]

*Tunneling* 6to4 menggunakan alamat *global prefix* 2002:WWXX:YYZZ::/48, dimana WWXX:YYZZ adalah *colon-hexadecimal* yang merepresentasikan alamat publik IPv4 suatu *site* atau *host*. [2] Struktur alamat *Tunneling* 6to4 ditunjukkan pada Gambar 2.5 berikut ini.



**Gambar 2.5** Struktur Alamat *Tunneling* 6to4 [5]

Contoh konfigurasi pengalaman 6to4 ditunjukkan seperti pada Gambar 2.6 berikut ini.

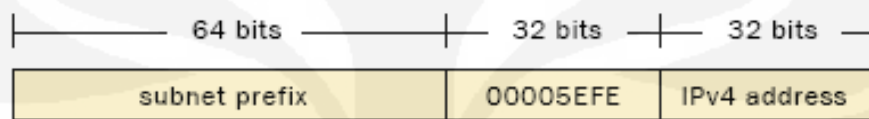


**Gambar 2.6** Contoh Konfigurasi Pengalaman 6to4 [2]

### 2.3.2 *Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)*

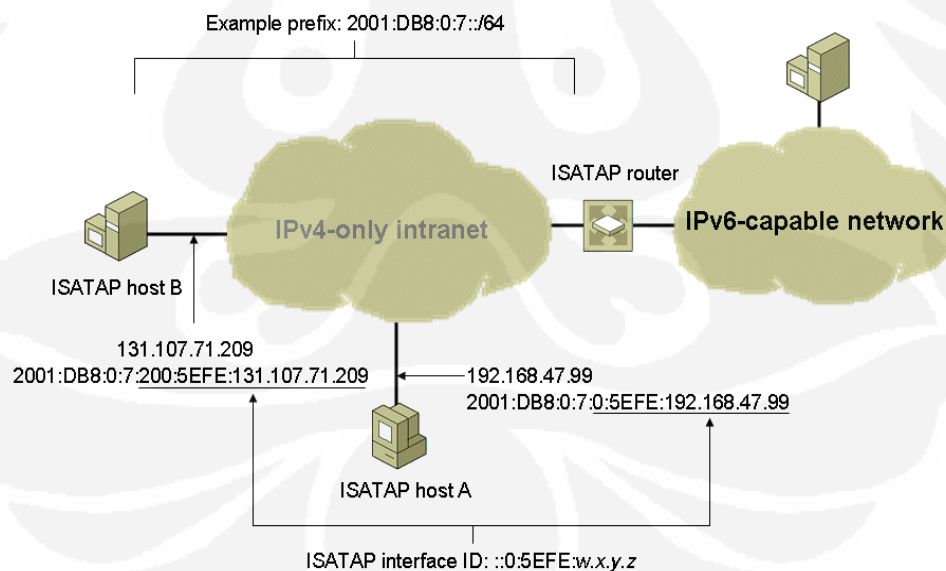
ISATAP merupakan suatu *tunneling* yang digunakan untuk menyediakan konektivitas IPv6 *unicast* diantara IPv6/IPv4 *host* melalui jaringan IPv4. ISATAP

*host* tidak membutuhkan konfigurasi manual dan dapat menciptakan alamat ISATAP menggunakan mekanisme pengalamatan *autoconfiguration*. Alamat ISATAP menggunakan *interface identifier* `::0:5EFE:w.x.y.z`, dimana *w.x.y.z* adalah alamat *private unicast* IPv4, atau `::200:5EFE:w.x.y.z`, dimana *w.x.y.z* adalah alamat *public unicast* IPv4. ISATAP *interface identifier* dikombinasikan dengan 64-bit prefix yang dipakai untuk alamat *unicast* IPv6, seperti *link-local* (`FE80::/64`), *unique local*, dan *global prefixes*. [2] Struktur alamat ISATAP ditunjukkan seperti pada Gambar 2.7 berikut ini.



**Gambar 2.7** Struktur Alamat *Tunneling* ISATAP [5]

Contoh konfigurasi pengalamatan ISATAP ditunjukkan seperti pada Gambar 2.8 berikut ini.



**Gambar 2.8** Contoh Konfigurasi Pengalamatan ISATAP [2]



## 2.4 Aplikasi Video Streaming

Video merupakan gambar-gambar yang bergerak. Didalam video menampilkan sejumlah gambar atau *frame* dengan kecepatan tertentu yang disebut dengan istilah *frame rate*, dihitung dalam skala *frame per second* (fps). Seperti halnya dengan jenis data yang lain, data video juga dapat disimpan, diedit, ataupun dikirim melalui jaringan.

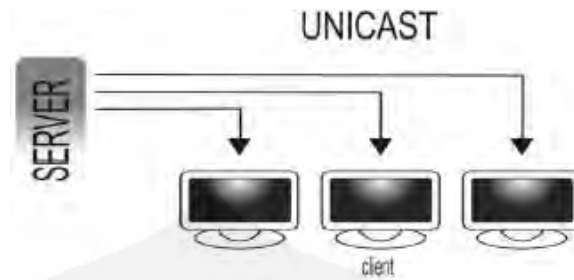
*Video streaming* merupakan suatu metode yang memanfaatkan suatu *streaming server* untuk mentransmisikan *digital video* melalui suatu jaringan data sehingga *video playback* dapat langsung dilakukan tanpa harus menunggu proses *download* selesai terlebih dahulu ataupun menyimpannya terlebih dahulu disisi *PC client*. Sistem *video streaming* melibatkan proses *encoding* terhadap isi dari data *video*, dan kemudian mentransmisikan *video streaming* melalui suatu jaringan (*wired* atau *wireless*), sehingga *client* tujuan dapat mengakses, melakukan *decoding*, dan menampilkan video tersebut secara *real-time*.

Teknologi *streaming* cenderung bersifat *bandwidth-dependent*, sehingga sangat bergantung pada kondisi jaringan. Agar *data stream* dapat di-*playback* secara baik, perlu diperhatikan beberapa pertimbangan supaya *data stream* memiliki *bit rate/data transfer rate* yang cukup rendah, karena dengan mengurangi *bit rate* berarti sama saja dengan mengirimkan lebih sedikit data. Mengurangi *bit rate* dapat dilakukan dengan cara antara lain membuat dimensi *frame* video menjadi lebih kecil, membuat jumlah *frame per second* (fps) video menjadi lebih rendah serta mengurangi jumlah informasi yang ada di setiap *frame* video melalui proses kompresi. [8]

### 2.4.1 Mode Jaringan Video Streaming

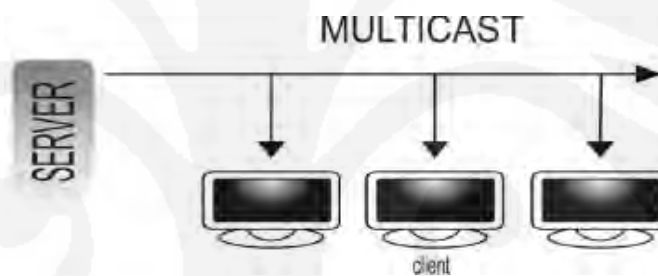
Suatu data informasi dapat dikirimkan melalui jaringan secara unicast maupun multicast.

- a. **Unicast**, bersifat *end-to-end*, di mana setiap *client* mendapatkan *stream data* yang berbeda dari *client* yang lain, meskipun pengiriman dilakukan secara simultan. Dengan menggunakan *server* yang sama, model koneksi *unicast* akan membutuhkan jumlah link koneksi sama sama dengan banyaknya jumlah *client*. [8]



Gambar 2.9 Streaming Unicast Mode [8]

- b. **Multicast**, server hanya mengirimkan satu jenis data stream saja yang kemudian diduplikasi oleh *router* khusus sebelum dikirim melalui jaringan ke *client-client*. Secara teknis, model koneksi *multicast* hanya bersifat komunikasi satu arah yang tidak jauh berbeda dengan sistem *broadcast* penyiaran televisi, sehingga fasilitas *on-demand* hampir tidak mungkin dilakukan. [8]



Gambar 2.10 Streaming Multicast Mode [8]

#### 2.4.2 Performansi Jaringan Video Streaming

Suatu jaringan dapat disebut ideal apabila mampu mengirimkan informasi apapun, tidak terbatas jumlah dan ukuran, serta tanpa menimbulkan *delay* ataupun *loss*. Akan tetapi dalam prakteknya akan sangat sulit untuk menciptakan jaringan dengan karakteristik seperti itu, karena *bit error*, *bit loss*, *delay*, *latency*, dan terbatasnya *bandwidth* merupakan hal-hal yang bersifat temporal. Faktor performansi dari sistem *video streaming* dalam hubungannya dengan jaringan dapat dijelaskan sebagai berikut :

a. **Bandwidth**

*Bandwidth* adalah jumlah data yang dapat melalui suatu jaringan, atau bagian dari jaringan, untuk setiap waktu tertentu. [8] *Bandwidth* pada jaringan bersifat terbagi, terbatas, dan berubah terhadap waktu. Suatu

jaringan tidak mampu menjamin *bandwidth* yang dibutuhkan untuk mentransmisikan *video* akan selalu tersedia.

**b. Delay.**

Secara umum *delay* adalah waktu tunda yang disebabkan oleh proses transmisi dari satu titik ke titik lain yang menjadi tujuannya. [9] Apabila data video menghabiskan terlalu banyak waktu pada saat berada di jaringan, maka hal tersebut akan menjadi tidak berguna, meskipun data video tersebut pada akhirnya berhasil diterima oleh *client*. Hal ini disebabkan di sisi *client* sistem masih melakukan proses *decoding* dan menampilkan video tersebut, sehingga total waktu yang dihabiskan akan terlalu lama untuk dapat disebut sebagai *real-time*. Persamaan 2.1 merupakan perhitungan untuk mencari *delay* yang disebabkan karena proses *encoding* dan *decoding*. [10]

$$d = Trdf - Trsd \quad (\text{Persamaan 2.1})$$

dimana,  $d$  = delay (detik)

$Trdf$  = selang waktu penerimaan keseluruhan paket (detik)

$Trsd$  = selang waktu pengiriman keseluruhan paket (detik)

**c. Packet loss** adalah satu atau lebih paket yang gagal melewati jaringan untuk mencapai tujuan. Persamaan 2.2 berikut ini merupakan perhitungan untuk mencari persentase jumlah paket yang hilang selama proses transmisi. [9]

$$L = \frac{A - B}{A} \times 100\% \quad (\text{Persamaan 2.2})$$

dimana,  $L$  = persentase jumlah paket yang hilang (%)

$A$  = jumlah paket yang dikirim (paket)

$B$  = jumlah paket yang diterima (paket)

Hilangnya sebagian dari data video yang dikirimkan melalui jaringan dapat disebabkan oleh banyak hal, seperti *congestion*, penolakan oleh sistem karena *delay* yang terlalu lama, ataupun kesalahan pada jaringan itu sendiri. Suatu sistem *video streaming* tidak dapat mengabaikan

kemungkinan terjadinya *data error* ataupun *data loss* selama proses transmisi, karena akan mengakibatkan kualitas yang buruk dari video pada saat ditampilkan. *Loss* yang terjadi pada jaringan dapat mengakibatkan keadaan yang lebih parah di sisi *client*, misalkan paket data pertama dari *frame-frame* video yang ditransmisikan itu rusak atau hilang selama berada di jaringan, maka seluruh paket data sisanya tidak akan dapat ditampilkan meskipun berhasil dikirimkan dan diterima oleh *client*.

### **2.4.3 Parameter-Parameter Aplikasi Video Streaming**

#### **2.4.3.1 Bit Rate**

*Bit rate* merupakan jumlah informasi yang disimpan dalam satu satuan waktu dalam suatu *file*. *Bit rate* dipengaruhi oleh *sample frequency*, jenis *encoding*, dan lain-lain. [11]

#### **2.4.3.2 Frame Rate**

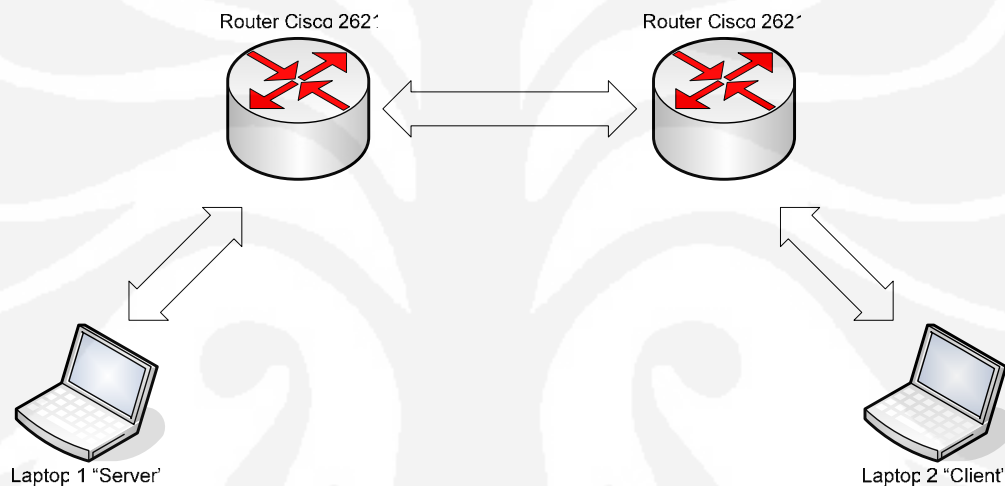
*Frame rate* merupakan banyaknya jumlah *frame* yang bisa dihasilkan atau ditampilkan dalam satu satuan detik. *Frame rate* digunakan untuk mensinkronisasi audio dan gambar, terutama dalam video. [12]

## BAB 3

### PERANCANGAN JARINGAN DAN METODE PENGAMBILAN DATA

#### 3.1 Topologi Jaringan

Rancangan jaringan yang digunakan adalah jaringan lokal yang terdiri dari 2 buah *mobile computer* yang berfungsi sebagai *client* dan *server* dengan platform Windows XP, serta 2 buah *router Cisco Series 2621* sebagai *intermediate device* yang menghubungkan *client* dan *server*. Secara global, bentuk topologi jaringan yang digunakan untuk proses pengujian ditunjukkan pada Gambar 3.1 berikut ini.



