

**ANALISA PERBANDINGAN KUALITAS PENGIRIMAN
DATA VOIP MENGGUNAKAN METODE L2TP/IPSEC
DENGAN OPENVPN MELALUI JARINGAN PUBLIK**

Skripsi



oleh

PONANG JAGAD PRAMUDHITYA

71160005

**PROGRAM STUDI INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA YOGYAKARTA**

2020

**ANALISA PERBANDINGAN KUALITAS PENGIRIMAN
DATA VOIP MENGGUNAKAN METODE L2TP/IPSEC
DENGAN OPENVPN MELALUI JARINGAN PUBLIK**

Skripsi



Diajukan kepada Program Studi Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana
Sebagai Salah Satu Syarat dalam Memperoleh Gelar
Sarjana Komputer

Disusun oleh

PONANG JAGAD PRAMUDHITYA

71160005

PROGRAM STUDI INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA YOGYAKARTA
2020

**HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS
AKHIR UNTUK KEPENTINGAN AKADEMIS SECARA ONLINE
UNIVERSITAS KRISTEN DUTA WACANA YOGYAKARTA**

Saya yang bertanda tangan di bawah ini:

NIM : 71160005
Nama : Ponang Jagad Pramudhitya
Prodi / Fakultas : Informatika / Teknologi Informasi
Judul Tugas Akhir : Analisa Perbandingan Kualitas Pengiriman Data
VoIP menggunakan Metode L2TP/IPsec dengan
OpenVPN melalui Jaringan Publik

bersedia menyerahkan Tugas Akhir kepada Universitas melalui Perpustakaan untuk keperluan akademis dan memberikan **Hak Bebas Royalti Non Eksklusif** (*Non-exclusive Royalty-free Right*) serta bersedia Tugas Akhirnya dipublikasikan secara online dan dapat diakses secara lengkap (*full access*).

Dengan Hak Bebas Royalti Noneklusif ini Perpustakaan Universitas Kristen Duta Wacana berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk database, merawat, dan memublikasikan Tugas Akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta. Demikian pernyataan ini saya buat dengan sebenar-benarnya.

Yogyakarta, 1 Oktober 2020

Yang menyatakan,



(71160005 – Ponang Jagad Pramudhitya)

PERNYATAAN KEASLIAN SKRIPSI

Saya menyatakan dengan sesungguhnya bahwa skripsi dengan judul:

**ANALISA PERBANDINGAN KUALITAS PENGIRIMAN DATA VOIP
MENGUNAKAN METODE L2TP/IPSEC DENGAN OPENVPN
MELALUI JARINGAN PUBLIK**

yang saya kerjakan untuk melengkapi sebagian persyaratan menjadi Sarjana Komputer pada pendidikan Sarjana Program Studi Informatika Fakultas Teknologi Informasi Universitas Kristen Duta Wacana, bukan merupakan tiruan atau duplikasi dari skripsi kesarjanaan di lingkungan Universitas Kristen Duta Wacana maupun di Perguruan Tinggi atau instansi manapun, kecuali bagian yang sumber informasinya dicantumkan sebagaimana mestinya.

Jika dikemudian hari didapati bahwa hasil skripsi ini adalah hasil plagiasi atau tiruan dari skripsi lain, saya bersedia dikenai sanksi yakni pencabutan gelar kesarjanaan saya.

Yogyakarta, 7 Oktober 2020

 

PONANG JAGAD PRAMUDHITYA
71160005

HALAMAN PERSETUJUAN

Judul Skripsi : ANALISA PERBANDINGAN KUALITAS
PENGIRIMAN DATA VOIP MENGGUNAKAN
METODE L2TP/IPSEC DENGAN OPENVPN
MELALUI JARINGAN PUBLIK

Nama Mahasiswa : PONANG JAGAD PRAMUDHITYA

N I M : 71160005

Matakuliah : Skripsi (Tugas Akhir)

Kode : TIW276

Semester : Gasal

Tahun Akademik : 2020/2021

Telah diperiksa dan disetujui di
Yogyakarta,
Pada tanggal 6 November 2020

Dosen Pembimbing I


Gani Indriyanta, Ir. M.T.

