

**ANALISIS PERBANDINGAN PROTOKOL *POINT-TO-POINT TUNNELING PROTOCOL* VPN DENGAN
PROTOKOL *LAYER TWO TUNNELING PROTOCOL* VPN PADA
JARINGAN IPV6**

SKRIPSI

Diajukan Untuk Memenuhi Salah Satu Syarat Untuk Memperoleh
Gelar Sarjana Teknik Pada Fakultas Teknik
Universitas Islam Riau Pekanbaru



M.SYAHYUTI ABJAR
153510736

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS ISLAM RIAU
PEKANBARU
2020**

LEMBAR PENGESAHAN PEMBIMBING SKRIPSI

Nama : **M.SYAHYUTI ABJAR**
NPM : 153510736
Fakultas : Teknik
Program Studi : Teknik Informatika
Jenjang Pendidikan : Strata 1 (S1)
Judul Skripsi : Analisis Perbandingan Protokol *Point-to-Point Tunneling Protocol* VPN Dengan Protokol *Layer Two Tunneling Protocol* VPN Pada Jaringan IPV6

Format sistematika dan pembahasan materi pada masing-masing bab dan sub bab dalam skripsi ini, telah dipelajari dan dinilai relatif telah memenuhi ketentuan-ketentuan dan kriteria-kriteria dalam metode penelitian ilmiah. Oleh karena itu, skripsi ini dinilai layak serta dapat disetujui untuk disidangkan dalam ujian Komprehensif.

Pekanbaru, 20 November 2020

**Disetujui Oleh :
Dosen Pembimbing**

Apri Siswanto, S.Kom., M.Kom

Disahkan Oleh :

Dekan Fakultas Teknik	Ketua Prodi Teknik Informatika
<u>Dr. Eng. Muslim, ST., MT</u>	<u>Arbi Haza Nasution, ST., M.Cs., M.Kom</u>

**LEMBAR PENGESAHAN
TIM PENGUJI UJIAN SKRIPSI**

Nama : **M.SYAHYUTI ABJAR**
NPM : 153510736
Fakultas : Teknik
Program Studi : Teknik Informatika
Jenjang Pendidikan : Strata 1 (S1)
Judul Skripsi : Analisis Perbandingan Protokol *Point-to-Point Tunneling Protocol* VPN Dengan Protokol *Layer Two Tunneling Protocol* VPN Pada Jaringan IPV6

Skripsi ini secara keseluruhan dinilai telah memenuhi ketentuan-ketentuan dan kaidah-kaidah dalam penulisan penelitian ilmiah serta telah diuji dan dapat dipertahankan dihadapan tim penguji. Oleh karena itu, Tim Penguji Ujian Skripsi Fakultas Teknik Universitas Islam Riau menyatakan bahwa mahasiswa yang bersangkutan dinyatakan **Telah Lulus Mengikuti Ujian Komprehensif Pada Tanggal 20 November 2020** dan disetujui serta diterima untuk memenuhi salah satu syarat guna memperoleh gelar Sarjana Strata Satu Bidang Ilmu **Teknik Informatika**

Pekanbaru, 20 November 2020

Tim Penguji

1. Dr. Evizal Abdul Kadir, M.Eng Sebagai Tim Penguji I (.....)
2. Yudhi Arta, ST., M.Kom Sebagai Tim Penguji II (.....)

**Disetujui Oleh :
Dosen Pembimbing**

Apri Siswanto, S.Kom., M.Kom

Disahkan Oleh :

Dekan Fakultas Teknik

Ketua Prodi Teknik Informatika

Dr. Eng. Muslim, ST., MT

**Arbi Haza Nasution, ST., M.Cs.,
M.Kom**

LEMBAR IDENTITAS PENULIS

Nama : M.Syahyuti Abjar

NPM : 153510736

Tempat / Tanggal Lahir : Sungai Tohor / 26 Februari 1997

Alamat Orang Tua : Jalan Hibrida KM.00, Pulau burung
Kab.indragiri Hilir

Nama Orang Tua

Nama Ayah : Abdul Muil

Nama Ibu : Muriah

No Hp / Telp : 0822 8674 1546

Fakultas : Teknik

Program Studi : Teknik Informatika

Masuk Th. Ajaran : 2015

Keluar Th. Ajaran : 2020

Judul Penelitian : Analisis Perbandingan Protokol *Point-to-Point Tunneling Protocol* VPN Dengan Protokol *Layer Two Tunneling Protocol* VPN Pada Jaringan IPV6

Pekanbaru,20 November 2020

M.Syahyuti Abjar

LEMBAR PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan dibawah ini :

Nama : **M.SYAHYUTI ABJAR**

Nama / Tanggal Lahir : Sungai Tohor / 26 Februari 1997

Alamat : Jalan Lumba-lumba Gg.Melati No.6

Adalah mahasiswa Universitas Islam Riau yang terdaftar pada :

Fakultas : Teknik

Program Studi : Teknik Informatika

Jenjang Pendidikan : Strata-1 (S1)

Dengan ini menyatakan dengan sesungguhnya bahwa skripsi yang saya tulis adalah benar dan asli hasil dari penelitian yang telah saya lakukan dengan judul “Analisis Perbandingan Protokol *Point-to-Point Tunneling Protocol* VPN Dengan Protokol *Layer Two Tunneling Protocol* VPN Pada Jaringan IPV6”. Apabila dikemudian hari ada yang merasa dirugikan dan atau menuntut karena penelitian ini menggunakan sebagian hasil tulisan atau karya orang lain tanpa mencantumkan nama penulis yang bersangkutan atau terbukti karya ilmiah ini **Bukan** karya saya sendiri atau **Plagiat** hasil karya orang lain, maka saya bersedia menerima sanksi sesuai peraturan perundangan yang berlaku.

Demikian surat pernyataan ini saya buat dengan sesungguhnya untuk dapat digunakan sebagaimana mestinya .

Pekanbaru, 20 November 2020

M.Syahyuti Abjar

HALAMAN PERSEMBAHAN



Assalamu'alaikum Warahmatullahi Wabarakatu..

Alhamdulillah puji syukur penulis ucapkan kepada Allah SWT atas segala rahmat dan karunia-Nya yang telah diberikan kepada penulis sehingga dapat menyelesaikan tugas akhir dengan judul “**Analisis Perbandingan Protokol *Point-to-Point Tunneling Protocol* VPN Dengan Protokol *Layer Two Tunneling Protocol* VPN Pada Jaringan IPV6**”.

Skripsi ini disusun untuk memenuhi persyaratan mencapai derajat strata-1 (S1) di program studi Teknik Informatika Fakultas Teknik Universitas Islam Riau. Penulis menyadari bahwa tanpa bantuan dari pihak-pihak lain, usaha yang penulis lakukan dalam menyelesaikan skripsi ini tidak akan membuahkan hasil yang berarti. Dalam kesempatan ini penulis ucapkan terima kasih kepada :

1. Allah SWT, karena hanya dengan izin dan karunia-Nya maka skripsi ini dapat selesai tepat pada waktunya. Segala puji bagi Allah yang maha mengabulkan segala doa.
2. Terkhusus orang tua tercinta yakni ayahanda dan ibunda tercinta beserta keluarga besar yang tak henti-hentinya seelau mensupport penulis dan membantu dalam segi materi dan moril serta do'a-do'anya sehingga penulis dapat menyelesaikan penulisan skripsi ini.
3. Bapak Apri Siswanto, ST., M.Kom selaku Dosen Pembimbing atas

bimbingan serta support dan motivasi yang diberikan.

4. Segenap Dosen Teknik Informatika, Universitas Islam Riau yang telah memberikan ilmu, pendidikan, dan pengetahuan kepada penulis selama duduk dibangku kuliah.
5. Teman – teman angkatan kelas D 2015 Teknik Informatika Univerisitas Islam Riau yang selalu memberikan semangat dan motivasi.

Akhir kata penulis mohon maaf atas kekeliruan dan kesalahan yang terdapat dalam skripsi ini dan berharap semoga skripsi ini dapat memberikan manfaat bagi pembaca.

Pekanbaru, 20 November 2020

M.Syahyuti Abjar

KATA PENGANTAR



Assalamu'alaikum Warahmatullahi Wabarokatuh,

Dengan mengucapkan Alhamdulillah segala puji dan syukur penulis panjatkan atas kehadiran Allah SWT, karena berkat rahmat dan hidayah-Nya penyusunan skripsi yang berjudul “Analisis Perbandingan Protokol *Point-to-Point Tunneling Protocol* VPN Dengan Protokol *Layer Two Tunneling Protocol* VPN Pada Jaringan IPv6” Laporan skripsi ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana Teknik Program strata-1 di jurusan Teknik Informatika, Fakultas Teknik, Universitas Islam Riau.

Penulis menyadari dalam penyusunan skripsi ini tidak akan selesai tanpa bantuan dari berbagai pihak. Karena itu pada kesempatan ini Penulis ingin mengucapkan terimakasih kepada :

1. Bapak Dr.Muslim M.Eng selaku Dekan Fakultas Teknik dan selaku penasehat akademis yang telah ikhlas dan sabar memberikan bimbingan dan arahan di sela-sela kesibukan beliau.
2. Bapak Arbi Haza Nasution, M.IT. selaku ketua Program Studi Teknik Informatika, Universitas Islam Riau
3. Bapak Apri Siswanto, S.Kom., M.Kom. selaku Dosen pembimbing sekaligus Dosen pengampu yang selalu memberikan motivasi dan semangat kepada Penulis.

4. Bapak Dr.Evizal M.Eng selaku penguji yang telah ikhlas dan sabar memberikan bimbingan dan arahan disela-sela kesibukan beliau.
5. Bapak Yudhi Arta S.T., M.T. selaku penguji yang telah ikhlas dan sabar memberikan bimbingan dan arahan disela-sela kesibukan beliau.
6. Segenap Dosen Teknik Informatika, Universitas Islam Riau yang telah memberikan ilmu, pendidikan, dan pengetahuan kepada penulis selama duduk dibangku kuliah.
7. Kedua orang tua atas do'a, bimbingan, serta moril dan materil yang diberikan.
8. Teman – teman angkatan 2015 Teknik Informatika Universitas Islam Riau yang selalu memberikan semangat dan motivasi.

Penulis menyadari penulisan skripsi ini tidak luput dari berbagai kekurangan. Penulis mengharapkan saran dan kritik demi kesempurnaan dan perbaikannya sehingga laporan skripsi ini dapat memberikan manfaat bagi bidang pendidikan dan penerapan dilapangan serta bisa dikembangkan lebih lanjut.

Pekanbaru, 20 November 2020

M.Syahyuti Abjar

**ANALISIS PERBANDINGAN PROTOKOL *POINT-TO-POINT*
TUNNELING PROTOCOL VPN DENGAN PROTOKOL *LAYER TWO*
TUNNELING PROTOCOL VPN PADA JARINGAN IPV6**

M.SYAHYUTI ABJAR
Program Studi Teknik Informatika Fakultas Teknik
Universitas Islam Riau
Email : msyahyutiabjar@student.uir.ac.id

Abstrak

Semakin berkembangnya teknologi informasi sekarang ini, maka kebutuhan akan informasi semakin meningkat. Dimana setiap orang membutuhkan informasi dalam waktu yang cepat, singkat dan akurat. Maka dibutuhkan suatu sarana yang mendukung hal tersebut. Oleh karena itu VPN diciptakan untuk menyelesaikan permasalahan dalam jaringan yang tidak aman. VPN memiliki beberapa *tunneling* yang dapat digunakan, seperti *Point To Point Tunneling Protocol* (PPTP) dan *Layer Two Tunneling Protocol* (L2TP). Pada penelitian ini akan menganalisa dan membandingkan kinerja protokol PPTP VPN dan protokol L2TP VPN. *Tunneling* yang akan digunakan jaringan berbasis IPV6. Penelitian ini bertujuan untuk mengetahui kinerja antara kedua *tunneling protocol* yaitu PPTP dan L2TP juga untuk memberikan informasi kepada admin tentang hasil kinerja kedua *tunneling* yaitu PPTP dan L2TP. Adapun parameter yang digunakan yaitu : *Delay*, *Jitter*, *Throughput*, *Packet loss*. Berdasarkan hasil pengujian yang telah dilakukan memberikan kesimpulan bahwa pada IPV6 (*Internet Protocol Versi 6*), nilai QoS (*Quality Of Service*) yang didapatkan pada *tunnel* L2TP (*Layer Two Tunneling Protocol*) lebih unggul dibandingkan *tunnel* PPTP (*Point-to-Point Tunneling Protocol*). Yaitu pada sisi *delay* dan *jitter*.

Kata kunci: *Point to Point Tunneling Protocol* (PPTP) dan *Layer Two Tunneling Protocol* (L2TP).

Comparative Analysis Of Protocol Point-to-Point Tunneling Protocol VPN With Layer Two Tunneling Protocol VPN On IPV6 Networks

M.SYAHYUTI ABJAR

Department Of Informatics Engineering
Islamic University Of Riau

Email : msyahyutiabjar@student.uir.ac.id

Abstrack

The more information technology develops now, the information needs will increase. Where everyone needs information in a fast, short and accurate manner. So we need a means to support this. Therefore a VPN was created to solve problems in insecure networks. VPN has several tunneling that can be used, such as Point-to-Point Tunneling Protocol (PPTP) and Layer Twi Tunneling Protocol (L2TP). This research will analyze and compare the performance oh the PPTP VPN protocol and the L2TP VPN protocol. Tunneling that will be used by IPV6 based network. This study aims to see the performance between the two tunneling protocols, namely PPTP and L2TP as well as to provide information to the admin about the performance results of the two tunneling, namely PPTP and L2TP. The parameters used are: Delay, Jitter, Throughput, Packet loss. Based on the test results that have shown that in IPV6 (Internet Protocol Version 6), the Qos (Quality of Service) value obtained in the L2TP (Layer Two Tunneling Protocol) tunnel is superior to the PPTP (Point-to-Point Tunneling Protocol) tunnel. Namely on the delay and jitter side.

Keyword: *Point to Point Tunneling Protocol (PPTP) dan Layer Two Tunneling Protocol (L2TP).*

DAFTAR ISI

HALAMAN JUDUL

LEMBAR IDENTITAS PENULIS

LEMBAR PERNYATAAN BEBAS PLAGIARISME

HALAMAN PERSEMBAHAN

KATA PENGANTAR i

ABSTRAK iii

ABSTRACT iv

DAFTAR ISI v

DAFTAR GAMBAR ix

DAFTAR TABEL xii

DAFTAR LAMPIRAN xiii

BAB I PENDAHULUAN

1.1. Latar Belakang 1

1.2. Identifikasi Masalah 2

1.3. Batasan Masalah 3

1.4. Rumusan Masalah 3

1.5. Tujuan 4

1.6. Manfaat 4

BAB II LANDASAN TEORI

2.1. Tinjauan Pustaka 5

2.2. Dasar Teori 8

2.2.1. Jaringan Komputer 8

2.2.1.1. <i>Peer to Peer</i>	9
2.2.1.2. <i>Client – Server</i>	9
2.2.2. Topologi Jaringan	10
2.2.3. <i>Virtual Private Network (VPN)</i>	14
2.2.3.1. Cara Kerja Dan Penggunaan <i>Virtual Private Network (VPN)</i>	15
2.2.3.2. Kelebihan Dan Kekurangan <i>Virtual Private Network (VPN)</i>	16
2.2.4. <i>Point To Point Tunneling Protocol (PPTP)</i>	16
2.2.5. <i>Layer Two Tunneling Protocol (L2TP)</i>	17
2.2.6. <i>Transmissions Control Protocol/Internet Protocol (TCP/IP)</i>	18
2.2.7. Wireshark	19
 BAB III METODOLOGI PENELITIAN	
3.1. Metode Penelitian	21
3.1.1. Metode Penelitian Informatika	21
3.2. Alat dan bahan Penelitian Yang Digunakan	22
3.2.1. Alat Penelitian.....	22
3.2.1.1. Spesifikasi Perangkat Keras (<i>Hardware</i>).....	22
3.2.1.2. Spesifikasi Perangkat Lunak (<i>Software</i>).....	23
3.3. Teknik Pengumpulan Data	24
3.4. Jenis Data	26
3.5. Pengembangan dan Perancangan Sistem	26
3.5.1. Desain Topologi.....	26

3.6. Parameter Kerja.....	27
3.6.1. Kerangka Permodelan	29
3.7. Skenario Pengujian Qos	30

BAB IV HASIL DAN PEMBAHASAN

4.1. Hasil Penelitian	31
4.2. Pengaturan PPTP	31
4.3. Pengaturan L2TP	35
4.4. Pengujian PPTP	40
4.4.1. Pengujian IPV6.....	40
4.4.2. Pengujian IPV4.....	49
4.5. Pengujian L2TP	58
4.5.1. Pengujian IPV6	58
4.5.2. Pengujian IPV4	67
4.6. Hasil Dari Proses Transfer Data yang Terekam Di Wireshark..	77
4.7. Hasil Enkripsi Pada Wireshark	80
4.7.1. Pengujian Pada Jaringan PPTP VPN	81
4.7.2. Pengujian Pada Jaringan L2TP VPN	81
4.7.3. Hasil <i>Sniffing</i> Pada Metode PPTP.....	82
4.7.4. Hasil <i>Sniffing</i> Pada Metode L2TP.....	83
4.8. Tabel Perbandingan Hasil Pengujian PPTP dan L2TP	84
4.8.1. Tabel Perbandingan IPV6	84
4.8.2. Tabel Perbandingan IPV4	85

BAB V PENUTUP

5.1. Kesimpulan 87

5.2. Saran 88

DAFTAR PUSTAKA



Dokumen ini adalah Arsip Milik :
Perpustakaan Universitas Islam Riau

DAFTAR GAMBAR

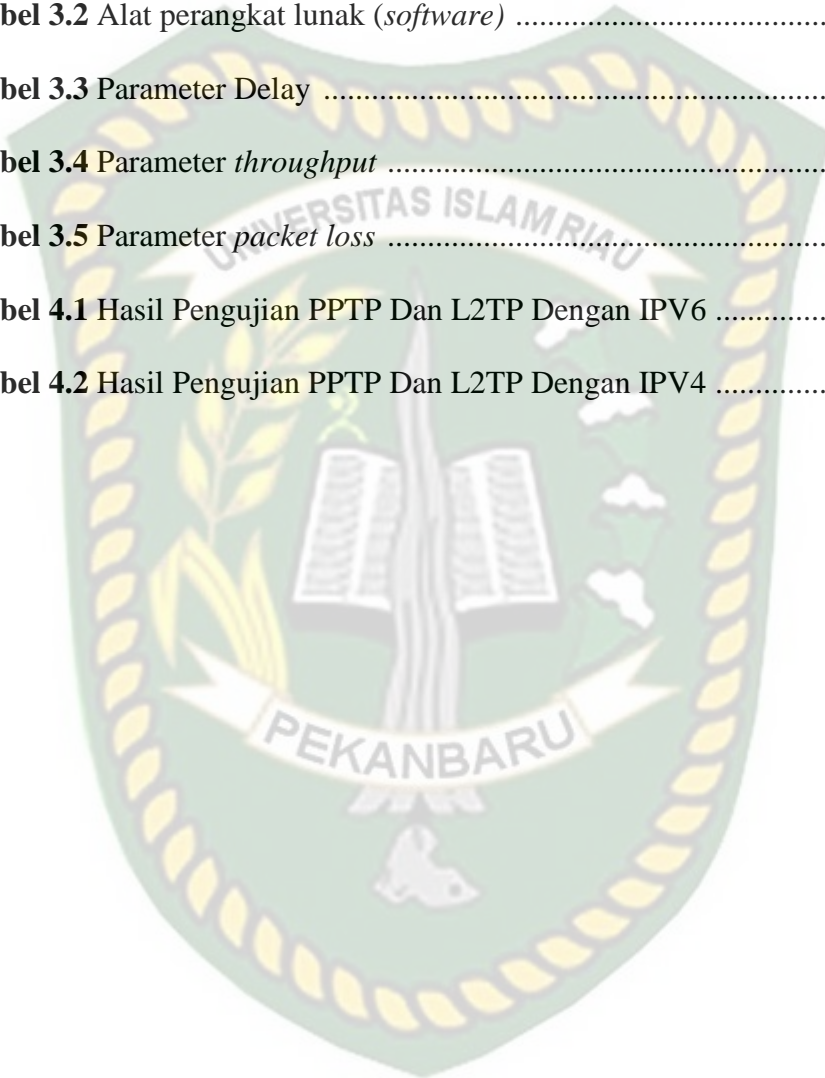
Gambar 2.1 Topologi Bus	13
Gambar 2.2 Topologi Star	13
Gambar 2.3 Topologi Ring	14
Gambar 3.1 Topologi Jaringan	26
Gambar 3.2 Skema Rancangan Penelitian	29
Gambar 4.1 Menu Login Winbox	32
Gambar 4.2 Menghidupkan PPTP Server	32
Gambar 4.3 IPV6 <i>address</i>	33
Gambar 4.4 IPV6 Route	34
Gambar 4.5 IPV6 <i>address client</i>	34
Gambar 4.6 IPV6 Route pada <i>client</i>	35
Gambar 4.7 Menu Login Winbox	36
Gambar 4.8 Menghidupkan L2TP Server	37
Gambar 4.9 IPV6 <i>address</i>	37
Gambar 4.10 IPV6 Route	38
Gambar 4.11 IPV6 <i>address client</i>	38
Gambar 4.12 IPV6 Route pada <i>client</i>	39
Gambar 4.13 Proses Pengujian Dengan Mendownload Data	40
Gambar 4.14 Hasil <i>Sniffing</i> setelah proses <i>download</i> selesai	40
Gambar 4.15 Hasil Pengujian IPV6 Audio dengan durasi 3 menit.....	41
Gambar 4.16 Hasil Pengujian IPV6 Audio dengan durasi 5 menit.....	42
Gambar 4.17 Grafik PPTP IPV6 Audio	43

Gambar 4.18	Hasil Pengujian IPV6 PPTP video dengan durasi 3 menit	44
Gambar 4.19	Hasil Pengujian IPV6 PPTP video dengan durasi 5 menit	45
Gambar 4.20	Grafik PPTP IPV6 Video	46
Gambar 4.21	Hasil Pengujian PPTP IPV6 File Durasi 3 Menit	47
Gambar 4.22	Hasil Pengujian PPTP IPV6 File Durasi 5 Menit	48
Gambar 4.23	Grafik PPTP IPV6 Video	49
Gambar 4.24	Hasil Pengujian IPV4 PPTP audio durasi 3 Menit	50
Gambar 4.25	Hasil Pengujian IPV4 PPTP audio durasi 5 menit	51
Gambar 4.26	Grafik IPV4 PPTP Audio	52
Gambar 4.27	Hasil Pengujian IPV4 PPTP video durasi 3 menit	53
Gambar 4.28	Hasil Pengujian IPV4 PPTP video durasi 5 menit	54
Gambar 4.29	Grafik IPV4 PPTP Video	55
Gambar 4.30	Hasil Pengujian IPV4 File durasi 3 menit	55
Gambar 4.31	Hasil Pengujian IPV4 File durasi 5 menit	57
Gambar 4.32	Grafik IPV4 PPTP File	58
Gambar 4.33	Hasil Pengujian IPV6 L2TP Audio durasi 3 menit	59
Gambar 4.34	Hasil Pengujian IPV6 L2TP audio durasi 5 menit	60
Gambar 4.35	Grafik IPV6 L2TP Audio	61
Gambar 4.36	Hasil Pengujian IPV6 L2TP video durasi 3 menit	62
Gambar 4.37	Hasil Pengujian IPV6 L2TP Video durasi 5 menit	63
Gambar 4.38	Grafik IPV6 L2TP Video	64
Gambar 4.39	Hasil Pengujian IPV6 L2TP File durasi 3 menit	65
Gambar 4.40	Hasil Pengujian IPV6 L2TP File durasi 5 menit	66

Gambar 4.41 Grafik IPV6 L2TP File	67
Gambar 4.42 Hasil Pengujian IPV4 L2TP Audio durasi 3 menit	68
Gambar 4.43 Hasil Pengujian IPV4 L2TP Audio durasi 5 menit	69
Gambar 4.44 Grafik IPV4 L2TP Audio	70
Gambar 4.45 Hasil Pengujian IPV4 L2TP video durasi 3 menit	70
Gambar 4.46 Hasil Pengujian IPV4 L2TP Video durasi 5 menit	71
Gambar 4.47 Grafik IPV4 L2TP Video	73
Gambar 4.48 Hasil Pengujian IPV4 L2TP File durasi 3 menit	73
Gambar 4.49 Hasil Pengujian IPV4 L2TP File durasi 5 menit	74
Gambar 4.50 Grafik IPV4 L2TP File	76
Gambar 4.51 Hasil dari Paket Transfer Audio PPTP.....	77
Gambar 4.52 Hasil dari Paket Transfer Video PPTP.....	78
Gambar 4.53 Hasil dari Paket Transfer File PPTP.....	78
Gambar 4.54 Hasil dari Paket Transfer Audio L2TP.....	79
Gambar 4.55 Hasil dari Paket Transfer Video L2TP.....	79
Gambar 4.56 Hasil dari Paket Transfer File L2TP.....	80
Gambar 4.57 Enkripsi Data Pada PPTP VPN.....	81
Gambar 4.58 Enkripsi Data Pada L2TP.....	82
Gambar 4.59 Hasil Pengujian Pada Metode PPTP.....	83
Gambar 4.60 Hasil Pengujian Pada Metode L2TP.....	84

DAFTAR TABEL

Tabel 3.1 Alat perangkat keras (<i>hardware</i>)	22
Tabel 3.2 Alat perangkat lunak (<i>software</i>)	23
Tabel 3.3 Parameter Delay	27
Tabel 3.4 Parameter <i>throughput</i>	27
Tabel 3.5 Parameter <i>packet loss</i>	28
Tabel 4.1 Hasil Pengujian PPTP Dan L2TP Dengan IPV6	82
Tabel 4.2 Hasil Pengujian PPTP Dan L2TP Dengan IPV4	82



DAFTAR LAMPIRAN

Lampiran 1. Konfigurasi PPTP	31
Lampiran 2. Konfigurasi L2TP	35



BAB I

PENDAHULUAN

1.1 Latar Belakang

Semakin berkembangnya teknologi informasi sekarang ini, maka kebutuhan akan informasi semakin meningkat. Dimana setiap orang membutuhkan informasi dalam waktu yang cepat, singkat dan akurat. Oleh karena itu, dibutuhkan suatu sarana yang dapat mendukung hal tersebut. Salah satunya adalah koneksi internet yang cepat dan stabil. Namun permasalahan yang sering timbul adalah faktor keamanan yang saat ini menjadi hal yang sangat penting untuk diperhatikan. Maka dibutuhkan suatu cara agar dapat memperoleh suatu informasi data, tukar menukar data, dilakukan dengan aman dan stabil. Oleh karena itulah VPN diciptakan untuk menyelesaikan permasalahan dalam jaringan yang tidak aman.