**Gambar 3.1** Topologi Global Jaringan untuk Proses Pengujian

Spesifikasi teknis untuk perangkat keras yang digunakan pada jaringan *test bed* adalah sebagai berikut :

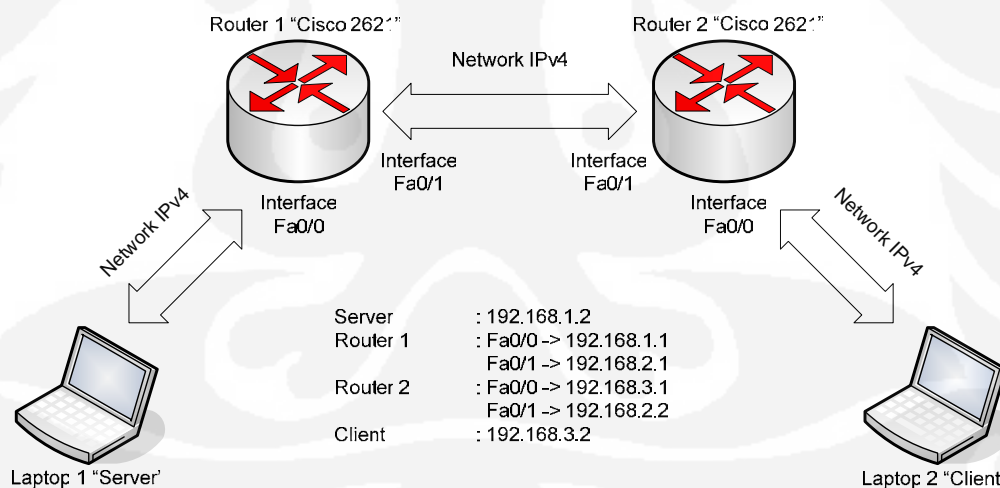
1. *Server* dengan platform Windows XP Service Pack 2  
Spesifikasi : Intel Core Duo Processor 2GHz, Memory 1G RAM, Ethernet 100Mbps.
2. *Client* dengan platform Windows XP Service Pack 2  
Spesifikasi : Intel Core Duo Processor 1.86GHz, Memory 1G RAM, Ethernet 100Mbps.
3. *Router 1* dan *Router 2*  
Spesifikasi : Cisco Router Series 2621

Untuk proses *streaming* yang dilakukan akan diinstall *software* VideoLAN Client (VLC) baik disisi *server* maupun disisi *client*. VLC dipilih karena dapat digunakan sebagai *server* maupun *client*. *Server* akan mengirimkan suatu *video* ke *client* secara *streaming*, kemudian disisi *client* akan menjalankan *video* tersebut secara *streaming*.

## 3.2 Konfigurasi Jaringan

### 3.2.1 Konfigurasi Jaringan IPv4 Murni

Konfigurasi jaringan terdiri dari 2 buah laptop dan 2 buah *router* yang pengalamatan IPv4 dikonfigurasi secara *manual*. Pada laptop 1 yang digunakan sebagai *server* akan diberikan alamat IP secara *static* dengan menggunakan IP *class* C. Begitu pula pada laptop 2 yang digunakan sebagai *client* akan diberikan alamat IP secara *static* dengan menggunakan IP *class* C. Untuk *router* 1 dan *router* 2 yang digunakan sebagai jembatan antara *network* laptop 1 dan laptop 2 akan diberikan alamat IP *class* C secara *static* pula. Konfigurasi jaringan IPv4 murni ditunjukkan seperti pada Gambar 3.2 berikut ini.

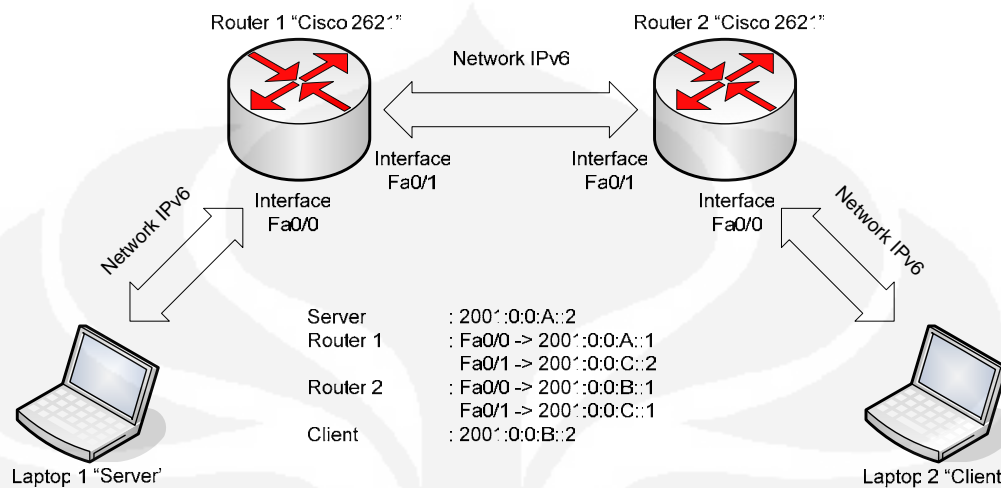


Gambar 3.2 Konfigurasi Jaringan IPv4 Murni

### 3.2.2 Konfigurasi Jaringan IPv6 Murni

Konfigurasi jaringan terdiri dari 2 buah laptop dan 2 buah *router* yang pengalamatan IPv6 dikonfigurasi secara *manual*. Pada laptop 1 dan laptop 2 akan diberikan alamat IPv6 tanpa melihat *class* IP tersebut, karena pada IPv6 tidak

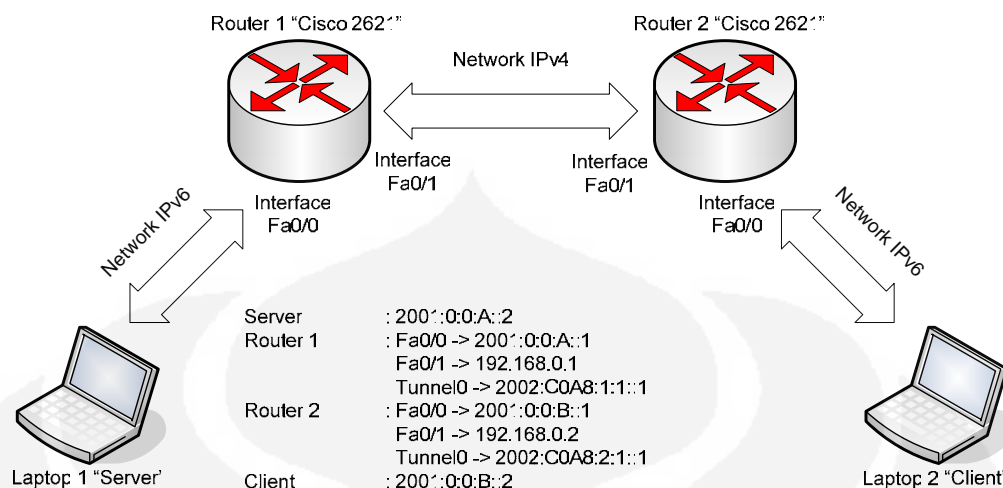
mengenal pengelompokan IP seperti pada IPv4. Konfigurasi jaringan IPv6 murni ditunjukkan seperti pada Gambar 3.3 berikut ini.



Gambar 3.3 Topologi Jaringan IPv6 Murni

### 3.2.3 Konfigurasi *Tunneling* 6to4

Konfigurasi jaringan terdiri dari 2 buah laptop dan 2 buah *router* yang pengalamatannya dikonfigurasi secara *manual*. Untuk rancangan IP pada laptop 1 dan laptop 2 sama dengan konfigurasi jaringan IPv6 murni. Untuk *router* 1 diberi alamat IP secara manual sebagai *router tunneling* 6to4, dimana *interface Fa0/0* diberi alamat IPv6 yang satu *network* dengan laptop 1, *interface Fa0/1* diberi alamat IPv4 dan *interface Tunnel0* diberi alamat *Tunneling* 6to4 menggunakan alamat *global prefix* 2002:WWXX:YYZZ::/48, dimana WWXX:YYZZ adalah *colon-hexadecimal* yang merepresentasikan alamat publik IPv4. Begitu pula untuk konfigurasi alamat IP pada *router* 2, *interface Fa0/0* diberi alamat IPv6 yang satu *network* dengan laptop 2, *interface Fa0/1* diberi alamat IPv4 dan *interface Tunnel0* diberi alamat *Tunneling* 6to4 menggunakan alamat *global prefix* 2002:WWXX:YYZZ::/48, dimana WWXX:YYZZ adalah *colon-hexadecimal* yang merepresentasikan alamat publik IPv4. Konfigurasi jaringan *Tunneling* 6to4 ditunjukkan seperti pada Gambar 3.4 berikut ini.

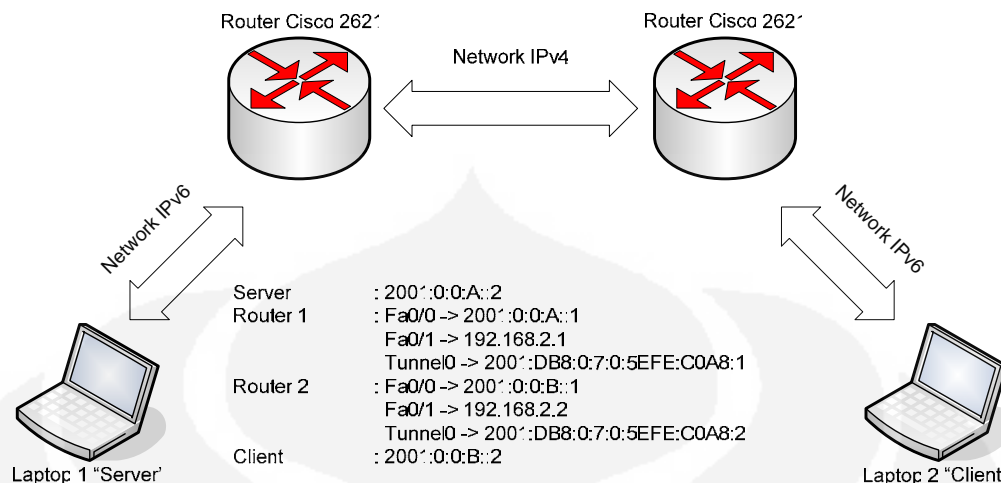


**Gambar 3.4** Topologi Jaringan *Tunneling 6to4*

### 3.2.4 Konfigurasi *Tunneling* ISATAP

Konfigurasi jaringan terdiri dari 2 buah laptop dan 2 buah *router* yang pengalamatannya dikonfigurasi secara manual. Pada laptop 1 dan laptop 2 akan diberikan alamat IPv6 secara manual. Sedangkan disisi *router* 1 dan *router* 2 akan diberikan alamat *private unicast* IPv4 secara manual juga. Secara otomatis, *router* 1 dan *router* 2 akan membentuk alamat IP *Tunneling* ISATAP yang terdiri dari 64 bit awal merupakan *global prefix* ISATAP, 32 bit berikutnya merupakan IPv6 dan 32 bit terakhir merupakan alamat IPv4 yang telah diubah ke bentuk *hexadecimal*. Oleh karena digunakan alamat *private unicast* IPv4 maka alamat ISATAP menggunakan *interface identifier* ::0:5EFE:w.x.y.z, dimana w.x.y.z adalah alamat *private unicast* IPv4. Konfigurasi jaringan *Tunneling* ISATAP ditunjukkan seperti pada Gambar 3.5 berikut ini.





Gambar 3.5 Topologi Jaringan Tunneling ISATAP

### 3.3 Software Pendukung

Software yang digunakan untuk mendukung skripsi yang dilakukan antara lain :

- VideoLAN Client (VLC), digunakan sebagai aplikasi untuk melakukan *streaming file-file* audio dan video dari berbagai jenis format. VLC dapat digunakan sebagai *streaming server* maupun *streaming client*. Disamping itu, VLC mampu bekerja dengan baik pada jaringan IPv4 dan IPv6.
- Wireshark, digunakan sebagai aplikasi untuk mengambil dan menganalisa *protocol-protocol* yang bekerja selama proses *streaming* maupun menganalisa trafik yang terjadi pada suatu *interface*.

### 3.4 Metode Pengambilan Data

Pengambilan data dilakukan dengan cara menjalankan *file* video dengan pengaturan *bit rate* yang bervariasi pada jaringan IPv4 murni, jaringan IPv6 murni, jaringan IPv6 dengan *Tunneling 6to4* dan ISATAP. Pengambilan data dilakukan pada tiap-tiap konfigurasi jaringan dimana proses *streaming* menggunakan VideoLAN Client yang diatur sebagai *server streaming* dan *client streaming*. Enkapsulasi yang digunakan untuk proses *streaming* menggunakan MPEG TS (*Moving Picture Experts Group Transport Stream*) yang merupakan *default setting* pada VLC. Program Wireshark dijalankan disisi *server* dan *client*

untuk melihat *protocol-protocol* yang berperan selama proses *streaming* berlangsung serta mengetahui parameter *delay* dan *packet loss* yang terjadi.