Dosen Pembimbing II


Joko Purwadi, M.Kom

HALAMAN PENGESAHAN

ANALISA PERBANDINGAN KUALITAS PENGIRIMAN DATA VOIP MENGUNAKAN METODE L2TP/IPSEC DENGAN OPENVPN MELALUI JARINGAN PUBLIK

Oleh: PONANG JAGAD PRAMUDHITYA / 71160005

Dipertahankan di depan Dewan Penguji Skripsi
Program Studi Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana - Yogyakarta
Dan dinyatakan diterima untuk memenuhi salah satu syarat memperoleh gelar
Sarjana Komputer
pada tanggal 27 Oktober 2020

Yogyakarta, 6 November 2020
Mengesahkan,

Dewan Penguji:

1. Gani Indriyanta, Ir. M.T.
2. Joko Purwadi, M.Kom
3. Nugroho Agus Haryono, M.Si
4. Laurentius Kuncoro Probo Saputra, S.T.,
M.Eng.



Dekan


(Restyandito, S.Kom., MSIS., Ph.D.)

Ketua Program Studi


(Gloria Virginia, Ph.D.)

**HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI
TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS SECARA ONLINE
UNIVERSITAS KRISTEN DUTA WACANA YOGYAKARTA**

Saya yang bertanda tangan di bawah ini:

NIM : 71160005
Nama : Ponang Jagad Pramudhitya
Prodi / Fakultas : Informatika / Teknologi Informasi
Judul Tugas Akhir : Analisa Perbandingan Kualitas Pengiriman Data
VoIP menggunakan Metode L2TP/IPsec dengan
OpenVPN melalui Jaringan Publik

bersedia menyerahkan Tugas Akhir kepada Universitas melalui Perpustakaan untuk keperluan akademis dan memberikan **Hak Bebas Royalti Non Eksklusif** (*Non-exclusive Royalty-free Right*) serta bersedia Tugas Akhirnya dipublikasikan secara online dan dapat diakses secara lengkap (*full access*).

Dengan Hak Bebas Royalti Non eksklusif ini Perpustakaan Universitas Kristen Duta Wacana berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk database, merawat, dan memublikasikan Tugas Akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta. Demikian pernyataan ini saya buat dengan sebenar-benarnya.

Yogyakarta, 1 Oktober 2020

Yang menyatakan,



(71160005 – Ponang Jagad Pramudhitya)

UCAPAN TERIMA KASIH

Puji syukur kepada Tuhan Yang Maha Esa atas berkat dan penyertaan-Nya yang telah diberikan-Nya kepada penulis selama ini, terutama pada masa pengerjaan dan penulisan skripsi yang berjudul “Analisis Perbandingan Kualitas Pengiriman Data VoIP menggunakan Metode L2tp/IPsec dengan OpenVPN melalui Jaringan Publik” ini dengan lancar.

Pada kesempatan ini, penulis juga mengucapkan terima kasih yang sebesar-besarnya terhadap pihak-pihak yang membantu dan mendukung penulis selama proses penyusunan skripsi ini. Ucapan ini penulis sampaikan untuk :

1. Bapak Ir. Gani Indriyanta, M.T. selaku pembimbing I yang telah membimbing dan membantu penulis dalam mengerjakan skripsi dan selalu memberikan saran, masukan dan motivasi untuk menyelesaikan skripsi ini. Terima kasih juga karena telah membantu penulis dalam pengurusan peminjaman IP publik ke Puspindika.
2. Bapak Joko Purwadi, S.Kom., M.Kom. selaku pembimbing II yang telah membimbing dan membantu penulis dalam mengerjakan skripsi dan selalu memberikan saran, masukan dan motivasi untuk menyelesaikan skripsi ini.
3. Pengelola Asrama Babadan UKDW yang telah mengizinkan penulis untuk melakukan penelitian dan pengambilan data di tempat.
4. Bapak Abet Narisworo, S.Kom., M.Kom. selaku kepala unit PPLK dan laboran Laboratorium Komputer UKDW yang telah mengizinkan penulis untuk melakukan penelitian dan pengambilan data di tempat.
5. Bapak Danny Sebastian, S.Kom., M.M., M.T. yang sering memberikan motivasi.
6. Teman-teman yang membantu penelitian ini, Yashinta Novita D., Emanuel Norman P. W., Krissanti Dewi, Alvin Wicaksono, Wilhelmus Krisvan P., Jeffrison Banni, Sinung Purnama Aji, dan Yosef D. Nugroho.
7. Teman-teman Bakul Pecel, DalangKondang, KINE KLUB, Keluarga Burjo Sinai dan Informatika 2016.

Penulis mengucapkan banyak terima kasih kepada pihak-pihak yang mendukung penulis selama ini.

