ANALISIS PERBANDINGAN PERFORMA POINT-TO-POINT TUNNELING PROTOCOL DAN ETHERNET OVER INTERNET PROTOCOL DALAM MEMBENTUK VPN

Robby Triadi Susanto[1] robbytriadi@gmail.com
Gani Indriyanta[2] ganind@ukdw.ac.id
R. Gunawan Santosa[3] gunawan@ukdw.ac.id

Abstract

Virtual Private Network (VPN) is a technology implemented as a solution to connect head and branch offices through a network. VPN enables all offices connected to be treated as a single broadcast domain or a single network, providing a private connection. VPN can be implemented over several protocols: Point-To-Point Tunneling Protocol (PPTP) and Ethernet over Internet Protocol (EoIP).

This research conducted through implementation of both protocols on a site-to site VPN and measuring each protocol's performance using throughput, packet loss and delay parameters obtained from real topology.

Overall result shows that EoIP performs better than PPTP. Within six days of observation, obtained data shows that EoIP has better throughput and less delay than PPTP, while PPTP has a smaller rate of packet loss than EoIP.

Kata kunci: *Virtual Private Network (VPN), Point-to-point Tunneling Procol (PPTP), Ethernet over Internet Protocol (EoIP)*

1. Pendahuluan

Saat ini, Internet telah menjadi kebutuhan yang pokok bagi organisasi.Berbagai teknologi yang dikembangkan pada jaringan Internet sudah mulai diimplementasikan pada organisasi. *Virtual Private Network (VPN)* merupakan salah satu teknologi yang diimplementasikan sebagai solusi atas kebutuhan untuk menghubungkan kantor pusat dan kantor cabang.VPN dapat menghubungkan kantor cabang dan kantor pusat melalui jaringan publik (misalnya Internet) seolah-olah menjadi sebuah jaringan privat dengan membuat sebuah "terowongan" *("tunnel")* tanpa membuat jalur khusus secara fisik, sehingga komunikasi antar kantor dalam organisasi dapat dilakukan secara aman.VPN memungkinkan membentuk kantor pusat dan kantor cabang menjadi satu *broadcast domain* atau satu *network* yang sama walaupun terpisah oleh jaringan publik, sehingga kantor pusat dan kantor cabang akan dapat berkomunkasi secara privat. Protokol yang digunakan untuk membentuk sebuah "terowongan" *(tunneling protocol)* ini bermacam-macam, diantaranya: *Point-To-Point Tunneling Protocol (PPTP),* dan *Ethernet over Internet Protocol (EoIP)* yang merupakan tunneling pada *Layer 2.*

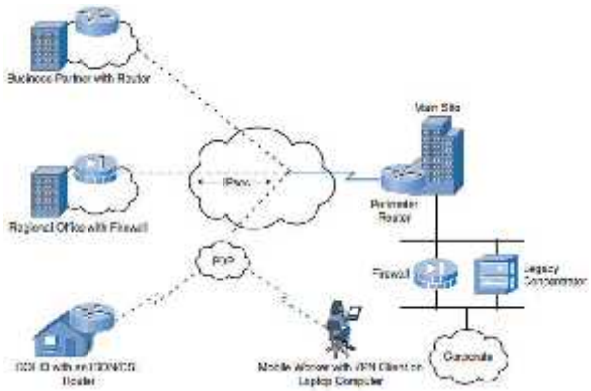
2. Teori Pendukung

2.1. *Virtual Private Network (VPN)*

Virtual Private Network (VPN) adalah tiruan dari sebuah fasilitas *Wide Area Network (WAN)* privat menggunakan fasilitas IP (termasuk Internet publik, atau *backbone*

[1]*Alumni Teknik Informatika, Fakultas Teknologi Informasi, Universitas Kristen Duta Wacana*
[2]*Dosen Teknik Informatika, Fakultas Teknologi Informasi, Universitas Kristen Duta Wacana*
[3] *DosenTeknik Informatika, Fakultas Teknologi Informasi, Universitas Kristen Duta Wacana*

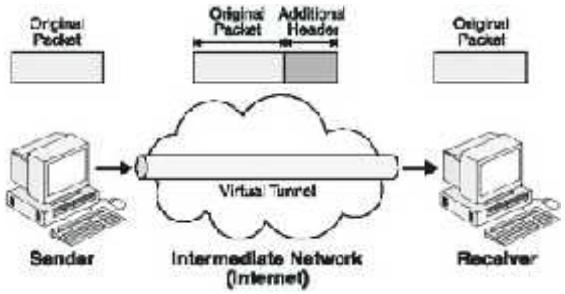
IP privat). (Gleeson, 2000). VPN menyediakan komunikasi privat antar *end user,* seperti *remote office* dan *telecommuters.* (Luo, 2005). Banyak organisasi menggunakan VPN untuk menghubungkan kantor, *home office,* rekan bisnis dan masih banyak lagi. Selain karena murah dan mudah digunakan, VPN juga digunakan karena mengutamakan keamanan. "VPN merupakan sebuah sarana untuk mengamankan dan memprivatkan pengiriman data melalui sebuah insfrastruktur jaringan yang tidak aman dan dapat digunakan bersama *(shared)*" (Vachon, 2008, halaman 402). VPN dikatakan aman karena semua data yang ditransimisikan melalui sebuah terowongan *(tunnel)* selalu dienkripsi menggunakan algortima-algoritma tertentu, bergantung pada protokol yang digunakan.