Pada skripsi ini, untuk menguji pengaruh besar *bit rate* terhadap *delay* dan *packet loss*, *file* video yang digunakan pada proses *streaming* diberi nama Video\_Tes\_Skripsi.mpg dengan durasi 29 detik, berukuran 9285 KB dan *frame rate* diatur 23,98 fps sesuai dengan *file* aslinya. *Streaming file* tersebut akan dilakukan dengan pengaturan *video codec* menggunakan mp4v dan *audio codec* menggunakan mpga serta pengaturan *bit rate* yang bervariasi untuk video dan audio, yaitu 1024-192, 512-128, dan 256-64. Nilai 1024-192 dapat diartikan bahwa *file* video dikirim dengan nilai *bit rate* video sebesar 1024 kbps dan *bit rate* audio sebesar 192 kbps. Nilai 512-128 dapat diartikan bahwa *file* video dikirim dengan nilai *bit rate* video sebesar 512 kbps dan *bit rate* audio sebesar 128 kbps. Nilai 256-64 dapat diartikan bahwa *file* video dikirim dengan nilai *bit rate* video sebesar 256 kbps dan *bit rate* audio sebesar 64 kbps. Untuk melakukan perubahan nilai *bit rate* audio dan video sudah tersedia pada VLC. Disamping itu pada saat proses *streaming* juga ditambahkan simulasi penambahan trafik pada jaringan dengan melakukan tes ping secara kontinyu dengan pemberian beban 64000 bytes baik dari *server* ke *client* maupun dari *client* ke *server*. Hal ini berlaku untuk semua bentuk konfigurasi jaringan.

Data yang diambil selama proses *streaming* berlangsung pada *Wireshark* yaitu *delay* dan *packet loss*. Data *delay* diambil dari lamanya waktu ketika paket pertama mulai dikirim sampai dengan paket terakhir yang berhasil terkirim, pada *Wireshark* ditunjukkan *Menu Toolbar Wireshark "Summary"* kemudian dilihat pada data "Between first and last packet" dan dihitung selisih antara *client* dan *server*. Data *packet loss* diambil dengan melihat besarnya paket yang hilang ketika proses *streaming* berlangsung, pada *Wireshark* ditunjukkan pada *Menu Toolbar Wireshark "Summary"* kemudian dilihat pada data "Packets" dan dihitung selisih antara jumlah paket yang tertangkap disisi *server* dan disisi *client*. Pengambilan data dilakukan sebanyak 10 kali untuk setiap pengaturan *bit rate* dan untuk empat macam konfigurasi jaringan. Untuk analisa *delay* akan didapatkan 30 data untuk setiap konfigurasi sehingga total akan didapatkan 120 data. Sedangkan untuk analisa *packet loss* akan didapatkan 30 data untuk setiap konfigurasi

sehingga total akan didapatkan 120 data. Jadi jumlah total keseluruhan data adalah 240 data.



## BAB 4 ANALISA

### 4.1 Pengambilan Data

Proses *streaming* pada skripsi ini dilakukan dengan menggunakan aplikasi VideoLAN *Client* yang diujikan pada empat konfigurasi yang berbeda, yaitu jaringan IPv4, jaringan IPv6, jaringan IPv6 *Tunneling* 6to4 dan jaringan IPv6 *Tunneling* ISATAP. Pengamatan data selama proses *streaming* dilakukan dengan menggunakan aplikasi tambahan *Wireshark*, dimana untuk mengambil data *delay* dan *packet loss* dapat dilakukan dengan memanfaatkan fitur-fitur yang ada pada *Wireshark*.

Pada VideoLAN *Client*, enkapsulasi yang digunakan untuk proses *streaming* menggunakan MPEG TS (*Moving Picture Experts Group Transport Stream*) yang merupakan *default setting* pada VLC. *File* yang digunakan pada proses *streaming* diberi nama Video\_Tes\_Skripsi.mpg dengan durasi 29 detik, berukuran 9285 KB dan *frame rate* diatur 23,98 fps sesuai dengan *file* aslinya. *Video streaming* dilakukan dengan pengaturan *video codec* menggunakan mp4v dan *audio codec* menggunakan mpga serta pengaturan *bit rate* yang bervariasi untuk video dan audio, yaitu

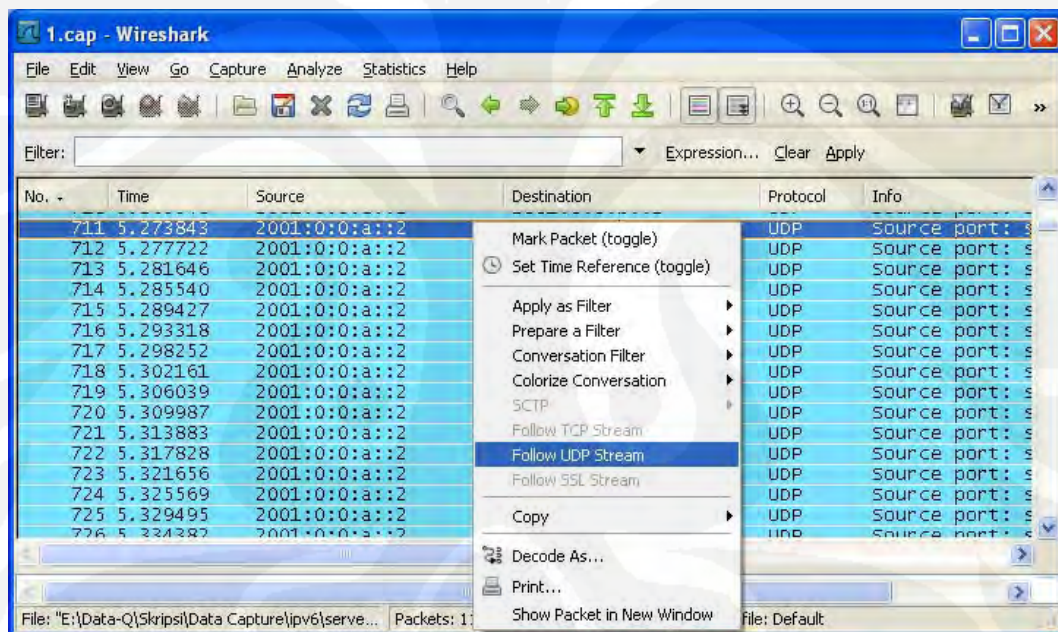
1. *Bit rate* video 1024 kbps dan audio 192 kbps, dengan jumlah paket yang tersimpan sebanyak 5011 paket.
2. *Bit rate* video 512 kbps dan audio 128 kbps, dengan jumlah paket yang tersimpan sebanyak 4747 paket.
3. *Bit rate* video 256 kbps dan audio 64 kbps, dengan jumlah paket yang tersimpan sebanyak 4530 paket.

Pengaturan *bit rate* yang bervariasi untuk satu *file* yang sama dimaksudkan untuk menguji pengaruh besar *bit rate* terhadap *delay* dan *packet loss* yang terjadi selama proses *streaming*. Aplikasi *Wireshark* dijalankan disisi *server* dan *client* untuk melihat *protocol-protocol* yang berperan selama proses *streaming* berlangsung serta mengetahui parameter *delay* dan *packet loss* yang terjadi.

Simulasi penambahan trafik pada jaringan dilakukan dengan tes ping secara kontinyu dengan beban sebesar 64000 *bytes* baik dari *server* ke *client*

maupun dari *client* ke *server*. Hal ini dilakukan dengan tujuan untuk memberikan gangguan trafik pada saat proses *streaming* berlangsung, sehingga diharapkan dapat mewakili kondisi jaringan yang sesungguhnya.

Parameter *delay* diambil dengan cara menjalankan aplikasi *Wireshark* disisi *client* dan *server* untuk menangkap semua trafik yang terjadi selama proses *streaming*. Setelah proses *streaming* selesai, pada *Wireshark* dilakukan proses *filtering* berdasarkan *protocol* yang berperan selama proses *streaming* disisi *client* dan *server*. Dengan melakukan *filtering* tersebut maka data yang terdapat pada *Wireshark* sudah murni hanya data *protocol* yang berperan selama proses *streaming* saja. Cara melakukan *filtering protocol* pada *Wireshark* ditunjukkan pada Gambar 4.1 berikut ini.



**Gambar 4.1** Cara Melakukan *Filter Protocol Streaming*

Kemudian parameter *delay* diambil dari selisih antara *latency* yang terjadi selama proses *streaming* dengan durasi waktu dari *file* video tersebut. Pada *Wireshark* ditunjukkan pada Gambar 4.2 berikut ini.

Traffic	Captured	Displayed	Marked
Packets	8538	5009	0
Between first and last packet	39,242 sec	29,977 sec	
Avg. packets/sec	217,575	167,094	
Avg. packet size	1426,378 bytes	1390,000 bytes	
Bytes	12178417	6962510	
Avg. bytes/sec	310343,634	232260,099	
Avg. MBit/sec	2,483	1,858	

**Gambar 4.2** Data Latency Pengiriman File Dari *Server* ke *Client*

Parameter *packet loss* diambil dengan melihat besarnya paket yang hilang ketika proses *streaming* berlangsung, Pada *Wireshark* ditunjukkan pada *Menu Toolbar Wireshark "Summary"* kemudian dilihat pada data "Packets". Lalu dihitung selisih antara jumlah paket yang ditangkap disisi *server* dan *client*. Hal ini ditunjukkan pada nilai paket yang diberi tanda lingkaran merah pada Gambar 4.3 berikut ini.

Wireshark: Summary			
File			
Name:	D:\Data Capture\6to4\Server\256\1.cap		
Length:	15674222 bytes		
Format:	Wireshark/tcpdump/... - libpcap		
Packet size limit:	65535 bytes		
Time			
First packet:	2009-06-02 09:53:43		
Last packet:	2009-06-02 09:54:20		
Elapsed:	00:00:37		
Capture			
Interface:	unknown		
Dropped packets:	unknown		
Capture filter:	unknown		
Display			
Display filter:	(ipv6.addr eq 2001:0:0:a::2 and ipv6.addr eq 2001:0:0:b::2) and (udp.port eq 1086 and udp.port eq 1234)		
Traffic	Captured	Displayed	Marked
Packets	10757	4520	0
Between first and last packet	37,157 sec	29,876 sec	
Avg. packets/sec	289,501	151,292	
Avg. packet size	1441,116 bytes	1390,000 bytes	
Bytes	15502086	6282800	
Avg. bytes/sec	417204,052	210296,572	
Avg. MBit/sec	3,338	1,682	

Wireshark: Summary			
File			
Name:	D:\Data Capture\6to4\Client\256\1.cap		
Length:	15743095 bytes		
Format:	Wireshark/tcpdump/... - libpcap		
Packet size limit:	65535 bytes		
Time			
First packet:	2009-06-02 09:53:39		
Last packet:	2009-06-02 09:54:16		
Elapsed:	00:00:36		
Capture			
Interface:	unknown		
Dropped packets:	unknown		
Capture filter:	unknown		
Display			
Display filter:	(ipv6.addr eq 2001:0:0:a::2 and ipv6.addr eq 2001:0:0:b::2) and (udp.port eq 1086 and udp.port eq 1234)		
Traffic	Captured	Displayed	Marked
Packets	10791	4520	0
Between first and last packet	36,942 sec	29,875 sec	
Avg. packets/sec	292,108	151,296	
Avg. packet size	1442,908 bytes	1390,000 bytes	
Bytes	15570415	6282800	
Avg. bytes/sec	421484,852	210301,761	
Avg. MBit/sec	3,372	1,682	

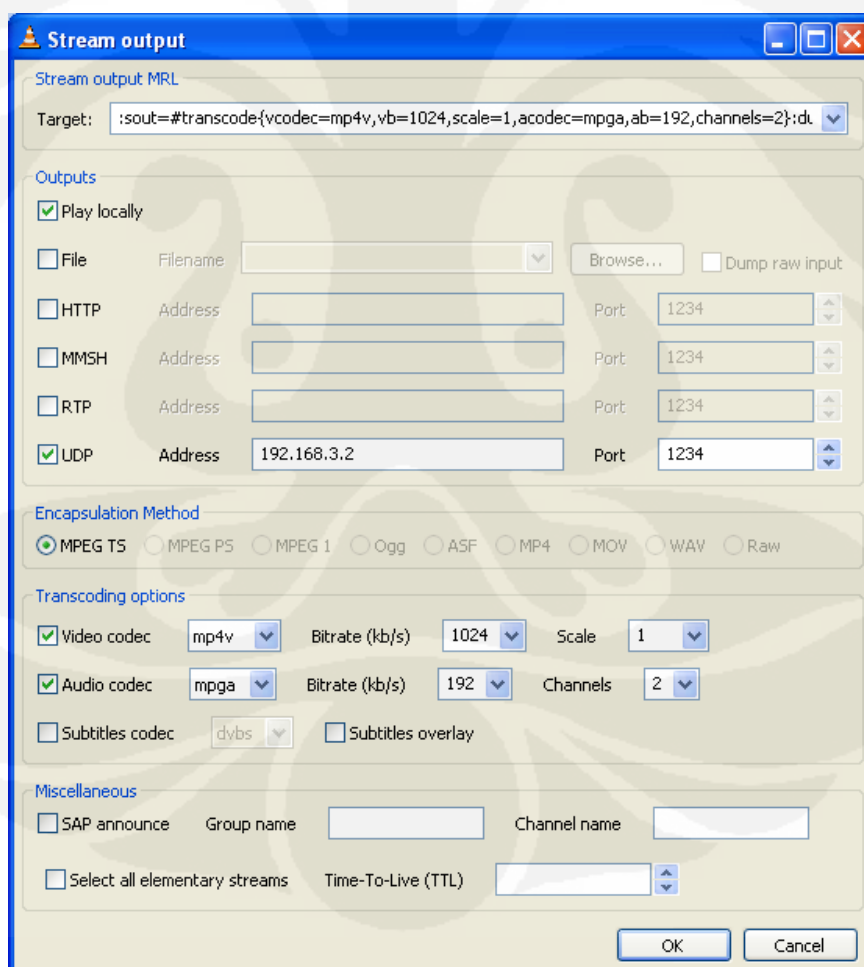
**Gambar 4.3** Data Jumlah Paket Disisi *Server* dan *Client* yang Ditangkap *Wireshark*

Pengambilan data dilakukan sebanyak 10 kali untuk pengaturan *bit rate* yang bervariasi mulai dari 1024-192, 512-128, dan 256-64 serta untuk empat macam konfigurasi jaringan. Untuk analisa *delay* akan didapatkan 30 data untuk setiap konfigurasi jaringan sehingga akan didapatkan 120 data. Sedangkan untuk analisa *packet loss* akan didapatkan 30 data untuk setiap konfigurasi jaringan sehingga akan didapatkan 120 data. Jadi jumlah keseluruhan data adalah 240 data.