Yogyakarta, 8 Oktober 2020

KATA PENGANTAR

Puji syukur kepada Tuhan Yang Maha Esa atas berkat dan penyertaan-Nya kepada penulis sehingga penulis dapat menyelesaikan skripsi yang berjudul “Analisis Perbandingan Kualitas Pengiriman Data VoIP menggunakan Metode L2tp/IPsec dengan OpenVPN melalui Jaringan Publik” dengan lancar

Tujuan penulisan skripsi ini adalah sebagai salah satu syarat kelulusan di Fakultas Teknologi Informasi Program Studi Informatika di Universitas Kristen Duta Wacana. Skripsi ini merupakan syarat untuk mendapatkan gelar sarjana strata 1 (S1).

Penulis menyadari bahwa skripsi dan penelitian ini masih memiliki kekurangan baik dari segi penulisan, materi dan lain-lain, sehingga penulis bersedia menerima kritik dan saran yang membangun dengan tujuan untuk membuat penelitian ini menjadi lebih baik dan berguna bagi banyak pihak.

ABSTRAKSI

VoIP (*Voice-over Internet Protocol*) adalah salah satu protokol yang melayani pengiriman data suara melalui jaringan komputer. Komunikasi VoIP diharapkan dapat dilakukan pada setiap lokasi yang dimiliki sebuah instansi atau organisasi dimana lokasi-lokasi tersebut berada di tempat berbeda sehingga membutuhkan metode untuk menghubungkan setiap jaringan lokal pada setiap lokasi agar dapat saling berkomunikasi dengan baik dan aman. Metode tersebut disebut dengan *tunneling* dimana memiliki beberapa pilihan metode seperti L2TP/IPsec dan OpenVPN.

Metode-metode tersebut akan diimplementasikan dan dianalisis pengaruhnya dengan kualitas pengiriman data VoIP. Penelitian ini akan dilakukan pada 2 (dua) lokasi, yaitu kampus Universitas Kristen Duta Wacana dan Asrama Babadan Universitas Kristen Duta Wacana. Penelitian akan dilakukan menggunakan metode L2TP/IPsec dan OpenVPN secara bergantian dan menggunakan *router* Mikrotik. Parameter yang akan diteliti adalah *delay*, *jitter*, *packet loss*, *throughput*, MOS subjektif dan MOS objektif dengan limitasi *bandwidth* pada 1 Mbps, 512 Kbps dan 384 Kbps di setiap pengujian metode *tunneling*.

Penelitian ini menyimpulkan bahwa L2TP/IPsec dinilai lebih unggul dibandingkan OpenVPN. L2TP/IPsec memperoleh nilai MOS yang lebih tinggi dengan nilai *delay*, *jitter* dan *packet loss* yang lebih kecil dan mampu mengirimkan data VoIP dengan optimal pada *bandwidth* yang terbatas dibandingkan OpenVPN sehingga L2TP/IPsec dinilai merupakan metode yang optimal digunakan oleh Universitas Kristen Duta Wacana untuk pengiriman VoIP.

Kata kunci : *VoIP (Voice-over Internet Protocol)*, *VPN*, *L2TP/IPsec*, *OpenVPN*, *Quality of Service*

DAFTAR ISI

PERNYATAAN KEASLIAN SKRIPSI.....	iii
HALAMAN PERSETUJUAN.....	iv
HALAMAN PENGESAHAN.....	v
HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI.....	vi
UCAPAN TERIMA KASIH.....	vii
KATA PENGANTAR	viii
ABSTRAKSI	ix
PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah.....	2
1.4 Tujuan Penelitian.....	2
1.5 Metode Penelitian.....	3
1.6 Sistematika Penulisan.....	4
TINJAUAN PUSTAKA DAN LANDASAN TEORI.....	5
2.1 Tinjauan Pustaka	5
2.2 Landasan Teori	8
2.2.1 Jaringan Komputer.....	8
2.2.2 Virtual Private Network.....	8
2.2.3 L2TP	9
2.2.4 IPsec.....	10
2.2.5 OpenVPN.....	11
2.2.6 Voice-over Internet Protocol	12
2.3 Studi Kasus.....	13
2.3.1 Lokasi Penelitian.....	13
2.3.2 Implementasi Jaringan	13
ANALISIS DAN PERANCANGAN SISTEM	14
3.1 Analisis Jaringan	14
3.1.1 Survei Lapangan	14
3.1.2 Pengecekan <i>bandwidth</i>	15
3.1 Analisis Kebutuhan	16
3.1.1 <i>Hardware</i>	16
3.1.2 Software	18