Gambar 1.Komponen dan Teknologi VPN
(Dikutip dari: Vachon, B dan Graziani, R. (2008). *Accessing the WAN – CCNA Exploration Companion Guide.* Indianapolis: Cisco Press, halaman 402.)

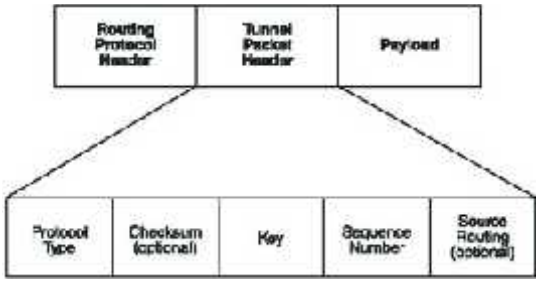
2.2. *VPN Tunneling*

Tunneling merupakan dasar atau inti dari teknologi VPN. "*Tunneling* adalah teknik enkapsulasi seluruh paket data ke dalam format protokol lain." (Gupta, 2003)."*Tunneling* mengijinkan penggunaan jaringan publik seperti Internet untuk membawa data kepada pengguna seolah-olah pengguna memiliki akses ke sebuah jaringan privat."(Vachon, 2008, halaman 409).*Tunneling* bekerja pada *Layer 2* Model *OSI Layer.*



Gambar 2.Proses *Tunneling*
Dikutip dari: Gupta, M. (2003). *Building a Virtual Private Network,* Part II Chapter 4. Ohio: Premier Press.

Gambar 2. menjelaskan bagaimana proses pengenkapsulasian paket data ke dalam format lain. Paket yang dienkapsulasi tidak dirubah, tetapi ditambahkan sebuah *header* yang pada saat paket ditransmisikan ke dalam jaringan.Hal ini membuat paket yang asli tidak berubah nilainya ketika dikirim dan diterima.



Gambar 3.Format Paket *Tunneling*
(Dikutip dari: Gupta, M. (2003). *Building a Virtual Private Network,* Part II Chapter 4. Ohio: Premier Press.)

Gambar di atas adalah format paket yang telah dienkripsi dan ditransmisikan melalui *tunnel.*Pengenkripsian dilakukan dengan menambahkan sebuah *header* baru pada paket yang akan ditransmisikan melalui *tunnel*, yaitu *tunnel packet header.* Berikut ini adalah penjelasan dari format paket *tunneling* seperti pada Gambar 2.7. (Gupta, 2003):

- ***Routing Protocol Header,*** berisi alamat IP asal tujuan. *Header* ini adalah *header* standar yang ada pada setiap paket karena transmisi paket melalui Internet pada umumnya berbasis IP.
- ***Tunnel Packet Header,*** *header* ini berisi lima *field,* yaitu:
  - ***Protocol type,*** berisi tipe protokol paket data yang asli.
  - ***Checksum,*** berisi *checksum* yang digunakan untuk mengetahui paket yang tidak sampai atau korup selama paket dikirimkan. Informasi ini tidak harus ada.
  - ***Key,*** berisi informasi yang digunakan untuk mengidentifikasi atau mengotentikasi sumber data yang aktual (inisiator).
  - ***Sequence number,*** berisi nomor urut paket yang ditransmisikan.
  - ***Source routing,*** berisi informasi *routing* tambahan. Informasi ini tidak harus ada.
- ***Payload,*** berisi paket asli yang dikirimkan oleh alamat asal. Selain itu, *payload* juga berisi *header* asli.

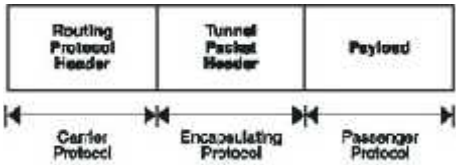
Dalam melakukan enkapsulasi, tunneling menggunakan tiga kelas protokol seperti yang ditunjukkan pada Gambar 4., yaitu:

- ***Carrier Protocol***

  Protokol ini berisi tentang informasi teknologi pembawa seperti: Frame Relay, ATM, dan MPLS. "Protokol ini digunakan untuk mengarahkan *tunneled packet* ke tujuan yang dimaksud melalui jaringan *(internetwork).*" (Gupta, 2003).Dalam penggunaannya di Internet, *carrier protocol* yang digunakan adalah IP. Namun, dibeberapa jaringan jaringan lain seperti *intranet,* protokol *routing* dapat juga berfungsi sebagai protokol pembawa.
- ***Encapsulating Protocol***

  Protokol ini adalah protokol pembungkus data yang asli."Protokol ini juga bertanggung jawab untuk membuat, merawat *(maintenance)* dan menutup *(terminate)* terowongan" (Gupta, 2003). Contoh protokol ini antara lain: *Generic Encapsulation Routing (GRE),* IPSec, L2F, PPTP dan L2TP.
- ***Passenger Protocol***

  Protokol ini berisi tentang data asli yang dibawa, seperti: IPX, AppleTalk, IPv4, IPv6, PPP dan *SLIP (Serial Line Internet Protocol)*). PPP dan SLIP adalah *passenger protocol* yang sering digunakan.



Gambar 4.Pemetaan Paket *Tunneling*
(Dikutip dari: Gupta, M. (2003). *Building a Virtual Private Network,* Part II Chapter 4. Ohio: Premier Press.)