Keuntungan VPN adalah penggunaan jaringan publik dengan hak dan pengaturan yang sama seperti menggunakan jaringan lokal. VPN memiliki beberapa *tunneling* yang dapat digunakan, diantaranya *Point to Point Tunneling Protocol* (PPTP) dan *Layer Two Tunneling Protocol* (L2TP). *Point to Point Tunneling Protocol* (PPTP) merupakan protokol jaringan yang mengubah paket PPP menjadi IP datagram agar dapat ditransmisikan melalui internet. PPTP juga dapat digunakan pada jaringan private LAN-to-LAN. Sedangkan *Layer Two Tunneling Protocol* (L2TP) adalah protokol tunneling yang memadukan dua buah protokol tunneling, yaitu L2F (Layer 2 Forwarding) milik Cisco dan PPTP milik Microsoft.

Pada penelitian ini akan menganalisa dan membandingkan kinerja protokol PPTP VPN dan protokol L2TP VPN. *Tunneling* yang akan digunakan menggunakan jaringan berbasis IPV6. Proses penelitian dimulai dengan merancang jaringan untuk menentukan topologi yang akan digunakan nantinya. Tahap berikutnya membuat skenario yang akan diterapkan pada *tunneling* PPTP dan L2TP. Kemudian *tools* yang akan digunakan untuk menganalisa performa *Quality Of Service* (QOS) nya ialah dengan menggunakan wireshark.

Penelitian ini juga akan menggunakan mikrotik yang dapat digunakan sebagai media untuk membangun sebuah akses VPN. Dengan adanya mikrotik, informasi dapat diteruskan ke alamat-alamat yang saling berjauhan dan berada di jaringan komputer yang berbeda. Kemudian, mikrotik juga berguna untuk meneruskan paket data dari suatu LAN ke LAN lainnya. Oleh karena itu, dibuatlah sebuah penelitian untuk membandingkan *tunneling* manakah yang paling bagus kinerjanya berdasarkan kecepatan proses routing saat melakukan pengiriman data, dengan penelitian yang berjudul “**Analisis Perbandingan Protokol Point To Point Tunneling Protocol VPN Dengan Protokol Layer Two Tunneling Protocol VPN Pada Jaringan IPV6**”.

1.2 Identifikasi Masalah

Berdasarkan latar belakang diatas, identifikasi masalah yang didapat yaitu, menguji penerapan *tunneling* PPTP dan L2TP dengan menggunakan IPV4 dan IPV6.

1.3 Batasan Masalah

Peneliti membatasi masalah ini diantaranya:

1. *Tunneling protocol* yang digunakan adalah *Point-to-Point Tunneling Protocol* (PPTP) dan *Layer Two Tunneling Protocol* (L2TP).
2. Hanya membahas mengenai performa *tunneling protocol* saat menggunakan PPTP dan L2TP dengan parameternya meliputi *delay*, *throughput*, *packet loss*, dan *jitter*.
3. Merancang jaringan untuk menentukan topologi yang akan digunakan
4. *Tools* yang akan digunakan untuk menganalisa parameter *Quality Of Service* (QOS) nya yaitu wireshark.

1.4 Rumusan Masalah

Berdasarkan latar belakang masalah diatas, rumusan masalah yang akan dijawab yaitu:

1. Bagaimana menentukan kelebihan dan kekurangan *tunneling* PPTP dan L2TP dalam melakukan pertukaran data ?
2. Bagaimana cara mengukur QOS (*delay*, *throughput*, *jitter*, *packet loss*) dari kedua *tunneling* tersebut ?
3. Bagaimana cara membuat perancangan topologi jaringan komputer dengan adanya *tunneling* PPTP dan L2TP ?

1.5 Tujuan

Tujuan pembuatan sistem ini yaitu:

1. Mengetahui kinerja antara kedua *tunneling protocol* yaitu PPTP dan L2TP setelah dilakukan pengujian dan mendapatkan hasil QOS (*Quality of service*) seperti *jitter, troughput, packet loss dan delay*.
2. Memberikan informasi kepada admin tentang hasil kinerja kedua *tunneling* yaitu PPTP dan L2TP.

1.6 Manfaat

Penulis memiliki beberapa manfaat antara lain:

1. Memberikan informasi kepada admin tentang hasil kinerja kedua *tunneling* yaitu PPTP dan L2TP.
2. Mengetahui performa *tunneling protocol* PPTP dan L2TP dalam implementasi pada mikrotik.

BAB II

LANDASAN TEORI

2.1 Tinjauan Pustaka

Dalam penelitian yang dilakukan oleh Henki Bayu Seta, Muhammad Ridwan, Theresia Wati (2015) tentang Perbandingan *Virtual Private Network* (VPN) Protokol Menggunakan *Point To Point Tunnel Protocol* (PPTP) dan *Open VPN*. Penelitian ini akan menjawab mengenai VPN dengan protokol apa yang mampu memberikan fitur keamanan dan kestabilan yang baik serta kebutuhan *user* seperti apa yang dapat dipenuhi oleh open VPN maupun PPTP. Penelitian ini menggunakan Mikrotik Router OS bertujuan untuk membandingkan VPN dengan menggunakan protokol PPTP dan Open VPN untuk melihat protokol mana yang lebih unggul dari segi keamanan dan *throughput* yang dihasilkan untuk digunakan sesuai dengan kebutuhan *user*. Sebelum mengimplementasikan VPN yang harus dilakukan adalah mempelajari dan melakukan analisis protokol Open VPN dan PPTP agar dapat menjadi bahan pertimbangan dalam melakukan perancangan VPN.

Kemudian menurut Joko Triyono, Rr.Yuliana Rachmawati K., Fahmi Dhimas Irnawan (2014) dalam penelitiannya tentang Analisis Perbandingan Kinerja Jaringan *Virtual Private Network* (VPN) Berbasis Mikrotik Menggunakan Protokol *Point-to-Point Tunneling Protocol* (PPTP) Dan *Layer Two Tunneling Protocol* (L2TP) Sebagai Media transfer Data. Teknologi *private network* (jaringan pribadi) adalah suatu komunikasi dalam jaringan sendiri yang terpisah dari jaringan umum. *Private network* sendiri dianggap lebih efisien karena

kecepatan transfer data yang lebih besar dari pada kecepatan transfer data pada jaringan Internet, selain itu masalah keamanan dianggap lebih bagus karena hanya bergerak dalam lingkup terbatas saja. Secara umum, VPN adalah sebuah proses dimana jaringan umum (*public network* atau *internet*) diamankan kemudian difungsikan menjadi sebuah jaringan privat (*private network*). Sebuah VPN tidak didefinisikan oleh rangkaian khusus atau router, tetapi didefinisikan oleh mekanisme keamanan dan prosedur-prosedur yang hanya mengizinkan penggunaanya yang ditunjuk akses ke VPN dan informasi yang mengalir melaluinya. Permasalahan yang dihadapi saat ini yang berada dalam 1 area berhubungan dan berkomunikasi dengan menggunakan *flashdisk* dan disket, juga menggunakan *sharing file* bagi yang sudah memiliki *Local Area Network* (LAN) sendiri. Sementara untuk berhubungan dengan antara kantor dan antar kantor menggunakan internet dan email untuk mengirim data dan berkomunikasi. Sehingga dibutuhkan jaringan privat untuk mempermudah akses file terhadap suatu tempat yang berbeda lokasi.

Analisis Jaringan *Virtual Private Network* (VPN) Menggunakan *Point-to-Point Tunneling Protocol* (PPTP) dan *Layer Two Tunneling Protocol* (L2TP), Dinas Perhubungan, Komunikasi dan Informasi (Dinhubkominfo) Kabupaten Banyumas yang diteliti oleh Syariful Ikhwan, Ahya Amalina (2017). Merupakan salah satu instansi pemerintahan yang telah menerapkan teknologi VPN menggunakan *tunneling* PPTP. Penerapan VPN di Dinhubkominfo bertujuan untuk melakukan pertukaran data yang aman antar Satuan Kerja Perangkat Daerah (SKPD) di Kabupaten Banyumas. Satuan Kerja Perangkat Daerah (SKPD) adalah

perangkat pemerintah daerah (Provinsi maupun Kabupaten/Kota) seperti Dinas, Badan, Kecamatan dan Kelurahan. Data yang digunakan pada proses VPN berupa data *text* pada *server* keuangan, *server* absensi, *server File Transfer Protocol* (FTP), dan *server Hyper Text Transfer Protocol* (HTTP). Data–data yang terdapat pada Dinhubkominfo ini merupakan data penting yang harus diamankan, khususnya data keuangan. Berdasarkan informasi dari pihak Dinhubkominfo bahwa keamanan *tunneling* PPTP mengalami kelemahan karena hanya menggunakan autentifikasi saja. Sehingga pihak Dinhubkominfo berencana untuk melakukan perubahan *tunneling* dengan menggunakan *tunneling* L2TP yang memiliki keamanan lebih baik dibandingkan PPTP. Namun perubahan *tunneling* ini perlu dilakukan pengujian karena dikhawatirkan akan mengganggu performansi jaringan tersebut pada saat melakukan pertukaran data.

Lalu didalam penelitian yang telah dilakukan oleh Syarif Hidayatullah, syafrudin (2019) tentang Perancangan *Wide Area Network* (WAN) Dengan Teknologi *Virtual Private Network* (VPN). Dengan dikembangkannya jaringan VPN yang teraplikasi pada jaringan WAN proses pengaksesan data dapat dilakukan dimana saja selama terkoneksi dengan internet, sehingga memungkinkan komunikasi data jarak jauh yang relevan. Karena memiliki manfaat yang sangat baik, kemudian dikembangkan berbagai jenis VPN seperti *Point-to-Point Protocol* (PPP), *winsock*, *Internet Protocol Security* (IPSec) dan *Open VPN* (Khasanah, 2014).

Kemudian Maryanto, Maisyaroh, Budi Santoso (2018) meneliti tentang Metode *Internet Protocol Security* (IPSec) Dengan *Virtual Private Network*

(VPN) Untuk Komunikasi Data. Dalam implementasinya, VPN terbagi menjadi remote access VPN dan site-to-site VPN. Site-to-site VPN digunakan untuk menghubungkan antara dua tempat yang letaknya saling berjauhan, seperti kantor pusat dengan kantor cabang. Remote access jenis VPN ini digunakan oleh pegawai perusahaan yang ingin terhubung ke jaringan lokal perusahaannya dari berbagai lokasi yang jauh. [Basri et al., 2017]. Sedangkan kesimpulannya, VPN adalah hubungan antara jaringan komputer yang satu dengan jaringan komputer yang lain secara privat melalui jaringan internet. VPN juga dapat diartikan sebagai *virtual network* atau *private network* yang berarti jaringan yang menggunakan internet sebagai perantara antar jaringan yang bersifat *private*, karena hanya orang tertentu yang dapat mengakses jaringan tersebut. Jika menggunakan VPN, maka orang tersebut akan merasa lebih aman dengan jalur lalu lintas data yang dilaluinya, karena dengan menggunakan VPN otomatis hanya orang-orang tertentu saja yang dapat mengaksesnya. VPN biasanya digunakan dalam hal-hal yang bersifat rahasia, misalkan data perusahaan, data-data user lainnya. Komunikasi data yang lewat akan diencapsulation (dibungkus) dan dienkripsi (*encrypt*), supaya data tersebut terjamin kerahasiaannya.

2.2 Dasar Teori

2.2.1 Jaringan Komputer

Menurut Melwin Syafrizal (2005), dalam bukunya “Pengantar Jaringan Komputer”, jaringan komputer adalah himpunan “interkoneksi” antara 2 komputer *autonomous* atau lebih yang terhubung dengan media transmisi kabel atau tanpa kabel (*wireless*). Bila sebuah komputer dapat membuat komputer lainnya restart, shutdown, atau melakukan control lainnya, maka komputer-

komputer tersebut bukan *autonomous* (tidak melakukan kontrol terhadap komputer lain dengan akses penuh). Didalam jaringan komputer dikenal sistem koneksi antarmode (komputer), yakni:

2.2.1.1 Peer to Peer

Peer artinya rekan sekerja. Peer-to-peer network adalah jaringan komputer yang terdiri dari beberapa komputer (biasanya tidak lebih dari 10 komputer dengan 1-2 printer). Untuk penggunaan khusus, seperti laboratorium komputer, riset, dan beberapa hal lain, maka model peer to peer ini bisa saja dikembangkan untuk koneksi lebih dari 10 hingga 100 komputer. Peer to peer adalah suatu model dimana tiap *Personal Computer* (PC) dapat memakai resource pada *Personal Computer* (PC) lain atau memberikan resourcenya untuk dipakai *Personal Computer* (PC) lain. Dengan kata lain dapat berfungsi sebagai client maupun server pada periode yang sama. Metode peer to peer ini pada sistem Windows dikenal sebagai Workgroup, dimana tiap-tiap komputer dalam satu jaringan dikelompokkan dalam satu kelompok kerja.

2.2.1.2 Client – Server

Selain pada jaringan local, sistem ini bisa juga diterapkan dengan teknologi internet dimana ada suatu unit komputer yang berfungsi sebagai server yang hanya memberikan layanan bagi komputer lain, dan client yang juga hanya meminta layanan dari server. Akses dilakukan secara transparan dari client dengan melakukan login terlebih dahulu ke server yang dituju. Client hanya bisa menggunakan resource yang disediakan server sesuai dengan otoritas yang diberikan oleh administrator. Aplikasi yang dijalankan pada sisi client bisa saja merupakan resource yang tersedia di server atau aplikasi yang di install di sisi

client namun hanya bisa dijalankan setelah terkoneksi ke server. Jenis layanan Client-Server antara lain:

1. **File server** : Memberikan layanan fungsi pengelolaan file.
2. **Print Server** : Memberikan layanan fungsi pencetakan.
3. **Database Server** : Proses- proses fungsional mengenai database dijalankan pada mesin ini dan stasiun lain dapat minta pelayanan.
4. **Document Information Processing (DIP)**: Memberikan pelayanan fungsi penyimpanan, manajemen, dan pengambilan data.

2.2.2 Topologi Jaringan

Topologi Jaringan Komputer adalah metode atau cara yang digunakan agar dapat menghubungkan satu komputer dengan komputer lainnya. Struktur atau jaringan yang digunakan untuk menghubungkan satu komputer dengan komputer lainnya bisa dengan menggunakan kabel ataupun nirkabel (tanpa kabel). Pada pelaksanaannya, ada beberapa macam topologi jaringan komputer yang digunakan sesuai dengan skala jaringan, tujuan, biaya, dan penggunaannya. Beberapa macam topologi jaringan tersebut adalah topologi ring, topologi bus, topologi star, topologi mesh, dan topologi tree. dll yang akan kita bahas satu satu beserta kerugian dan keuntungannya. Pengertian topologi jaringan menurut para ahli sebagai berikut:

a. Zymon Machajewski

Pengertian topologi jaringan komputer menurut Zymon Machajewski (2007) adalah seperangkat komputer yang saling terhubung secara bersamaan satu dengan lainnya dengan tujuan utama, yakni untuk saling berbagi sumberdaya.

Internet adalah salah satu sumberdaya yang saat ini banyak digunakan di dalam suatu jaringan komputer.

b. Jafar Noor Yudianto

Pengertian topologi jaringan komputer menurut Jafar Noor Yudianto (2007) adalah suatu sistem yang terdiri atas sebuah beberapa komputer yang didesain untuk bisa saling berbagi sumber daya (printer, CPU), berkomunikasi (surel, pesan instan), dan bisa mengakses informasi (peramban web).

c. Umi Probeykti

Pengertian topologi jaringan komputer menurut Umi Probeykti (2007) adalah suatu sekumpulan komputer yang terpisah-pisah akan tetapi saling berhubungan dalam melakukan tugasnya. Contoh, dua buah komputer dapat dikatakan terhubung jika keduanya bisa saling bertukar informasi. Bentuk koneksi tersebut bisa melalui: kawat tembaga, fiber optik, gelombang mikro, satelit komunikasi.

d. Abdul Kadil

Definisi topologi jaringan komputer menurut Abdul Kadil (2014) adalah suatu hubungan dua buah simpul (umumnya berupa komputer) atau lebih yang tujuan utamanya yaitu untuk melakukan pertukaran data.

e. Izaas El Said

Definisi topologi jaringan komputer menurut Izaas El Said (2014) adalah sebuah sistem dimana terdapat beberapa komputer yang saling terhubung, agar bisa saling berbagi informasi dan juga sumber daya yang dimilikinya.

f. Budhi Irawan

Pengertian topologi jaringan komputer menurut menurut Budhi Irawan (2005) adalah suatu sistem yang terdiri atas komputer dan perangkat jaringan lainnya yang saling bekerja sama untuk mencapai suatu tujuan yang sama.

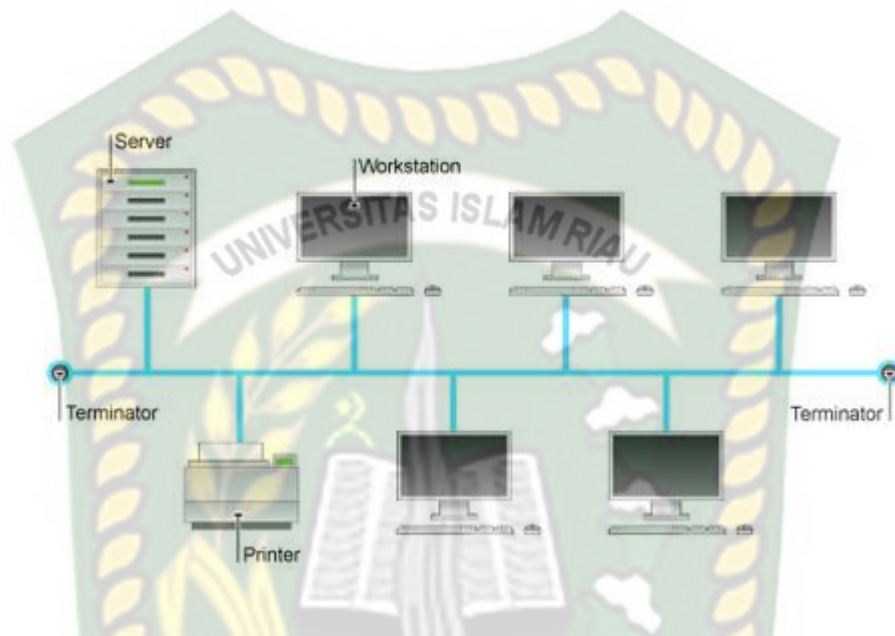
g. Kristanto

Pengertian topologi jaringan komputer menurut Kristanto (2003) adalah sekelompok komputer otonom yang saling terhubung satu sama lain, dengan memakai satu protokol komunikasi sehingga semua komputer yang saling terhubung tersebut bisa berbagi informasi, program, sumber daya dan juga bisa saling menggunakan perangkat keras lainnya secara bersamaan, misalnya printer, harddisk, lain-lain. Berikut jenis-jenis topologi jaringan adalah sebagai berikut:

1. Topologi Bus

Topologi bus adalah topologi yang cukup sederhana jika dibandingkan dengan topologi lainnya. Topologi bus umumnya digunakan pada instalasi jaringan berbasis fiber optic, selanjutnya digabungkan dengan topologi star/topologi bintang untuk menghubungkan client atau node. Topologi bus hanya

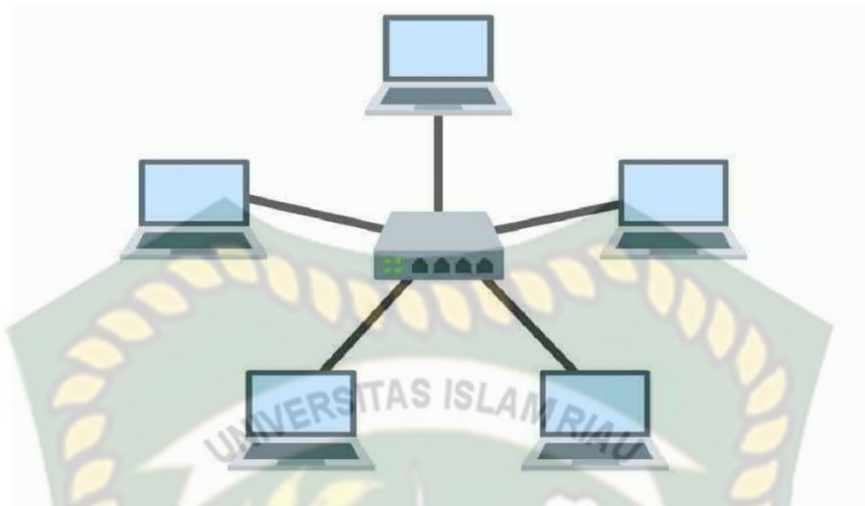
menggunakan satu kabel type coaxial di sepanjang node client. Biasanya, ujung kabel coaxial tersebut diberikan T konektor yang merupakan kabel end to end.



Gambar 2.1 Topologi Bus

2. Topologi Star

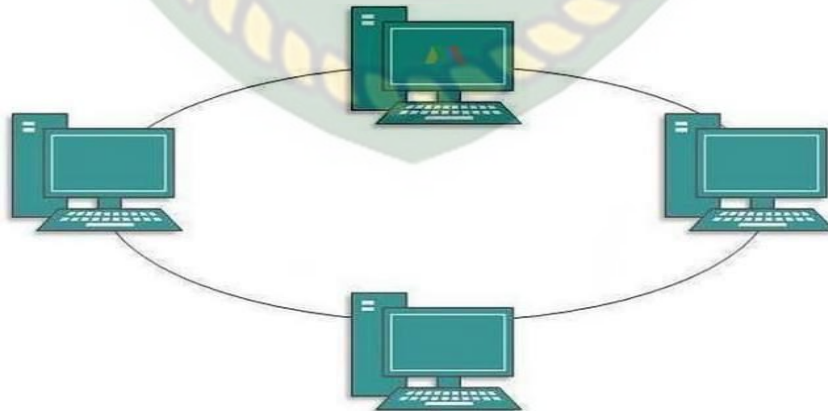
Topologi star atau topologi bintang adalah salah satu bentuk topologi jaringan yg umumnya memakai switch/ hub utk menghubungkan client satu dgn client lainnya.



Gambar 2.2 Topologi Star

3. Topologi Ring

Topologi ring atau cincin adalah salah satu topologi jaringan yg menghubungkan satu pc/komputer dengan pc/komputer yang lain dalam satu buah rangkaian melingkar, serupa dengan cincin. Kebanyakan topologi ini cuma memanfaatkan kartu LAN untuk menghubungkan computer satu dengan pc/komputer yang lain.