## 4.2 Dokumentasi Proses Pengambilan Data

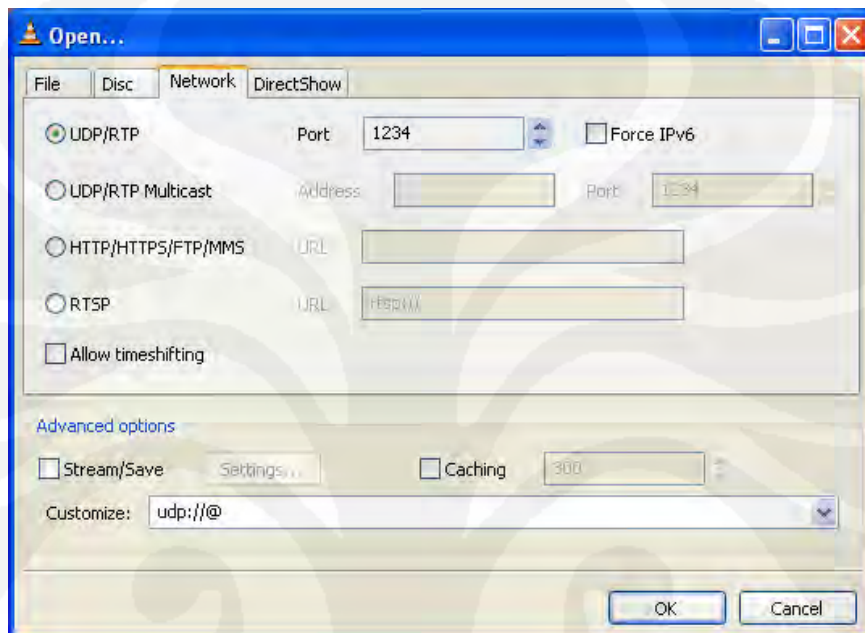
### 4.2.1 Jaringan IPv4

Proses *streaming* pada konfigurasi jaringan IPv4 menggunakan protokol UDP dengan port 1234. Contoh pengaturan *server* dan *client* pada VLC ditunjukkan pada Gambar 4.4 dan Gambar 4.5 berikut ini.



Gambar 4.4 Pengaturan *Server* pada VLC untuk Jaringan IPv4

Disisi *server* hanya dimasukkan satu jenis *IP client* sehingga ketika proses *streaming* berlangsung maka hanya ada satu *client* yang dapat menerima *streaming* tersebut. Disisi *client* dapat mengaktifkan VLC-nya secara terus-menerus dan *streaming* akan langsung terjadi ketika *server* mulai menjalankan *video streaming*.



**Gambar 4.5** Pengaturan *Client* pada VLC untuk jaringan IPv4

Oleh karena koneksi yang digunakan untuk mengontrol pengiriman data adalah UDP maka *transport protocol* yang berperan selama proses *streaming* adalah UDP, disamping itu juga akan muncul *protocol IP* karena selama proses *streaming* secara bersamaan juga dilakukan tes ping dengan beban 64000 *bytes* secara kontinyu, seperti ditunjukkan pada Gambar 4.6 dan Gambar 4.7 berikut ini. Contoh yang diambil adalah proses *streaming* dengan pengaturan *bit rate* 1024-192.



No.	Time	Source	Destination	Protocol	Info
1432	6.570506	192.168.1.2	192.168.3.2	UDP	Source port: anet-
1433	6.574411	DTS 30939.646644444	PTS 30939.646644444	MPEG PES	
1434	6.579290	192.168.1.2	192.168.3.2	UDP	Source port: anet-
1435	6.584155	192.168.1.2	192.168.3.2	UDP	Source port: anet-
1436	6.589072	192 kb/s	44.1 kHz	MPEG-1	Audio Layer 2
1437	6.593990	192.168.1.2	192.168.3.2	UDP	Source port: anet-
1438	6.598826	192.168.1.2	192.168.3.2	UDP	Source port: anet-
1439	6.603708	192.168.1.2	192.168.3.2	UDP	Source port: anet-
1440	6.608584	192.168.1.2	192.168.3.2	UDP	Source port: anet-
1441	6.613454	192 kb/s	44.1 kHz	MPEG-1	Audio Layer 2
1442	6.616591	192.168.1.2	192.168.3.2	IP	Fragmented IP prot
1443	6.616616	192.168.1.2	192.168.3.2	IP	Fragmented IP prot
1444	6.616625	192.168.1.2	192.168.3.2	IP	Fragmented IP prot
1445	6.616633	192.168.1.2	192.168.3.2	IP	Fragmented IP prot
1446	6.616642	192.168.1.2	192.168.3.2	IP	Fragmented IP prot
1447	6.616653	192.168.1.2	192.168.3.2	IP	Fragmented IP prot
1448	6.616661	192.168.1.2	192.168.3.2	IP	Fragmented IP prot

Gambar 4.6 Hasil *Packet Sniffing* IPv4 pada Wireshark Disisi *Server*

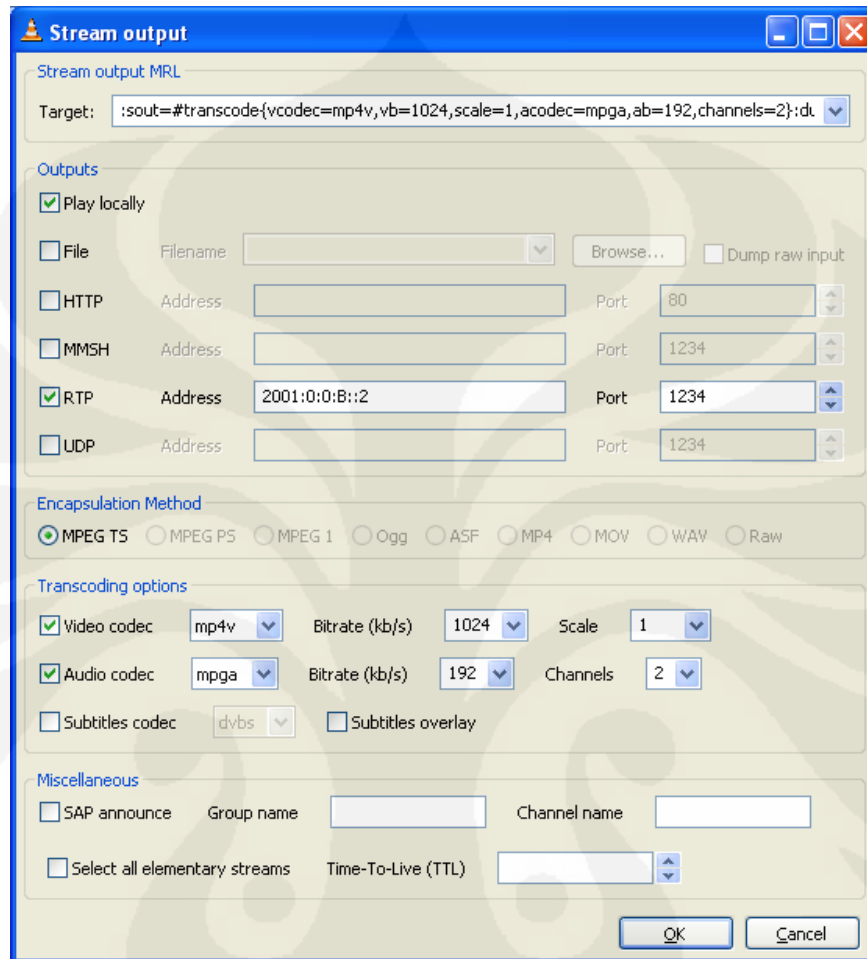
No.	Time	Source	Destination	Protocol	Info
1061	5.536142	192.168.3.2	192.168.1.2	IP	Fragmented IP prot
1062	5.536154	192.168.3.2	192.168.1.2	IP	Fragmented IP prot
1063	5.536164	192.168.3.2	192.168.1.2	IP	Fragmented IP prot
1064	5.536175	192.168.3.2	192.168.1.2	IP	Fragmented IP prot
1065	5.536187	192.168.3.2	192.168.1.2	IP	Fragmented IP prot
1066	5.536198	192.168.3.2	192.168.1.2	IP	Fragmented IP prot
1067	5.536207	192.168.3.2	192.168.1.2	ICMP	Echo (ping) reply
1068	5.536273	192.168.1.2	192.168.3.2	UDP	Source port: anet-
1069	5.536295	192.168.1.2	192.168.3.2	UDP	Source port: anet-
1070	5.544430	192.168.1.2	192.168.3.2	UDP	Source port: anet-
1071	5.544462	192.168.1.2	192.168.3.2	UDP	Source port: anet-
1072	5.546699	192.168.1.2	192.168.3.2	UDP	Source port: anet-
1073	5.550522	192.168.1.2	192.168.3.2	UDP	Source port: anet-
1074	5.554292	192.168.1.2	192.168.3.2	UDP	Source port: anet-
1075	5.558127	192.168.1.2	192.168.3.2	UDP	Source port: anet-
1076	5.562263	192.168.1.2	192.168.3.2	UDP	Source port: anet-

Gambar 4.7 Hasil *Packet Sniffing* IPv4 pada Wireshark Disisi *Client*

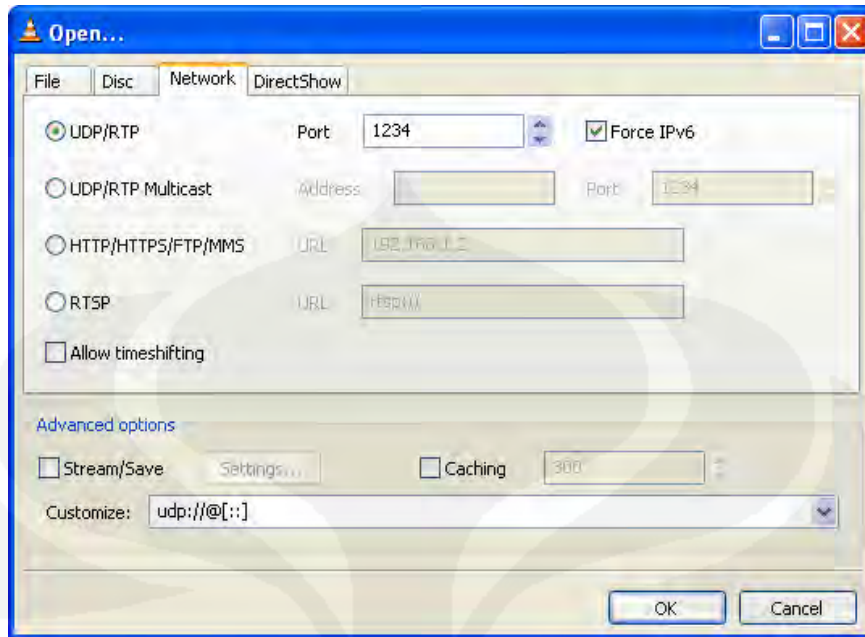
#### 4.2.2 Jaringan IPv6, Tunneling 6to4 dan ISATAP

Proses *streaming* pada konfigurasi jaringan IPv6, *tunneling* 6to4 dan ISATAP menggunakan protokol RTP dengan port 1234 serta melakukan *force* IPv6 yang tujuannya agar paket dapat melewati jaringan IPv6. Disisi *server* hanya dimasukkan satu jenis IP *client* sehingga ketika proses *streaming* berlangsung hanya ada satu *client* yang dapat menerima *streaming* tersebut. Disisi *client* dapat mengaktifkan VLC-nya secara terus-menerus dan *streaming* akan langsung terjadi

ketika *server* mulai menjalankan *video streaming*. Contoh pengaturan *server* dan *client* pada VLC ditunjukkan pada Gambar 4.8 dan Gambar 4.9 berikut ini.