2.3. *Point-to-Point Tunneling Protocol (PPTP)*

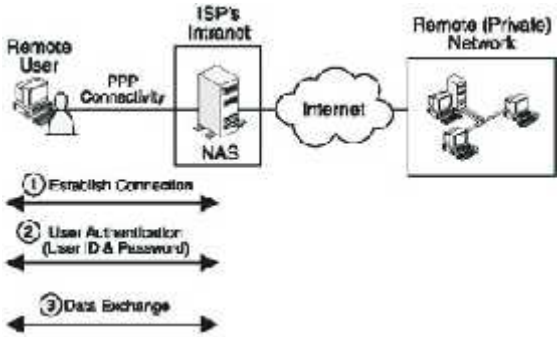
Definisi PPTP menurut **Microsoft** (diakses dari http://technet.microsoft.com/en-us/library/cc768084.aspxpada tanggal 5 April 2012) yaitu: "*Point-To-Point Tunneling Protocol* adalah protokol jaringan yang memungkinkan transfer data yang aman dari sebuah *remote client* ke sebuah *enterprise server* yang privat dengan membuat sebuah *virtual private network(VPN)* melalui jaringan data berbasis TCP/IP." *Point-To-Point Tunneling Protocol (PPTP)* dikembangkan oleh *PPTP Consortium***(Microsoft Corporation, Ascend Communications, 3COM, US Robotics,** dan **ECI Telematics).**PPTP adalah sebuah protokol jaringan yang mengenkapsulasi paket PPP kedalam IP datagram untuk transmisi melalui Internet atau jaringan publik.

Menurut Gupta (2003), dua fenomena yang memainkan peran utama dalam suksesnya PPTP dalam hubungan jarak jauh yang aman adalah:

- **Penggunaan *PSTN (Public Switched Telephone Networks)***
  Pengimplementasian PPTP yang dapat dilakukan PSTN membuat proses penyebaran PPTP menjadi sangat sederhana dan membutuhkan biaya yang relatif kecil. Hal ini membuat koneksi perusahaan-perusahaan besar yang berbasis *leased line* dan *dedicated communication server* dapat benar-benar dihilangkan.
- **Dukungan untuk protokol Non-IP**
  Walaupun fungsi PPTP yang sebenarnya untuk digunakan pada jaringan berbasis IP, namun PPTP dapat digunakan pada protokol yang lain seperti TCP/IP, IPX, NetBEUI, dan NetBIOS.

"PPP memainkan peranan utama dalam transaksi berbasis PPTP…PPTP adalah perpanjangan logika dari PPP sehingga PPTP tidak merubah inti dari teknologi PPP."(Gupta, 2003). Gupta (2003) juga menjelaskan fungsi PPP dalam transaksi berbasis PPTP seperti pada Gambar 5., yaitu:

- Mendirikan dan mengakhiri koneksi fisik komunikasi antara dua ujung.
- Mengotentikasi *client* PPTP.
- Mengenkripsi datagram pada protokol IPX, NetBEUI, NetBIOS, dan TCP/IP untuk membuat datagram PPP dan mengamankan pertukaran data.



Gambar 5.Tiga Tanggung Jawab PPP dalam Transaksi PPTP

(Dikutip dari: Gupta, M. (2003). *Building a Virtual Private Network,* Part II Chapter 5. Ohio: Premier Press.)

"Secara arsitektur, PPTP membagi fungsi *Remote Access Server (RAS)* antara *PPTP access concentrator (PAC)* dimana *remote user* melakukan *'dial'* ke dalamnya, dan *PPTPNetwork Server (PNS)* yang mengakhiri sesi PPP pada *remote client,* menyediakan akes ke jaringan perusahaan dan berperan sebagai *server* untuk satu PAC atau lebih." (Snader, 2005).

Setelah koneksi PPTP pada *client* dan *server* terbentuk, PPTP menggunakan beberapa pesan untuk mengendalikan koneksi. Pesan tersebut digunakan untuk merawat *(maintenance),* memanajemen dan mengakhiri *tunnel* PPTP. Karena PPTP dibentuk berdasarkan alamat IP, baik di sisi *client* maupun *server,* maka secara otomatis *TCP port* nomor 1723 akan dialokasikan dan dipesan pada masing-masing sisi.

Gambar 6.Paket Pengendali Koneksi PPTP
(Dikutip dari: http://technet.microsoft.com/en-us/library/cc779919(v=ws.10).aspx pada tanggal 22 September 2012.)

Pada gambar di atas (Gambar 6.), Snader (2005) menjelaskan bahwa *panjangfield* adalah panjang keseluruhan dari sebuah pesan PPTP, termasuk *header.PPTP message type* selalu diatur ke 1.Pesan ini menunjukkan pesan pengendali.Sedangkan *magic cookie,* selalu memiliki nilai 0x1a2b3c4d. Hal ini digunakan untuk melakukan sinkronisasi dengan *data stream* TCP. Jika pesan berikutnya tidak memiliki nilai tersebut, maka penerima akan mengetahui bahwa penerima telah kehilangan sinkronisasi.

Tabel 1.
Pesan Pengendali PPTP *(PPTP Control Message)*
(Dikutip dari: Snader, Jon. C. (2005).*VPNs Illustrated: Tunnels, VPNs, and IPsec,*Chapter4 Section 4.5. New Jersey: Addison Wesley Professional.)