3.2	Perancangan Sistem	19
3.2.1	Desain Topologi Jaringan	19
3.2.2	Implementasi dan Tahapan Pengujian	20
3.2.3	Skenario Pengujian	21
3.2.4	Analisis Sistem	22
	IMPLEMENTASI DAN ANALISIS DATA	28
4.1	Implementasi Skenario	28
4.1.1	Konfigurasi Dasar Mikrotik.....	28
4.1.2	Konfigurasi L2TP/IPsec	29
4.1.3	Konfigurasi OpenVPN.....	33
4.1.4	Konfigurasi Asterisk Server.....	39
4.1.5	Instalasi Zoiper	41
4.2	Analisis Data Pengujian	42
4.2.1	Analisis L2TP/IPsec	43
4.2.2	Analisis OpenVPN.....	59
4.3	Perbandingan Data pada Setiap Metode.....	73
4.3.1.	<i>Delay</i>	73
4.3.2.	<i>Jitter</i>	75
4.3.3.	<i>Packet Loss</i>	76
4.3.4.	<i>Throughput</i>	77
4.3.5.	MOS Subjektif.....	79
4.3.6.	MOS Objektif	80
4.4	Analisis Data	82
	KESIMPULAN DAN SARAN.....	84
5.1	Kesimpulan.....	84
5.2	Saran	84
	Daftar Pustaka	85
	LAMPIRAN.....	1

DAFTAR TABEL

Tabel 3. 1 Spesifikasi Mikrotik RB951Ui-2HnD	16
Tabel 3. 2 Spesifikasi Mikrotik RB931-2nD (hAP-Mini)	17
Tabel 3. 3 Spesifikasi Virtual Machine	17
Tabel 3. 4 Pengalamatan IP Address	20
Tabel 3. 5 Skenario pemanggilan antar user	22
Tabel 3. 6 Kategori delay berdasarkan TIPHON	23
Tabel 3. 7 Kategori jitter berdasarkan TIPHON	24
Tabel 3. 8 Kategori packet loss berdasarkan TIPHON	25
Tabel 3. 9 Deskripsi penilaian MOS subjektif	25
Tabel 3. 10 Nilai Ief berdasarkan codec yang digunakan pada VoIP server	27
Tabel 3. 11 Pengkategorian nilai MOS berdasarkan ITU-T P.800	27
Tabel 4. 1 Data pengujian delay pada L2TP/IPsec	43
Tabel 4. 2 Kategori delay berdasarkan TIPHON	45
Tabel 4. 3 Data pengujian jitter pada L2TP/IPsec	45
Tabel 4. 4 Kategori jitter berdasarkan TIPHON	48
Tabel 4. 5 Data paket loss pada L2TP/IPsec	48
Tabel 4. 6 Kategori delay berdasarkan TIPHON	50
Tabel 4. 7 Data throughput pada metode L2TP/IPsec	50
Tabel 4. 8 Data MOS subjektif	52
Tabel 4. 9 Kategori MOS subjektif pada L2TP/IPsec	55
Tabel 4. 10 Tabel perhitungan Id berdasarkan delay pada L2TP/IPsec	55
Tabel 4. 11 Penghitungan R-faktor pada L2TP/IPsec	56
Tabel 4. 12 Konversi nilai R-Faktor menjadi MOS pada L2TP/IPsec	56
Tabel 4. 13 Pengkategorian nilai MOS objektif pada L2TP/IPsec	58
Tabel 4. 14 Tabel delay pada OpenVPN	59
Tabel 4. 15 Pengkategorian delay pada OpenVPN sesuai dengan TIPHON	60
Tabel 4. 16 Tabel jitter pada OpenVPN	60
Tabel 4. 17 Pengkategorian jitter pada OpenVPN berdasarkan TIPHON	63
Tabel 4. 18 Tabel packet loss pada OpenVPN	63
Tabel 4. 19 Pengkategorian packet loss berdasarkan TIPHON	65
Tabel 4. 20 Data throughput pada OpenVPN	65

Tabel 4. 21 Data subjektif MOS pada OpenVPN	67
Tabel 4. 22 Tabel kategori MOS Subjektif OpenVPN	69
Tabel 4. 23 Penghitungan nilai Id pada OpenVPN	70
Tabel 4. 24 Penghitungan R-faktor pada OpenVPN.....	71
Tabel 4. 25 Konversi nilai R-Faktor menjadi MOS pada OpenVPN.....	71
Tabel 4. 26 Pengkategorian nilai MOS objektif pada L2TP/IPsec	73
Tabel 4. 27 Tabel perbandingan delay antar metode L2TP/IPsec dengan OpenVPN	73
Tabel 4. 28 Perbandingan jitter antara L2TP/IPsec dengan OpenVPN	75
Tabel 4. 29 Perbandingan pakcet loss antara L2TP/IPsec dengan OpenVPN	76
Tabel 4. 30 Perbandingan throughput antara L2TP/IPsec dengan OpenVPN	77
Tabel 4. 31 Perbandingan nilai MOS subjektif antara L2TP/IPsec dengan OpenVPN	79
Tabel 4. 32 Perbandingan nilai MOS objektif antara L2TP/IPsec dengan OpenVPN	80