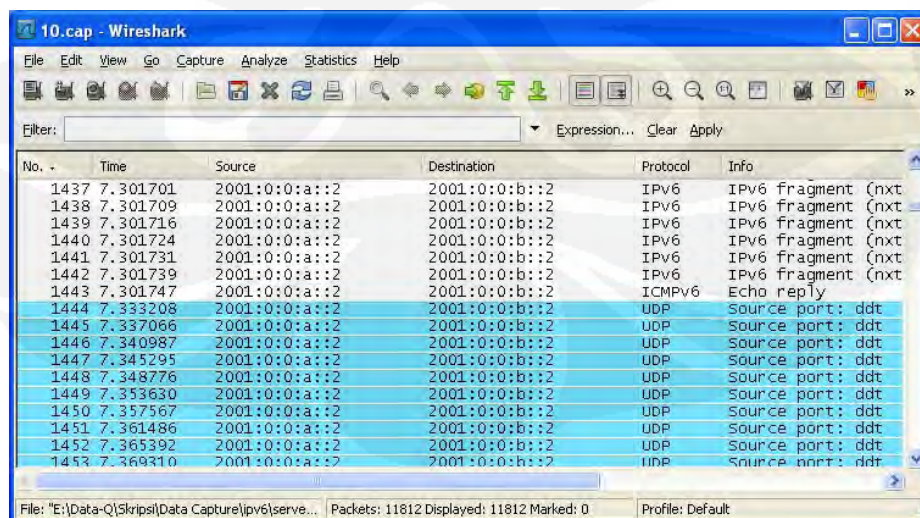


**Gambar 4.8** Pengaturan *Server* pada VLC untuk Jaringan IPv6, 6to4 dan ISATAP

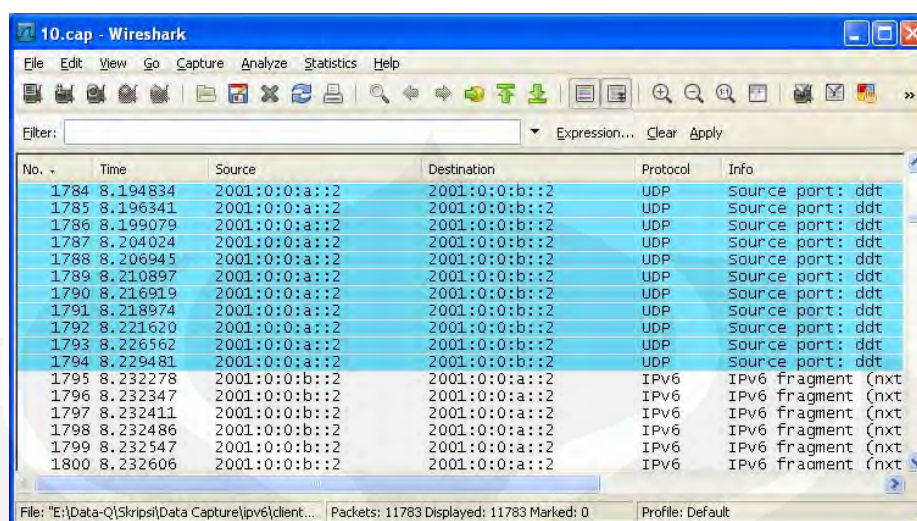


**Gambar 4.9** Pengaturan *Client* pada VLC untuk Jaringan IPv6, 6to4 dan ISATAP

Oleh karena koneksi yang digunakan untuk mengontrol pengiriman data adalah RTP maka *transport protocol* yang berperan selama proses *streaming* adalah UDP, disamping itu juga akan muncul *protocol* IPv6 karena selama proses *streaming* secara bersamaan juga dilakukan tes ping dengan beban 64000 *bytes* secara kontinyu, seperti ditunjukkan pada Gambar 4.10 dan Gambar 4.11 berikut ini.



**Gambar 4.10** Hasil *Packet Sniffing* IPv6 pada Wireshark Disisi *Server*



Gambar 4.11 Hasil *Packet Sniffing* IPv6 pada Wireshark Disisi *Client*

### 4.3 Analisa Konfigurasi Jaringan

Konfigurasi IPv4 murni, IPv6 murni, maupun IPv6 dengan *Tunneling* 6to4 dan ISATAP yang digunakan pada tugas akhir ini mempunyai topologi jaringan yang sama dimana terdiri dari 2 buah laptop yang berfungsi sebagai *server* dan *client* dan 2 buah *router* sebagai *intermediate device* yang menghubungkan 2 *network* yang berbeda antara *server* dan *client*. Dengan begitu akan didapatkan hasil perbandingan yang sama untuk semua konfigurasi karena topologi tidak mengalami perubahan sama sekali.

#### 4.3.1 Konfigurasi Jaringan IPv4

Seluruh komponen dalam topologi jaringan IPv4 diberi alamat IPv4 *class C* dan ditambahkan *static routing* dikedua *router*. Oleh karena seluruh jaringan menggunakan IPv4 maka selama proses transmisi data hanya terjadi proses *routing* dan *forwarding packet*.

Apabila dilakukan *traceroute* dari *server* (192.168.1.2) ke *client* (192.168.3.2) ataupun sebaliknya dari *client* (192.168.3.2) ke *server* (192.168.1.2) maka akan didapatkan hasil seperti Gambar 4.12 berikut ini.

```

C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\AdiPrayitno>
C:\Documents and Settings\AdiPrayitno>
C:\Documents and Settings\AdiPrayitno>tracert 192.168.3.2

Tracing route to 192.168.3.2 over a maximum of 30 hops

  1    1 ms    1 ms    1 ms  192.168.1.1
  2    1 ms    1 ms    1 ms  192.168.2.2
  3    1 ms    <1 ms   <1 ms  192.168.3.2

Trace complete.

C:\Documents and Settings\AdiPrayitno>
C:\Documents and Settings\AdiPrayitno>
C:\Documents and Settings\AdiPrayitno>

C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Muamar>
C:\Documents and Settings\Muamar>
C:\Documents and Settings\Muamar>tracert 192.168.1.2

Tracing route to 192.168.1.2 over a maximum of 30 hops

  1    <1 ms   <1 ms   <1 ms  192.168.3.1
  2    1 ms    1 ms    1 ms  192.168.2.1
  3    <1 ms   <1 ms   <1 ms  192.168.1.2

Trace complete.

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

```

Gambar 4.12 Hasil Traceroute IPv4

Dari hasil *traceroute* tersebut ditunjukkan bahwa *client* dengan *network* (192.168.1.0) akan berkomunikasi ke *server* dengan *network* (192.168.3.0) melalui *network* (192.168.2.0) yang dibentuk oleh *router* 1 dan *router* 2. Untuk konfigurasi selengkapnya dapat dilihat pada Lampiran 1.

### 4.3.2 Konfigurasi Jaringan IPv6

Konfigurasi jaringan IPv6 murni tidak jauh berbeda dengan konfigurasi pada IPv4 murni, hanya saja untuk pemberian alamat IP sudah tidak mengacu pada *class* IP karena pada IPv6 tidak mengenal *class* IP. Seluruh komponen dalam topologi jaringan IPv6 diberi alamat IPv6 dan ditambahkan *static routing* di kedua *router*. Seperti halnya pada IPv4, karena seluruh *network* menggunakan IPv6 maka selama proses transmisi data hanya terjadi proses *routing* dan *forwarding packet*.

```

C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\AdiPrayitno>
C:\Documents and Settings\AdiPrayitno>
C:\Documents and Settings\AdiPrayitno>tracert 2001:0:0:b::2

Tracing route to 2001:0:0:b::2 over a maximum of 30 hops

  1    1 ms    1 ms    <1 ms  2001:0:0:a::1
  2    2 ms    2 ms    2 ms   2001:0:0:c::1
  3    2 ms    2 ms    2 ms   2001:0:0:b::2

Trace complete.

C:\Documents and Settings\AdiPrayitno>
C:\Documents and Settings\AdiPrayitno>
C:\Documents and Settings\AdiPrayitno>_

C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Muamar>
C:\Documents and Settings\Muamar>
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    2 ms     2 ms     2 ms   2001:0:0:c::2
  3    4 ms     2 ms     2 ms   2001:0:0:a::2

Trace complete.

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

```

Gambar 4.13 Hasil Traceroute IPv6

Apabila dilakukan *traceroute* dari *server* (2001:0:0:A::2) ke *client* (2001:0:0:B::2) ataupun sebaliknya dari *client* (2001:0:0:B::2) ke *server* (2001:0:0:A::2) maka akan didapatkan hasil seperti Gambar 4.13. Dari hasil *traceroute* tersebut ditunjukkan bahwa *client* akan berkomunikasi ke *server* melalui *router* 1 (2001:0:0:C::2) dan *router* 2 (2001:0:0:C::1). Untuk konfigurasi selengkapnya dapat dilihat pada Lampiran 2.

### 4.3.3 Konfigurasi Jaringan Tunneling 6to4

Pada konfigurasi jaringan *tunneling* 6to4, *server* dan *client* diberi alamat IPv6. Konfigurasi disisi *router* akan mengalami perbedaan bila dibandingkan dengan konfigurasi *router* pada jaringan IPv4 dan IPv6 murni. Pada *router* 1, *interface* Fa0/1 yang berhadapan dengan jaringan IPv4 akan diberikan alamat IPv4 (192.168.0.1) dan *interface* Fa0/0 yang berhadapan dengan *server* diberikan alamat IPv6 (2001:0:0:A::1/64). Sedangkan *interface* Tunnel0 diberikan alamat IP (2002:C0A8:1:1::1/64) yang merupakan alamat *global prefix tunneling* 6to4

dikombinasikan dengan alamat IPv4. Pada *router 2*, *interface Fa0/1* yang berhadapan dengan jaringan IPv4 akan diberikan alamat IPv4 (192.168.0.2) dan *interface Fa0/0* yang berhadapan dengan *client* diberikan alamat IPv6 (2001:0:0:B::1/64). Sedangkan *interface Tunnel0* diberikan alamat IP (2002:C0A8:2:1::1/64) yang merupakan alamat *global prefix tunneling 6to4* dikombinasikan dengan alamat IPv4.

Pada *tunneling 6to4*, terdapat tiga buah *routing* yang ditambahkan pada *router*. Pertama, *static routing* untuk melewati jaringan dengan cakupan IP (2002::/16) melalui *interface Tunnel0*. Kedua, *static routing* untuk melewati seluruh jaringan IPv6 dengan cakupan IP (::/0) melalui alamat *global prefix tunneling 6to4* dikombinasi dengan IPv4. Dan ketiga, *routing RIP* untuk merutekan alamat IPv4.

Untuk proses *routing* dari *server* ke *client*, ketika IP *server* (2001:0:0:A::2) masuk ke *router 1* maka akan langsung dilewatkan ke alamat (2002:C0A8:1:1::1) melalui *interface Tunnel0*. Didalam *interface Tunnel0*, alamat (2002:C0A8:1:1::1) yang akan masuk ke network IPv4 diterjemahkan oleh proses *tunneling* sehingga didapatkan alamat IPv4 (192.168.0.1) yang merupakan alamat *interface Fa0/1*. Setelah diketahui jalur IP yang akan dilewati, *router 1* akan mencari alamat IPv4 yang satu network sehingga bertemu dengan alamat IPv4 (192.168.0.2) yang merupakan alamat *interface Fa0/1 router 2*. Alamat IPv4 ini akan diterjemahkan selama proses *tunneling* sehingga didapatkan alamat IP (2002:C0A8:2:1::1) dan akhirnya akan bertemu dengan IP *client* (2001:0:0:B::2). Begitu pula untuk proses *routing* dari *client* ke *server*.

Apabila dilakukan *traceroute* dari *server* (2001:0:0:A::2) ke *client* (2001:0:0:B::2) ataupun sebaliknya dari *client* (2001:0:0:B::2) ke *server* (2001:0:0:A::2) maka akan didapatkan hasil seperti Gambar 4.14 berikut ini.

```

C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\AdiPrayitno>
C:\Documents and Settings\AdiPrayitno>
C:\Documents and Settings\AdiPrayitno>tracert 2001:0:0:b::2

Tracing route to 2001:0:0:b::2 over a maximum of 30 hops

  1  <1 ms    1 ms    <1 ms    2001:0:0:a::1
  2   4 ms    4 ms    4 ms    2002:c0a8:2:1::1
  3   4 ms    4 ms    4 ms    2001:0:0:b::2

Trace complete.

C:\Documents and Settings\AdiPrayitno>
C:\Documents and Settings\AdiPrayitno>
C:\Documents and Settings\AdiPrayitno>_

```

```

C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Muamar>
C:\Documents and Settings\Muamar>
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    3 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>
C:\Documents and Settings\Muamar>
C:\Documents and Settings\Muamar>

```

Gambar 4.14 Hasil Traceroute Tunneling 6to4

Dari hasil *traceroute* tersebut ditunjukkan bahwa *client* akan berbicara ke *server* melalui *router* 1 (2002:C0A8:1:1::1) dan *router* 2 (2002:C0A8:2:1::1) yang merupakan IP Tunneling 6to4. Untuk konfigurasi selengkapnya dapat dilihat pada Lampiran 3.

#### 4.3.4 Konfigurasi Jaringan Tunneling ISATAP

Pada konfigurasi jaringan *tunneling* ISATAP, *server* dan *client* diberi alamat IPv6. Konfigurasi disisi *router* akan mengalami perbedaan bila dibandingkan dengan konfigurasi *router* pada jaringan IPv4 dan IPv6 murni. Pada *router* 1, *interface Fa0/1* yang berhadapan dengan jaringan IPv4 akan diberikan alamat IPv4 (192.168.0.1) dan *interface Fa0/0* yang berhadapan dengan *server* diberikan alamat IPv6 (2001:0:0:A::1/64). Sedangkan *interface Tunnel0* diberikan alamat IP (2001:DB8:0:7:0:5EFE:C0A8:1/64) yang merupakan alamat *tunneling* ISATAP. Pada *router* 2, *interface Fa0/1* yang berhadapan dengan jaringan IPv4 akan diberikan alamat IPv4 (192.168.0.2) dan *interface Fa0/0* yang berhadapan



dengan *client* diberikan alamat IPv6 (2001:0:0:B::1/64). Sedangkan *interface Tunnel0* diberikan alamat IP (2001:DB8:0:7:0:5EFE:C0A8:2/64) yang merupakan alamat *tunneling* ISATAP.

Pada *tunneling* ISATAP, hanya terdapat dua buah *routing* yang ditambahkan pada *router*. Pertama, *static route* untuk melewati seluruh jaringan IPv6 dengan cakupan IP (::/0) melalui alamat ISATAP pada *interface Tunnel0*. Dan kedua, *routing* RIP untuk merutekan alamat IPv4. Hal inilah yang membedakan *routing* pada *tunneling* 6to4 dengan *tunneling* ISATAP dimana pada *tunneling* 6to4 menggunakan tiga *routing* sedangkan *tunneling* ISATAP menggunakan dua *routing*.

Proses *routing* dari *server* ke *client* dijelaskan berikut ini. Ketika IP *server* (2001:0:0:A::2) masuk ke *router* 1 maka akan berkomunikasi dengan alamat *tunneling* ISATAP (2001:DB8:0:7:0:5EFE:C0A8:1). Didalam *interface Tunnel0*, alamat 2001:DB8:0:7:0:5EFE:C0A8:1 yang akan masuk ke network IPv4 diterjemahkan oleh proses *tunneling* sehingga didapatkan alamat IPv4 (192.168.0.1) yang merupakan alamat *interface Fa0/1*. Setelah diketahui jalur IP yang akan dilewati, *router* 1 akan mencari alamat IPv4 yang satu network sehingga bertemu dengan alamat IPv4 (192.168.0.2) yang merupakan alamat *interface Fa0/1* *router* 2. Alamat IPv4 ini akan diterjemahkan selama proses *tunneling* sehingga didapatkan alamat IP (2001:DB8:0:7:0:5EFE:C0A8:2) dan akhirnya akan bertemu dengan IP *client* (2001:0:0:B::2). Begitu pula untuk proses *routing* dari *client* ke *server*.