Kode	Pesan
Connection Control Management	
1	Start-Control-Conection-Request
2	Start-Control-Conection-Reply
3	Start-Control-Conection-Request
4	Start-Control-Conection-Reply
5	Echo-Request
6	Echo-Reply
Call Management	
7	Outgoing-Call-Request
8	Outgoing-Call-Reply
9	Incoming-Call-Request
10	Incoming-Call-Reply
11	Incoming-Call-Connected
12	Call-Clear-Request
13	Call-Disconnect-Notify
Error Reporting	
14	WAN-Error-Notify
PPP Session Control	
15	Set-Link_Info

Tabel di atas adalah sebagian tipe dan format perintah dari perintah pengendali yang digunakan pada saat *tunnel PPTP* terbentuk.

2.4. *Ethernet over Internet Protocol (EoIP)*

Ethernet over Internet Protocol (EoIP) adalah protokol yang dikembangkan oleh **MikroTik** yang membuat sebuah *Ethernet tunnel* antara dua *router* dengan menggunakan koneksi IP.*Interface* EOIP terlihat sebagai *interface Ethernet* biasa (secara logikal). Ketika fungsi *bridging* diaktifkan, semua data yang ditransmisikan melalui *Ethernet protocol* pada kedua *router*akan dijembatani *(bridge)* seolah-olah kedua *router* dihubungkan dengan kabel. Protokol ini dapat berjalan di atas *PPTP tunnel* dan *IPIP tunnel* atau yang lain yang berjalan di atas koneksi IP.

EoIP menggunakan protokol GRE untuk mengenkapsulasi data agar terbentuk sebuah *EoIP Tunnel.* Urutan enkapsulasi pada protokol EoIP adalah sebagai berikut: *Internet Protocol (IP)* pada *Layer 3* akan dienkapsulasi dengan menggunakan teknologi *Ethernet II* pada *Layer 2.* Hasil enkapsulasi tersebut kemudian mengenkapsulasi protokol *Generic Routing Encapsulation (GRE).*Dengan cara inilah proses pembentukan *EoIP tunnel* terjadi dan digunakan untukmengirim dan menerima data. (Pramudya, 2009).EoIP bekerja menggunakan Tunnel ID yang harus bernilai sama antara kedua *router* yang memiliki *EoIP interface* dalam membentuk sebuah *EoIP Tunnel.* (Cahyadi, 2010). "*EoIPinterface* terlihat sebagai sebuah *interface Ethernet.*" (MikroTik, 2004). Dalam pengimplementasiannya, *EoIP Tunnel* membutuhkan satu buah *IP Public* pada kedua *router* yang akan dihubungkan.

3. Hasil dan Pembahasan

3.1. *Hardware*

- *Router* ***MikroTik-PC x86***

  Router ini digunakan di PPUKDW. Spesifikasi *router* **MikroTik**PC x86 adalah sebagai berikut:

CPU	: Pentium 731MHz
MainStorage	: 246.9MB
RAM	: 179.4MB
LAN *port*	: 7
Versi RouterOS	: 4.3
License	: Level 4

- *Router* ***MikroTik RB192***

  Router ini digunakan di SMA Budya Wacana. Spesifikasi *router* **MikroTik**RB192 adalah sebagai berikut:

CPU	: MIPS 4Kc V0.11
Main Storage	: 61.4 MB
RAM	: 29.4 MB
LAN port	: 9
Wireless port	: 2
Versi RouterOS	: 3.0
License	: Level 4

3.2. *Bandwidth* dan IP Publik

- **PPUKDW**

IP Publik	: 222.124.22.30
Upload	: 2048 Kbps
Download	: 512 Kbps

- **SMA Budya Wacana**

IP Publik	: 110.136.160.106
Upload	: 64 Kbps
Download	: 1024 Kbps

3.3. Rancangan Topologi Penelitian

Penelitian akan dimplementasikan pada topologi riil menggunakan jaringan Internet. Rancangan topologi yang akan digunakan dalam penelitian ini adalah sebagai berikut:

Gambar 7. **Topologi Penelitian**

Implementasi akan dilakukan pada dua tempat, PPUKDW dan SMA Budya Wacana dengan 2 (dua) buah *router* sesuai dengan spesifikasi yang terdapat pada subbab 3.1. dan 1 (satu) unit komputer *client* serta 1 (satu) unit komputer *server* sesuai dengan topologi di atas.Pengalamatan IP yang akan dikonfigurasi pada *interface router* dan komputer untuk penelitian sesuai dengan topologi tersebut seperti pada Tabel 2.