DAFTAR GAMBAR

Gambar 2. 1 Ilustrasi VPN	9
Gambar 2. 2 Ilustrasi pemberian Authentication Header pada header packet	10
Gambar 2. 3 Ilustrasi ESP	11
Gambar 2. 4 Perbedaan penggunaan jenis-jenis driver	12
Gambar 3. 1 Topologi awal di setiap lokasi penelitian	14
Gambar 3. 2 Bandwidth Lab D UKDW	15
Gambar 3. 3 Bandwidth Asrama Babadan	15
Gambar 3. 4 Mikrotik RB951Ui-2HnD	16
Gambar 3. 5 Mikrotik RB931-2nD (hAP-Mini)	17
Gambar 3. 6 Desain topologi yang akan diimplementasi	19
Gambar 3. 7 Tampilan paket yang termonitor Wireshark.....	23
Gambar 3. 8 Tampilan detil paket RTP untuk memperoleh jitter dan packet loss	24
Gambar 4. 1 Skenario L2TP/IPsec	30
Gambar 4. 2 Skenario OpenVPN	33
Gambar 4. 3 Membuka tampilan /system Certificates di Mikrotik.....	34
Gambar 4. 4 Membuat CA-template.....	34
Gambar 4. 5 Membuat Server-Template.....	35
Gambar 4. 6 Membuat Client-Template	35
Gambar 4. 7 Hasil akhir seluruh template.....	36
Gambar 4. 8 Hasil certificate yang telah dibuat di sisi Mikrotik Lab-D.....	36
Gambar 4. 9 Hasil certificate export	37
Gambar 4. 10 Hasil import certificate pada sisi client	38
Gambar 4. 11 Konfigurasi jaringan pada Ubuntu server	39
Gambar 4. 12 File extensions.conf.....	40
Gambar 4. 13 File sip.conf.....	40
Gambar 4. 14 Login Zoiper.....	41
Gambar 4. 15 Tampilan konfirmasi IP Asterisk tujuan	42
Gambar 4. 16 Tampilan pilihan jenis konfigurasi Asterisk yang tersedia	42
Gambar 4. 17 Tampilan apabila berhasil melakukan registrasi	42
Gambar 4. 18 Grafik data delay pada L2TP/IPsec	44
Gambar 4. 19 Grafik jitter menggunakan metode L2TP/IPsec	47

Gambar 4. 20 Grafik data packet loss menggunakan L2TP/IPsec	49
Gambar 4. 21 Grafik throughput L2TP/IPsec	51
Gambar 4. 22 Grafik MOS subjektif pada L2TP/IPsec	54
Gambar 4. 23 Grafik MOS objektif pada L2TP/IPsec	58
Gambar 4. 24 Grafik delay pada OpenVPN.....	59
Gambar 4. 25 Grafik jitter pada OpenVPN.....	62
Gambar 4. 26 Grafik packet loss pada OpenVPN.....	64
Gambar 4. 27 Grafik throughput pada OpenVPN.....	66
Gambar 4. 28 Grafik MOS Subjektif pada OpenVPN	69
Gambar 4. 29 Grafik MOS objektif pada OpenVPN	72
Gambar 4. 30 Grafik perbandingan rata-rata delay antar metode.....	74
Gambar 4. 31 Grafik perbandingan standar deviasi delay antar metode	74
Gambar 4. 32 Grafik perbandingan rata-rata jitter antar metode	75
Gambar 4. 33 Grafik perbandingan standar deviasi jitter antar metode	76
Gambar 4. 34 Grafik perbandingan rata-rata packet loss antar metode	77
Gambar 4. 35 Grafik perbandingan standar deviasi packet loss antar metode	77
Gambar 4. 36 Grafik perbandingan rata-rata throughput antar metode	78
Gambar 4. 37 Grafik perbandingan standar deviasi throughput antar metode	79
Gambar 4. 38 Grafik perbandingan rata-rata MOS subjektif antar metode	80
Gambar 4. 39 Grafik perbandingan standar deviasi MOS Subjektif	80
Gambar 4. 40 Grafik perbandingan rata-rata MOS objektif antar metode	81
Gambar 4. 41 Grafik perbandingan standar deviasi MOS objektif antar metode	81