Gambar 2.3 Topologi Ring

2.2.3 *Virtual Private Network (VPN)*

Virtual Private Network (VPN) adalah sebuah teknologi jaringan komputer yang dikembangkan oleh perusahaan skala besar yang menghubungkan antar jaringan diatas jaringan lain menggunakan internet yang membutuhkan jalur *privacy* dalam komunikasinya (Forouzan, 2007). Sifat pribadi *Virtual Private Network (VPN)* berarti bahwa traffic data *Virtual Private Network (VPN)* yang pada umumnya tidak terlihat, atau di enkapsulasi oleh lalu lintas jaringan yang mendasarinya. Dalam istilah yang lebih teknis, di link lapisan protokol jaringan virtual dikatakan terowongan atau *tunnel* yang melewati jaringan transportasi yang mendasarinya. Istilah *Virtual Private Network (VPN)* dapat digunakan untuk menggambarkan berbagai macam konfigurasi jaringan dan protokol. Tiga fungsi utama *Virtual Private Network (VPN)* (Cisco System Inc., 2003) yaitu :

1. Enkripsi

Pengirim dapat mengenkripsi paket data sebelum dikirim melewati jaringan, sehingga jika paket data disadap tidak akan terbaca.

2. Integritas Data

Penerima dapat memastikan bahwa data dikirimkan melalui jaringan *Internet* tanpa mengalami perubahan.

3. Autentikasi Sumber Data

Penerima dapat membuktikan keaslian sumber paket data, menjamin sumber informasi.

2.2.3.1 Cara Kerja Dan Penggunaan *Virtual Private Network (VPN)*

1. *Virtual Private Network (VPN)* mendukung banyak protokol jaringan seperti *Point-to-Point Tunneling Protocol (PPTP)*, *Layer Two Tunneling Protocol*

(L2TP), *Internet Protocol Security* (IPSec) dan SOCKS. Protokol ini membantu cara kerja *Virtual Private Network* (VPN) untuk memproses otentikasi.

2. *Virtual Private Network* (VPN) klien dapat membuat sambungan dan mengidentifikasi orang-orang yang diberi wewenang di jaringan.
3. Jaringan *Virtual Private Network* (VPN) juga dikripsi akan meningkatkan fitur keamanan, hal ini juga berarti bahwa *Virtual Private Network* (VPN) biasanya tidak terlihat pada jaringan yang lebih besar.
4. Teknologi saat ini semakin banyak mendasarkan perkembangan *Virtual Private Network* (VPN) karena mobilitas yang disediakan dan saat ini *Virtual Private Network* juga membuka jalan untuk koneksi Wi-Fi dan jaringan nirkabel pribadi.

2.2.3.2 Kelebihan Dan Kekurangan *Virtual Private Network* (VPN)

Kelebihan *Virtual Private Network* (VPN):

1. *Virtual Private Network* (VPN) adalah solusi biaya efektif untuk organisasi bisnis besar dengan fasilitas jaringan khusus
2. Meningkatkan mobilitas organisasi dengan langsung menghubungkan jaringan rumah atau para pekerja yang mobile di organisasi
3. Fitur keamanan dapat disesuaikan.

Kekurangan *Virtual Private Network* (VPN):

Dengan penyediaan akses ke karyawan secara global, faktor keamanan adalah risiko tersendiri. Hal ini juga menempatkan informasi sensitif perusahaan

dapat diakses secara global. *Virtual Private Network* (VPN) membutuhkan perhatian ekstra untuk penetapan sistem keamanan yang jelas.

2.2.4 Point To Point Tunneling Protocol (PPTP)

Point-to Point Tunneling Protocol (PPTP) adalah suatu protokol jaringan yang memungkinkan pengiriman data secara aman dari remote client kepada server perusahaan swasta dengan membuat suatu virtual private network *Virtual Private Network* (VPN) melalui jaringan data berbasis *Transfer Control Protocol/Internet Protocol* (TCP/IP). *Point-to-Point Tunneling Protocol* (PPTP) merupakan protokol jaringan yang memungkinkan pengamanan transfer data dari remote client (client yang berada jauh dari server) ke server pribadi perusahaan dengan membuat sebuah *Virtual Private Network* (VPN) melalui *Transfer Control Protocol/Internet Protocol* (TCP/IP) (Snader, 2005). Protokol ini dikembangkan oleh Microsoft dan Cisco. *Point-to-Point Tunneling Protocol* (PPTP) merupakan protokol jaringan yang mengubah paket *Point-to-Point Protocol* (PPP) menjadi *Internet Protocol* (IP) datagram agar dapat ditransmisikan melalui internet. *Point-to-Point Tunneling Protocol* (PPTP) juga dapat digunakan pada jaringan private LAN-to-LAN. *Point-to-Point Tunneling Protocol* (PPTP) terdapat sejak dalam sistem operasi Windows NT Workstation versi 4.0. Komputer yang berjalan dengan sistem operasi tersebut dapat menggunakan protokol *Point-to-Point Tunneling Protocol* (PPTP) dengan aman untuk terhubung dengan private network sebagai client dengan remote access melalui internet. *Point-to-Point Tunneling Protocol* (PPTP) juga dapat digunakan oleh komputer yang terhubung dengan *Local Area Network* (LAN) untuk membuat *Virtual Private Network* (VPN) melalui *Local Area Network* (LAN).

2.2.5 Layer Two Tunneling Protocol (L2TP)

Layer Two Tunneling Protocol (L2TP) adalah protokol tunneling yang memadukan dua buah protokol tunneling, yaitu *Layer 2 Forwarding (L2F)* milik Cisco dan *Point-to Point Tunneling Protocol (PPTP)* milik Microsoft (Gupta, 2003). Pada awalnya, semua produk Cisco menggunakan *Layer 2 Forwarding (L2F)* untuk mengurus tunnelingnya, sedangkan operating system Microsoft yang terdahulu hanya menggunakan *Point-to Point Tunneling Protocol (PPTP)* untuk melayani penggunaanya yang ingin bermain dengan tunnel. Namun saat ini, Microsoft Windows NT/2000 telah dapat menggunakan *Point-to Point Tunneling Protocol (PPTP)* atau *Layer Two Tunneling Protocol (L2TP)* dalam teknologi *Virtual Private Network (VPN)*-nya. Seperti *Point-to Point Tunneling Protocol (PPTP)*, *Layer Two Tunneling Protocol (L2TP)* juga mendukung protokol-protokol non-ip. Protokol *Layer Two Tunneling Protocol (L2TP)* lebih banyak digunakan pada *Virtual Private Network (VPN)* non-internet (frame relay, ATM, dsb). *Layer Two Tunneling Protocol (L2TP)* biasanya digunakan dalam membuat *Virtual Private Dial Network (VPDN)* yang dapat bekerja membawa semua jenis protokol komunikasi didalamnya. *Layer Two Tunneling Protocol (L2TP)* memungkinkan penggunaanya untuk tetap dapat terkoneksi dengan jaringan lokal milik mereka dengan policy keamanan yang sama dan dari manapun mereka berada, melalui koneksi *Virtual Private Network (VPN)* atau *Virtual Private Dial Network (VPDN)*. Koneksi ini seringkali dianggap sebagai sarana memperpanjang jaringan lokal milik penggunaanya, namun melalui media publik.

2.2.6 *Transmissions Control Protocol/Internet Protocol (TCP/IP)*

Pengertian *Transmissions Control Protocol/Internet Protocol (TCP/IP)* adalah singkatan dari *Transmission Control Protocol/Internet Protocol*. TCP/IP merupakan standar komunikasi data yang digunakan untuk dalam proses tukar-menukar data dari satu komputer ke komputer lain pada jaringan Internet. Karena berupa kumpulan protokol (protocol suite) maka Protokol ini tidaklah mampu berdiri sendiri. TCP/IP merupakan yang paling banyak dipakai pada saat ini. Data tersebut diimplementasikan dalam bentuk software atau perangkat lunak pada sistem operasi. Istilah yang diberikan kepada perangkat lunak tersebut yaitu TCP/IP stack. Pengertian TCP/IP Menurut Para Ahli. Berikut ini adalah beberapa pengertian TCP/IP menurut para ahli:

Menurut Forouzan dan Chung Fegan (2007, pp 43-46), menyatakan TCP/IP adalah suatu hierarki protokol yang terdiri atas modul-modul yang interaktif, yang mana tiap-tiap modul tersebut memiliki fungsionalitas yang spesifik.

Menurut Kozierok (2005), bahwa TCP/IP yaitu satu set standar aturan komunikasi data yang dipakai dalam proses transfer data dari satu komputer ke komputer yang lainnya dalam jaringan komputer tanpa memandang perbedaan jenis hardware yang digunakan.

2.2.7 Wireshark

Wireshark adalah sebuah tools open source yang berfungsi sebagai network packet analyzer. Sebuah network packet analyzer akan berusaha mengcapture packet data dan menampilkan sedetail mungkin jika memungkinkan. Profesi yang sering memakai wireshark adalah sebagai berikut:

- a. Network administrators untuk mengetahui troubleshoot network problems
- b. Network security engineers untuk mengetahui security problems
- c. Developers untuk debug protocol implementations
- d. Semua orang yang ingin mengetahui network protocol internals

Fitur yang dimiliki oleh wireshark adalah sebagai berikut:

- a. Tersedia untuk UNIX dan Windows
- b. Capture live packet langsung dari interface.
- c. Menampilkan packet secara very detailed protocol information.
- d. Open and save packet data captured.
- e. Import and export packet data
- f. Filter packet
- g. Search for packet yang dikehendaki
- h. Mewarnai packet display yang di filter
- i. Mewarnai variasi statistic

BAB III

METODOLOGI PENELITIAN

3.1 Metode Penelitian

Pengertian metode penelitian adalah langkah yang dimiliki dan dilakukan oleh peneliti dalam rangka untuk mengumpulkan informasi atau data serta melakukan investigasi pada data yang telah didapatkan tersebut. Metode penelitian memberikan gambaran rancangan penelitian yang meliputi antara lain: prosedur dan langkah-langkah yang harus ditempuh, waktu penelitian, sumber data, dan dengan langkah apa data-data tersebut diperoleh dan selanjutnya diolah dan dianalisis.

3.1.1 Metode Penelitian Informatika

Metode Penelitian informatika mempunyai tiga paradigma didalam penelitiannya diantaranya sebagai berikut:

1. Teori

Maksudnya adalah pendekatan yang berlandaskan kepada ilmu matematika. Untuk mendapatkan teori yang valid perlu dilalui proses pendefinisian, pembuatan teorema, pembuktian, penginterpretasian hasil.

2. Abstraksi atau Pemodelan

Maksudnya ialah pendekatan yang berlandaskan pada metode perancangan atau eksperimen terdiri dari formula, prediksi, metode atau prototype.

3. Produk atau Sistem

Pendekatan penelitian guna menghasilkan suatu produk, sistem, tool atau *device* baik *hardware* maupun *software*. Tahapan perencanaan, perancangan, pembangunan, pengujian, penerapan dan evaluasi.

3.2 Alat dan Bahan Penelitian yang Digunakan

3.2.1 Alat Penelitian

Adapun spesifikasi perangkat keras (*Hardware*) yang digunakan untuk melakukan simulasi jaringan dan spesifikasi dan spesifikasi perangkat lunak (*Software*) yang dibutuhkan untuk sistem yang akan dibangun adalah sebagai berikut:

3.2.1.1 Spesifikasi Perangkat Keras (*Hardware*)

Adapun spesifikasi perangkat keras (*Hardware*) yang dibutuhkan sebagai server atau *pc* yang akan digunakan dalam penelitian ini adalah sebagai berikut:

Tabel 3.1 Alat perangkat keras (*hardware*)

No	Nama Perangkat	Spesifikasi	Fungsi
1	Server	<ul style="list-style-type: none"> • <i>Processor</i> intel core i5 • RAM 2.00 GB • Harddisk 300 GB • <i>Type System</i> 64-bit • <i>Operating System</i> 	Untuk mengelola sebuah jaringan komputer.
2	PC	<ul style="list-style-type: none"> • <i>Processor</i> amd • RAM 4.00 GB • <i>Type System</i> 64-bit 	Meminta layanan dari server untuk

		<ul style="list-style-type: none"> • Hardisk 500 GB 	mengakses sebuah data.
3	Kabel <i>Unshielded Twisted Pair</i> (UTP)	<i>Straight-through</i>	Untuk menghubungkan dua perangkat yang berbeda.
4	Mikrotik	HAP Series	Digunakan untuk jaringan komputer yang berskala kecil maupun skala besar

3.2.1.2 Spesifikasi Perangkat Lunak (*Software*)

Perangkat lunak (*Software*) yang digunakan dalam pembuatan simulasi jaringan ini adalah sebagai berikut:

Tabel 3.2 Alat perangkat lunak (*software*)

No	Nama Perangkat	Spesifikasi	Fungsi
1	PC	<ul style="list-style-type: none"> • <i>Operating System:</i> Windows 7 	
2	Winbox		Berguna untuk melakukan konektivitas dan

			konfigurasi mikrotik menggunakan MAC Address atau protocol IP.
3	Wireshark	Type 3.0.5	Aplikasi yang digunakan untuk melakukan analisa parameter jaringan komputer.
4	Filezilla		Untuk mengkoneksikan dari sisi <i>server</i> ke <i>client</i> yang bertujuan untuk proses transfer paket data.

3.3 Teknik Pengumpulan Data

Pengumpulan data merupakan langkah yang penting untuk mendapatkan data yang benar dan meyakinkan agar hasil yang didapat tidak menyimpang dari

tujuan yang diharapkan sebelumnya, maka dari itu penulis melakukan langkah langkah penelitian sebagai berikut :

1. Analisis

Metode ini berguna untuk menganalisa kebutuhan perangkat keras (*hardware*) dan perangkat lunak (*software*). Dan juga untuk menganalisa sebuah topologi yang dirancang, menganalisa proses dari pengiriman sebuah audio, video dan file sehingga hasil analisa dapat ditampilkan, bagus atau tidaknya kualitas pengiriman audio, video dan file yang dikirim.

2. Perancangan

Pada tahap ini akan menterjemahkan segala kebutuhan yang telah didapatkan dari tahap analisis kedalam bentuk arsitektur perangkat lunak untuk diimplementasikan kepada aplikasi yang dibuat.

3. Pengujian

Dalam tahap pengujian ini dilakukan dengan menggunakan aplikasi untuk mendapatkan hasil pengujian yang sedang berjalan dan mengetahui hasil yang ditampilkan.

4. Dokumentasi

Pada proses ini, penulis juga melakukan studi pustaka, membaca dan mempelajari buku-buku acuan, serta sumber lainnya yang berkaitan dengan penelitian untuk dijadikan referensi.

3.4 Jenis Data

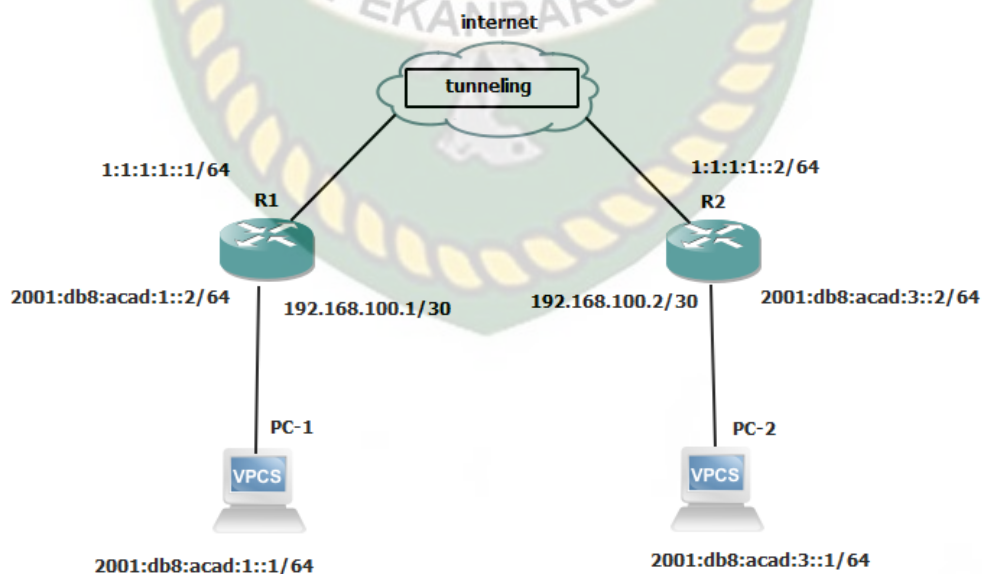
1. Data Sekunder

Yaitu sumber data penelitian yang diperoleh melalui tinjauan pustaka, buku, bukti yang telah ada dan literature-literature yang berkaitan dengan masalah yang penulis buat dan diambil dalam bentuk baik yang sudah dipublikasikan secara umum maupun tidak.

3.5 Pengembangan dan Perancangan Sistem

3.5.1 Desain Topologi

Pada simulasi jaringan ini menggunakan jaringan *local* yang terdiri dari 2 pc laptop, satu berfungsi sebagai *server* dan satunya lagi berfungsi sebagai *client* dengan *system* operasi *windows 7*. Topologi jaringan nya bisa dilihat seperti gambar dibawah ini:



Gambar 3.1 Topologi jaringan

Pada gambar topologi fisik diatas, dalam merancang jaringan ini menggunakan 2 router mikrotik yang saling terhubung. Lalu akan di setting untuk bisa terhubung ke pc maupun laptop.

3.6 Parameter Kerja

1. Delay

Delay adalah waktu yang dibutuhkan data untuk menempuh jarak dari asal ke tujuan. *Delay* dapat dipengaruhi oleh jarak, media fisik, kongesti atau juga waktu proses yang lama.

Tabel 3.3 Parameter Delay

Kategori Delay	Besar Delay
Excellent	< 150 ms
Good	150 s/d 300 ms
Poor	300 s/d 450 ms
Unnacceptable	> 450 ms

2. Throughput

Throughput, yaitu kecepatan transfer data efektif, yang diukur dalam bps. *Throughput* merupakan jumlah total kedatangan paket yang sukses diamati pada *destination* selama interval waktu tertentu dibagi oleh durasi interval waktu tersebut.

Tabel 3.4 Parameter *throughput*

Kategori Throughput	Throughput (bps)
Sangat Bagus	100-75

Bagus	75-50
Sedang	50-25
Jelek	<25

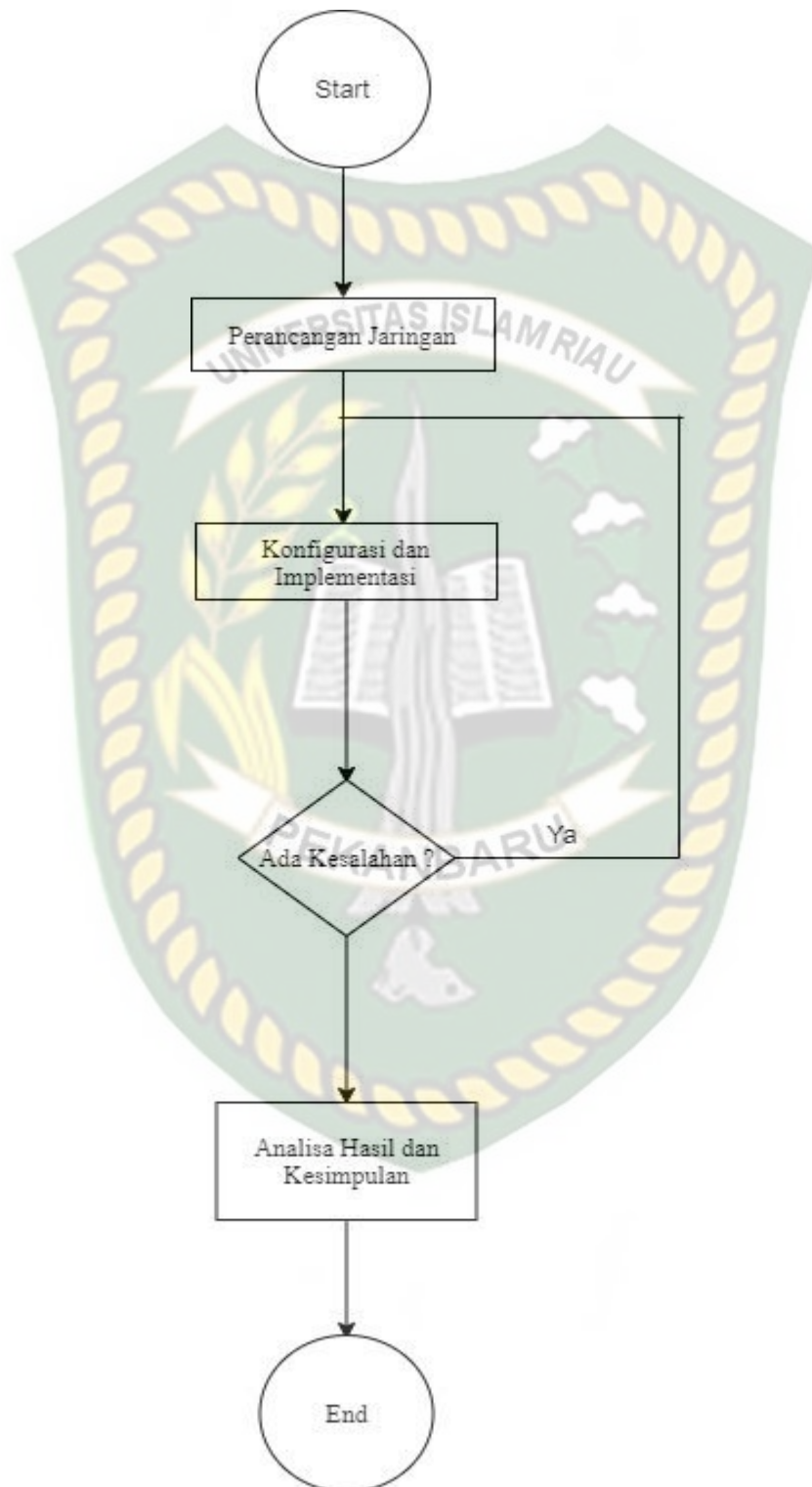
3. Packet loss

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

Tabel 3.5 Parameter *packet loss*

Kategori Degradasi	Packet Loss
Sangat Bagus	0
Bagus	3 %
Sedang	15 %
Jelek	25 %

3.6.1 Kerangka Permodelan



Gambar 3.2 Skema Rancangan Penelitian

Pada gambar 3.2 diatas, penjelasan dari skema penelitian ini diawali dengan melakukan perancangan jaringan, setelah semua dirancang langkah selanjutnya adalah melakukan konfigurasi dan implementasi. Konfigurasi jaringan ini menggunakan ipv4 dan ipv6. Jika gagal, maka lakukan konfigurasi ulang. Jika konfigurasi berhasil, maka akan lanjut ke tahap selanjutnya. Kemudian setelah itu dilakukan pengujian dan analisa hasil. Untuk menganalisa performa *Quality of Service* (QoS) ini menggunakan *tools* yang disebut wireshark. Lalu setelah dianalisa, diambil kesimpulan dari hasil analisa tersebut, dan kemudian selesai.

3.7 Skenario Pengujian Qos

Pada tugas akhir ini akan dilakukan pengujian pada pengujian Qos dengan beberapa macam skenario, yaitu:

1. Dilakukan pengukuran *Quality of Service* (QOS) seperti *throughput*, *delay*, *jitter* dan *packet loss* untuk mendapatkan suatu data berupa nilai. Data yang dikirim berupa audio, video dan file ke *client*.
2. Melakukan pengukuran *Quality of Service* (Qos) sebuah audio, video dan file yang akan di *share* menggunakan aplikasi filezilla.

BAB IV

HASIL DAN PEMBAHASAN

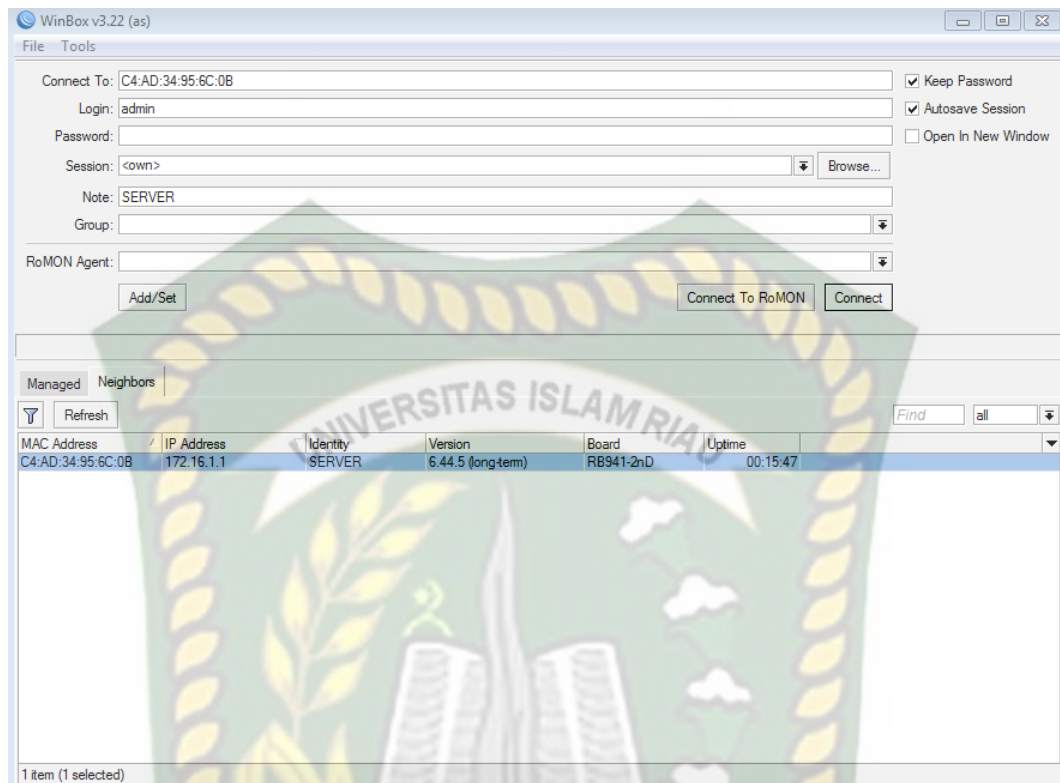
4.1 Hasil Penelitian

Berdasarkan analisa dan perancangan pada bab sebelumnya, penelitian ini membahas tentang perbandingan pada PPTP (*Point-To-Point Tunneling Protocol*) dan L2TP (*Layer Two Tunneling Protocol*) untuk mengetahui performa Qos (*Quality Of Service*) dari kedua tunneling tersebut. Selain itu, pengujian ini dilakukan dengan cara mentransfer sebuah paket data dari *server* ke *client* maupun sebaliknya. Yang dimana hasil akhirnya didapatkan yaitu berupa data berbentuk nilai.