Tabel 2.
Pengalamatan IP

Unit	Alamat IP
Gateway Router PPUKDW (IP Publik)	222.124.22.30
Gateway Router SMA Budya Wacana (IP Publik)	110.136.160.106
Gateway Router PPUKDW (IP *PPTP Tunneling*)	10.10.100.1/24
Gateway Router SMA Budya Wacana (IP *PPTP Tunneling*)	10.10.100.2/24
Gateway Router PPUKDW (IP *EOIP Tunneling*)	10.10.200.1/30
Gateway Router SMA Budya Wacana (IP *EOIP Tunneling*)	10.10.200.2/30
DAT Server (VPN Host PPUKDW)	172.17.1.200/24
PC 1 (VPN Host SMA Budya Wacana)	192.168.103.5/24

3.4. Skema Pengujian

Pengujian dilakukan untuk menguji performa berdasarkan *throughput, packet loss* dan *delay.* Pengujian dilakukan dengan mengambil sampel dari setiap skenario tersebut. Pengujian direncanakan dilakukan selama 6 (enam) hari, dengan menjalankan aplikasi yang telah disediakan **Microsoft Certified Desktop Aplication Training.** Penelitian dilakukan mulai pukul 08.00 – 16.00 dengan interval waktu 1 (satu) jam. Setiap interval, dilakukan satu kali pengambilan untuk sampel data selama 10 (sepuluh) menit untuk satu protokol. Sampel data yang diambil berupa *throughput, delay* dan *packet loss.* Desain ini berlaku untuk kedua protokol, dan dilakukan secara bergantian, yang akan dijelaskan melalui tabel di bawah ini (Tabel 3.)

Tabel 3.
Waktu Perencanaan Pengujian

Hari, Tanggal	Waktu	Lama Pengujian	Protokol yang Diuji
Senin-Sabtu, 22-27 Oktober 2012	08.00 – 09.00	10 menit	EoIP
		10 menit	PPTP
	09.00 – 10.00	10 menit	EoIP
		10 menit	PPTP
	10.00 – 11.00	10 menit	EoIP
		10 menit	PPTP

Tabel 3. (Lanjutan)
Waktu Perencanaan Pengujian

	11.00 – 12.00	10 menit	EoIP
		10 menit	PPTP
	12.00 – 13.00	10 menit	EoIP
		10 menit	PPTP
	13.00 – 14.00	10 menit	EoIP
		10 menit	PPTP
	14.00 – 15.00	10 menit	EoIP
		10 menit	PPTP
	15.00 – 16.00	10 menit	EoIP
		10 menit	PPTP

3.4.1. Pengujian *Throughput*

Pengujian *throughput* dilakukan sebanyak satu kali dalam satu interval waktu (satu sesi). Pengambilan data dilakukan setiap detik selama 10 (sepuluh) menit pada trafik TCP.

Tabel 4.
Skema Pengujian *Throughput*

Sesi	Lama Pengambilan Data	EoIP	PPTP
08.00 – 09.00	10 Menit	TCP	TCP
09.00 – 10.00	10 Menit	TCP	TCP
10.00 – 11.00	10 Menit	TCP	TCP
11.00 – 12.00	10 Menit	TCP	TCP
12.00 – 13.00	10 Menit	TCP	TCP
13.00 – 14.00	10 Menit	TCP	TCP
14.00 – 15.00	10 Menit	TCP	TCP
15.00 – 16.00	10 Menit	TCP	TCP

Pengujian *throughput* dilakukan dengan mengirimkan trafik TCP menggunakan **JPerf.** Aplikasi ini mampu mengirimkan trafik TCP atau UDP serta melakukan pengukuran *throughput* untuk melakukan *monitoring* jaringan. Karena aplikasi ini bersifat *client-server,* maka pada penelitian ini, *DAT Server* sesuai dengan topologi di atas akan bertindak sebagai *server side,* sedangkan PC1 akan bertindak sebagai *client side.*

3.4.2. Pengujian *Delay*

Pengujian *delay* dilakukan dengan cara *sniffing packet* menggunakan aplikasi **Wireshark.** Seperti pengujian *throughput, sniffing* dilakukan pada paket TCP selama 10 (sepuluh) menit. File hasil *capture packet* selama *sniffing* kemudian diolah menggunakan aplikasi **Microsoft Excel** untuk mendapatkan rata-rata *delay* selama satu sesi.

3.4.3. Pengujian *Packet Loss*

Pengujian *packet loss* dilakukan dengan menggunakan aplikasi **Wireshark.** Paket TCP karena bersifat *connection oriented* yang memiliki mekanisme pengiriman ulang paket *(packet retransmission)* apabila terdapat kegagalan atau hilang sampai tujuan, sehingga paket yang gagal atau hilang dapat dilakukan pengujian untuk dihitung. Pada **Wireshark,** paket yang dikirim ulang akan diberi warna hitam. *Packet loss* dihitung berdasarkan jumlah paket yang gagal dikirimkan dibagi dengan total paket dikalikan dengan 100% (*packet loss* ditampilkan berdasarkan persentase). Pada **Wireshark,** *packet loss* dapat dihitung dengan membagi paket yang *displayed* dengan *total packet.*

3.5. Analisis Hasil Pengujian

Analisis hasil pengujian yang telah dilakukan selama 6 (enam) hari diselesaikan menggunakan metode pengujian statistik. Metode tersebut digunakan untuk membantu menemukan kesimpulan yang didapat secara matematis dari hasil pengolahan data yang ada.

Pengujian statistik dilakukan untuk membandingkan performa Protokol EoIP dan PPTP menggunakan 3(tiga) parameter yang didapatkan, yaitu rata-rata *throughput, packet loss,* dan *delay,* baik pada sisi *server* maupun *client* setiap harinya, serta membandingkan performa kedua protokol tersebut selama 6 (enam) hari. Dengan demikian, diharapkan hasil dari penggunaan metode pengujian statistik ini dapat membantu membuat kesimpulan dari perbandingan performa kedua protokol tersebut dan dapat melengkapi kesimpulan yang dari penelitian yang telah dilakukan.