BAB I

PENDAHULUAN

1.1 Latar Belakang

Converged network adalah salah satu metode pemanfaatan jalur jaringan yang mulai dikembangkan dan digunakan di dunia. Penggunaan *converged network* sendiri bermanfaat dalam pembuatan atau perubahan infrastruktur jaringan agar menjadi lebih mudah. Hal tersebut disebabkan karena *converged network* dapat menyatukan jalur komunikasi seperti data *voice*, *text* dan media, yang sebelumnya terpisah menjadi 1 (satu) jalur fisik saja sehingga dapat mempermudah skalabilitas jaringan. Kemampuan tersebut menyebabkan *converged network* menjadi salah satu pilihan metode pengiriman data yang baik digunakan pada instansi-instansi yang membutuhkan jaringan yang mudah untuk dikembangkan terutama untuk kemampuan pengiriman data *voice*. Jaringan tersebut juga dapat dikembangkan menjadi jaringan yang lebih besar lagi karena banyak instansi atau instansi yang memiliki kantor cabang di tempat yang berbeda sehingga diperlukan metode *tunneling* untuk transmisi data yang aman karena jaringan akan melewati jaringan publik. Hal tersebut memungkinkan adanya akses dari pihak luar secara tidak sengaja ataupun sengaja ke dalam jalur tersebut.

Metode *tunneling* sering digunakan untuk menghubungkan *local network* suatu jaringan ke *local network* suatu jaringan lainnya sehingga setiap *client* dari masing-masing *local network* dapat saling bertukar informasi. Metode *tunneling* yang sering digunakan adalah VPN (*Virtual Private Network*). Metode ini mengenkripsi setiap data yang lewat dengan IPsec (*Internet Protocol Security*) atau OpenVPN sehingga data tetap aman walaupun melewati jaringan publik. Kedua metode tersebut dapat menggunakan banyak metode enkripsi dimana salah satunya adalah AES-256 bit. IPsec sendiri merupakan *protocol* pelengkap untuk metode L2TP (*Layer 2 Tunneling Protocol*) untuk melakukan enkripsi data berdasarkan IP (*Internet Protocol*). Hal tersebut dapat membuat data lebih aman selama pengiriman melalui jalur publik karena data telah dienkripsi.

Dengan penggunaan metode *tunneling* tersebut, tingkat keamanan data menjadi meningkat. Tetapi hal tersebut juga diperkirakan dapat mempengaruhi

kualitas pengiriman data. Maka dari itu penulis akan menganalisa perbedaan pengaruh penggunaan metode OpenVPN dan L2TP/IPsec dalam kualitas pengiriman data suara menggunakan layanan VoIP (*Voice over Internet Protocol*).

1.2 Rumusan Masalah

Rumusan masalah yang dapat diperoleh dari latar belakang diatas adalah sebagai berikut :

- a. Bagaimana perbedaan implementasi OpenVPN dan L2TP/IPsec pada transmisi VoIP?
- b. Bagaimana perbedaan kualitas pengiriman data VoIP dengan menggunakan L2TP/IPsec dan OpenVPN?

1.3 Batasan Masalah

Penelitian ini memiliki batasan masalah sebagai berikut :

- a. Implementasi konfigurasi akan dilakukan pada jaringan *backbone* antara Gedung Agape dan Asrama Babadan
- b. Metode *tunneling* yang digunakan adalah L2TP/IPsec dan OpenVPN
- c. Konfigurasi diimplementasikan pada *router* Mikrotik
- d. *User* menggunakan *smartphone device* untuk melakukan penelitian dan percobaan
- e. Data yang akan dianalisa adalah *data delay packet RTP, packet loss, jitter, throughput* dan *MOS (Mean Opinion Score)*
- f. Aplikasi *wireshark* digunakan untuk menganalisa paket VoIP yang dikirimkan.

1.4 Tujuan Penelitian

Penelitian ini bertujuan untuk menganalisa kualitas pengiriman data VoIP menggunakan metode L2TP/IPsec yang dibandingkan dengan metode OpenVPN. Perbandingan kedua metode tersebut berguna untuk mengetahui kelebihan dan kekurangan setiap metode VPN pada proses pengiriman data VoIP sehingga dapat diketahui metode yang lebih baik atau lebih optimal dalam mengirimkan data VoIP. Penelitian ini akan diimplementasikan dan dijadikan sebagai evaluasi kualitas pada jaringan Universitas Kristen Duta Wacana untuk keperluan pengiriman data VoIP.