Apabila dilakukan *traceroute* dari *server* (2001:0:0:A::2) ke *client* (2001:0:0:B::2) ataupun sebaliknya dari *client* (2001:0:0:B::2) ke *server* (2001:0:0:A::2) maka akan didapatkan hasil seperti Gambar 4.15 berikut ini.

```

C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\AdiPrayitno>
C:\Documents and Settings\AdiPrayitno>
C:\Documents and Settings\AdiPrayitno>tracert 2001:0:0:b::2

Tracing route to 2001:0:0:b::2 over a maximum of 30 hops

  1  <1 ms    <1 ms    1 ms    2001:0:0:a::1
  2   4 ms     4 ms     4 ms    2001:db8:0:7:0:5efe:192.168.0.2
  3   4 ms     4 ms     4 ms    2001:0:0:b::2

Trace complete.

C:\Documents and Settings\AdiPrayitno>
C:\Documents and Settings\AdiPrayitno>
C:\Documents and Settings\AdiPrayitno>

C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Muamar>
C:\Documents and Settings\Muamar>
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   3 ms     3 ms     3 ms    2001:db8:0:7:0:5efe:192.168.0.1
  3   4 ms     4 ms     5 ms    2001:0:0:a::2

Trace complete.

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

```

Gambar 4.15 Hasil Traceroute Tunneling ISATAP

Dari hasil *traceroute* tersebut ditunjukkan bahwa *client* akan berbicara ke *server* melalui *router* 1 (2001:DB8:0:7:0:5EFE:C0A8:1) dan *router* 2 (2001:DB8:0:7:0:5EFE:C0A8:2) yang merupakan IP *Tunneling* ISATAP. Untuk konfigurasi selengkapnya dapat dilihat pada Lampiran 4.

#### 4.4 Analisa Pengaruh *Bit Rate* terhadap *Delay* dan *Packet Loss*

Nilai *bit rate* yang digunakan pada proses *encoding* dan *decoding* berpengaruh terhadap *delay* dan *packet loss* yang terjadi selama proses *streaming*. *Bit rate* merupakan jumlah informasi yang disimpan dalam satu satuan waktu dalam suatu *file*. [8] *Bit rate* sangat dipengaruhi oleh jenis *encoding* yang digunakan selama proses *streaming*. Pada skripsi ini hanya digunakan satu jenis *codec video* mp4v dan *codec audio* mpga. Hal ini dilakukan untuk menguji pengaruh besar *bit rate* terhadap *delay* dan *packet loss* yang terjadi selama proses *streaming*.

#### 4.4.1 Analisa Pengaruh *Bit Rate* terhadap *Packet Loss*

*Packet loss* merupakan satu atau lebih paket yang gagal melewati jaringan untuk mencapai tujuan. [10] Beberapa penyebab adanya *packet loss* yaitu *congestion*, penolakan oleh sistem karena *delay* yang terlalu lama, ataupun kesalahan pada jaringan itu sendiri. *Packet loss* diperoleh dengan menghitung paket yang berhasil dikirim oleh *server* dikurangi dengan paket yang berhasil diterima oleh *client*, seperti ditunjukkan pada Persamaan 2.2.

Dari pengujian yang dilakukan, ditunjukkan bahwa dengan melakukan perubahan *bit rate* video dan audio pada proses *encoding* dan *decoding file* video yang akan digunakan dalam proses *streaming* maka akan berpengaruh terhadap jumlah *packet loss* selama proses *streaming*.

Nilai *packet loss* yang ditunjukkan pada Tabel 4.1 berikut merupakan nilai rata-rata dari 10 kali pengambilan data untuk setiap konfigurasi jaringan, yang diambil dari data pada Lampiran 5, Lampiran 6, Lampiran 7 dan Lampiran 8.

**Tabel 4.1** Data *Packet Loss* untuk Setiap Konfigurasi Jaringan

Bit Rate	Packet Loss (Packet)			
	IPv4	IPv6	6to4	ISATAP
<b>Video=1024, Audio=192</b>	82.9	7.2	7.8	7.7
<b>Video=512, Audio=128</b>	30.6	6.5	8.8	8.1
<b>Video=256, Audio=64</b>	9	5.9	5.7	4

Persentase *packet loss* disisi *client* untuk setiap konfigurasi terhadap jumlah paket yang dikirimkan oleh *server* ditunjukkan pada Tabel 4.2 berikut ini.

**Tabel 4.2** Persentase *Packet Loss* untuk Setiap Konfigurasi Jaringan

Bit Rate	Persentase Packet Loss (%)			
	IPv4	IPv6	6to4	ISATAP
<b>Video=1024, Audio=192</b>	1.65	0.14	0.16	0.15
<b>Video=512, Audio=128</b>	0.64	0.14	0.18	0.16
<b>Video=256, Audio=64</b>	0.20	0.13	0.11	0.08

Untuk pengaturan *bit rate* 1024-192, konfigurasi IPv4 mempunyai persentase *packet loss* terbesar 1.65%, diikuti *tunneling* 6to4 0.16%, *tunneling* ISATAP

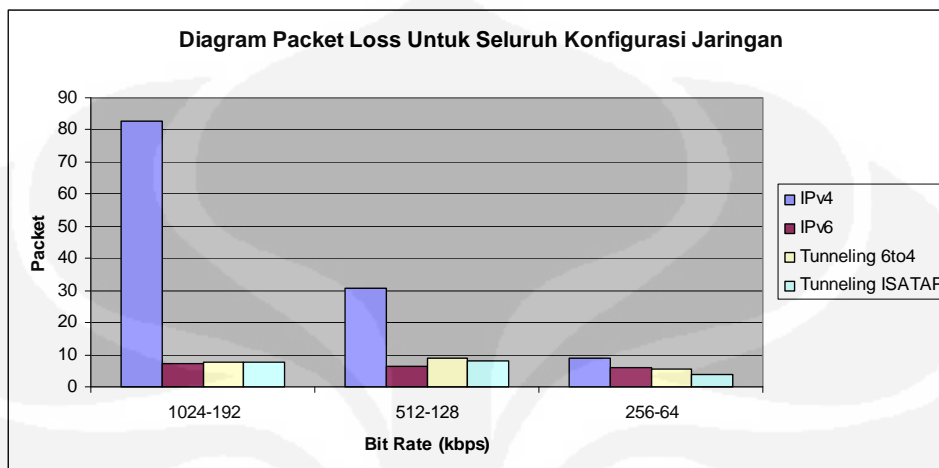
0.15%, dan IPv6 0.14%. Untuk pengaturan *bit rate* 512-128, konfigurasi IPv4 mempunyai persentase *packet loss* terbesar 0.64%, diikuti *tunneling* 6to4 0.18%, *tunneling* ISATAP 0.16%, dan IPv6 0.14%. Sedangkan untuk pengaturan *bit rate* 256-64, konfigurasi IPv4 mempunyai persentase *packet loss* terbesar 0.20%, diikuti IPv6 0.13%, *tunneling* 6to4 0.11% dan *tunneling* ISATAP 0.08%.

Seperti dijelaskan pada proses pengambilan data sebelumnya, aplikasi *video streaming* yang dijalankan pada setiap konfigurasi jaringan digunakan *protocol* UDP. Hal tersebut karena *protocol* UDP merupakan *connectionless transport protocol* dimana tidak mendukung pengiriman kembali paket apabila ada yang hilang, sehingga bisa diketahui jumlah paket yang hilang. Hal tersebut dilakukan untuk menghindari *delay* yang besar selama proses *streaming*. Dari data Tabel 4.3 diatas ditunjukkan bahwa untuk konfigurasi jaringan IPv4 mempunyai *packet loss* terbanyak bila dibanding dengan konfigurasi lainnya. Penyebab tingginya *packet loss* yang muncul dikarenakan format *header* IPv4 yang lebih kompleks bila dibandingkan dengan format *header* IPv6 yang lebih sederhana. Disamping itu, pada IPv4 tidak tersedianya *flow label field* seperti pada IPv6 yang mampu mengetahui aliran paket dari ujung ke ujung dan mengidentifikasi paket yang memerlukan lalu lintas *real-time* seperti *video streaming*.

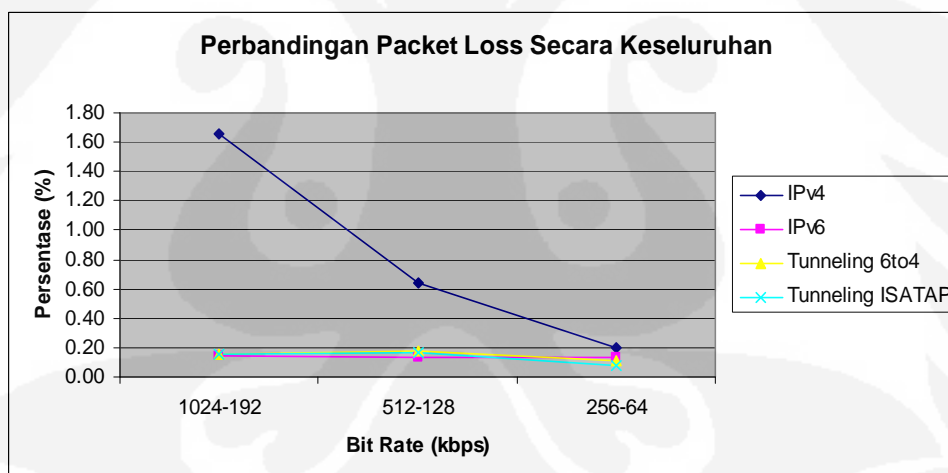
Konfigurasi *tunneling* 6to4 dan ISATAP mempunyai *packet loss* yang lebih kecil juga dibandingkan dengan IPv4 karena pada konfigurasi *tunneling* mempunyai dua segment alamat, yaitu IPv4 dan IPv6. Sehingga ada saatnya ketika paket-paket *real-time* masih dapat ditangani secara khusus oleh header IPv6 agar tidak banyak yang hilang.

Konfigurasi IPv6 mempunyai *packet loss* terkecil bila dibandingkan dengan ketiga konfigurasi yang lain. Akan terjadi penyimpangan ketika *bit rate* diatur pada nilai 256-64 dimana IPv6 mempunyai *packet loss* lebih besar dibandingkan dengan *tunneling* 6to4 dan ISATAP. Untuk *packet loss* *tunneling* 6to4 lebih besar dibanding dengan *tunneling* ISATAP karena selama proses *streaming* 6to4 melewati routing yang lebih banyak dibanding ISATAP sehingga kemungkinan kehilangan paket juga dapat terjadi.

Diagram perbandingan *bit rate* terhadap *packet loss* serta persentase *packet loss* untuk seluruh konfigurasi jaringan ditunjukkan pada Gambar 4.16 dan 4.17 berikut ini.

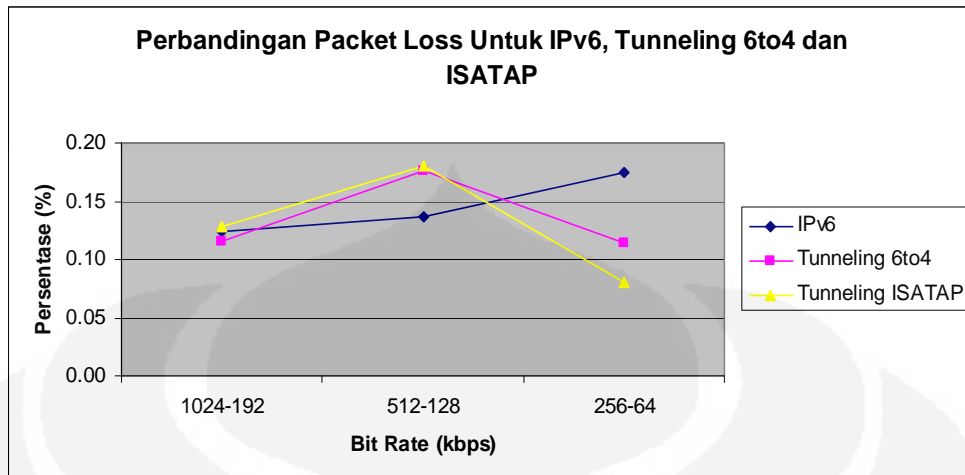


**Gambar 4.16** Diagram *Bit Rate* Terhadap *Packet Loss* untuk Seluruh Konfigurasi Jaringan



**Gambar 4.17** Grafik *Bit Rate* Terhadap *Packet Loss* untuk Seluruh Konfigurasi Jaringan

Karena grafik perbandingan *packet loss* untuk konfigurasi IPv6, *tunneling 6to4*, dan ISATAP memiliki nilai yang hampir sama sehingga pada grafik tidak terlihat perbedaannya, maka Gambar 4.18 berikut ini khusus membandingkan persentase *packet loss* untuk ketiga konfigurasi tersebut.