Parameter yang digunakan pada pengujian kedua tunneling protokol ini ada empat, diantaranya *throughput*, *delay*, *jitter* dan *packet loss*. Lalu IP (*Internet Protocol*) yang digunakan yaitu IPV6 (*Internet Protocol Versi 6*) dan IPV4 (*Internet Protocol Versi 4*). Subjek penelitian ini adalah berupa file, audio dan video. Kemudian pengujian ini menggunakan durasi 3 menit dan 5 menit. Alasan memilih durasi tersebut salah satunya ialah menghemat dalam segi waktu.

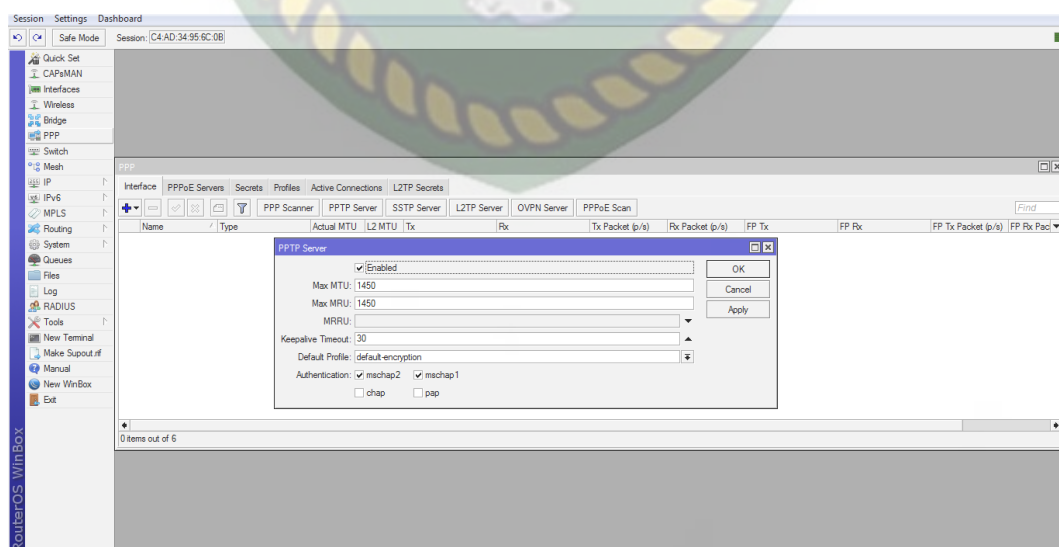
4.2 Pengaturan PPTP

Pada penelitian ini, dalam melakukan pengaturan PPTP ini terdapat beberapa proses yang dikerjakan. Langkah pertama yaitu login melalui aplikasi Winbox dengan mengklik MAC address atau ip address. Bisa kita lihat pada gambar berikut ini:



Gambar 4.1 Menu login Winbox

Pastikan router sudah terhubung ke internet. Baik melalui wifi maupun hotspot. Kemudian masuk ke menu PPP → interface → PPTP Server. Untuk menghidupkan PPTP Server.



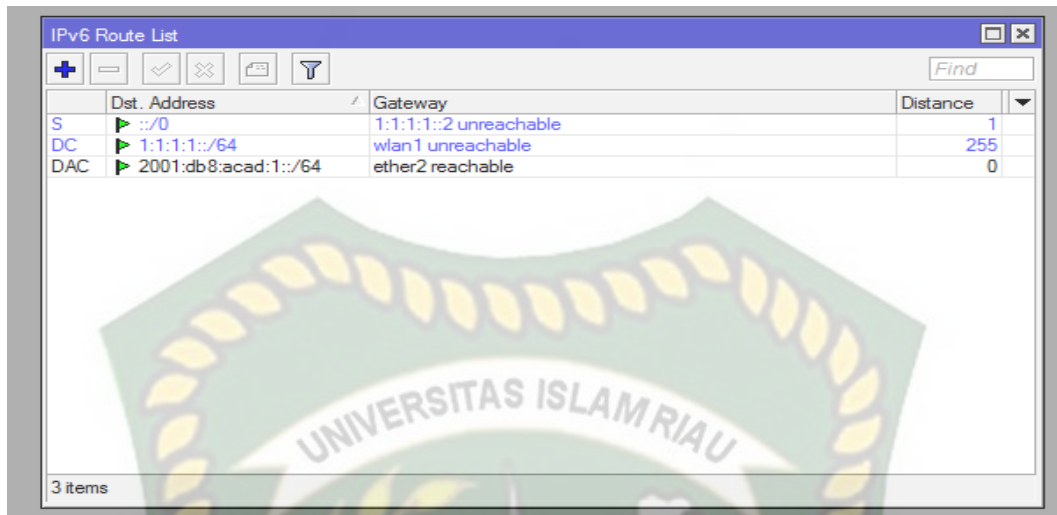
Gambar 4.2 Menghidupkan PPTP Server

Langkah selanjutnya IPV6 → addresses → +. Untuk menginputkan ip address nya

	Address	From Pool	Interface	Advertise
G	1:1:1:1::1/64		wlan 1	yes
G	2001:db8:acad:1::2/64		ether2	yes
DL	fe80::c6ad:34ff:fe95:6c0b/64		ether2	no
DL	fe80::c6ad:34ff:fe95:6c0f/64		wlan 1	no

Gambar 4.3 IPV6 address

Pada gambar diatas, *ip address* 1:1:1:1::1/64 merupakan ip publik. Yang bertujuan untuk menghubungkan ke *client*. Kemudian *ip address* 2001:db8:acad:1::2/64 merupakan ip router nya. Selanjutnya pengaturan routing IPV6 → Route. Bisa dilihat pada gambar berikut ini:

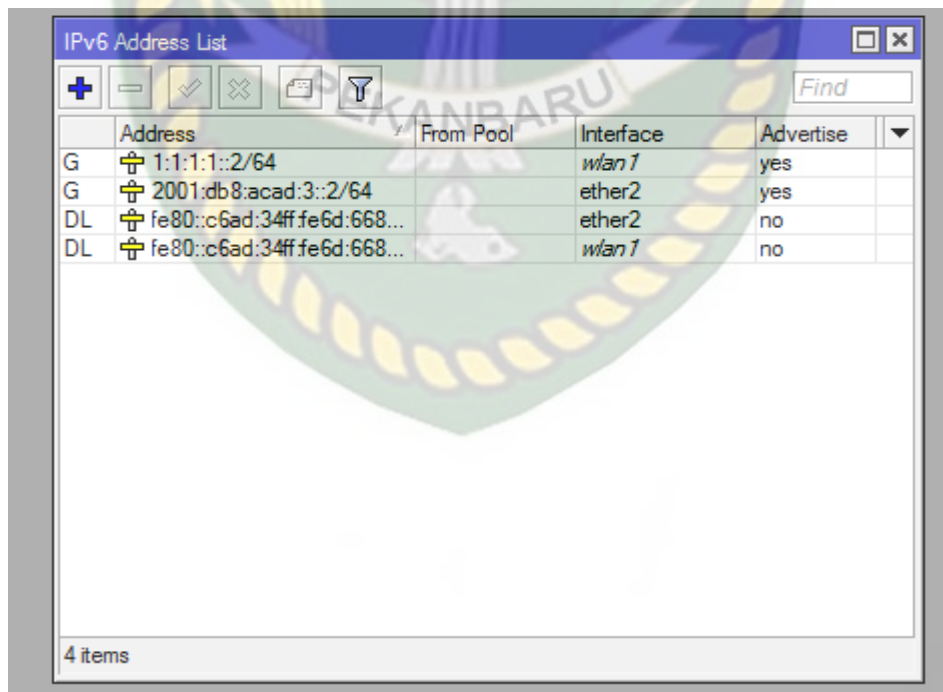


	Dst. Address	Gateway	Distance
S	::/0	1:1:1:1:2 unreachable	1
DC	1:1:1:1::/64	wlan1 unreachable	255
DAC	2001:db8:acad:1::/64	ether2 reachable	0

3 items

Gambar 4.4 IPV6 route

Selanjutnya pada sisi *client*, pengaturannya juga tak jauh berbeda. Langkah pertama masuk ke PPP → interface → lalu klik + → PPTP Client. Lalu, pengaturan *ip address* pada client bisa dilihat pada gambar berikut ini:



	Address	From Pool	Interface	Advertise
G	1:1:1:1::2/64		wlan1	yes
G	2001:db8:acad:3::2/64		ether2	yes
DL	fe80::c6ad:34ff:fe6d:668...		ether2	no
DL	fe80::c6ad:34ff:fe6d:668...		wlan1	no

4 items

Gambar 4.5 IPV6 address client

Pada gambar diatas, *ip address* 1:1:1:1::2/64 merupakan ip publik. Yang bertujuan untuk menghubungkan ke *server*. Kemudian *ip address*

2001:db8:acad:3::2/64 merupakan ip router pada sisi *client*. Selanjutnya pengaturan routing nya bisa dilihat pada gambar berikut ini:

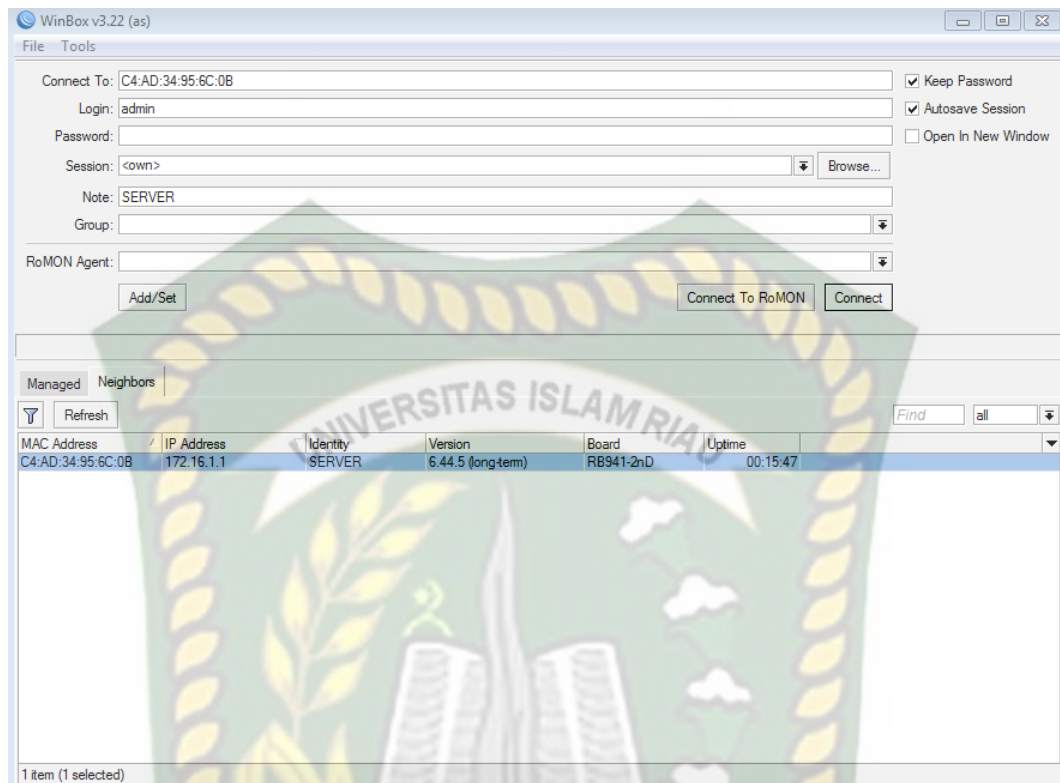
	Dst. Address	Gateway	Distance
S	▶ ::/0	1:1:1:1:1 unreachable	1
DC	▶ 1:1:1:1::/64	wlan1 unreachable	255
DAC	▶ 2001:db8:acad:3::/64	ether2 reachable	0

3 items

Gambar 4.6 IPV6 Route pada *client*

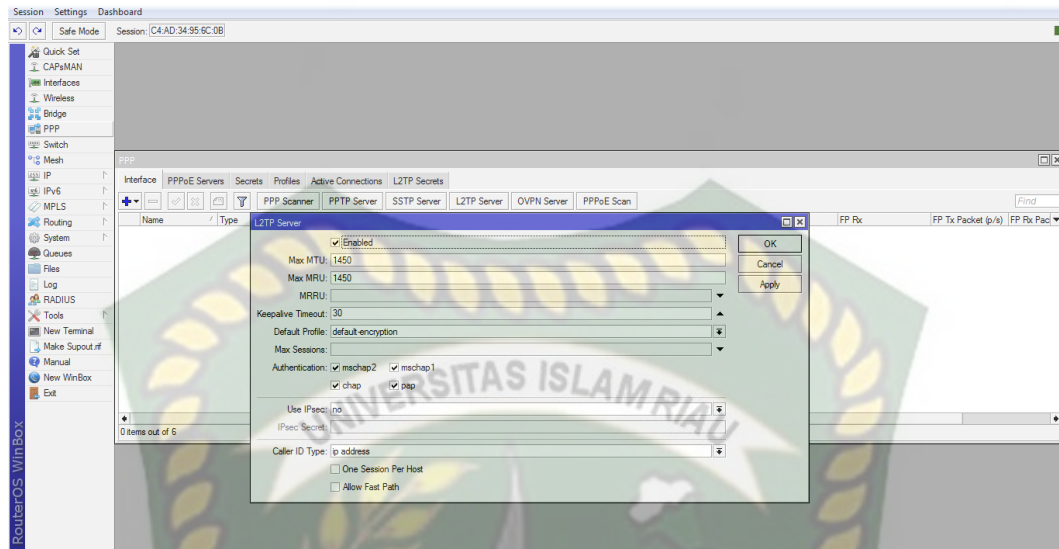
4.3 Pengaturan L2TP

Pada penelitian selanjutnya dalam melakukan pengaturan L2TP ini juga tidak jauh berbeda dengan konfigurasi L2TP. Langkah awal yang dilakukan yaitu login melalui aplikasi Winbox dengan mengklik MAC address atau ip address. Bisa kita lihat pada gambar berikut ini:



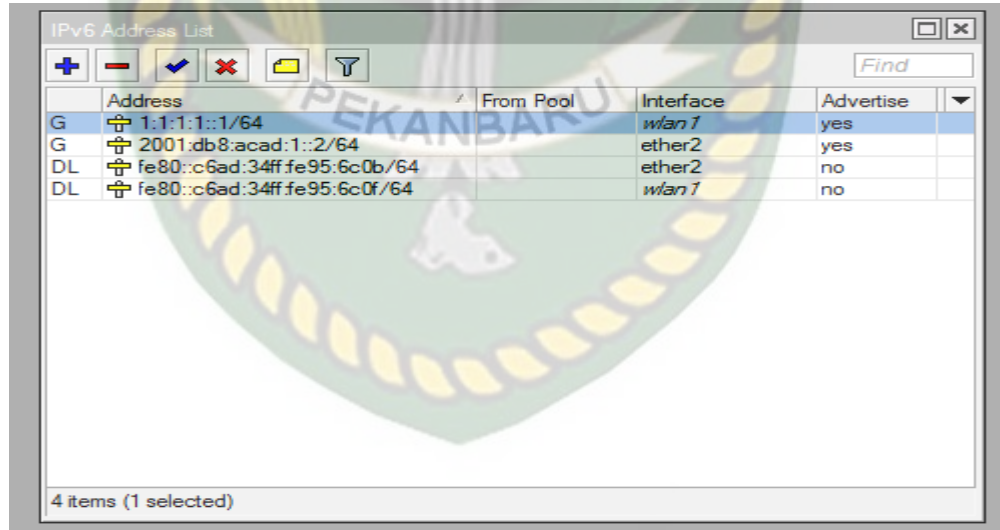
Gambar 4.7 Menu login Winbox

Pastikan router sudah terhubung ke internet. Baik melalui wifi maupun hotspot. Kemudian masuk ke menu PPP → interface → L2TP Server. Untuk menghidupkan L2TP Server.



Gambar 4.8 Menghidupkan L2TP Server

Langkah selanjutnya IPV6 → addresses → +. Untuk menginputkan ip address nya



Gambar 4.9 IPV6 address

Pada gambar diatas, *ip address* 1:1:1::1/64 merupakan ip publik. Yang bertujuan untuk menghubungkan ke *client*. Kemudian *ip address* 2001:db8:acad:1::2/64 merupakan ip router nya. Selanjutnya pengaturan routing IPV6 → Route. Bisa dilihat pada gambar berikut ini:

	Dst. Address	Gateway	Distance
S	::0	1:1:1:1:2 unreachable	1
DC	1:1:1:1::/64	wlan1 unreachable	255
DAC	2001:db8:acad:1::/64	ether2 reachable	0

3 items

Gambar 4.10 IPV6 route

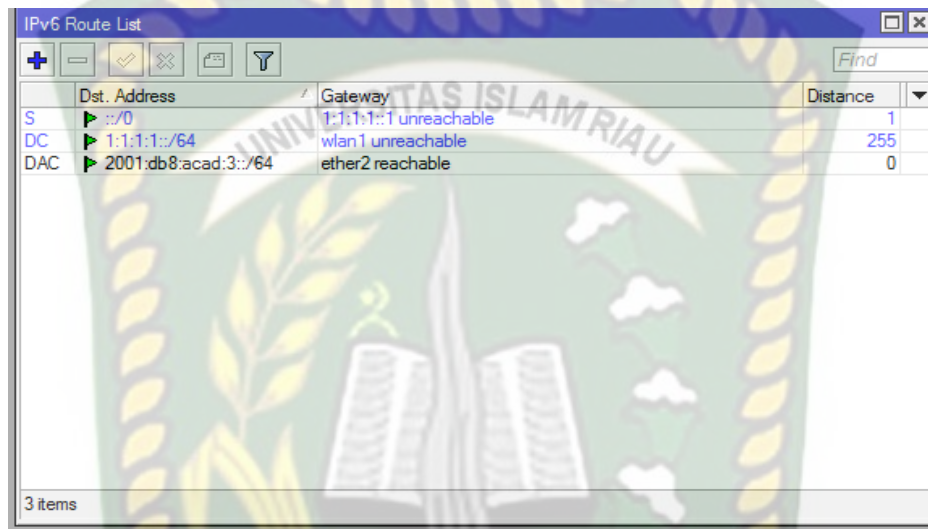
Selanjutnya pada sisi *client*, pengaturannya juga tak jauh berbeda. Langkah pertama masuk ke PPP → interface → lalu klik + → PPTP Client. Lalu, pengaturan *ip address* pada client bisa dilihat pada gambar berikut ini:

	Address	From Pool	Interface	Advertise
G	1:1:1:1::2/64		wlan1	yes
G	2001:db8:acad:3::2/64		ether2	yes
DL	fe80::c6ad:34ff:fe6d:668...		ether2	no
DL	fe80::c6ad:34ff:fe6d:668...		wlan1	no

4 items

Gambar 4.11 IPV6 address client

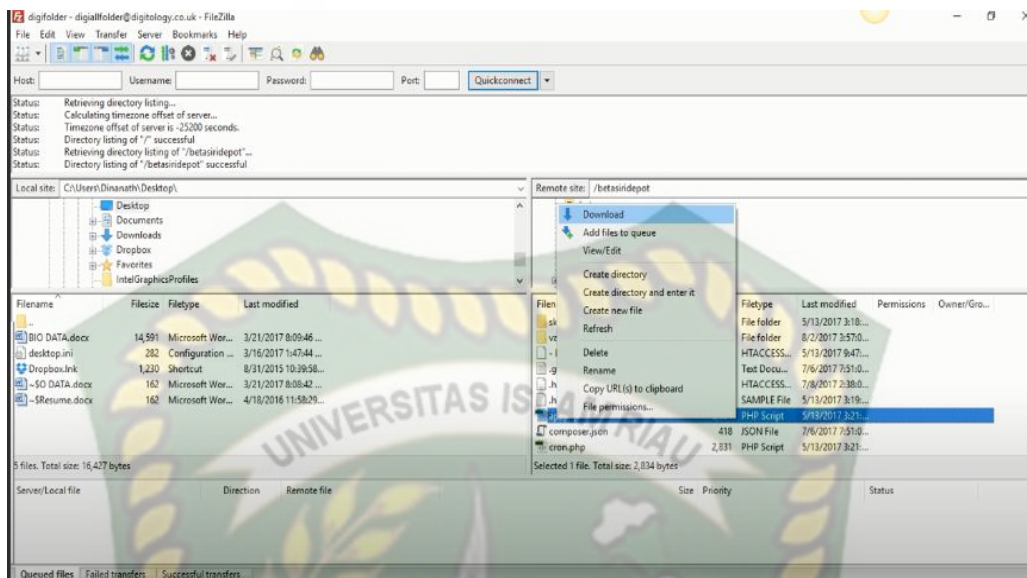
Pada gambar diatas, *ip address* 1:1:1:1::2/64 merupakan ip publik. Yang bertujuan untuk menghubungkan ke *server*. Kemudian *ip address* 2001:db8:acad:3::2/64 merupakan ip router pada sisi *client*. Selanjutnya pengaturan routing nya bisa dilihat pada gambar berikut ini:



	Dst. Address	Gateway	Distance
S	:::0	1:1:1:1::1 unreachable	1
DC	1:1:1:1::/64	wlan1 unreachable	255
DAC	2001:db8:acad:3::/64	ether2 reachable	0

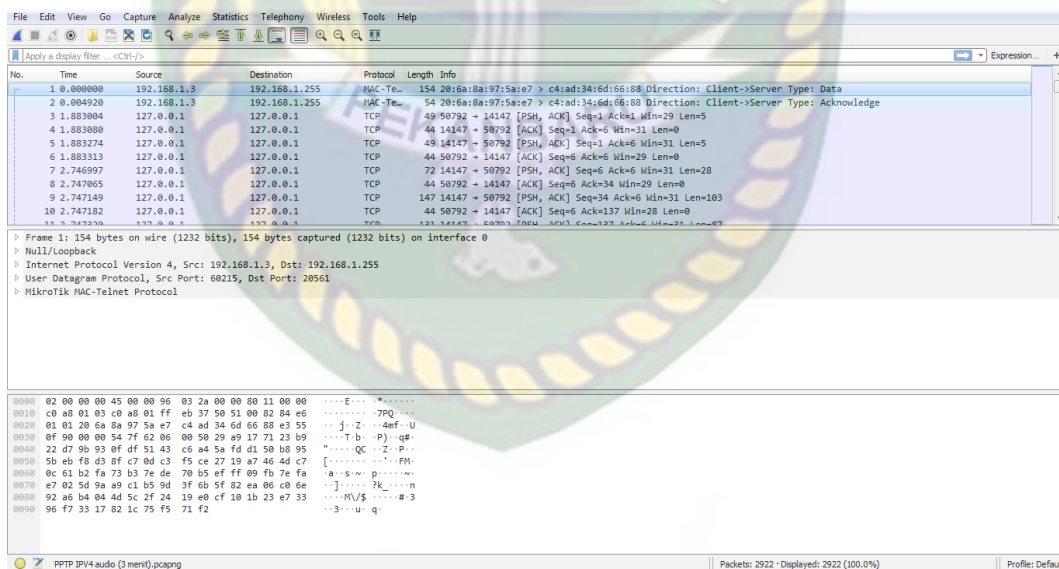
Gambar 4.12 IPV6 Route pada *client*

Proses selanjutnya yaitu tahap pengujian menggunakan aplikasi Filezilla. Sisi *client* akan *mendownload* paket data yang berada disisi *server*. Dan pada saat proses download berlangsung, *tools* Wireshark dihidupkan agar dapat dilakukan pengukuran QoS nya untuk mencari sebuah data berbentuk nilai. Berikut sekilas gambar dari proses *download* data dari *client* ke *server* sebagai berikut:



Gambar 4.13 Proses Pengujian Dengan Mendownload Data

Dan berikut salah satu hasil sniffing pada Wireshark setelah dilakukan pengujian bisa dilihat pada gambar berikut ini:



Gambar 4.14 Hasil *Sniffing* setelah proses *download* selesai

4.4 Pengujian PPTP

Pengujian Ini dilakukan dengan menggunakan metode *Point-to-Point Tunneling Protocol* (PPTP). Subjek penelitian yang akan digunakan ialah berupa audio, video dan file. Pengujian ini dilakukan dengan menentukan

durasi selama 3 dan 5 menit. Hal ini dikarenakan agar proses pengujian ini lebih menghemat waktu.