1.5 Metode Penelitian

Metodologi yang akan digunakan dalam penelitian ini adalah

a. Survei lapangan

Penulis akan melakukan survei topologi dan konfigurasi jaringan yang sudah digunakan pada setiap lokasi. Data yang akan diambil adalah jarak antar lokasi, jenis *router*, dan konfigurasi yang sudah ada agar penelitian ini tidak mengganggu konektivitas jaringan yang sudah ada.

b. Pengumpulan informasi

Informasi dikumpulkan melalui studi pustaka dengan membaca dan memahami metode-metode yang telah diteliti dan diimplementasikan melalui literatur, buku maupun jurnal yang membahas tentang *tunneling*, keamanan, VoIP, VPN, IPsec, OpenVPN, *OSI Layer*, konsep jaringan WAN (*Wide Area Network*) dan *Point-to-Point Protocol*.

c. Perancangan

Melakukan perancangan untuk simulasi *tunneling* yang akan digunakan dengan alat yang berbeda dari alat yang akan diteliti untuk mengurangi resiko apabila terjadi *error* konfigurasi. Simulasi tersebut akan dibuat sesuai dengan topologi yang sudah dianalisa sebelumnya. Simulasi ini akan terus dilakukan hingga berhasil terhubung dengan benar. Konfigurasi yang diimplementasikan adalah konfigurasi VPN dengan IPsec, OpenVPN, *routing*, dan *Point-to-Point Protocol*. Penulis juga akan merancang skenario pengambilan data dan penelitian yang akan diimplementasikan selanjutnya. Skenario tersebut juga akan disimulasikan terlebih dahulu untuk mendapatkan data awal sebagai pembanding data yang akan diteliti.

d. Konfigurasi

Melakukan konfigurasi pada alat sesungguhnya setelah seluruh proses perancangan dan simulasi berhasil diimplementasikan. Konfigurasi dibedakan menjadi 2 jenis konfigurasi, yaitu konfigurasi menggunakan OpenVPN dan konfigurasi menggunakan IPsec di setiap lokasi.

e. Pengujian/Evaluasi

Penulis akan mengambil data berdasarkan skenario yang sudah dirancang. Pengujian ini dilakukan pada alat yang digunakan pada setiap lokasi. Pengujian dilakukan dengan memberi beban *traffic* pada jaringan *backbone* dengan melakukan VoIP yang melalui antar lokasi dengan Gedung Agape sebagai lokasi pusat.

f. Analisis dan evaluasi

Data yang sudah diperoleh akan dianalisa dan dilakukan perbandingan antar metode yang digunakan. Hasil analisis tersebut dapat disimpulkan sebagai pengaruh penggunaan metode *tunneling* pada performa VoIP.

1.6 Sistematika Penulisan

BAB I PENDAHULUAN membahas tentang gambaran umum penelitian yang akan dilakukan oleh penulis. Bab ini mencakup latar belakang penelitian, rumusan masalah, batasan penelitian, metode penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA DAN LANDASAN TEORI membahas tentang tinjauan dari berbagai penelitian terkait yang sudah dilakukan sebelumnya. Landasan teori berisi tentang teori-teori yang terkait dengan penelitian dan menjadi dasar teori yang akan digunakan selama penelitian sebagai acuan utama.

BAB III ANALISIS DAN PERANCANGAN SISTEM membahas tentang bagaimana rancangan sistem yang akan diterapkan pada penelitian ini dan bagaimana proses analisisnya. Analisis dilakukan berdasarkan kondisi jaringan awal, analisis kebutuhan dan rancangan pengimplementasian konfigurasi.

BAB IV IMPLEMENTASI DAN ANALISIS DATA membahas tentang implementasi konfigurasi dari rancangan yang telah dibuat secara detil. Hasil dari pengimplementasian tersebut akan dianalisa sebagai perbandingan antar metode yang telah dikonfigurasi.

BAB V KESIMPULAN DAN SARAN membahas tentang rangkuman dan kesimpulan yang diperoleh selama penelitian dan saran yang dapat diberikan untuk pengembangan penelitian dan sistem yang akan digunakan di kemudian hari.

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan pada analisis yang telah didapatkan di Subbab 4.3 pada penelitian ini, maka penulis dapat membuat kesimpulan sebagai berikut :

- 1) L2TP/IPsec lebih unggul dibandingkan dengan OpenVPN karena L2TP/IPsec memiliki nilai *delay*, *jitter* dan *packet loss* yang lebih kecil dan stabil.
- 2) L2TP/IPsec lebih mampu menangani transmisi VoIP secara optimal walau dengan *bandwidth* yang kecil karena memperoleh nilai *delay*, *jitter*, *packet loss* dan MOS yang lebih baik dibandingkan OpenVPN pada skenario 384 Kbps.
- 3) Kebutuhan banyaknya *bandwidth* bersifat linier terhadap nilai setiap panggilan. Penelitian ini memperoleh hasil bahwa transmisi VoIP melalui jalur *tunnel* membutuhkan setidaknya 150 Kbps hingga 250 Kbps untuk setiap panggilan dan berlaku untuk kelipatannya.