**Gambar 4.18** Grafik *Bit Rate* Terhadap *Packet Loss* untuk Konfigurasi IPv6, *Tunneling 6to4* dan ISATAP

#### 4.4.2 Analisa Pengaruh *Bit Rate* terhadap *Delay*

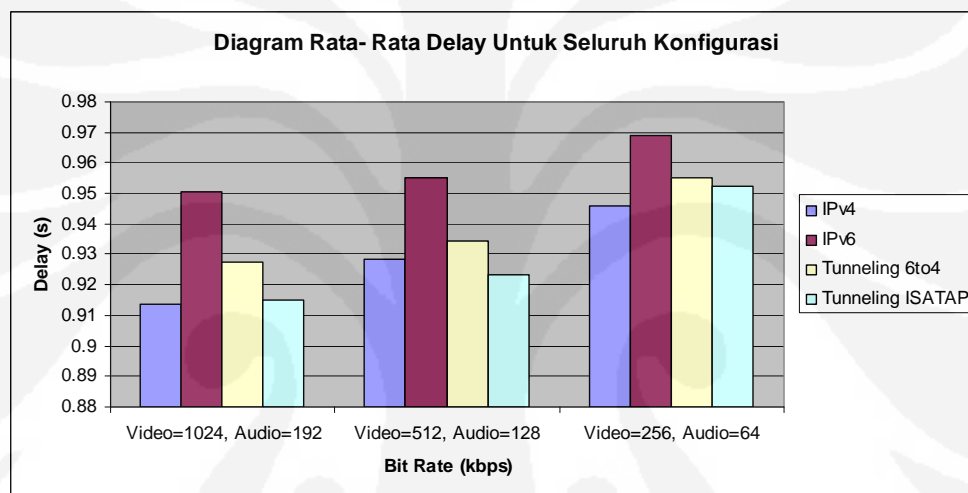
Yang dimaksud *delay* dalam hal ini adalah waktu tunda yang disebabkan oleh proses transmisi dari satu titik ke titik lain yang menjadi tujuannya. [9] Perhitungannya dapat dilakukan mengurangi selang waktu penerimaan keseluruhan paket dengan selang waktu pengiriman keseluruhan paket, seperti ditunjukkan pada Persamaan 2.1. Dalam proses *video streaming*, apabila data video menghabiskan terlalu banyak waktu pada saat berada di jaringan maka tidak dapat disebut sebagai *real-time*.

Dari skripsi yang dilakukan, ditunjukkan bahwa dengan melakukan perubahan *bit rate* video dan audio pada proses *encoding* dan *decoding file* video yang akan digunakan dalam proses *streaming* maka akan berpengaruh terhadap *delay* yang terjadi selama proses *streaming*, seperti ditunjukkan pada Tabel 4.3 berikut ini.

**Tabel 4.3** Data *Delay* untuk Setiap Konfigurasi Jaringan

Bit Rate (kbps)	Rata-Rata Delay (second)			
	IPv4	IPv6	6to4	ISATAP
Video=1024, Audio=192	0.9135	0.9503	0.9276	0.9149
Video=512, Audio=128	0.9286	0.955	0.9345	0.9232
Video=256, Audio=64	0.946	0.9689	0.9549	0.9523

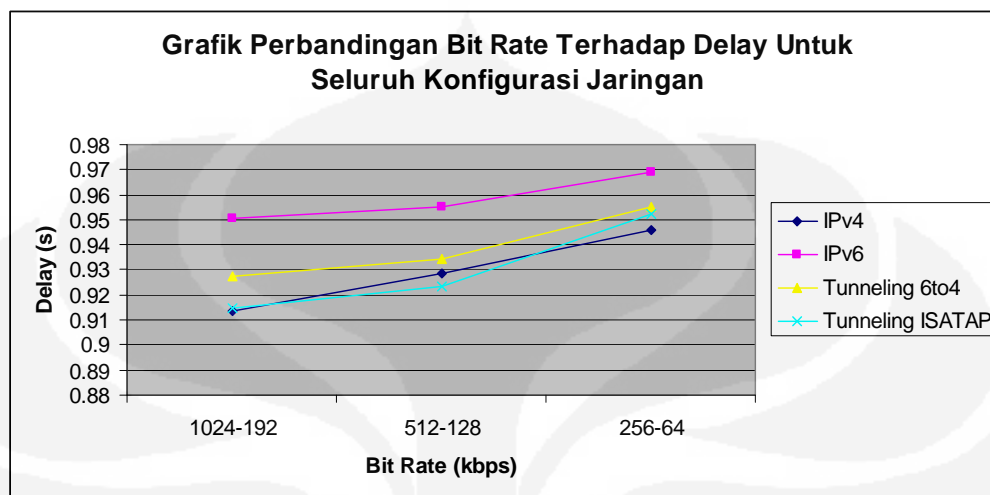
Nilai *delay* pada Tabel 4.1 diatas merupakan nilai rata-rata dari 10 kali pengambilan data untuk setiap konfigurasi jaringan, yang diambil dari data pada Lampiran 9, Lampiran 10, Lampiran 11 dan Lampiran 12. Dari data Tabel 4.3 diatas ditunjukkan bahwa untuk setiap konfigurasi jaringan, semakin kecil nilai *bit rate* yang digunakan untuk proses *encoding* dan *decoding* maka akan semakin besar *delay* yang dihasilkan selama proses *streaming*. Semakin besar nilai *bit rate* yang digunakan untuk proses *encoding* dan *decoding* maka akan semakin kecil *delay* yang dihasilkan. Diagram perbandingan *bit rate* terhadap *delay* untuk seluruh konfigurasi jaringan ditunjukkan pada Gambar 4.19 berikut ini.



**Gambar 4.19** Diagram *Bit Rate* Terhadap *Delay* untuk Seluruh Konfigurasi Jaringan

Untuk pengaturan *bit rate* 1024-192, *tunneling* 6to4 dan ISATAP mempunyai delay 1.54% lebih besar dan 0.15% lebih besar dibanding IPv4 serta 2.39% lebih kecil dan 1.37% lebih kecil dibanding IPv6. Untuk pengaturan *bit rate* 512-128, *tunneling* 6to4 dan ISATAP mempunyai delay 0.64% lebih besar dan 0.58 % lebih kecil dibanding IPv4 serta 2.15% lebih kecil dan 1.21% lebih kecil dibanding IPv6. Sedangkan untuk pengaturan *bit rate* 256-64, *tunneling* 6to4 dan ISATAP mempunyai delay 0.94% lebih besar dan 0.67% lebih besar dibanding IPv4 serta 1.44% lebih kecil dan 0.27% lebih kecil dibanding IPv6. Grafik perbandingan *delay* terhadap besarnya *bit rate* untuk konfigurasi IPv4,

IPv6, *tunneling* 6to4 dan *tunneling* ISATAP ditunjukkan seperti pada Gambar 4.20 berikut ini.



**Gambar 4.20** Grafik Perbandingan *Bit Rate* Terhadap *Delay* untuk Seluruh Konfigurasi Jaringan

IPv6 mempunyai *delay* yang lebih besar dibanding dengan IPv4 disebabkan IPv6 mempunyai *field* tambahan pada bagian *header* yaitu 20-bit *flow label* yang mampu mengetahui aliran paket dari ujung ke ujung dan dapat mencari paket yang memerlukan lalu lintas *real-time* serta memerlukan penanganan khusus. Dengan begitu, IPv6 mempunyai *delay* lebih lama karena akan mengidentifikasi terlebih dahulu paket-paket yang memerlukan lalu lintas *real-time* seperti *video streaming*. Untuk *tunneling* 6to4 dan ISATAP rata-rata mempunyai *delay* yang lebih kecil dibandingkan dengan IPv6 tetapi mempunyai *delay* yang lebih besar bila dibandingkan dengan IPv4.

*Delay* pada konfigurasi *tunneling* 6to4 lebih besar bila dibandingkan dengan konfigurasi *tunneling* ISATAP. Hal ini karena *tunneling* 6to4 menggunakan *routing* yang lebih panjang bila dibandingkan dengan *routing* pada *tunneling* ISATAP. Banyaknya *routing* akan sangat berpengaruh terhadap kinerja dari suatu jaringan karena paket yang dikirim akan mengalami proses yang lebih lama didalam jaringan.



#### 4.5 Analisa Perbandingan Kinerja Secara Keseluruhan

Secara keseluruhan, konfigurasi IPv6 mempunyai jumlah *packet loss* yang lebih kecil bila dibandingkan dengan IPv4, akan tetapi IPv6 mempunyai *delay* yang relatif lebih besar dibandingkan IPv4. Hal tersebut memang sebanding karena semakin sedikit paket yang hilang berarti waktu pengiriman paket semakin lama karena berhasil mengirimkan paket lebih banyak. Hal ini dikarenakan IPv6 mempunyai *field* tambahan yaitu 20-bit *flow label* pada bagian *header* yang mampu mengidentifikasi paket yang berada didalam jaringan, terutama paket-paket yang memerlukan lalu lintas *real-time* serta memerlukan penanganan khusus seperti *video streaming*.

Jika ditinjau dari hasil pengujian untuk kedua mekanisme *tunneling* 6to4 dan ISATAP, *tunneling* ISATAP mempunyai keunggulan baik dilihat dari sisi *delay* maupun *packet loss* yang ditimbulkan. Meskipun begitu kedua *tunneling* tersebut mempunyai ketangguhan yang hampir sama dengan IPv6 karena dilihat dari besarnya *delay* dan *packet loss* yang tidak jauh berbeda dengan *delay* dan *packet loss* yang dihasilkan pada IPv6. Oleh karena itu, kedua *tunneling* tersebut sudah cukup tangguh untuk diimplementasikan didalam suatu jaringan untuk proses transisi dari IPv4 ke IPv6.

Perubahan *bit rate* pada proses *encoding* dan *decoding file* video yang akan digunakan sebagai *video streaming* mempengaruhi besar kecilnya *delay* dan *packet loss* yang ditimbulkan selama proses *streaming*. Oleh karena itu, untuk mendapatkan hasil *video streaming* yang maksimal tanpa harus membebani trafik didalam jaringan maka perlu dilakukan pengecilan *bit rate* tersebut, terutama jika menggunakan VideoLAN *Client* sebagai media untuk melakukan *video streaming*. Dari hasil pengujian, ditunjukkan bahwa untuk pengaturan *bit rate* 256-64 mempunyai hasil yang paling maksimal. Apabila dilihat dari sisi *delay* dan *packet loss*, pada *video streaming* lebih diutamakan didapatkan jumlah *packet loss* yang kecil dengan *delay* yang besar daripada didapatkan jumlah *packet loss* yang besar dengan *delay* yang kecil. Karena pada saat menjalankan *video streaming*, lebih baik melihat gambar dari *video* dengan kualitas yang bagus walaupun dengan *delay* yang agak lama, dibandingkan dengan melihat gambar *video* yang rusak walaupun mempunyai *delay* yang lebih cepat.

Yang paling penting dan perlu diperhatikan adalah pengujian ini masih terbatas pada jaringan lokal (*test bed*) dimana hanya diberikan simulasi penambahan trafik pada jaringan dengan melakukan tes ping secara kontinyu dengan beban sebesar 64000 *bytes* baik dari *server* ke *client* maupun dari *client* ke *server*. Apabila diimplementasikan pada jaringan yang sesungguhnya maka ada kemungkinan hal-hal lain terjadi. Oleh karena itu, sangat penting untuk mengatur *bit rate* dari *file* video yang akan digunakan untuk *streaming* agar dapat memperoleh hasil yang maksimal, yaitu mendapatkan *delay* dan *packet loss* sekecil mungkin tanpa mengabaikan kualitas gambar dan suara dari *video streaming* tersebut.

## BAB 5

### KESIMPULAN

1. Konfigurasi IPv4 dengan pengaturan *bit rate* 1024-192 mempunyai persentase *packet loss* terbesar 1.65%, diikuti *tunneling* 6to4 0.16%, *tunneling* ISATAP 0.15%, dan IPv6 0.14%.
2. Untuk pengaturan *bit rate* 512-128, konfigurasi IPv4 mempunyai persentase *packet loss* terbesar 0.64%, diikuti *tunneling* 6to4 0.18%, *tunneling* ISATAP 0.16%, dan IPv6 0.14%.
3. Sedangkan untuk pengaturan *bit rate* 256-64, konfigurasi IPv4 mempunyai persentase *packet loss* terbesar 0.20%, diikuti IPv6 0.13%, *tunneling* 6to4 0.11% dan *tunneling* ISATAP 0.08%.
4. Konfigurasi *tunneling* 6to4 dan ISATAP dengan pengaturan *bit rate* 1024-192 mempunyai delay 1.54% lebih besar dan 0.15% lebih besar dibanding IPv4 serta 2.39% lebih kecil dan 1.37% lebih kecil dibanding IPv6.
5. Untuk pengaturan *bit rate* 512-128, *tunneling* 6to4 dan ISATAP mempunyai delay 0.64% lebih besar dan 0.58 % lebih kecil dibanding IPv4 serta 2.15% lebih kecil dan 1.21% lebih kecil dibanding IPv6.
6. Sedangkan untuk pengaturan *bit rate* 256-64, *tunneling* 6to4 dan ISATAP mempunyai delay 0.94% lebih besar dan 0.67% lebih besar dibanding IPv4 serta 1.44% lebih kecil dan 0.27% lebih kecil dibanding IPv6.
7. *Tunneling* ISATAP mempunyai keunggulan dibanding dengan *tunneling* 6to4 baik dilihat dari sisi *delay* maupun *packet loss* dimana *delay* pada ISATAP sebesar 0.9149-0.9523 detik dan 6to4 sebesar 0.9276-0.9549 detik, serta persentase *packet loss* pada ISATAP sebesar 0.08-0.16% dan 6to4 sebesar 0.11-0.18%.
8. Konfigurasi IPv6, *tunneling* 6to4, dan ISATAP secara umum mempunyai *delay* yang lebih besar dibanding dengan IPv4, akan tetapi mempunyai jumlah *packet loss* yang lebih kecil dibanding IPv4.
9. Pada *video streaming*, lebih diutamakan didapatkan jumlah *packet loss* yang kecil dengan *delay* yang besar daripada didapatkan jumlah *packet loss* yang besar dengan *delay* yang kecil.