Perbandingan hasil pengujian *throughput* dilakukan dengan dugaan bahwa Protokol PPTP memiliki *throughput* yang lebih besar dari Protokol EoIP. Dugaan tersebut nantinya akan menjadi H_1dan kebalikan dari dugaan tersebut akan menjadi H_0.Untuk perbandingan hasil pengujian *packet loss,* dilakukan dengan dugaan bahwa Protokol PPTP memiliki *packet loss* yang lebih kecil dari Protokol EoIP. Dugaan tersebut nantinya akan menjadi H_1dan kebalikan dari dugaan tesebut akan menjadi H_0. Sedangkan perbandingan hasil pengujian *delay* dilakukan dengan dugaan bahwa Protokol PPTP memiliki *delay* yang lebih kecil dari Protokol EoIP. Dugaan tersebut nantinya akan menjadi H_1dan kebalikan dari dugaan tesebut akan menjadi H_0.

Berikut ini adalah analisis hasil pengujian *throughput* yang dilakukan pada hari Senin, 22 Oktober 2012 menggunakan metode pengujian statistik Distribusi T *(T-Test):*

Tabel 5.
Data Pengujian *Throughput* pada Hari Senin, 22 Oktober 2012

Pengujian ke-	Waktu (Pukul)	Protokol EoIP	Protokol PPTP	Selisih
1	08.00 – 09.00	0.09	0.12	-0.03
2	09.00 – 10.00	0.14	0.12	0.02
3	10.00 – 11.00	0.14	0.13	0.01
4	11.00 – 12.00	0.02	0.04	-0.02
5	12.00 – 13.00	0.18	0.17	0.01
6	13.00 – 14.00	0.16	0.00	0.16
7	14.00 – 15.00	0.02	0.07	-0.05
8	15.00 – 16.00	0.16	0.09	0.07

Langkah uji statistiknya adalah:

1. Menentukan hipotesis:

$$H_0 : \mu_{EoIP} - \mu_{PPTP} \geq 0 \; vs \; H_1 : \mu_{EoIP} - \mu_{PPTP} < 0$$

   Dengan:
   H_0 : Pada hari Senin, baik di sisi *server* maupun *client,* rata-rata *throughput* pada Protokol EoIP lebih besar dari atau sama dengan rata-rata *throughput* pada Protokol PPTP.
   H_1 : Pada hari Senin, baik di sisi *server* maupun *client,* rata-rata *throughput* pada Protokol EoIP lebih kecil dari rata-rata *throughput* pada Protokol PPTP.
2. Statistik uji:

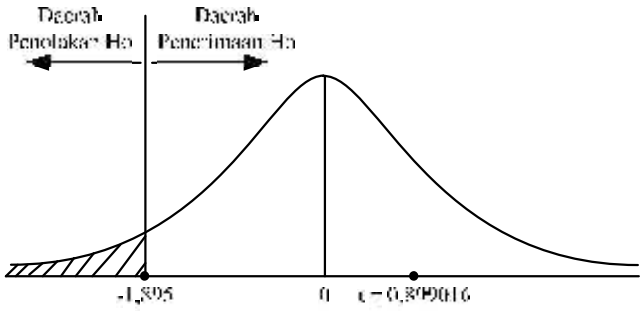
$$t_h = \frac{\overline{x}_D - 0}{S_D/\sqrt{n_D}}$$

3. Tingkat signifikansi α = 0,05; sehingga n_D – 1 = 7 dan $t_{(7;0,05)}$ = 1,895 (nilai tersebut berasal dari Tabel Distribusi t). n_D adalah jumlah pengujian yang dilakukan. Dalam penelitian ini nilai n_D = 8.
4. Daerah Penolakan H_0:
   H_0 ditolak bila t_h< -1,895
5. Hitungan:

$$\overline{x}_D = 0{,}021250;\; s_D = 0{,}066855;\; \sqrt{n_D} = \sqrt{8} = 2{,}828427, \text{ sehingga}$$

$$t_h = \frac{0{,}021250}{0{,}066855/2{,}828427} = 0{,}899016$$

6. Kesimpulan:



Gambar 8. **Grafik Distribusi t Perbandingan *Throughput***

H_0 diterima karena nilai t tidak berada pada daerah penolakan H_0. Hal ini berarti pernyataan yang menyatakan bahwa pada hari Senin, baik di sisi *server* maupun *client,* rata-rata *throughput* pada Protokol EoIP lebih besar dari atau sama dengan rata-rata *throughput* pada Protokol PPTP dapat diterima. Dengan kata lain, pada hari Senin, baik di sisi *server* maupun *client,* rata-rata *throughput* pada Protokol EoIP **lebih baik daripada** rata-rata *throughput* pada Protokol PPTP pada tingkat signifikansi 5%.

Perhitungan menggunakan metode pengujian statistik di atas dilakukan untuk semua hasil pengujian *(throughput, packet loss,* dan *delay),* baik pada sisi *server* maupun pada sisi *client.* Dari perhitungan tersebut, didapatkan hasil seperti yang dijelaskan pada subbab berikutnya.

3.5.1. Analisis *Throughput*

Salah satu parameter yang mempengaruhi performaadalah besar kecilnya *throughput* yang dihasilkan. Semakin besar *throughput,* maka semakin baik performa dari jaringan tersebut, begitu pula sebaliknya. Berikut ini hasil analisis setelah dilakukan perhitungan.