4.4.1 Pengujian IPV6

Pengujian ini dilakukan dengan menggunakan jaringan IPV6. Subjek penelitian yang digunakan ialah audio, video dan file.

a. Pengujian Audio

Pengujian ini dilakukan dengan cara mendownload sebuah audio baik dari sisi *server* maupun *client* melalui aplikasi filezilla. Dan kemudian proses download tadi akan dianalisa menggunakan aplikasi wireshark dengan durasi yang telah ditentukan. Pengujian audio ini memiliki ukuran 47.5 MB menggunakan durasi 3 menit 3 detik. Hasil capture analisa dari proses transfer paket data bisa dilihat pada gambar berikut:

Statistics			
<u>Measurement</u>	<u>Captured</u>	<u>Displayed</u>	<u>Marked</u>
Packets	2361	2361 (100.0%)	—
Time span, s	183.271	183.271	—
Average pps	12.9	12.9	—
Average packet size, B	56	56	—
Bytes	132726	132726 (100.0%)	0
Average bytes/s	724	724	—
Average bits/s	5793	5793	—

Gambar 4.15 Hasil Pengujian IPV6 Audio dengan durasi 3 menit

Gambar diatas merupakan hasil pengujian PPTP IPV6 audio dengan durasi selama 3 menit.

a. Pengujian *Troughput*

$$\textit{Throughput} = 132726 / 183271$$

$$\textit{Throughput} = 0,72 \text{ Bps}$$

b. Pengujian *Delay*

$$\text{Rata – rata Delay} = 183271 / 2361$$

$$\text{Rata – rata Delay} = 0,077 \text{ s}$$

$$\text{Rata – rata Delay} = 77,62 \text{ ms}$$

c. Pengujian *Jitter*

$$\text{Jitter} = (183271 - 0,077) / 2361$$

$$\text{Jitter} = 183270,92 / 2361$$

$$\text{Jitter} = 0,077 \text{ s}$$

$$\text{Jitter} = 77,62 \text{ ms}$$

d. Pengujian *Packet Loss*

$$\text{Packet Loss} = ((2361 - 2361) / 2361) \times 100\%$$

$$\text{Packet Loss} = 0 \%$$

Selanjutnya pada pengujian ini dilakukan dengan menggunakan *Wireshark* yaitu *mendownload* audio dengan durasi 5 menit 5 detik. Dan kemudian berikut hasil capture Analisa dari proses transfer paket data dengan durasi selama 5 menit, sebagai berikut:

Statistics			
Measurement	Captured	Displayed	Marked
Packets	3920	3920 (100.0%)	—
Time span, s	305.882	305.882	—
Average pps	12.8	12.8	—
Average packet size, B	56	56	—
Bytes	218000	218000 (100.0%)	0
Average bytes/s	712	712	—
Average bits/s	5701	5701	—

Gambar 4.16 Hasil Pengujian IPV6 Audio dengan durasi 5 menit

Gambar diatas merupakan hasil pengujian PPTP IPV6 audio dengan durasi selama 5 menit.

a. Pengujian *Troughput*

$$\textit{Throughput} = 218000 / 305882$$

$$\textit{Throughput} = 0,71 \text{ Bps}$$

b. Pengujian *Delay*

$$\text{Rata – rata } \textit{Delay} = 305882 / 3920$$

$$\text{Rata – rata } \textit{Delay} = 0,078 \text{ s}$$

$$\text{Rata – rata } \textit{Delay} = 78,03 \text{ ms}$$

c. Pengujian *Jitter*

$$\textit{Jitter} = (305882 - 0,078) / 3920$$

$$\textit{Jitter} = 305881,92 / 3920$$

$$\textit{Jitter} = 0,078 \text{ s}$$

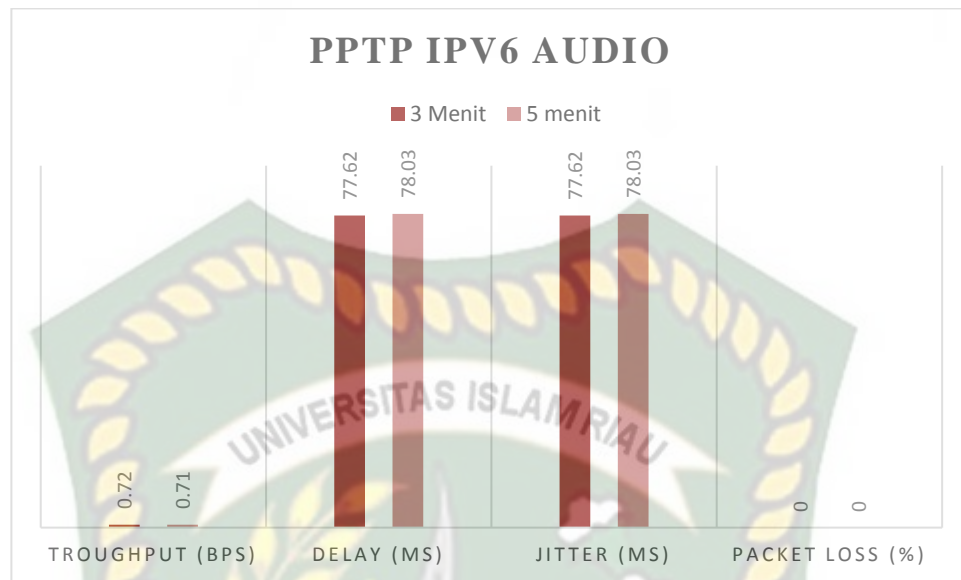
$$\textit{Jitter} = 78,03 \text{ ms}$$

d. Pengujian *Packet Loss*

$$\textit{Packet Loss} = ((3920 - 3920) / 3920) \times 100\%$$

$$\textit{Packet Loss} = 0 \%$$

Kemudian hasil grafik dari PPTP IPV6 audio setelah dilakukan perhitungan untuk mencari parameter QoS nya bisa dilihat pada gambar dibawah ini:



Gambar 4.17 Grafik PPTP IPV6 Audio

b. Pengujian Video

Cara melakukan pengujian ini yaitu *client* akan mengunduh sebuah paket data berupa video yang berada pada sisi *server*, kemudian proses unduhan akan dianalisa dengan durasi yang telah ditentukan. Cara menganalisanya dengan menggunakan aplikasi wireshark untuk mencari parameter QoS nya, yang dimana hasil tersebut akan ditampilkan berupa nilai. Pengujian ini menggunakan video yang memiliki ukuran 84,7 MB dengan durasi 3 menit 6 detik. Berikut hasil capture dari analisa pengujian video dengan durasi 3 menit sebagai berikut:

Statistics			
Measurement	Captured	Displayed	Marked
Packets	2585	2585 (100.0%)	—
Time span, s	186.623	186.623	—
Average pps	13.9	13.9	—
Average packet size, B	76	76	—
Bytes	197474	197474 (100.0%)	0
Average bytes/s	1058	1058	—
Average bits/s	8465	8465	—

Gambar 4.18 Hasil Pengujian IPV6 PPTP video dengan durasi 3 menit

a. Pengujian *Throughput*

$$\text{Throughput} = 197474 / 186623$$

$$\text{Throughput} = 1,05 \text{ Bps}$$

b. Pengujian *Delay*

$$\text{Rata - rata Delay} = 186623 / 2585$$

$$\text{Rata - rata Delay} = 0,072 \text{ s}$$

$$\text{Rata - rata Delay} = 72,19 \text{ ms}$$

c. Pengujian *Jitter*

$$\text{Jitter} = (186623 - 0,072) / 2585$$

$$\text{Jitter} = 186622,92 / 2585$$

$$\text{Jitter} = 0,072 \text{ s}$$

$$\text{Jitter} = 72,19 \text{ ms}$$

d. Pengujian *Packet Loss*

$$\text{Packet Loss} = ((2585 - 2585) / 2585) \times 100\%$$

$$\text{Packet Loss} = 0 \%$$

Pengujian ini dilakukan dengan *mendownload* video dengan ukuran 84,7 MB dengan durasi 5 menit 2 detik. Kemudian berikut hasil capture analisa proses transfer video dengan durasi selama 5 menit sebagai berikut:

Statistics			
Measurement	Captured	Displayed	Marked
Packets	4341	4341 (100.0%)	—
Time span, s	302.153	302.153	—
Average pps	14.4	14.4	—
Average packet size, B	55	55	—
Bytes	238854	238854 (100.0%)	0
Average bytes/s	790	790	—
Average bits/s	6324	6324	—

Gambar 4.19 Hasil Pengujian IPV6 PPTP video dengan durasi 5 menit

a. Pengujian *Throughput*

$$\textit{Throughput} = 238854 / 302153$$

$$\textit{Throughput} = 0,79 \text{ Bps}$$

b. Pengujian *Delay*

$$\text{Rata – rata } \textit{Delay} = 302153 / 4341$$

$$\text{Rata – rata } \textit{Delay} = 0,069 \text{ s}$$

$$\text{Rata – rata } \textit{Delay} = 69,6 \text{ ms}$$

c. Pengujian *Jitter*

$$\textit{Jitter} = (302153 - 0,069) / 4341$$

$$\textit{Jitter} = 302152,93 / 4341$$

$$\textit{Jitter} = 0,069 \text{ s}$$

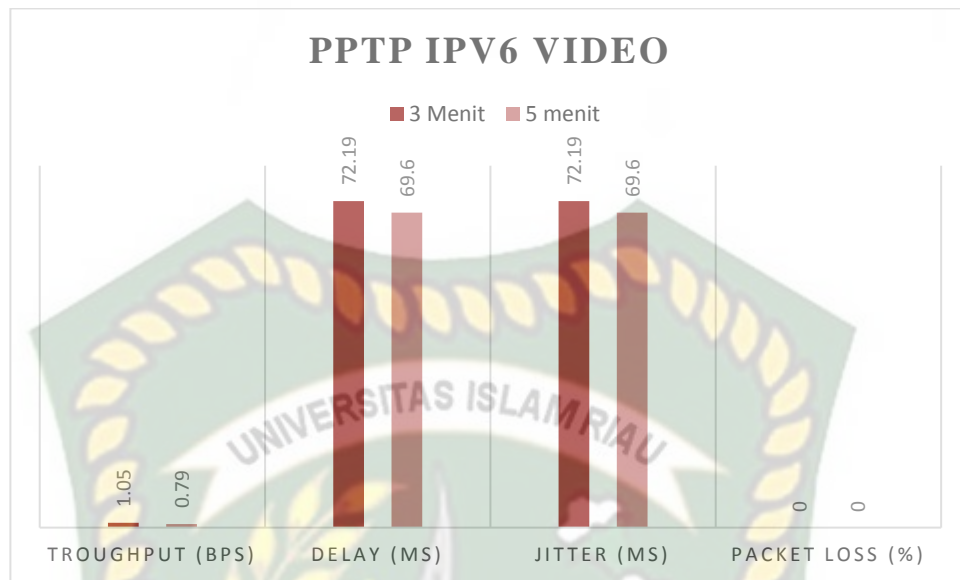
$$\textit{Jitter} = 69,6 \text{ ms}$$

d. Pengujian *Packet Loss*

$$\textit{Packet Loss} = ((4341 - 4341) / 4341) \times 100\%$$

$$\textit{Packet Loss} = 0 \%$$

Hasil grafik dari PPTP IPV6 video setelah dilakukan perhitungan bisa dilihat pada gambar dibawah ini:



Gambar 4.20 Grafik PPTP IPV6 Video

c. Pengujian File

Pengujian ini dilakukan dengan cara sisi *client* akan mendownload sebuah paket data berupa file dengan ukuran 2.32 GB pada durasi 3 menit 8 detik yang berada dari sisi *server*. Dan langkah selanjutnya dalam proses download tersebut akan dilakukan analisa dengan menggunakan aplikasi wireshark. Hal ini bertujuan untuk mencari nilai parameter QoS nya. Berikut hasil capture analisa pengujian transfer file sebagai berikut:

Statistics			
Measurement	Captured	Displayed	Marked
Packets	2568	2568 (100.0%)	—
Time span, s	188.167	188.167	—
Average pps	13.6	13,6	—
Average packet size, B	56	56	—
Bytes	142966	142966 (100.0%)	0
Average bytes/s	759	759	—
Average bits/s	6078	6078	—

Gambar 4.21 Hasil Pengujian PPTP IPV6 File Durasi 3 Menit

a. Pengujian Throughput

$$\text{Throughput} = 142966 / 188167$$

$$\text{Throughput} = 0,75 \text{ Bps}$$

b. Pengujian *Delay*

$$\text{Rata - rata Delay} = 188167 / 2568$$

$$\text{Rata - rata Delay} = 0,073 \text{ s}$$

$$\text{Rata - rata Delay} = 73,27 \text{ ms}$$

c. Pengujian *Jitter*

$$\text{Jitter} = (188167 - 0,073) / 2568$$

$$\text{Jitter} = 188167,92 / 2568$$

$$\text{Jitter} = 0,073 \text{ s}$$

$$\text{Jitter} = 73,27 \text{ ms}$$

d. Pengujian *Packet Loss*

$$\text{Packet Loss} = ((2568 - 2568) / 2568) \times 100\%$$

$$\text{Packet Loss} = 0 \%$$

Pengujian selanjutnya yaitu *mendownload* file ukuran 2.32 GB dengan durasi 5 menit 3 detik. Dan berikut hasil capture analisa pengujian file dengan durasi 5 menit sebagai berikut:

Statistics			
Measurement	Captured	Displayed	Marked
Packets	4018	4018 (100.0%)	—
Time span, s	303.810	303.810	—
Average pps	13.2	13.2	—
Average packet size, B	69	69	—
Bytes	276669	276669 (100.0%)	0
Average bytes/s	910	910	—
Average bits/s	7285	7285	—

Gambar 4.22 Hasil Pengujian PPTP IPV6 File Durasi 5 Menit

a. Pengujian *Troughput*

$$\text{Throughput} = 276669 / 303810$$

$$\text{Throughput} = 0,91 \text{ Bps}$$

b. Pengujian *Delay*

$$\text{Rata – rata } Delay = 303810 / 4018$$

$$\text{Rata – rata } Delay = 0,075 \text{ s}$$

$$\text{Rata – rata } Delay = 75,61 \text{ ms}$$

c. Pengujian *Jitter*

$$Jitter = (303810 - 0,075) / 4018$$

$$Jitter = 303809,92 / 4018$$

$$Jitter = 0,075 \text{ s}$$

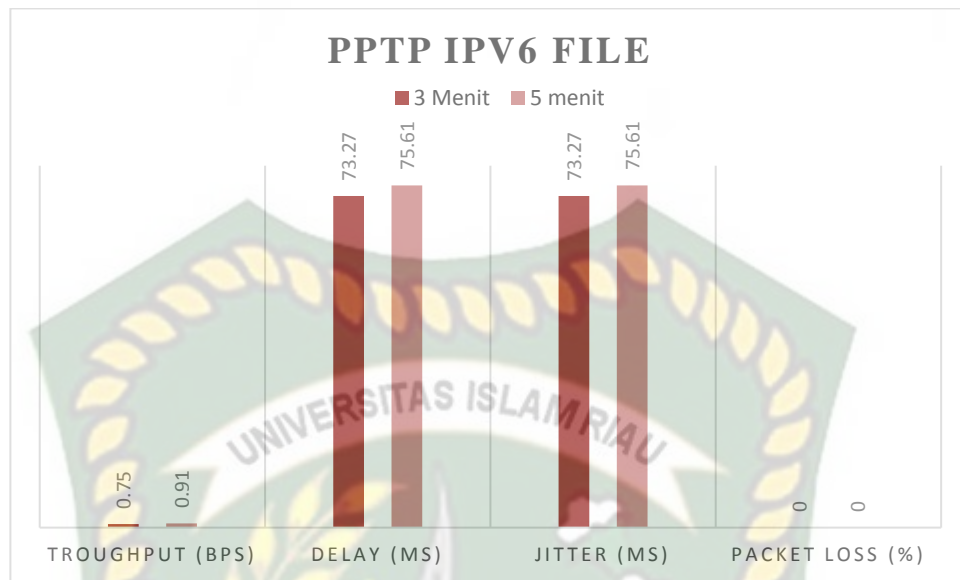
$$Jitter = 75,61 \text{ ms}$$

d. Pengujian *Packet Loss*

$$Packet Loss = ((4018 - 4018) / 4018) \times 100\%$$

$$Packet Loss = 0 \%$$

Kemudian ini bentuk grafik dari pengujian file setelah dilakukan perhitungan untuk mencari parameter QoS nya, bisa dilihat pada gambar dibawah ini sebagai berikut:



Gambar 4.23 Grafik PPTP IPV6 Video

4.4.2 Pengujian IPV4

Pengujian yang dilakukan dengan menggunakan jaringan IPV4. Subjek penelitian yang diuji ialah berupa audio, video dan file.

a. Pengujian Audio

Cara pengujian nya adalah dengan mendownload file berupa audio baik dari sisi *server* maupun *client* melalui aplikasi filezilla. Lalu proses download akan dianalisa lewat aplikasi wireshark dengan durasi yang telah ditentukan. Disini penulis menggunakan audio dengan ukuran 47,5 MB dengan durasi selama 3 menit 2 detik . Hasil capture analisa dari proses transfer paket data tersebut bisa dilihat pada gambar berikut:

Statistics			
Measurement	Captured	Displayed	Marked
Packets	2922	2922 (100.0%)	—
Time span, s	182.906	182.906	—
Average pps	16.0	16.0	—
Average packet size, B	52	52	—
Bytes	151350	151350 (100.0%)	0
Average bytes/s	827	827	—
Average bits/s	6619	6619	—

Gambar 4.24 Hasil Pengujian IPV4 PPTP audio durasi 3 Menit

a. Pengujian *Throughput*

$$\textit{Throughput} = 151350 / 182906$$

$$\textit{Throughput} = 0,82 \text{ Bps}$$

b. Pengujian *Delay*

$$\text{Rata – rata Delay} = 182906 / 2922$$

$$\text{Rata – rata Delay} = 0,062 \text{ s}$$

$$\text{Rata – rata Delay} = 62,59 \text{ ms}$$

c. Pengujian *Jitter*

$$\textit{Jitter} = (182906 - 0,062) / 2922$$

$$\textit{Jitter} = 182905,93 / 2922$$

$$\textit{Jitter} = 0,062 \text{ s}$$

$$\textit{Jitter} = 62.59 \text{ ms}$$

d. Pengujian *Packet Loss*

$$\textit{Packet Loss} = ((2922 - 2922) / 2922) \times 100\%$$

$$\textit{Packet Loss} = 0 \%$$

Kemudian berikut hasil dari analisa transfer data audio dengan waktu 5 menit 6 detik bisa dilihat pada gambar dibawah ini:

Statistics			
Measurement	Captured	Displayed	Marked
Packets	4821	4821 (100.0%)	—
Time span, s	306.542	306.542	—
Average pps	15.7	15.7	—
Average packet size, B	52	52	—
Bytes	249748	249748 (100.0%)	0
Average bytes/s	814	814	—
Average bits/s	6517	6517	—

Gambar 4.25 Hasil Pengujian IPV4 PPTP audio durasi 5 menit

a. Pengujian *Troughput*

$$\textit{Throughput} = 249748 / 306542$$

$$\textit{Throughput} = 0,81 \text{ Bps}$$

b. Pengujian *Delay*

$$\text{Rata – rata Delay} = 306542 / 4821$$

$$\text{Rata – rata Delay} = 0,063 \text{ s}$$

$$\text{Rata – rata Delay} = 63,58 \text{ ms}$$

c. Pengujian *Jitter*

$$\textit{Jitter} = (306542 - 0,063) / 4821$$

$$\textit{Jitter} = 306541,93 / 4821$$

$$\textit{Jitter} = 0,063 \text{ s}$$

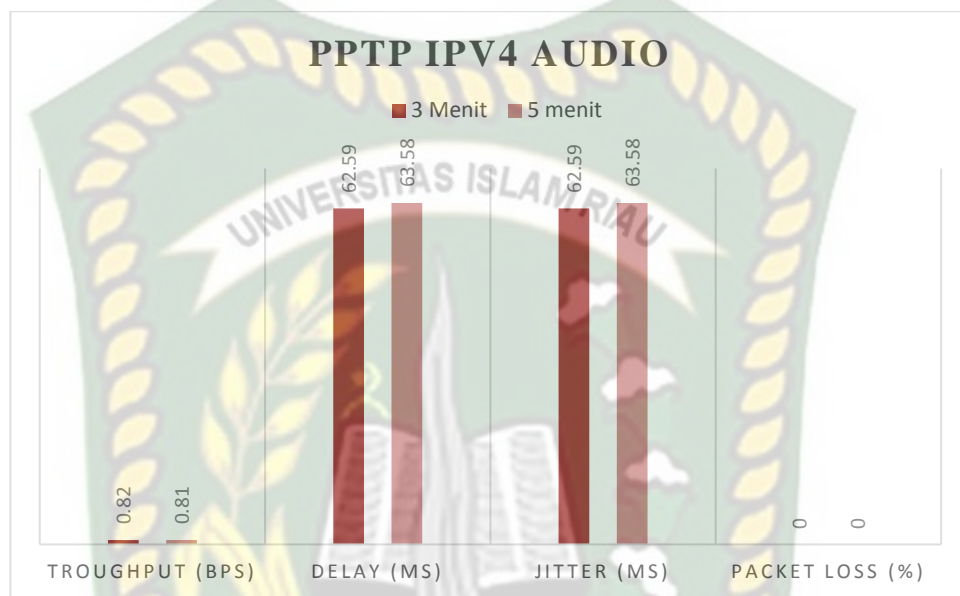
$$\textit{Jitter} = 63,58 \text{ ms}$$

d. Pengujian *Packet Loss*

$$\textit{Packet Loss} = ((4821 - 4821) / 4821) \times 100\%$$

$$\textit{Packet Loss} = 0 \%$$

Berikut bentuk grafik dari hasil pengujian IPV4 audio setelah dilakukan perhitungan untuk mencari parameter QoS nya, bisa dilihat pada gambar dibawah ini:



Gambar 4.26 Grafik IPV4 PPTP Audio

b. Pengujian Video

Cara melakukan pengujian ini yaitu pada sisi *client* akan mengunduh sebuah paket data berupa video dengan ukuran 84.7 MB yang dimana file tersebut awalnya berada pada sisi *server*, kemudian proses unduhan akan dianalisa dengan durasi 3 menit 1 detik. Cara menganalisanya dengan menggunakan aplikasi wireshark untuk mencari perhitungan parameter QoS nya, yang dimana hasil tersebut akan ditampilkan suatu data berbentuk nilai. Berikut hasil capture dari analisa pengujian IPV4 PPTP video sebagai berikut:

Statistics			
Measurement	Captured	Displayed	Marked
Packets	2831	2831 (100.0%)	—
Time span, s	181.695	181.695	—
Average pps	15.6	15.6	—
Average packet size, B	51	51	—
Bytes	144215	144215 (100.0%)	0
Average bytes/s	793	793	—
Average bits/s	6349	6349	—

Gambar 4.27 Hasil Pengujian IPV4 PPTP video durasi 3 menit

a. Pengujian *Troughput*

$$\textit{Throughput} = 144215 / 181695$$

$$\textit{Throughput} = 0,79 \text{ Bps}$$

b. Pengujian *Delay*

$$\text{Rata – rata Delay} = 181695 / 2831$$

$$\text{Rata – rata Delay} = 0,064 \text{ s}$$

$$\text{Rata – rata Delay} = 64,18 \text{ ms}$$

c. Pengujian *Jitter*

$$\textit{Jitter} = (181695 - 0,064) / 2831$$

$$\textit{Jitter} = 181694,93 / 2831$$

$$\textit{Jitter} = 0,064 \text{ s}$$

$$\textit{Jitter} = 64,18 \text{ ms}$$

d. Pengujian *Packet Loss*

$$\textit{Packet Loss} = ((2831 - 2831) / 2831) \times 100\%$$

$$\textit{Packet Loss} = 0 \%$$

Kemudian berikut hasil dari analisa transfer data video dengan waktu 5 menit 1 detik bisa dilihat pada gambar dibawah ini:

Statistics			
Measurement	Captured	Displayed	Marked
Packets	4718	4718 (100.0%)	—
Time span, s	301.438	301.438	—
Average pps	15.7	15.7	—
Average packet size, B	52	52	—
Bytes	244812	244812 (100.0%)	0
Average bytes/s	812	812	—
Average bits/s	6497	6497	—

Gambar 4.28 Hasil Pengujian IPV4 PPTP video durasi 5 menit

a. Pengujian *Troughput*

$$\textit{Throughput} = 244812 / 301438$$

$$\textit{Throughput} = 0,81 \text{ Bps}$$

b. Pengujian *Delay*

$$\text{Rata – rata Delay} = 301438 / 4718$$

$$\text{Rata – rata Delay} = 0,063 \text{ s}$$

$$\text{Rata – rata Delay} = 63,89 \text{ ms}$$

c. Pengujian *Jitter*

$$\textit{Jitter} = (301438 - 0,063) / 4718$$

$$\textit{Jitter} = 301437,93 / 4718$$

$$\textit{Jitter} = 0,063 \text{ s}$$

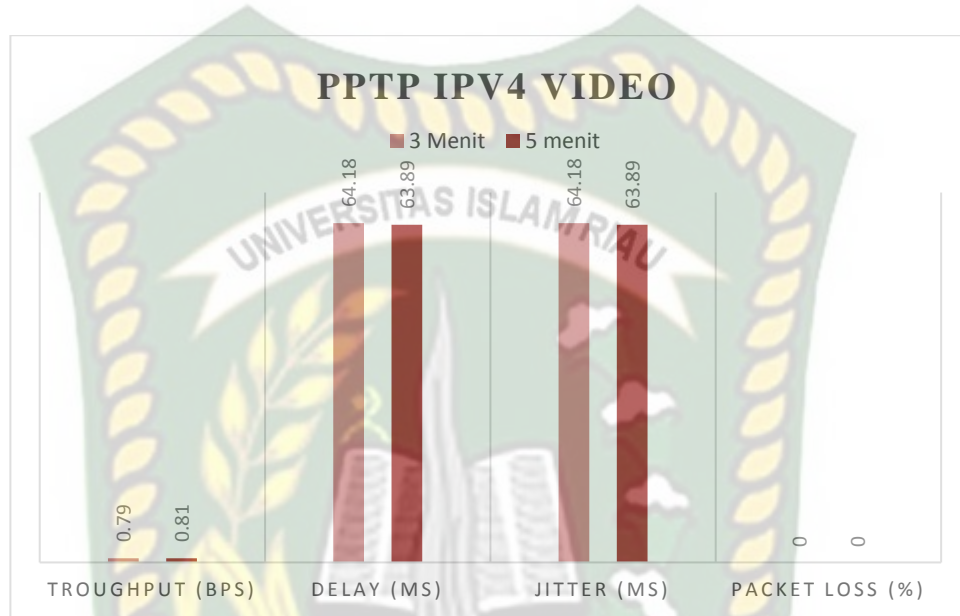
$$\textit{Jitter} = 63,89 \text{ ms}$$

d. Pengujian *Packet Loss*

$$\textit{Packet Loss} = ((4718 - 4718) / 4718) \times 100\%$$

$$\textit{Packet Loss} = 0 \%$$

Kemudian bentuk grafik dari IPV4 PPTP video setelah dilakukan perhitungan untuk mencari parameter QoS nya bisa kita lihat pada gambar dibawah ini sebagai berikut:



Gambar 4.29 Grafik IPV4 PPTP Video

c. Pengujian File

Pengujian ini dilakukan dengan cara sisi *client* akan *mendownload* sebuah paket data berupa file berukuran 2.32 GB yang berada dari sisi *server* lewat aplikasi Filezilla. Dan langkah selanjutnya ialah dalam proses *download* tersebut akan dilakukan analisa dengan menggunakan aplikasi wireshark. Hal ini bertujuan untuk mencari nilai parameter QoS nya. Berikut hasil capture analisa pengujian transfer file dengan durasi 3 menit 3 detik sebagai berikut:

Statistics			
Measurement	Captured	Displayed	Marked
Packets	3061	3061 (100.0%)	—
Time span, s	183.114	183.114	—
Average pps	16.7	16.7	—
Average packet size, B	69	69	—
Bytes	212667	212667 (100.0%)	0
Average bytes/s	1161	1161	—
Average bits/s	9291	9291	—

Gambar 4.30 Hasil Pengujian IPV4 File durasi 3 menit

- a. Pengujian *Throughput*

$$\textit{Throughput} = 221667 / 183114$$

$$\textit{Throughput} = 1,16 \text{ Bps}$$

- b. Pengujian *Delay*

$$\text{Rata – rata Delay} = 183114 / 3061$$

$$\text{Rata – rata Delay} = 0,059 \text{ s}$$

$$\text{Rata – rata Delay} = 59,82 \text{ ms}$$

- c. Pengujian *Jitter*

$$\textit{Jitter} = (183114 - 0,059) / 3061$$

$$\textit{Jitter} = 183113,94 / 3061$$

$$\textit{Jitter} = 0,059 \text{ s}$$

$$\textit{Jitter} = 59,82 \text{ ms}$$

- d. Pengujian *Packet Loss*

$$\textit{Packet Loss} = ((3061 - 3061) / 3061) \times 100\%$$

$$\textit{Packet Loss} = 0 \%$$

Kemudian berikut hasil dari analisa transfer file dengan waktu 5 menit bisa dilihat pada gambar dibawah ini:

Statistics			
Measurement	Captured	Displayed	Marked
Packets	4922	4922 (100.0%)	—
Time span, s	299.032	299.032	—
Average pps	16.5	16.5	—
Average packet size, B	62	62	—
Bytes	305618	305618 (100.0%)	0
Average bytes/s	1022	1022	—
Average bits/s	8176	8176	—

Gambar 4.31 Hasil Pengujian IPV4 File durasi 5 menit

a. Pengujian *Throughput*

$$\text{Throughput} = 305618 / 299032$$

$$\text{Throughput} = 1,02 \text{ Bps}$$

b. Pengujian *Delay*

$$\text{Rata – rata Delay} = 299032 / 4922$$

$$\text{Rata – rata Delay} = 0,060 \text{ s}$$

$$\text{Rata – rata Delay} = 60,75 \text{ ms}$$

c. Pengujian *Jitter*

$$\text{Jitter} = (299032 - 0,060) / 4922$$

$$\text{Jitter} = 299031,94 / 4922$$

$$\text{Jitter} = 0,060 \text{ s}$$

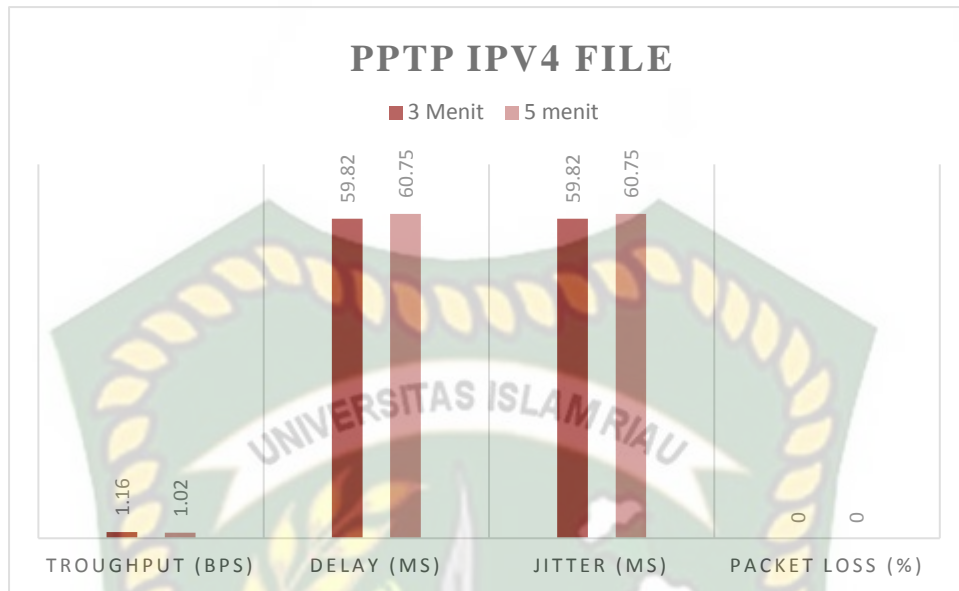
$$\text{Jitter} = 60,75 \text{ ms}$$

d. Pengujian *Packet Loss*

$$\text{Packet Loss} = ((4922 - 4922) / 4922) \times 100\%$$

$$\text{Packet Loss} = 0 \%$$

Kemudian bentuk grafik dari IPV4 PPTP file setelah dilakukan perhitungan untuk mencari parameter QoS nya bisa kita lihat pada gambar dibawah ini sebagai berikut:



Gambar 4.32 Grafik IPV4 PPTP File

4.5 Pengujian L2TP

Pengujian Ini dilakukan dengan menggunakan metode *Layer Two Tunneling Protocol* (L2TP). Subjek penelitian yang akan digunakan ialah berupa audio, video dan file. Pengujian ini dilakukan dengan menentukan durasi selama 3 dan 5 menit. Hal ini dikarenakan agar proses pengujian ini lebih menghemat waktu.

4.5.1 Pengujian IPV6

Pengujian ini dilakukan dengan menggunakan jaringan IPV6. Subjek penelitian yang digunakan ialah audio, video dan file.

a. Pengujian Audio

Pengujian ini dilakukan dengan cara sisi *client* akan mendownload file yang berada pada sisi *server*. Disini file tersebut berupa audio yang berukuran 47.5 MB dengan waktu yang digunakan selama 3 menit 50 detik. Peneliti menganalisa proses download dengan menggunakan sebuah *tools* yang

bernama wireshark. Hal itu bertujuan untuk mencari hasil parameter QoS nya dengan data berupa nilai. Berikut hasil dari analisa transfer data IPV6 L2TP audio bisa dilihat pada gambar dibawah ini:

Statistics			
Measurement	Captured	Displayed	Marked
Packets	3098	3098 (100.0%)	—
Time span, s	350.285	350.285	—
Average pps	8.8	8.8	—
Average packet size, B	74	74	—
Bytes	229603	229603 (100.0%)	0
Average bytes/s	655	655	—
Average bits/s	5243	5243	—

Gambar 4.33 Hasil Pengujian IPV6 L2TP Audio durasi 3 menit

a. Pengujian *Troughput*

$$\textit{Throughput} = 229603 / 350285$$

$$\textit{Throughput} = 0,65 \text{ Bps}$$

b. Pengujian *Delay*

$$\text{Rata – rata Delay} = 350285 / 3098$$

$$\text{Rata – rata Delay} = 0,113 \text{ s}$$

$$\text{Rata – rata Delay} = 113,06 \text{ ms}$$

c. Pengujian *Jitter*

$$\textit{Jitter} = (350285 - 0,113) / 3098$$

$$\textit{Jitter} = 350284,88 / 3098$$

$$\textit{Jitter} = 0,113 \text{ s}$$

$$\textit{Jitter} = 113,06 \text{ ms}$$

d. Pengujian *Packet Loss*

$$\textit{Packet Loss} = ((3098-3098) / 3098) \times 100\%$$

$$\textit{Packet Loss} = 0 \%$$

Kemudian hasil pengujian dengan durasi 5 menit 33 detik bisa dilihat pada gambar berikut ini:

Statistics			
Measurement	Captured	Displayed	Marked
Packets	4402	4402 (100.0%)	—
Time span, s	333.313	333.313	—
Average pps	13.2	13.2	—
Average packet size, B	52	52	—
Bytes	228235	228235 (100.0%)	0
Average bytes/s	684	684	—
Average bits/s	5477	5477	—

Gambar 4.34 Hasil Pengujian IPV6 L2TP audio durasi 5 menit

a. Pengujian *Throughput*

$$\textit{Throughput} = 228235 / 333313$$

$$\textit{Throughput} = 0,68 \text{ Bps}$$

b. Pengujian *Delay*

$$\text{Rata – rata Delay} = 333313 / 4402$$

$$\text{Rata – rata Delay} = 0,075 \text{ s}$$

$$\text{Rata – rata Delay} = 75,71 \text{ ms}$$

c. Pengujian *Jitter*

$$\textit{Jitter} = (333313 - 0,075) / 4402$$

$$\textit{Jitter} = 333312,92 / 4402$$

$$\textit{Jitter} = 0,075 \text{ s}$$

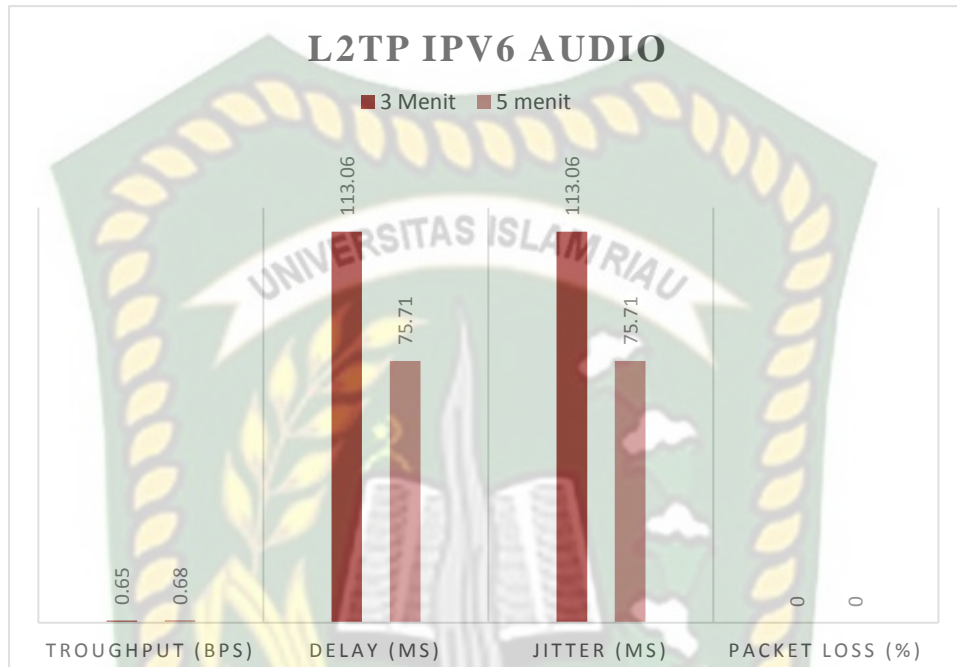
$$\textit{Jitter} = 75,71 \text{ ms}$$

d. Pengujian *Packet Loss*

$$\textit{Packet Loss} = ((4402 - 4402) / 4402) \times 100\%$$

$$\textit{Packet Loss} = 0 \%$$

Kemudian berikut bentuk grafik setelah dilakukan perhitungan untuk mencari QoS nya bisa dilihat pada gambar dibawah ini:



Gambar 4.35 Grafik IPV6 L2TP Audio

b. Pengujian Video

Cara melakukan pengujian ini yaitu pada sisi *client* akan mengunduh sebuah paket data berupa video berukuran 84.7 MB yang dimana file tersebut asalnya berada pada sisi *server*, kemudian proses unduhan akan dianalisa dengan durasi 3 menit 22 detik. Cara menganalisanya dengan menggunakan *tools* yang bernama wireshark untuk mencari perhitungan parameter QoS nya, yang dimana hasil tersebut akan ditampilkan dalam bentuk nilai. Berikut hasil capture dari analisa pengujian IPV6 L2TP video dengan durasi 3 menit sebagai berikut:

Statistics			
Measurement	Captured	Displayed	Marked
Packets	3173	3173 (100.0%)	—
Time span, s	202.002	202.002	—
Average pps	15.7	15.7	—
Average packet size, B	52	52	—
Bytes	166418	166418 (100.0%)	0
Average bytes/s	823	823	—
Average bits/s	6590	6590	—

Gambar 4.36 Hasil Pengujian IPV6 L2TP video durasi 3 menit

a. Pengujian *Troughput*

$$\textit{Throughput} = 166418 / 202002$$

$$\textit{Throughput} = 0,82 \text{ Bps}$$

b. Pengujian *Delay*

$$\text{Rata – rata } \textit{Delay} = 202002 / 3173$$

$$\text{Rata – rata } \textit{Delay} = 0,063 \text{ s}$$

$$\text{Rata – rata } \textit{Delay} = 63,66 \text{ ms}$$

c. Pengujian *Jitter*

$$\textit{Jitter} = (202002 - 0,063) / 3173$$

$$\textit{Jitter} = 202001,93 / 3173$$

$$\textit{Jitter} = 0,063 \text{ s}$$

$$\textit{Jitter} = 63,66 \text{ ms}$$

d. Pengujian *Packet Loss*

$$\textit{Packet Loss} = ((3173 - 3173) / 3173) \times 100\%$$

$$\textit{Packet Loss} = 0 \%$$

Kemudian hasil pengujian dengan durasi 5 menit 1 detik bisa dilihat pada gambar berikut ini:

Statistics			
Measurement	Captured	Displayed	Marked
Packets	5043	5043 (100.0%)	—
Time span, s	301.240	301.240	—
Average pps	16.7	16.7	—
Average packet size, B	63	63	—
Bytes	316099	316099 (100.0%)	0
Average bytes/s	1049	1049	—
Average bits/s	8394	8394	—

Gambar 4.37 Hasil Pengujian IPV6 L2TP Video durasi 5 menit

a. Pengujian *Throughput*

$$\textit{Throughput} = 316099 / 301240$$

$$\textit{Throughput} = 1,04 \text{ Bps}$$

b. Pengujian *Delay*

$$\text{Rata – rata Delay} = 301240 / 5043$$

$$\text{Rata – rata Delay} = 0,059 \text{ s}$$

$$\text{Rata – rata Delay} = 59,73 \text{ ms}$$

c. Pengujian *Jitter*

$$\textit{Jitter} = (301240 - 0,059) / 5043$$

$$\textit{Jitter} = 301239,94 / 5043$$

$$\textit{Jitter} = 0,059 \text{ s}$$

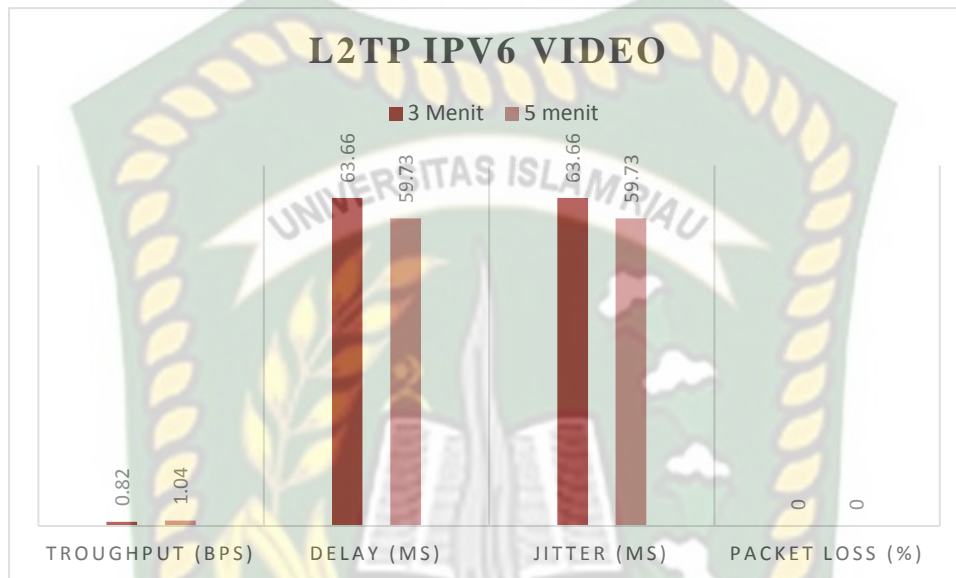
$$\textit{Jitter} = 59,73 \text{ ms}$$

d. Pengujian *Packet Loss*

$$\textit{Packet Loss} = ((5043 - 5043) / 5043) \times 100\%$$

$$\textit{Packet Loss} = 0 \%$$

Kemudian bentuk grafik dari IPV6 L2TP video setelah dilakukan perhitungan untuk mencari parameter QoS nya bisa kita lihat pada gambar dibawah ini sebagai berikut:



Gambar 4.38 Grafik IPV6 L2TP Video

c. Pengujian File

Pengujian ini dilakukan dengan cara sisi *client* akan *mendownload* sebuah paket data berupa file berukuran 2.32 GB yang berada dari sisi *server*. Dan langkah selanjutnya dalam proses *download* tersebut akan dilakukan analisa dengan menggunakan aplikasi wireshark. Hal ini bertujuan untuk mencari nilai parameter QoS nya. Didalam pengujian ini peneliti menggunakan durasi selama 3 menit 3 detik. Berikut hasil capture analisa pengujian transfer file sebagai berikut:

Statistics			
Measurement	Captured	Displayed	Marked
Packets	3169	3169 (100.0%)	—
Time span, s	183,562	183,562	—
Average pps	17,3	17,3	—
Average packet size, B	50	50	—
Bytes	159591	159591 (100.0%)	0
Average bytes/s	869	869	—
Average bits/s	6955	6955	—

Gambar 4.39 Hasil Pengujian IPV6 L2TP File durasi 3 menit

a. Pengujian *Throughput*

$$\textit{Throughput} = 159591 / 183562$$

$$\textit{Throughput} = 0,86 \text{ Bps}$$

b. Pengujian *Delay*

$$\text{Rata – rata Delay} = 183562 / 3169$$

$$\text{Rata – rata Delay} = 0,057 \text{ s}$$

$$\text{Rata – rata Delay} = 57,92 \text{ ms}$$

c. Pengujian *Jitter*

$$\textit{Jitter} = (183562 - 0,057) / 3169$$

$$\textit{Jitter} = 183561,94 / 3169$$

$$\textit{Jitter} = 0,057 \text{ s}$$

$$\textit{Jitter} = 57,92 \text{ ms}$$

d. Pengujian *Packet Loss*

$$\textit{Packet Loss} = ((3169 - 3169) / 3169) \times 100\%$$

$$\textit{Packet Loss} = 0 \%$$

Kemudian hasil pengujian dengan durasi 5 menit bisa dilihat pada gambar berikut ini:

Statistics			
Measurement	Captured	Displayed	Marked
Packets	5457	5457 (100.0%)	—
Time span, s	300.511	300.511	—
Average pps	18.2	18.2	—
Average packet size, B	61	61	—
Bytes	331006	331006 (100.0%)	0
Average bytes/s	1101	1101	—
Average bits/s	8811	8811	—

Gambar 4.40 Hasil Pengujian IPv6 L2TP File durasi 5 menit

a. Pengujian *Throughput*

$$\textit{Throughput} = 331006 / 300511$$

$$\textit{Throughput} = 1,10 \text{ Bps}$$

b. Pengujian *Delay*

$$\text{Rata – rata Delay} = 300511 / 5457$$

$$\text{Rata – rata Delay} = 0,055 \text{ s}$$

$$\text{Rata – rata Delay} = 55,06 \text{ ms}$$

c. Pengujian *Jitter*

$$\textit{Jitter} = (300511 - 0,055) / 5457$$

$$\textit{Jitter} = 300510,94 / 5457$$

$$\textit{Jitter} = 0,055 \text{ s}$$

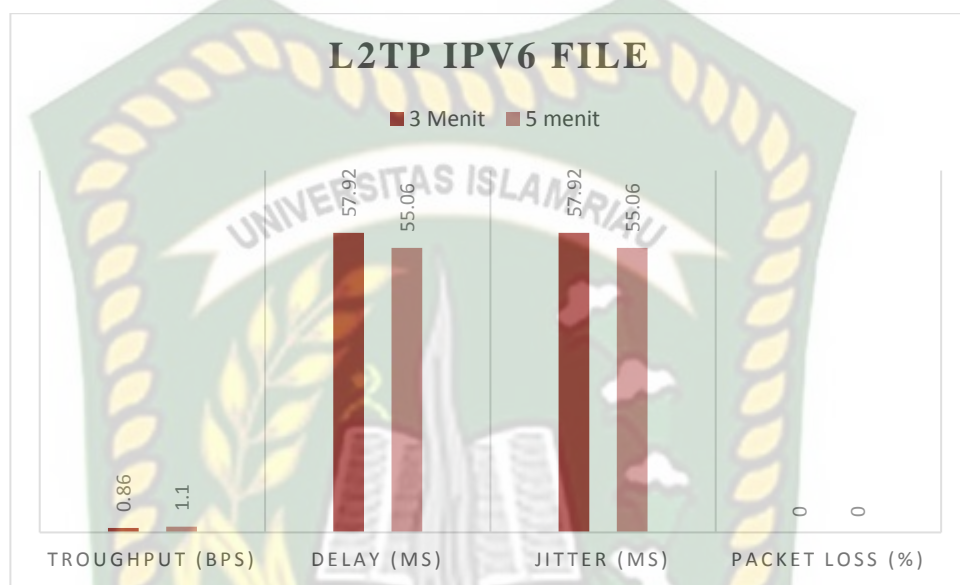
$$\textit{Jitter} = 55,06 \text{ ms}$$

d. Pengujian *Packet Loss*

$$\textit{Packet Loss} = ((5457 - 5457) / 5457) \times 100\%$$

$$\textit{Packet Loss} = 0 \%$$

Kemudian bentuk grafik dari IPV6 L2TP file setelah dilakukan perhitungan untuk mencari parameter QoS nya bisa kita lihat pada gambar dibawah ini sebagai berikut:



Gambar 4.41 Grafik IPV6 L2TP File

4.5.2 Pengujian IPV4

a. Pengujian audio

Pengujian ini dilakukan dengan cara sisi *client* akan mendownload file yang berada pada sisi *server*. Disini file tersebut berupa audio berukuran 47.5 MB Dengan durasi selama 3 menit 12 detik. Peneliti menganalisa proses download dengan menggunakan sebuah *tools* yang bernama wireshark. Hal itu bertujuan untuk mencari hasil parameter QoS nya dengan data berupa nilai. Berikut hasil dari analisa transfer data IPV4 L2TP audio bisa dilihat pada gambar dibawah ini:

Statistics			
Measurement	Captured	Displayed	Marked
Packets	3058	3058 (100.0%)	—
Time span, s	192.522	192.522	—
Average pps	15.9	15.9	—
Average packet size, B	52	52	—
Bytes	159094	159094 (100.0%)	0
Average bytes/s	826	826	—
Average bits/s	6610	6610	—

Gambar 4.42 Hasil Pengujian IPV4 L2TP Audio durasi 3 menit

a. Pengujian *Throughput*

$$\textit{Throughput} = 159094 / 192522$$

$$\textit{Throughput} = 0,82 \text{ Bps}$$

b. Pengujian *Delay*

$$\text{Rata – rata Delay} = 192522 / 3058$$

$$\text{Rata – rata Delay} = 0,062 \text{ s}$$

$$\text{Rata – rata Delay} = 62,95 \text{ ms}$$

c. Pengujian *Jitter*

$$\textit{Jitter} = (192522 - 0,062) / 3058$$

$$\textit{Jitter} = 192521,93 / 3058$$

$$\textit{Jitter} = 0,062 \text{ s}$$

$$\textit{Jitter} = 62,95 \text{ ms}$$

d. Pengujian *Packet Loss*

$$\textit{Packet Loss} = ((3058 - 3058) / 3058) \times 100\%$$

$$\textit{Packet Loss} = 0 \%$$

Kemudian hasil pengujian dengan durasi 5 menit 5 detik bisa dilihat pada gambar berikut ini:

Statistics			
Measurement	Captured	Displayed	Marked
Packets	5310	5310 (100.0%)	—
Time span, s	305.963	305.963	—
Average pps	17.4	17.4	—
Average packet size, B	101	101	—
Bytes	536673	536673 (100.0%)	0
Average bytes/s	1754	1754	—
Average bits/s	14k	14k	—

Gambar 4.43 Hasil Pengujian IPV4 L2TP Audio durasi 5 menit

a. Pengujian *Throughput*

$$\textit{Throughput} = 536673 / 305963$$

$$\textit{Throughput} = 1,75 \text{ Bps}$$

b. Pengujian *Delay*

$$\text{Rata – rata Delay} = 305963 / 5310$$

$$\text{Rata – rata Delay} = 0,057 \text{ s}$$

$$\text{Rata – rata Delay} = 57,62 \text{ ms}$$

c. Pengujian *Jitter*

$$\textit{Jitter} = (305963 - 0,057) / 5310$$

$$\textit{Jitter} = 305962,94 / 5310$$

$$\textit{Jitter} = 0,057 \text{ s}$$

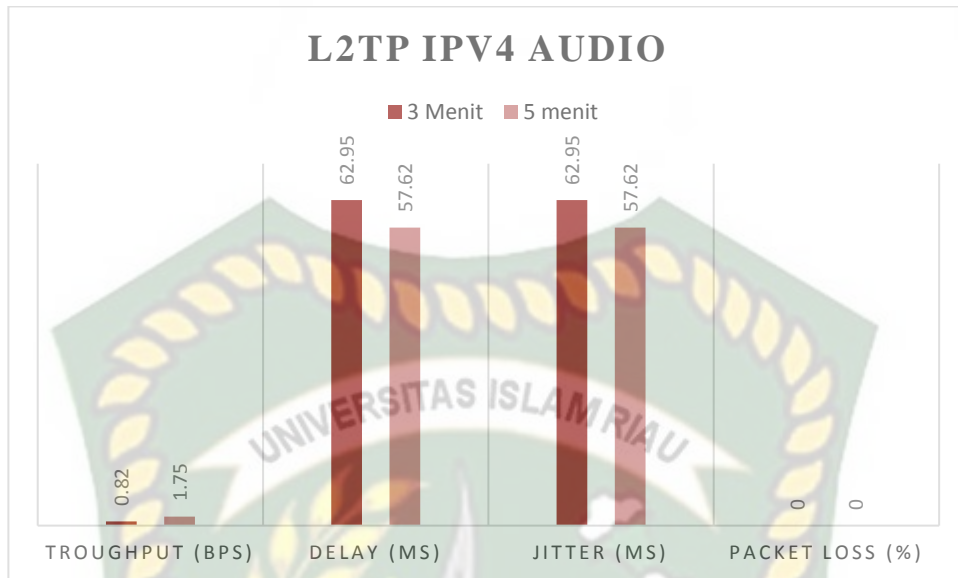
$$\textit{Jitter} = 57,62 \text{ ms}$$

d. Pengujian *Packet Loss*

$$\textit{Packet Loss} = ((5310 - 5310) / 5310) \times 100\%$$

$$\textit{Packet Loss} = 0 \%$$

Kemudian berikut bentuk grafik setelah dilakukan perhitungan untuk mencari QoS nya bisa dilihat pada gambar dibawah ini:



Gambar 4.44 Grafik IPV4 L2TP Audio

b. Pengujian Video

Cara melakukan pengujian ini yaitu pada sisi *client* akan mengunduh sebuah paket data berupa video berukuran 84.7 MB yang dimana file tersebut asalnya berada pada sisi *server*, kemudian proses unduhan akan dianalisa dengan durasi selama 3 menit 6 detik. Cara menganalisanya dengan menggunakan *tools* yang bernama wireshark untuk mencari perhitungan parameter QoS nya, yang dimana hasil tersebut akan ditampilkan dalam bentuk nilai. Berikut hasil capture dari analisa pengujian IPV4 L2TP video sebagai berikut:

Measurement	Captured	Displayed	Marked
Packets	3342	3342 (100.0%)	—
Time span, s	186.871	186.871	—
Average pps	17.9	17.9	—
Average packet size, B	68	68	—
Bytes	227959	227959 (100.0%)	0
Average bytes/s	1219	1219	—
Average bits/s	9758	9758	—

Gambar 4.45 Hasil Pengujian IPV4 L2TP video durasi 3 menit

a. Pengujian *Throughput*

$$\text{Throughput} = 227959 / 186871$$

$$\text{Throughput} = 1,21 \text{ Bps}$$

b. Pengujian *Delay*

$$\text{Rata – rata Delay} = 186671 / 3342$$

$$\text{Rata – rata Delay} = 0,055 \text{ s}$$

$$\text{Rata – rata Delay} = 55,91 \text{ ms}$$

c. Pengujian *Jitter*

$$\text{Jitter} = (186671 - 0,055) / 3342$$

$$\text{Jitter} = 186670,94 / 3342$$

$$\text{Jitter} = 0,055 \text{ s}$$

$$\text{Jitter} = 55,85 \text{ ms}$$

d. Pengujian *Packet Loss*

$$\text{Packet Loss} = ((3342 - 3342) / 3342) \times 100\%$$

$$\text{Packet Loss} = 0 \%$$

Kemudian hasil pengujian dengan durasi 5 menit 1 detik bisa dilihat pada gambar berikut ini:

Statistics			
<u>Measurement</u>	<u>Captured</u>	<u>Displayed</u>	<u>Marked</u>
Packets	4973	4973 (100.0%)	—
Time span, s	301.982	301.982	—
Average pps	16.5	16.5	—
Average packet size, B	52	52	—
Bytes	256590	256590 (100.0%)	0
Average bytes/s	849	849	—
Average bits/s	6797	6797	—

Gambar 4.46 Hasil Pengujian IPV4 L2TP Video durasi 5 menit

a. Pengujian *Throughput*

$$\textit{Throughput} = 256590 / 301982$$

$$\textit{Throughput} = 0,84 \text{ Bps}$$

b. Pengujian *Delay*

$$\text{Rata – rata } \textit{Delay} = 301982 / 4973$$

$$\text{Rata – rata } \textit{Delay} = 0,060 \text{ s}$$

$$\text{Rata – rata } \textit{Delay} = 60,72 \text{ ms}$$

c. Pengujian *Jitter*

$$\textit{Jitter} = (301982 - 0,060) / 4973$$

$$\textit{Jitter} = 301981,94 / 4973$$

$$\textit{Jitter} = 0,060 \text{ s}$$

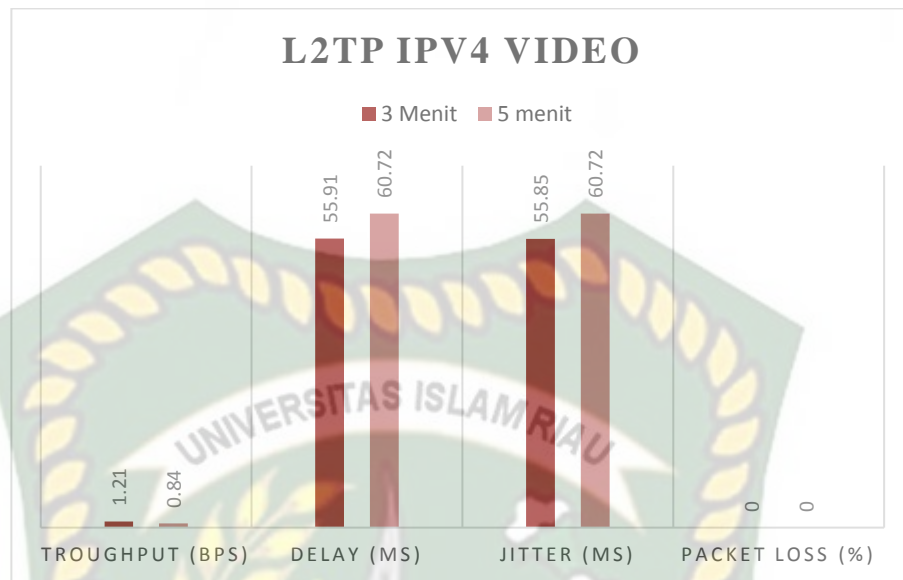
$$\textit{Jitter} = 60,72 \text{ ms}$$

d. Pengujian *Packet Loss*

$$\textit{Packet Loss} = ((4973 - 4973) / 4973) \times 100\%$$

$$\textit{Packet Loss} = 0 \%$$

Kemudian bentuk grafik dari IPV6 L2TP video setelah dilakukan perhitungan untuk mencari parameter QoS nya bisa kita lihat pada gambar dibawah ini sebagai berikut:



Gambar 4.47 Grafik IPV4 L2TP Video

c. Pengujian File

Pengujian ini dilakukan dengan cara sisi *client* akan mendownload sebuah paket data berupa file yang berada dari sisi *server*. Dan langkah selanjutnya dalam proses download tersebut akan dilakukan analisa dengan menggunakan aplikasi wireshark. Hal ini bertujuan untuk mencari nilai parameter QoS nya. Didalam pengujian ini peneliti menggunakan durasi selama 3 menit. Berikut hasil capture analisa pengujian transfer file sebagai berikut:

Statistics			
Measurement	Captured	Displayed	Marked
Packets	3129	3129 (100.0%)	—
Time span, s	179.711	179.711	—
Average pps	17.4	17.4	—
Average packet size, B	51	51	—
Bytes	158533	158533 (100.0%)	0
Average bytes/s	882	882	—
Average bits/s	7057	7057	—

Gambar 4.48 Hasil Pengujian IPV4 L2TP File durasi 3 menit

a. Pengujian *Throughput*

$$\text{Throughput} = 158533 / 179711$$

$$\text{Throughput} = 0,88 \text{ Bps}$$

b. Pengujian *Delay*

$$\text{Rata – rata Delay} = 179711 / 3129$$

$$\text{Rata – rata Delay} = 0,057 \text{ s}$$

$$\text{Rata – rata Delay} = 57,43 \text{ ms}$$

c. Pengujian *Jitter*

$$\text{Jitter} = (179711 - 0,057) / 3129$$

$$\text{Jitter} = 179710,94 / 3129$$

$$\text{Jitter} = 0,057 \text{ s}$$

$$\text{Jitter} = 57,43 \text{ ms}$$

d. Pengujian *Packet Loss*

$$\text{Packet Loss} = ((3129 - 3129) / 3129) \times 100\%$$

$$\text{Packet Loss} = 0 \%$$

Kemudian hasil pengujian dengan durasi 5 menit bisa dilihat pada gambar berikut ini:

Measurement	Captured	Displayed	Marked
Packets	5262	5262 (100.0%)	—
Time span, s	307.895	307.895	—
Average pps	17.1	17.1	—
Average packet size, B	62	62	—
Bytes	324953	324953 (100.0%)	0
Average bytes/s	1055	1055	—
Average bits/s	8443	8443	—

Gambar 4.49 Hasil Pengujian IPV4 L2TP File durasi 5 menit

a. Pengujian *Troughput*

$$\textit{Throughput} = 324953 / 307895$$

$$\textit{Throughput} = 1,05 \text{ Bps}$$

b. Pengujian *Delay*

$$\text{Rata – rata } \textit{Delay} = 307895 / 5262$$

$$\text{Rata – rata } \textit{Delay} = 0,058 \text{ s}$$

$$\text{Rata – rata } \textit{Delay} = 58,51 \text{ ms}$$

c. Pengujian *Jitter*

$$\textit{Jitter} = (307895 - 0,058) / 5262$$

$$\textit{Jitter} = 307894,94 / 5262$$

$$\textit{Jitter} = 0,058 \text{ s}$$

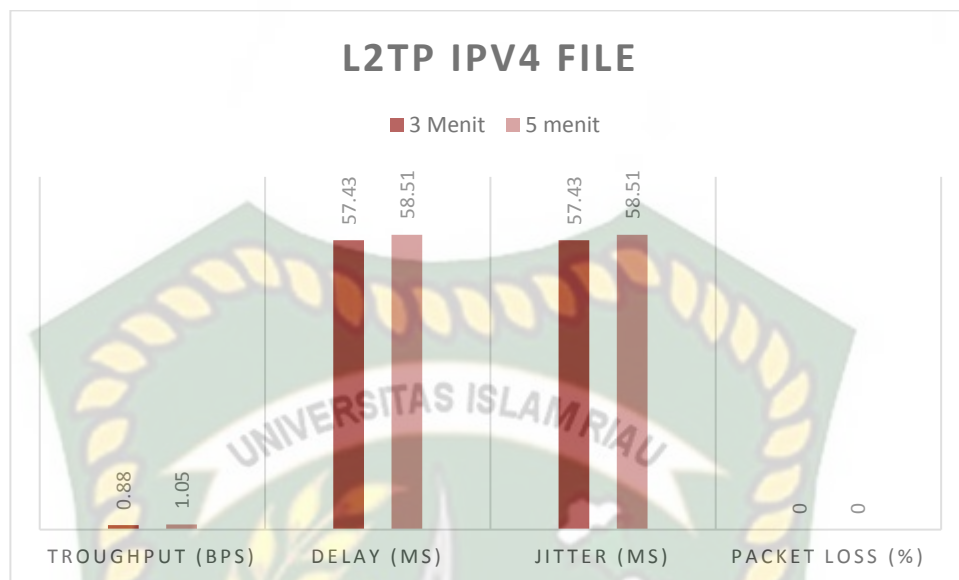
$$\textit{Jitter} = 58,51 \text{ ms}$$

d. Pengujian *Packet Loss*

$$\textit{Packet Loss} = ((5262 - 5262) / 5262) \times 100\%$$

$$\textit{Packet Loss} = 0 \%$$

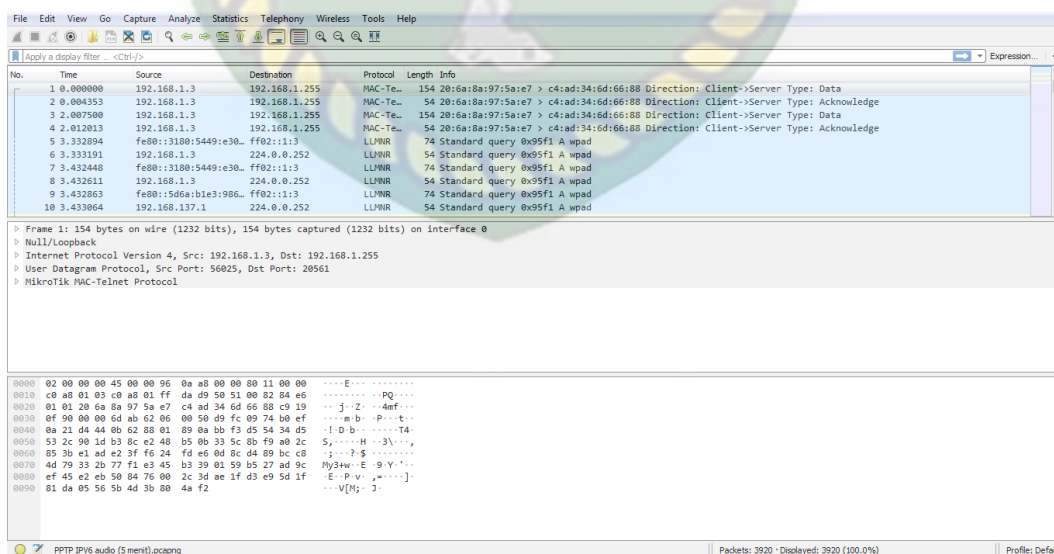
Kemudian bentuk grafik dari IPV4 L2TP file setelah dilakukan perhitungan untuk mencari parameter QoS nya bisa kita lihat pada gambar dibawah ini sebagai berikut:



Gambar 4.50 Grafik IPV4 L2TP File

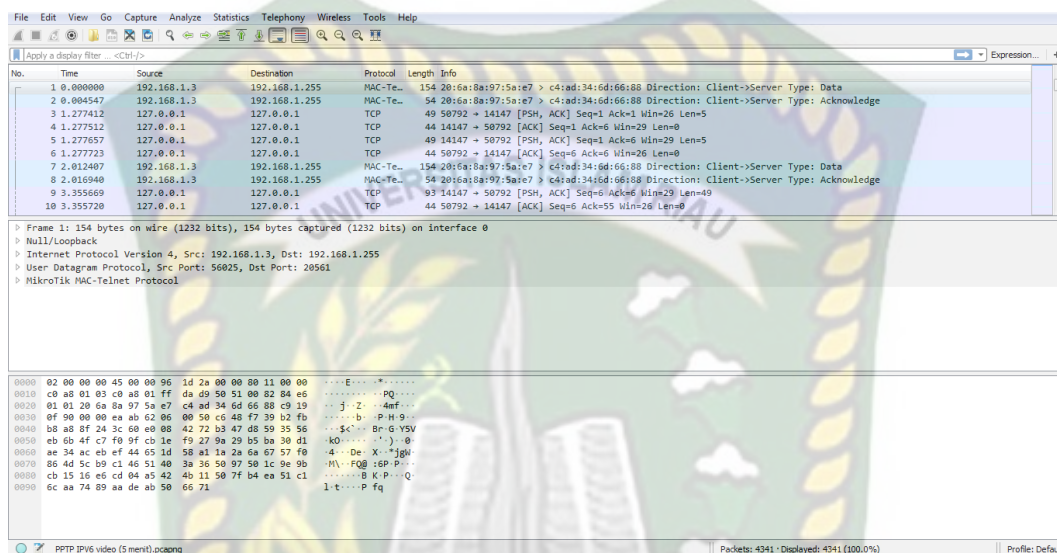
4.6 Hasil Dari Proses Transfer Data yang Terekam Di Wireshark

Pada tahapan metode PPTP, hasil dari proses transfer data dari *server* ke *client* dengan menggunakan VPN yang berupa audio, video dan file terekam pada Wireshark. Dan bentuk paket yang terekam pada Wireshark dapat dilihat pada gambar berikut ini:



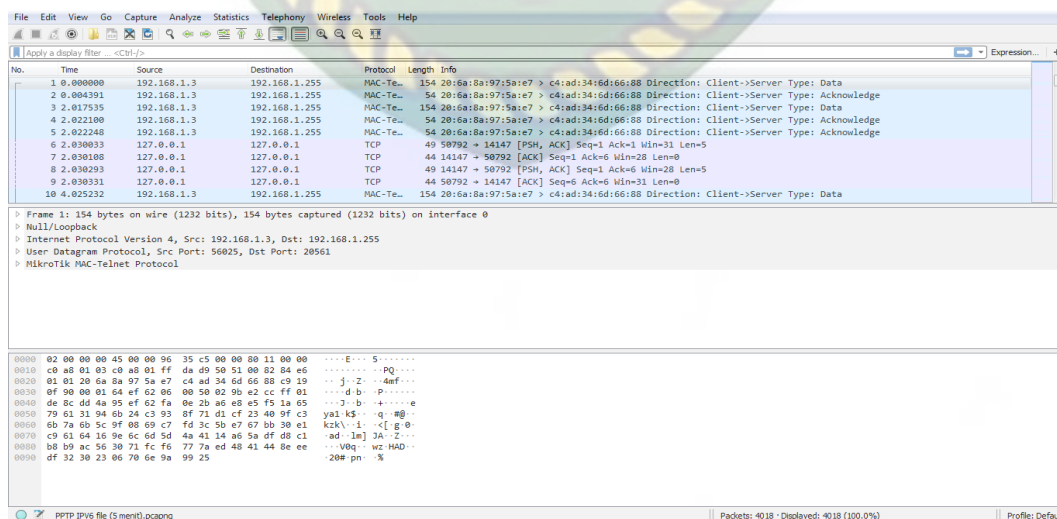
Gambar 4.51 Hasil dari Paket Transfer Audio PPTP

Kemudian setelah proses pengujian audio, dilakukan pengujian transfer paket video. Bentuk paket nya bisa dilihat pada gambar dibawah ini yaitu:



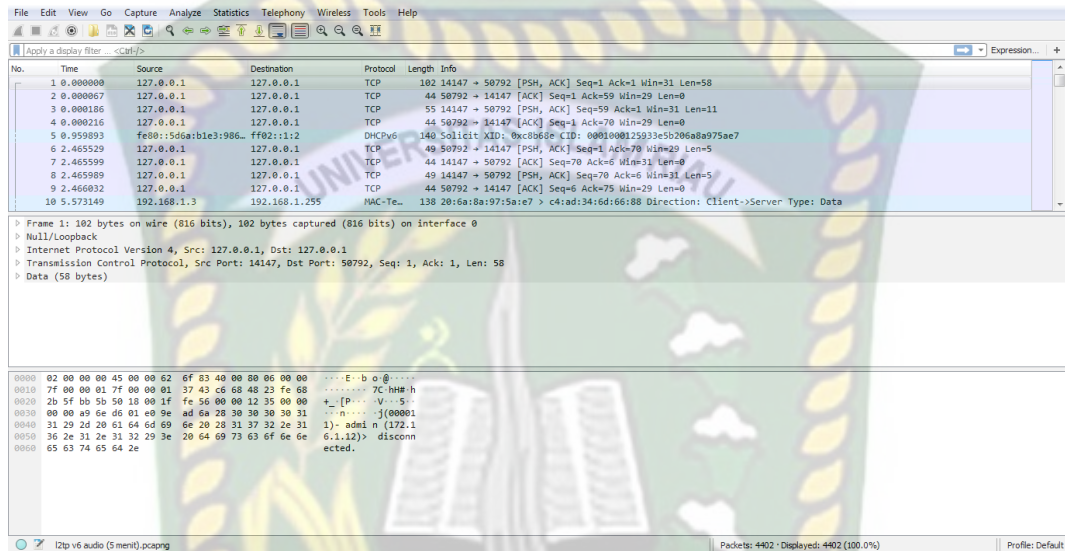
Gambar 4.52 Hasil Dari Transfer Paket Video PPTP

Selanjutnya pengujian dilakukan pada transfer paket berupa sebuah file. Bentuk paket yang terekam pada wireshark bisa dilihat pada gambar berikut ini:



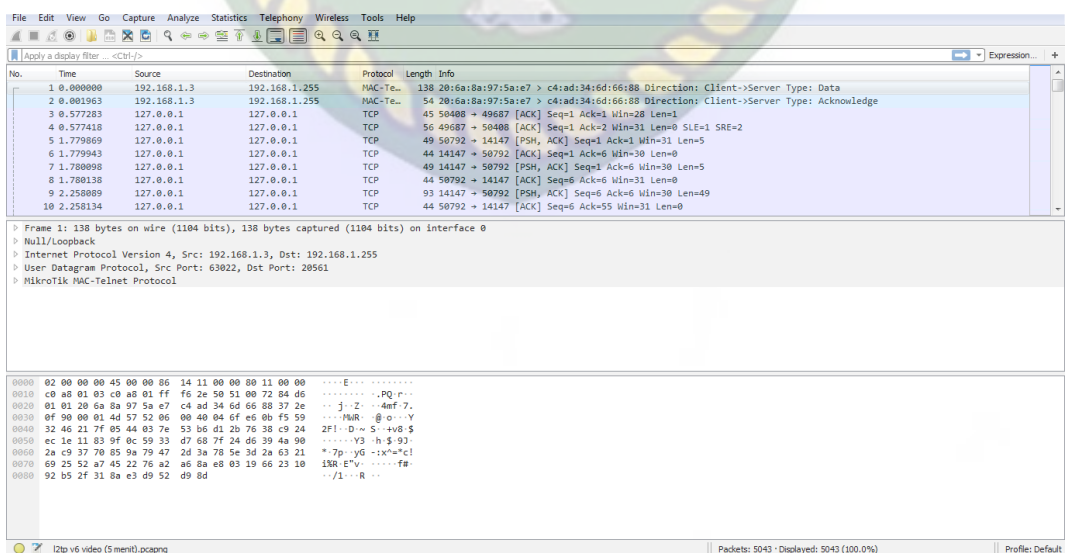
Gambar 4.53 Hasil Dari Transfer Paket File PPTP

Kemudian proses transfer data pada metode L2TP VPN, yaitu berupa paket audio, video dan file. Untuk melihat hasil dari proses transfer data yang telah terekam pada wireshark bisa dilihat pada gambar berikut ini:



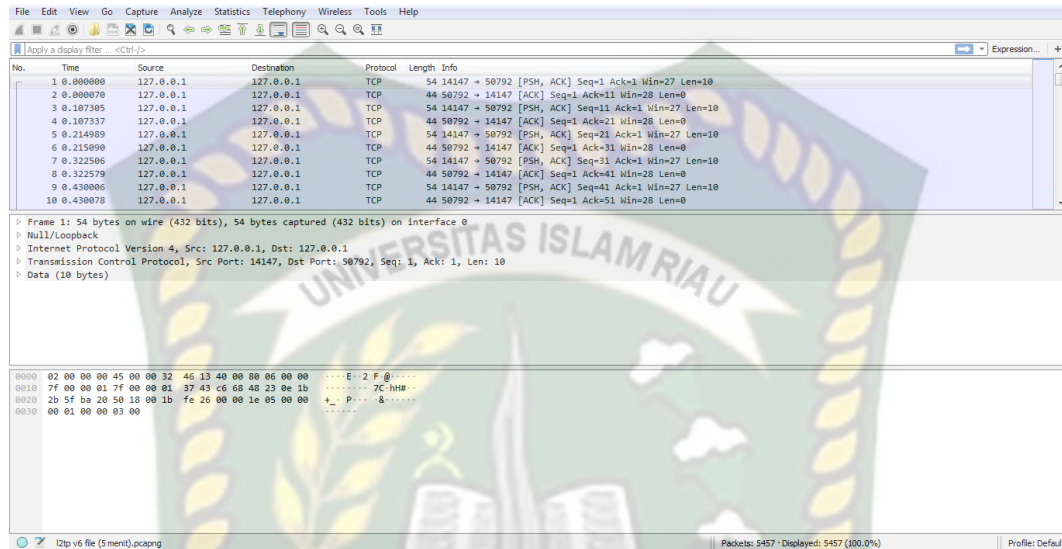
Gambar 4.54 Hasil Dari Transfer Paket Audio L2TP

Selanjutnya, bentuk paket yang terekam disaat proses pengujian video L2TP bisa dilihat pada gambar berikut ini:



Gambar 4.55 Hasil Dari Transfer Paket Video L2TP

Pada tahap selanjutnya, paket yang terekam di wireshark berupa proses transfer file bisa dilihat pada gambar berikut ini:



Gambar 4.56 Hasil Dari Transfer Paket File L2TP

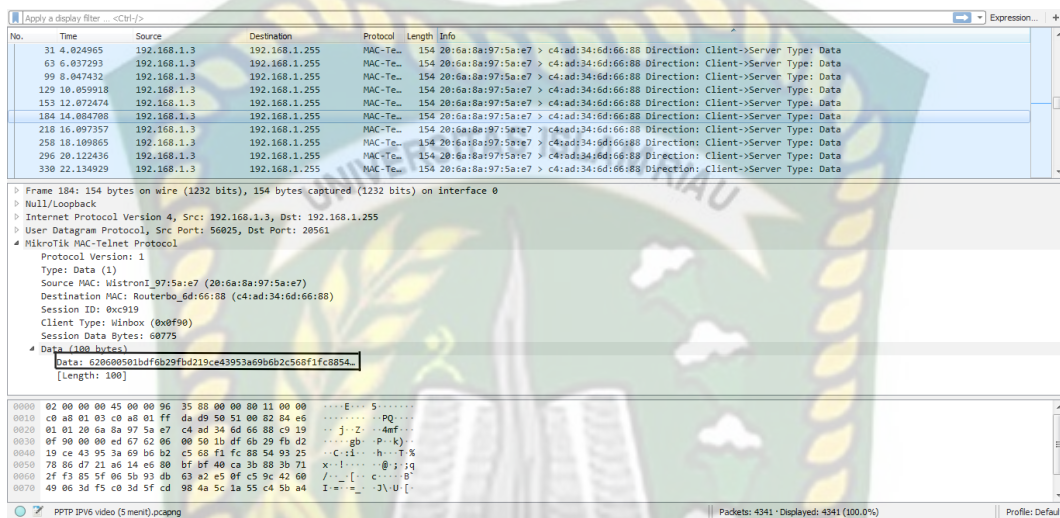
Berdasarkan analisa VPN pada kedua *tunneling* tersebut, paket data yang telah ditransfer tersebut diterima dengan baik pada sisi *client*, baik pada metode PPTP maupun L2TP. Hanya saja letak perbedaannya terdapat pada saat perhitungan parameter QoS nya. Yakni nilai yang didapat setelah dilakukan perhitungan pada hasil yang terekam pada wireshark. Dari segi keamanannya terkhusus pada PPTP rentan untuk diblokir dan tidak cocok dijadikan keamanan online. Berbeda halnya dengan metode L2TP.

4.7 Hasil Enkripsi Pada Wireshark

Pada bagian ini akan dijelaskan hasil dari enkripsi pada kedua metode, baik pada PPTP maupun L2TP.

4.7.1 Pengujian Pada Jaringan PPTP VPN

Pengujian ini dilakukan dengan menggunakan router mikrotik. Hal ini dilakukan dengan proses *sniffing* dari luar jaringan PPTP VPN.

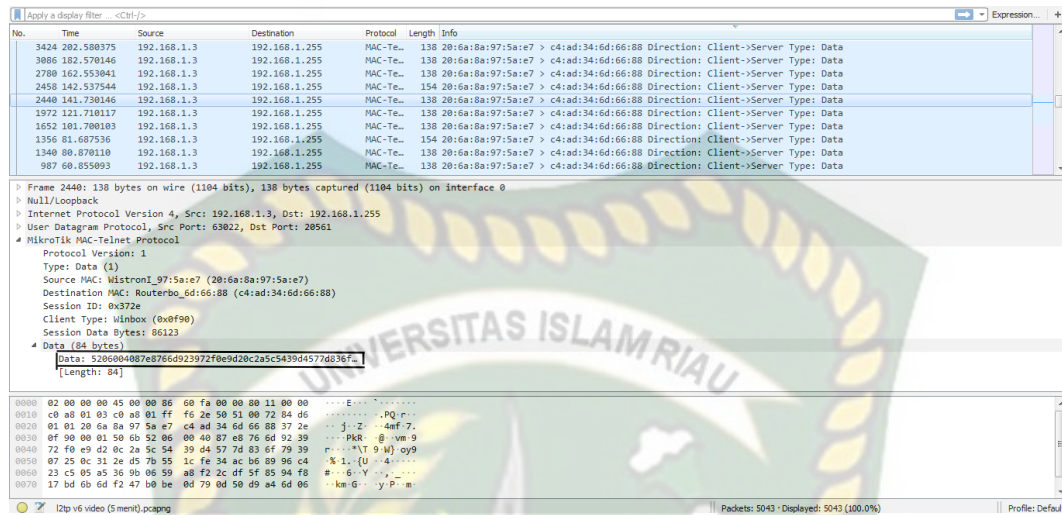


Gambar 4.57 Enkripsi Data Pada PPTP VPN

Pada pengujian ini, server mencoba melakukan koneksi ke alamat IP 192.168.1.255. Kemudian pada bagian protokol yang terlihat adalah MAC-Telnet, seperti pada gambar 4.57, dan pada keterangan dapat dilihat bahwa data telah terenkripsi.

4.7.2 Pengujian Pada Jaringan L2TP VPN

Pengujian L2TP VPN ini dilakukan dengan menggunakan router mikrotik. Hal ini dilakukan dengan *sniffing* dari luar jaringan L2TP VPN.



Gambar 4.58 Enkripsi Data Pada L2TP VPN

Pada pengujian ini, server mencoba melakukan koneksi ke alamat IP 192.168.1.255. Lalu pada bagian protokol yang terlihat adalah MAC-Telnet, seperti pada gambar 4.58, dan pada keterangan dapat dilihat bahwa data telah terenkripsi.

4.7.3 Hasil *Sniffing* Pada Metode PPTP

Tools Wireshark digunakan untuk menangkap setiap paket yang lewat diantara server dan *client* dengan metode PPTP. Konsep yang dibuat ialah server akan berkomunikasi dengan *client* dengan cara server mengirimkan data ke *client*. Hasil *sniffing* akan terlihat data yang dikirimkan server ke *client*.

No.	Time	Source	Destination	Protocol	Length	Info
2476	175.845126	127.0.0.1	127.0.0.1	TCP	54	14147 → 50792 [PSH, ACK] Seq=13836 Ack=91 Win=29 Len=10
2471	175.845195	127.0.0.1	127.0.0.1	TCP	44	50792 → 14147 [ACK] Seq=91 Ack=13846 Win=29 Len=0
2472	175.880890	192.168.1.3	192.168.1.255	MAC-Telnet	154	20:6a:8a:97:5a:e7 > c4:ad:34:6d:66:88 Direction: Client->Server Type: Data
2473	175.887818	192.168.1.3	192.168.1.255	MAC-Telnet	54	20:6a:8a:97:5a:e7 > c4:ad:34:6d:66:88 Direction: Client->Server Type: Acknowledge
2474	175.160834	127.0.0.1	127.0.0.1	TCP	54	14147 → 50792 [PSH, ACK] Seq=13848 Ack=91 Win=29 Len=10
2475	175.160104	127.0.0.1	127.0.0.1	TCP	44	50792 → 14147 [ACK] Seq=91 Ack=13856 Win=29 Len=0
2476	175.267474	127.0.0.1	127.0.0.1	TCP	54	14147 → 50792 [PSH, ACK] Seq=13856 Ack=91 Win=29 Len=10
2477	175.267544	127.0.0.1	127.0.0.1	TCP	44	50792 → 14147 [ACK] Seq=91 Ack=13866 Win=29 Len=0
2478	175.374981	127.0.0.1	127.0.0.1	TCP	54	14147 → 50792 [PSH, ACK] Seq=13866 Ack=91 Win=29 Len=10
2479	175.375847	127.0.0.1	127.0.0.1	TCP	44	50792 → 14147 [ACK] Seq=91 Ack=13876 Win=29 Len=0
2480	175.482586	127.0.0.1	127.0.0.1	TCP	54	14147 → 50792 [PSH, ACK] Seq=13876 Ack=91 Win=29 Len=10
2481	175.482575	127.0.0.1	127.0.0.1	TCP	44	50792 → 14147 [ACK] Seq=91 Ack=13886 Win=29 Len=0
2482	175.977689	192.168.1.3	239.255.255.250	SSDP	206	M-SEARCH * HTTP/1.1
2483	175.977740	192.168.137.1	239.255.255.250	SSDP	206	M-SEARCH * HTTP/1.1
2484	176.012685	127.0.0.1	127.0.0.1	TCP	63	14147 → 50792 [PSH, ACK] Seq=13886 Ack=91 Win=29 Len=19
2485	176.012768	127.0.0.1	127.0.0.1	TCP	44	50792 → 14147 [ACK] Seq=91 Ack=13905 Win=29 Len=0
2486	176.027837	127.0.0.1	127.0.0.1	TCP	54	14147 → 50792 [PSH, ACK] Seq=13905 Ack=91 Win=29 Len=10
2487	176.027710	127.0.0.1	127.0.0.1	TCP	44	50792 → 14147 [ACK] Seq=91 Ack=13915 Win=29 Len=0
2488	176.580100	127.0.0.1	127.0.0.1	TCP	54	14147 → 50792 [PSH, ACK] Seq=13915 Ack=91 Win=29 Len=10
2489	176.580176	127.0.0.1	127.0.0.1	TCP	44	50792 → 14147 [ACK] Seq=91 Ack=13925 Win=29 Len=0
2490	176.980082	192.168.1.3	239.255.255.250	SSDP	206	M-SEARCH * HTTP/1.1
2491	176.980220	192.168.137.1	239.255.255.250	SSDP	206	M-SEARCH * HTTP/1.1
2492	177.009921	127.0.0.1	127.0.0.1	TCP	54	14147 → 50792 [PSH, ACK] Seq=13925 Ack=91 Win=29 Len=10
2493	177.009982	127.0.0.1	127.0.0.1	TCP	44	50792 → 14147 [ACK] Seq=91 Ack=13935 Win=29 Len=0
2494	177.027470	127.0.0.1	127.0.0.1	TCP	63	14147 → 50792 [PSH, ACK] Seq=13935 Ack=91 Win=29 Len=19
2495	177.027534	127.0.0.1	127.0.0.1	TCP	44	50792 → 14147 [ACK] Seq=91 Ack=13954 Win=29 Len=0
2496	177.095094	192.168.1.3	192.168.1.255	MAC-Telnet	154	20:6a:8a:97:5a:e7 > c4:ad:34:6d:66:88 Direction: Client->Server Type: Data
2497	177.095972	192.168.1.3	192.168.1.255	MAC-Telnet	54	20:6a:8a:97:5a:e7 > c4:ad:34:6d:66:88 Direction: Client->Server Type: Acknowledge
2498	177.128179	127.0.0.1	127.0.0.1	TCP	54	14147 → 50792 [PSH, ACK] Seq=13954 Ack=91 Win=29 Len=10
2499	177.128256	127.0.0.1	127.0.0.1	TCP	44	50792 → 14147 [ACK] Seq=91 Ack=13964 Win=29 Len=0
2500	177.780841	127.0.0.1	127.0.0.1	TCP	54	14147 → 50792 [PSH, ACK] Seq=13964 Ack=91 Win=29 Len=10
2501	177.780891	127.0.0.1	127.0.0.1	TCP	44	50792 → 14147 [ACK] Seq=91 Ack=13974 Win=29 Len=0

Gambar 4.59 Hasil Pengujian Pada Metode PPTP

Hasil *sniffing* pada gambar 4.59 memperlihatkan bahwa terdapat beberapa protokol yang tertangkap yaitu: MAC-Telnet, TCP dan SSDP. *Source* yaitu alamat asal dan sedangkan *destination* merupakan alamat yang dituju.

4.7.4 Hasil Sniffing Pada Metode L2TP

Tools Wireshark digunakan untuk menangkap setiap paket yang lewat diantara server dan *client* menggunakan metode L2TP. Konsep yang dibuat ialah server akan berkomunikasi dengan *client* dengan cara server mengirimkan data ke *client*. Hasil *sniffing* akan terlihat data yang dikirimkan server ke *client*.

The screenshot shows a Wireshark capture of network traffic. The main pane displays a list of captured packets with the following columns: No., Time, Source, Destination, Protocol, Length, and Info. The traffic includes LLMNR (Standard query), NBNS (Name query), TCP (ACK, PSH), and MAC-T (Client-Server Type: Data) packets. The source and destination addresses are visible for each packet.

Gambar 4.60 Hasil Pengujian Pada Metode L2TP

Hasil *sniffing* pada gambar 4.60 memperlihatkan bahwa terdapat beberapa protokol yang tertangkap yaitu: LLMNR, NBNS, TCP dan MAC - Telnet. *Source* yaitu alamat asal dan sedangkan *destination* merupakan alamat yang dituju.

4.8 Tabel Perbandingan Hasil Pengujian PPTP Dan L2TP

4.8.1 Tabel Perbandingan IPV6

Tabel 4.1 Hasil Pengujian PPTP Dan L2TP Dengan IPV6

Durasi	Subjek	PPTP				L2TP			
		Throughput	Delay	Jitter	Packet Loss	Throughput	Delay	Jitter	Packet Loss
3 Menit	Audio	0.72 bps	77.62 ms	77.62 ms	0 %	0.65 bps	113.06 ms	113.06 ms	0 %
	Video	1.05 bps	72.19 ms	72.19 ms	0 %	0.82 bps	63.66 ms	63.66 ms	0 %
	File	0.75 bps	73.27 ms	73.27 ms	0 %	0.86 bps	57.92 ms	57.92 ms	0 %
5 Menit	Audio	0.71 bps	78.03 ms	78.03 ms	0 %	0.68 bps	75.71 ms	75.71 ms	0 %
	Video	0.79 bps	69.6 ms	69.6 ms	0 %	1.04 bps	59.73 ms	59.73 ms	0 %
	File	0.91 bps	75.61 ms	75.61 ms	0 %	1.1 bps	55.06 ms	55.06 ms	0 %

Tabel diatas adalah hasil pengujian PPTP dan L2TP dengan menggunakan IPV6 yang diuji menggunakan *tools* yang bernama wireshark. Dan pengujian ini dilakukan dengan durasi selama 3 dan 5 menit, karena untuk lebih menghemat pada sisi waktu. Kemudian ditabel diatas, pengujian kedua *tunneling* dengan menggunakan jaringan IPV6 ini dapat dinilai bahwa PPTP unggul tipis dengan sisi *throughput* nya. Dan untuk sisi *delay* dan *jitter* nya L2TP lebih dominan. Untuk *Packet loss*, kedua *tunneling* ini mendapat nilai akhir yang sama, yaitu 0.

4.8.2 Tabel Perbandingan IPV4

Tabel 4.2 Hasil Pengujian PPTP Dan L2TP Dengan IPV4

Durasi	Subjek	PPTP				L2TP			
		Throughput	Delay	Jitter	Packet Loss	Throughput	Delay	Jitter	Packet Loss
3 Menit	Audio	0.82 bps	62.59 ms	62.59 ms	0 %	0.82 bps	62.95 ms	62.95 ms	0 %
	Video	0.79 bps	64.18 ms	64.18 ms	0 %	1.21 bps	55.91 ms	55.91 ms	0 %
	File	1.16 bps	59.82 ms	59.82 ms	0 %	0.88 bps	57.43 ms	57.43 ms	0 %
5 Menit	Audio	0.81 bps	63.58 ms	63.58 ms	0 %	1.75 bps	57.62 ms	57.62 ms	0 %
	Video	0.81 bps	63.89 ms	63.89 ms	0 %	0.84 bps	60.72 ms	60.72 ms	0 %
	File	1.02 bps	60.75 ms	60.75 ms	0 %	1.05 bps	58.51 ms	58.51 ms	0 %

Tabel diatas adalah hasil pengujian dengan jaringan IPV4 menggunakan *tools* wireshark. Kemudian subjek yang digunakan untuk analisa berupa audio, video dan file. Dan disini peneliti melakukan analisa dengan durasi selama 3 dan 5 menit. Hal ini dikarenakan agar didalam pengujian ialah salah satunya menghemat dalam segi waktu. Berdasarkan tabel diatas, dapat dijelaskan bahwa pengujian kedua *tunneling* tersebut dengan jaringan IPV4, L2TP lebih unggul pada sisi *throughput*. Terutama

pada pengujian audio durasi 5 menit, selisih nilai yang didapat ialah 0,94 bps. Pada sisi *delay* dan *jitter* L2TP juga lebih dominan.

Setelah dilakukan analisa dapat disimpulkan bahwa dari kedua metode VPN tersebut L2TP lebih baik dalam segi keamanannya maupun dari hasil perhitungan Qos yang telah dilakukan. Kemudian pada metode PPTP, jenis protokol yang terekam disaat proses transfer data dari server ke *client* ialah MAC-Telnet, TCP dan SSDP. Sedangkan pada metode L2TP, jenis protokol yang terekam pada wireshark disaat proses transfer data yang berlangsung dari server ke *client* ialah LLMNR, NBNS, MAC-Telnet dan TCP. Dengan menggunakan VPN ini, paket data yang dikirimkan tidak dapat terbaca. Jadi, pihak luar tidak dapat mengetahui jenis paket data yang telah dikirimkan.

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil analisa yang telah dilakukan pada penelitian ini, maka dapat diambil kesimpulan sebagai berikut:

1. Pada IPV6 (*Internet Protocol Versi 6*), nilai QoS (*Quality Of Service*) yang didapatkan pada tunnel L2TP (*Layer Two Tunneling Protocol*) lebih unggul dibandingkan tunnel PPTP (*Point-to-Point Tunneling Protocol*). Yaitu pada sisi *delay* dan *jitter*.
2. Pengujian pada kedua *tunneling* ini rata-rata mendapatkan nilai *delay* dan *jitter* yang sama.
3. Dalam pengujian yang dilakukan menggunakan IPV4 (*Internet Protocol Versi 4*), terutama pada durasi yang dilakukan selama 5 menit, terlihat sisi *throughput* pada tunnel L2TP unggul jauh.
4. Parameter pada sisi *packet loss* untuk pengujian kedua *tunneling* ini mendapatkan hasil yang sama yaitu 0.
5. Pengujian ini dilakukan dengan menggunakan aplikasi Filezilla dan Wireshark.

5.2 Saran

Saran yang dapat diberikan dari hasil penelitian Analisis Perbandingan Protokol *Point-to-Point Tunneling Protocol* VPN Dengan Protokol *Layer Two Tunneling Protocol* VPN Pada Jaringan IPV6 adalah sebagai berikut:

1. Diharapkan pengujian ini dikembangkan lagi dengan beberapa *client* sehingga pada sisi *server* bisa *transfer* paket data ke banyak *client*.
2. Pengujian selanjutnya perlu dicoba dengan menggunakan linux sebagai OS (*Operating System*) nya.
3. Untuk pengalamatan IP (*Internet Protocol*) *address* harus pastikan dengan benar sesuai dengan topologi perancangan.

DAFTAR PUSTAKA

- Hidayatullah., Syarif, Syafrudin. 2019. *Perancangan Wide Area Network (WAN) Dengan Teknologi Virtual Private Network (VPN)*. Vol 5, No 1 (2019).
- Ikhwan, Syariful., Ahya, Amalina. 2017. *Analisis Jaringan Virtual Private Network (VPN) Menggunakan Point-to-Point Tunneling Protocol (PPTP) dan Layer Two Tunneling Protocol (L2TP)*. Banyumas: Dinas Perhubungan, Komunikasi dan Informasi (Dinhubkominfo) Kabupaten Banyumas.
- Maryanto., Maisyaroh., dan Santoso, Budi. 2018. *Metode Internet Protocol Security (IPSec) Dengan Virtual Private Network (VPN) Untuk Komunikasi Data*. Jurnal.unismabekasi.ac.id.
- Novendra, Yoldi. 2018. *Analisis Perbandingan Kinerja Routing OSPF Dan EIGRP*. *IT Journal Research and Development*, 2 (2), 97 – 106.
- Seta, Bayu, Henki., Ridwan, Muhammad., dan Wati, Theresia. 2015. *Perbandingan Virtual Private Network (VPN) Protokol Menggunakan Point to Point Tunnel Protocol (PPTP) dan Open VPN*. *ejournal.stikom-bali*.
- Sulianto, Agus. 2018. *Analisa Perbandingan Router Cisco 7200 Dengan Router Mikrotik RB1000 Untuk Mencari Nilai Qos*, Universitas Islam Riau.
- Syafrizal, Melwin. 2005. *Pengantar Jaringan Komputer*. C.V. ANDI OFFSET.
- Triyono, joko., K, Rahcmawati, Yuliana, Rr., dan Irnawan, Fahmi, Dhimas. 2014. *Analisis Perbandingan Kinerja Jaringan Virtual Private Network (VPN) Berbasis Mikrotik Menggunakan Protokol Point-to-Point Tunneling*

Protocol (PPTP) Dan Layer Two Tunneling Protocol (L2TP) Sebagai Media Transfer Data. Institut Sains & Teknologi AKPRIND Yogyakarta.



Dokumen ini adalah Arsip Miik :

Perpustakaan Universitas Islam Riau