## DAFTAR PUSTAKA

- [1]. Introduction to IP Version 6, Microsoft Corporation's, February 2008.
- [2]. IPv6 Transition Technologies, Microsoft Corporation's, January 2008.
- [3]. CISCO Networking Academy, "Network Fundamentals", CCNA Exploration 4.0 (CISCO SYSTEMS, Inc., 2007).
- [4]. Somad, Wahidi. "Interkoneksi IPv6 dan IPv4 dengan Mekanisme Automatic Tunneling", Ilmu komputer.com, 2003.
- [5]. Tremblay, Jean Francois. Lind, Mikael. "IPv6 Tunneling Techniques", Hexago Inc., September, 2006.
- [6]. Wikipedia, "Tunneling Protocol", Diakses 24 Maret 2009 dari Wikipedia.  
[http://en.wikipedia.org/wiki/Tunneling\\_protocol](http://en.wikipedia.org/wiki/Tunneling_protocol)
- [7]. Wikipedia, "6to4", Diakses 24 Maret 2009 dari Wikipedia.  
<http://en.wikipedia.org/wiki/6to4>
- [8]. Eko Arianto, Kristian. "Analisa Performansi Metode USOT Untuk Video Streaming", Institut Teknologi Telkom, November, 2008.
- [9]. Siwabessy, Yoan. "Analisis Performansi TCP Reno dan TCP Sack Dalam Mobile Ad Hoc Network (MANET) dengan Menggunakan Algoritma Routing DSDV", Institut Teknologi Telkom, November, 2008.
- [10]. Jirka Klaue. Berthold Rathke. Adam Wolisz, "Evalvid-A Framework for Video Transmission and Quality Evaluation", Proc. of the 13<sup>th</sup> International Conference On Modeling Techniques and Tools for Computer Performance, Urbana, Illinois, USA, September, 2003.
- [11]. Wikipedia, "Bit Rate", Diakses 10 Juni 2009 dari Wikipedia.  
[http://en.wikipedia.org/wiki/Bit\\_rate](http://en.wikipedia.org/wiki/Bit_rate)
- [12]. Wikipedia, "Frame Rate", Diakses 10 Juni 2009 dari Wikipedia.  
[http://en.wikipedia.org/wiki/Frame\\_rate](http://en.wikipedia.org/wiki/Frame_rate)

## LAMPIRAN

### Lampiran 1 : Konfigurasi Router IPv4 Murni

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

Current configuration : 754 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
```

```
=====
```

```
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 IPv6 Murni

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

Current configuration : 794 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
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

```

```

=====

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 Tunneling 6to4

```

C2600-ROUTER1#sh run
Building configuration...

Current configuration : 1126 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 ROUTER_2
ip address 192.168.0.1 255.255.255.252
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:C0A8:2:1::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

```

```

=====
C2600-ROUTER2#sh run
Building configuration...

Current configuration : 1104 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
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 Tunneling ISATAP

```
C2600-ROUTER1#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
```

```

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

```

=====

```

C2600-ROUTER2#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
  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 : Rata-Rata Packet Loss untuk Konfigurasi Jaringan IPv4

IPv4	Bit Rate (Video=256, Audio=64)			Bit Rate (Video=512, Audio=128)			Bit Rate (Video=1024, Audio=192)		
	Packet		Packet Loss	Packet		Packet Loss	Packet		Packet Loss
	Server	Client		Server	Client		Server	Client	
1	4530	4517	13	4747	4742	5	5011	5001	10
2	4530	4526	4	4747	4499	248	5011	5010	1
3	4530	4525	5	4747	4739	8	5011	5010	1
4	4530	4522	8	4747	4739	8	5011	4999	12
5	4530	4526	4	4747	4741	6	5011	4995	16
6	4530	4517	13	4747	4747	0	5011	4995	16
7	4530	4519	11	4747	4742	5	5011	4995	16
8	4530	4519	11	4747	4742	5	5011	4960	51
9	4530	4522	8	4747	4739	8	5011	4527	484
10	4530	4517	13	4747	4734	13	5011	4789	222
<b>Rata-Rata Packet Loss</b>			<b>9</b>			<b>30.6</b>			<b>82.9</b>

Lampiran 6 : Rata-Rata Packet Loss untuk Konfigurasi Jaringan IPv6

IPv6	Bit Rate (Video=256, Audio=64)			Bit Rate (Video=512, Audio=128)			Bit Rate (Video=1024, Audio=192)		
	Packet		Packet Loss	Packet		Packet Loss	Packet		Packet Loss
	Server	Client		Server	Client		Server	Client	
1	4530	4520	10	4747	4747	0	5011	5001	10
2	4530	4516	14	4747	4743	4	5011	5001	10
3	4530	4526	4	4747	4743	4	5011	4996	15
4	4530	4530	0	4747	4736	11	5011	5009	2
5	4530	4529	1	4747	4744	3	5011	5009	2
6	4530	4521	9	4747	4736	11	5011	5009	2
7	4530	4523	7	4747	4746	1	5011	5011	0
8	4530	4529	1	4747	4738	9	5011	4996	15
9	4530	4517	13	4747	4739	8	5011	5010	1
10	4530	4530	0	4747	4733	14	5011	4996	15
<b>Rata-Rata Packet Loss</b>			<b>5.9</b>			<b>6.5</b>			<b>7.2</b>



Lampiran 7 : Rata-Rata Packet Loss untuk Konfigurasi Jaringan Tunneling 6to4

6to4	Bit Rate (Video=256, Audio=64)			Bit Rate (Video=512, Audio=128)			Bit Rate (Video=1024, Audio=192)		
	Packet		Packet Loss	Packet		Packet Loss	Packet		Packet Loss
	Server	Client		Server	Client		Server	Client	
1	4530	4520	10	4747	4735	12	5011	5006	5
2	4530	4518	12	4747	4736	11	5011	5005	6
3	4530	4524	6	4747	4736	11	5011	5006	5
4	4530	4529	1	4747	4735	12	5011	5001	10
5	4530	4530	0	4747	4741	6	5011	5001	10
6	4530	4519	11	4747	4736	11	5011	5001	10
7	4530	4525	5	4747	4747	0	5011	5006	5
8	4530	4530	0	4747	4740	7	5011	5005	6
9	4530	4522	8	4747	4741	6	5011	4998	13
10	4530	4526	4	4747	4735	12	5011	5003	8
<b>Rata-Rata Packet Loss</b>			<b>5.7</b>			<b>8.8</b>			<b>7.8</b>

Lampiran 8 : Rata-Rata Packet Loss untuk Konfigurasi Jaringan Tunneling ISATAP

ISATAP	Bit Rate (Video=256, Audio=64)			Bit Rate (Video=512, Audio=128)			Bit Rate (Video=1024, Audio=192)		
	Packet		Packet Loss	Packet		Packet Loss	Packet		Packet Loss
	Server	Client		Server	Client		Server	Client	
1	4530	4530	0	4747	4742	5	5011	5010	1
2	4530	4529	1	4747	4746	1	5011	4999	12
3	4530	4526	4	4747	4742	5	5011	5011	0
4	4530	4528	2	4747	4735	12	5011	4998	13
5	4530	4529	1	4747	4735	12	5011	4999	12
6	4530	4530	0	4747	4736	11	5011	4998	13
7	4530	4519	11	4747	4735	12	5011	5011	0
8	4530	4521	9	4747	4736	11	5011	4998	13
9	4530	4520	10	4747	4736	11	5011	5011	0
10	4530	4528	2	4747	4746	1	5011	4998	13
<b>Rata-Rata Packet Loss</b>			<b>4</b>			<b>8.1</b>			<b>7.7</b>

Lampiran 9 : Rata-Rata Delay untuk Konfigurasi Jaringan IPv4

IPv4	Bit Rate (Video=1024, Audio=192)			Bit Rate (Video=512, Audio=128)			Bit Rate (Video=256, Audio=64)		
	Latency (second)	Delay (second)	Throughput (bytes/sec)	Latency (second)	Delay (second)	Throughput (bytes/sec)	Latency (second)	Delay (second)	Throughput (bytes/sec)
1	29.893	0.893	227192.13	29.947	0.947	215034.42	30.021	1.021	204916.362
2	30	1	226788.251	29.954	0.954	203964.316	29.943	0.943	205267.839
3	30.001	1.001	226776.196	29.905	0.905	215203.661	29.929	0.929	205318.215
4	29.872	0.872	227256.468	29.904	0.904	215210.363	29.985	0.985	205117.016
5	29.831	0.831	227384.849	29.925	0.925	215145.51	29.94	0.94	205228.351
6	29.832	0.832	227377.319	30.024	1.024	214706.218	29.841	0.841	205557.314
7	29.831	0.831	224300.715	29.935	0.935	215120.757	29.863	0.863	205500.602
8	29.976	0.976	224702.819	29.936	0.936	215114.109	30.023	1.023	204901.204
9	29.99	0.99	204992.963	29.904	0.904	215208.937	29.896	0.896	205409.336
10	29.909	0.909	217444.199	29.852	0.852	215355.92	30.019	1.019	204928.894
<b>Rata-Rata Delay</b>		<b>0.9135</b>			<b>0.9286</b>			<b>0.946</b>	
<b>Rata-Rata Throughput</b>			<b>223421.5909</b>			<b>214006.4211</b>			<b>205214.5133</b>

Lampiran 10 : Rata-Rata Delay untuk Konfigurasi Jaringan IPv6

IPv6	Bit Rate (Video=1024, Audio=192)			Bit Rate (Video=512, Audio=128)			Bit Rate (Video=256, Audio=64)		
	Latency (second)	Delay (second)	Throughput (bytes/sec)	Latency (second)	Delay (second)	Throughput (bytes/sec)	Latency (second)	Delay (second)	Throughput (bytes/sec)
1	29.892	0.892	232547.731	30.025	1.025	219763.285	30.02	1.02	210314.215
2	30.04	1.04	231867.641	29.946	0.946	220158.779	29.828	0.828	210444.89
3	29.881	0.881	232403.783	29.946	0.946	220157.948	29.928	0.928	210211.992
4	29.977	0.977	232263.81	29.875	0.875	220353.807	30.009	1.009	208898.95
5	29.977	0.977	232262.469	29.993	0.993	219859.221	29.964	0.964	210095.158
6	29.977	0.977	232264.725	29.967	0.967	217032.359	30.02	1.02	210279.836
7	30.027	1.027	231969.911	29.872	0.872	220371.776	29.907	0.907	210220.251
8	29.842	0.842	232703.93	29.996	0.996	219930.22	29.984	0.984	209956.244
9	30.001	1.001	232118.749	29.905	0.905	220272.91	30.009	1.009	210409.006
10	29.889	0.889	232708.202	30.025	1.025	220455.21	30.02	1.02	209750.403
<b>Rata-Rata Delay</b>		<b>0.9503</b>			<b>0.955</b>			<b>0.9689</b>	
<b>Rata-Rata Throughput</b>			<b>232311.0951</b>			<b>219835.5515</b>			<b>210058.0945</b>

Lampiran 11 : Rata-Rata Delay untuk Konfigurasi Jaringan Tunneling 6to4

6to4	Bit Rate (Video=1024, Audio=192)			Bit Rate (Video=512, Audio=128)			Bit Rate (Video=256, Audio=64)		
	Latency (second)	Delay (second)	Throughput (bytes/sec)	Latency (second)	Delay (second)	Throughput (bytes/sec)	Latency (second)	Delay (second)	Throughput (bytes/sec)
1	29.945	0.945	232368.987	29.864	0.864	220389.164	29.875	0.875	210301.781
2	29.953	0.953	232264.66	29.875	0.875	220351.145	29.902	0.902	210017.566
3	29.977	0.977	232218.147	30.042	1.042	220350.443	29.966	0.966	209847.084
4	29.894	0.894	232531.751	29.863	0.863	220391.371	30.03	1.03	209636.155
5	29.875	0.875	232175.689	29.926	0.926	220209.184	29.961	0.961	210166.537
6	29.91	0.91	231962.835	30.042	1.042	220353.704	30.03	1.03	210339.742
7	29.977	0.977	232079.819	30.042	1.042	219634.758	29.93	0.93	210150.926
8	29.96	0.96	232207.044	29.938	0.938	220077.901	30.02	1.02	209751.223
9	29.875	0.875	232543.623	29.893	0.893	220498.634	29.898	0.898	210231.816
10	29.91	0.91	232499.406	29.86	0.86	220416.621	29.937	0.937	210143.109
<b>Rata-Rata Delay</b>		<b>0.9276</b>			<b>0.9345</b>			<b>0.9549</b>	
<b>Rata-Rata Throughput</b>			<b>232285.1961</b>			<b>220267.2925</b>			<b>210058.5939</b>

Lampiran 12 : Rata-Rata Delay untuk Konfigurasi Jaringan Tunneling ISATAP

ISATAP	Bit Rate (Video=1024, Audio=192)			Bit Rate (Video=512, Audio=128)			Bit Rate (Video=256, Audio=64)		
	Latency (second)	Delay (second)	Throughput (bytes/sec)	Latency (second)	Delay (second)	Throughput (bytes/sec)	Latency (second)	Delay (second)	Throughput (bytes/sec)
1	29.875	0.875	232215.697	29.869	0.869	219561.697	29.863	0.863	210338.41
2	29.875	0.875	232543.645	29.887	0.887	220314.243	29.988	0.988	209926.575
3	30.027	1.027	231966.859	30.039	1.039	220172.342	29.891	0.891	210239.611
4	29.952	0.952	232533.029	29.867	0.867	220366.731	29.938	0.938	210142.191
5	29.941	0.941	232588.328	30.039	1.039	220476.443	29.964	0.964	209939.651
6	29.875	0.875	231966.559	29.875	0.875	220353.57	29.941	0.941	210116.824
7	29.863	0.863	232275.67	29.863	0.863	220394.921	29.863	0.863	210338.432
8	29.875	0.875	232601.268	29.875	0.875	220353.66	30.019	1.019	209754.17
9	29.863	0.863	231964.203	29.879	0.879	220326.137	29.988	0.988	209926.468
10	30.003	1.003	232621.045	30.039	1.039	219609.272	30.068	1.068	209418.745
<b>Rata-Rata Delay</b>		<b>0.9149</b>			<b>0.9232</b>			<b>0.9523</b>	
<b>Rata-Rata Throughput</b>			<b>232327.6303</b>			<b>220192.9016</b>			<b>210014.1077</b>