- **Analisis per Hari**

Tabel 6.
Analisis Perbandingan *Throughput* per Hari

Hari, Tanggal	***Server/ Client***	
	EoIP	**PPTP**
Senin, 22 Oktober 2012	lebih baik	-
Selasa, 23 Oktober 2012	lebih baik	-
Rabu, 24 Oktober 2012	lebih baik	-
Kamis, 25 Oktober 2012	lebih baik	-
Jum'at, 26 Oktober 2012	lebih baik	-
Sabtu, 27 Oktober 2012	lebih baik	-

- **Analisis selama 6 (Enam) Hari**

Tabel 7.
Analisis Perbandingan *Throughput* selama 6 (Enam) Hari

Lama Penelitian	***Server/ Client***	
	EoIP	PPTP
6 (enam) hari	lebih baik	-

Dari penelitian dan perhitungan menggunakan metode pengujian statistik terhadap *throughput,* baik di sisi *server* maupun *client* dapat disimpulkan bahwa:

- Protokol EoIP memiliki rata-rata *throughput* yang lebih baik daripada Protokol PPTP setiap harinya.

- Dalam kurun waktu 6 (enam) hari, kecendurungan rata-rata *throughput* pada Protokol EoIP lebih baik daripada Protokol PPTP.
- Dalam kurun waktu 6 (enam) hari, kecendurungan rata-rata *throughput* menunjukkan bahwa rata-rata *throughput* yang dihasilkan oleh Protokol EoIP lebih besar dari rata-rata *throughput* yang dihasilkan oleh Protokol PPTP.

3.5.2. Analisis *Packet Loss*

Parameter kedua yang mempengaruhi performaadalah besar kecilnya *packet loss.Packet loss* dengan prosentase yang besar mengakibatkan *bandwidth* yang dibutuhkan pada sebuah jaringan menjadi lebih besar karena paket yang hilang harus dikirim berulang-ulang hingga paket tersebut sampai pada tujuan. Dengan demikian, semakin kecil prosentasi *packet loss,* semakin baik performa jaringan. Berikut ini hasil analisis setelah dilakukan perhitungan.

- **Analisis per Hari**

Tabel 8.
Analisis Perbandingan *Packet Loss* per Hari

Hari, Tanggal	*Server*		*Client*	
	EoIP	**PPTP**	**EoIP**	**PPTP**
Senin, 22 Oktober 2012	lebih baik	-	lebih baik	-
Selasa, 23 Oktober 2012	lebih baik	-	lebih baik	-
Rabu, 24 Oktober 2012	lebih baik	-	lebih baik	-
Kamis, 25 Oktober 2012	lebih baik	-	lebih baik	-
Jum'at, 26 Oktober 2012		lebih baik	-	lebih baik
Sabtu, 27 Oktober 2012	lebih baik	-	-	lebih baik

- **Analisis selama 6 (Enam) Hari**

Tabel 9.
Analisis Perbandingan *Packet Loss* selama 6 (Enam) Hari

Lama Penelitian	*Server*		*Client*	
	EoIP	PPTP	EoIP	PPTP
6 (enam) hari	-	lebih baik	-	lebih baik

Dari penelitian dan perhitungan menggunakan metode pengujian statistik terhadap *packet loss,* baik di sisi *server* maupun *client* dapat disimpulkan bahwa:

- Pada sisi *server,* rata-rata *packet loss* pada Protokol EoIP yang lebih baik daripada Protokol PPTP terdapat pada hari Senin-Kamis dan Sabtu. Sedangkan pada hari Jum'at, rata-rata *packet loss* pada Protokol PPTP lebih baik daripada Protokol EoIP.
- Pada sisi *client,* rata-rata *packet loss* pada Protokol EoIP yang lebih baik daripada Protokol PPTP terdapat pada hari Senin-Kamis. Sedangkan pada hari Jum'at dan Sabtu, rata-rata *packet loss* pada Protokol PPTP lebih baik daripada Protokol EoIP.
- Dalam kurun waktu 6 (enam) hari, kecendurungan rata-rata *packet loss* pada Protokol PPTP lebih baik daripada Protokol EoIP.

3.5.3. Analisis *Delay*

Parameter ketiga yang mempengaruhi performaadalah besar kecilnya *delay.* Berikut ini hasil analisis dari kesimpulan yang didapatkan dari perhitungan pada Subbab 4.6.2 dan 4.6.3.

- **Analisis per Hari**

Tabel 10.
Analisis Perbandingan *Delay* per Hari

Hari, Tanggal	*Server*		*Client*	
	EoIP	PPTP	EoIP	PPTP
Senin, 22 Oktober 2012	lebih baik	-	lebih baik	-
Selasa, 23 Oktober 2012	lebih baik	-	lebih baik	-
Rabu, 24 Oktober 2012	lebih baik	-	lebih baik	-
Kamis, 25 Oktober 2012	lebih baik	-	lebih baik	-
Jum'at, 26 Oktober 2012	lebih baik	-	-	lebih baik
Sabtu, 27 Oktober 2012	lebih baik	-	lebih baik	-

- **Analisis selama 6 (Enam) Hari**

Tabel 11.
Analisis Perbandingan *Delay* selama 6 (Enam) Hari

Lama Penelitian	*Server*		*Client*	
	EoIP	PPTP	EoIP	PPTP
6 (enam) hari	lebih baik	-	lebih baik	-

Dari penelitian dan perhitungan menggunakan metode pengujian statistik terhadap *delay,* baik di sisi *server* maupun *client* dapat disimpulkan bahwa:

- Pada sisi *server,* rata-rata *delay* pada Protokol EoIP lebih baik daripada Protokol PPTP setiap harinya.
- Pada sisi *client,* rata-rata *delay* pada Protokol EoIP yang lebih baik daripada Protokol PPTP terdapat pada hari Senin-Kamis dan Sabtu. Sedangkan pada hari Sabtu, rata-rata *delay* pada Protokol PPTP lebih baik daripada Protokol EoIP.
- Dalam kurun waktu 6 (enam) hari, kecendurungan rata-rata *delay* pada Protokol EoIP lebih baik daripada Protokol PPTP.