Berdasarkan poin-poin diatas, peneliti merekomendasikan untuk menggunakan metode L2TP/IPsec sebagai metode *tunneling* yang lebih optimal untuk penanganan VoIP *traffic* antar gedung atau wilayah di Universitas Kristen Duta Wacana. L2TP/IPsec juga diakui memiliki keamanan yang tidak berbeda jauh dengan OpenVPN. Hal tersebut menyimpulkan penggunaan L2TP/IPsec dapat menyebabkan VoIP *traffic* lebih optimal dengan keamanan yang lebih baik daripada metode *tunneling* yang sering digunakan seperti PPP.

5.2 Saran

Berikut ini adalah saran penulis terhadap pengembangan penelitian ini yang dapat dikembangkan dalam penelitian selanjutnya adalah menambah jumlah panggilan agar kondisi penelitian dapat menjadi simulasi implementasi VoIP menggunakan jalur *tunnel* dan membuat konfigurasi untuk memberi prioritas *bandwidth* untuk transmisi paket VoIP.

Daftar Pustaka

- Al-khatib, A. A., & Hassan, R. (2018). Impact of IPSec Protocol on the Performance of Network Real-Time Applications: A Review. *International Journal of Network Security*, 20(5), 2.
- Angelo, R. (2019). SECURE PROTOCOLS AND VIRTUAL PRIVATE NETWORKS: AN EVALUATION. *Issues in Information Systems*, 20(3), 37-46.
- Basem, B., Ghalwash, A. Z., & Sadek, R. A. (2015). Multilayer Secured SIP Based VoIP Architecture. *International Journal of Computer Theory and Engineering*, 7(6).
- Feilner, M. (2006). *OpenVPN: Building and integrating virtual private networks*. Packt Publishing Ltd.
- Kashif, M., Malik, S. A., Abdullah, M. T., Umair, M., & Khan, P. W. (2018). A Systematic Review of Cyber Security and Classification of Attacks in Networks. *International Journal of Advanced Computer Science and Applications*, 9(6), 201.
- Keromytis, A. D. (2009). Voice over IP: Risks, Threats and Vulnerabilities.
- Martin, A., Gamess, E., Urribarri, D., & Gómez, J. (2018). A Proposal for A High Availability Architecture for VoIP Telephone Systems based on Open Source Software. *(IJACSA) International Journal of Advanced Computer Science and Applications*, 9(9), 10.
- Radmand, P., Singh, J., Talevski, A., Domingo-Prieto, M., & Arnedo-Moreno, J. (2011). THE IMPACT OF SECURITY ON VOIP CALL QUALITY. *Journal of Mobile Multimedia*, 7(1).
- Rianda, F., Satwiko, A. G., & Karimah, S. A. (2018). Perbandingan Mean Opinion Score (MOS) pada Jaringan VoIP Menggunakan Proportional Integral Controller Enhanced (PIE) dan Droptail. *e-Proceeding of Engineering : Vol.5*, 8002.

- Rosu, S. M., Popescu, M. M., Dragoi, G., & Guica, I. R. (2012). The Virtual Enterprise Network based on IPSec VPN Solutions and Management. *International Journal of Advanced Computer Science and Applications*, 3(11), 26.
- Ryu, D.-H., & Nam, S.-H. (2008). Implementation of Wireless VoIP System based on VPN. *7th WSEAS Int. Conf. on Electronics, Hardware, Wireless and Optical Communications*.
- Syafrizal, M. (2005). *Pengantar jaringan komputer*. Penerbit Andi.
- Tahir, M., Li, M., Ayoub, N., Shehzaib, U., & Wagan, A. (2018). A Novel DDoS Floods Detection and Testing Approaches for Network Traffic based on Linux Techniques. *International Journal of Advanced Computer Science and Applications*, 9(2), 341.
- Tanutama, L. S., Poernama, R. A., Yansen, & Riani, W. (2008). Performansi Komunikasi VoIPSIP dengan GSM Melalui GSM Gateway. *Jurnal Teknik Komputer*, 100-108.
- Waliullah, M., & Gan, D. (2014). Wireless LAN Security Threats & Vulnerabilities. *International Journal of Advanced Computer Science and Applications*, 5(1), 176.