4. Kesimpulan

Berdasarkan hasil penelitian yang telah diuraikan pada Bab 4, diperoleh beberapa kesimpulan, yaitu:

a. Dalam keseharian, baik dari sisi *server* maupun sisi *client,* Protokol EoIP memiliki performa yang lebih baik daripada Protokol PPTP karena Protokol EoIP memiliki rata-rata *throughput* yang lebih besar dari Protokol PPTP serta rata-rata *packet loss* dan *delay* yang lebih kecil dari Protokol PPTP.
b. Dalam kurun waktu 6 (enam) hari, baik dari sisi *server* maupun sisi *client,* Protokol EoIP memiliki kecenderungan *(trend)* performa yang lebih baik daripada Protokol PPTP dalam hal rata-rata *throughput* dan *delay.* Sedangkan dalam hal rata-rata *packet loss,* rata-rata *packet loss* pada Protokol PPTP lebih baik daripada Protokol EoIP.
c. Dalam keadaan pada topologi riil, performa yang paling baik dan optimal, dapat dilakukan pada hari Jum'at dan Sabtu karena pada kedua hari ini rata-rata *throughput, packet loss* dan *delay* lebih kecil dibanding hari Senin-Kamis.
d. Dari hasil implementasi dan pengujian yang diterapkan pada topologi riil, diamati bahwa pembentukan VPN menggunakan kedua protokol yang diimplementasi dan diuji dipengaruhi oleh trafik atau lalu lintas data pada jaringan lokal di masing-masing titik.

5. Penutup

Demikianlah penelitian dan analisis perbandingan performa yang dilakukan terhadap implementasi *Point-to-Point Tunneling Protocol (PPTP)* dan *Ethernet over*

Internet Protocol (EoIP) berdasarkan 3 (tiga) parameter, yaitu *throughput, packet loss* dan *delay.* Semoga penelitian ini dapat memberi pertimbangan dalam pemilihan protokol yang akan diterapkan pada sebuahVPN sehingga protokol yang digunakan dan diterapkan dapat membentuk sebuah VPN dengan performa yang lebih optimal.

Daftar Pustaka

Cahyadi, D. (2010). Pemanfaatan Fitur Tunneling Menggunakan Virtual Interface EoIP di MikrotikRouterOS Untuk Koneksi Bridging Antar Kantor Melalui Jaringan ADSL Telkom Speedy. *Jurnal Informatika Mulawarman.* Samarinda: Universitas Mulawarman, 5(2), 50 - 54. Diakses pada tanggal 10 September 2012 dari http://informatikamulawarman.files.word press.com/2011/10/01-jurnal-informatika-mulawarman-feb-2011.pdf

Feilner, M. (2006). *OpenVPN: Building and Integrating Virtual Private Network.* Birmingham: Packt Publishing.

Gupta, M. (2003). *Building a Virtual Private Network.* Ohio: Premier Press.

Lewis, M. (2006). *Comparing, Designing, and Deploying VPNs.* Indianapolis: Cisco Press.

Luo, W., Pignataro, C., Bokotey, D. & Chan, A. (2005). *Layer 2 VPN Architectures.* Indianapolis: Cisco Press.

Microsoft. (2012). *Understanding PPTP (Windows NT 4.0).* Diakses pada tanggal 12 September 2012 dari http://technet.microsoft.com/en-us/library/cc768084.aspx

Mikrotik. (2004). *Manual: Interface/EoIP.* Diakses pada tanggal 10 September 2012 dari http://wiki.mikrotik.com/wiki/Manual:Interface/EoIP

_____. (2008). *PPTP.* Diakses pada tanggal 10 September 2012 dari http://www.mikrotik.com/testdocs/ros/2.9/interface/pptp.php

Pramudya, N. (2009). *Implementasi Dan Analisis Point-To-Point Tunneling Protocol Serta Ethernet Over Internet Protocol Sebagai Metode Untuk Membuat Virtual Private Network.* Diakses pada tanggal 5 September 2012 dari http://sinta.ukdw.ac.id/sinta/search.jsp?query=pptp&btnsearch= Cari

Santosa, G. R. (2004). *Statistik.* Yogyakarta: Penerbit Andi.

Scott, C., Wolfe, P., & Erwin M. (1999). *Virtual Private Network, Second Edition.* California: O'Reilly.

Snader, J.C. (2005). *VPN Illustrated: Tunnels, VPNs, and IPsec.* New Jersey, Addison Wesley Professional.

Vachon, B., & Graziani, R. (2008). *Accessing the WAN – CCNA Exploration Companion Guide.* Indianapolis: Cisco Press.