ISSN 2549-4805

ANALISA PERBANDINGAN PROTOKOL PPTP DAN L2TP MENGGUNAKAN VIDEO CALL MELALUI JARINGAN *VIRTUAL PRIVATE NETWORK* (VPN)

COMPARATIVE ANALYSIS PPTP PROTOCOL AND L2TP USING VIDEO CALL THROUGH VIRTUAL PRIVATE NETWORK (VPN)

Raisul Azhar[1], Ezra Romliyanto[2]
[1.] Dosen Program Studi Teknik Informatika STMIK Bumigora Mataram
[2.] Mahasiswa Program Studi Teknik Informatika STMIK Bumigora Mataram
Jl. Ismail Marzuki Mataram 83127
E-mail: [1]raisul.azhar@stmikbumigora.ac.id, [2]romliyantoe@gmail.com

Abstract

The existence of Internet as media is so needed by society in which technology information provides facilitation to people in communicating without thinking the distance that often becomes a barrier. Internet networkused as media of communication, whether as public or private media is called a Virtual Private Network (VPN). It functions is to perform tunneling in order to connect between two different networks. Virtual Private Network (VPN) is a virtual connection which is private.It is called VPN because this network is a network Virtual not physically. Virtual Private Network (VPN) is used to connect or interconnect people each other in long distance relationship, for example, the agency or office that the location is far away. Based on testing and analysis of throughput parameters can be concluded that using PPTP protocol to the H263 codec has a value lower than the L2TP protocol H263 codec. Therrefore, the value of the parameters of the test showed that using L2TP VPN protocol is better than using the PPTP protocol.

Keywords :Virtual Private Network, L2TP, PPTP,Quality of Service(QoS).

1. PENDAHULUAN

Perkembangan media informasi begitu sangat cepat, hal ini terbukti dengan berkembangnya teknologi informasi dan komunikasi khususnya media internet. Dewasa ini kehadiran internet sudah menjadi sebuah kubutuhan mengingat teknologi informasi memberikan kemudahan dalam melakukan komunikasi tanpa memikirkan jarak yang sering menjadi penghalang atau penghambat dalam melakukan sebuah komunikasi. Maka dari itu sangat diperlukan sebuah jaringan internet yang digunakan sebagai media komunikasi baik komunikasi melalui jalur publik maupun jalur privat atau yang kerap disebut dengan *Virtual Private Network* (VPN) guna melakukan sebuah tunneling yang berfungsi melakukan koneksi antara 2 (dua) jaringan yang berbeda.

Virtual Private Network (VPN) merupakan sebuah koneksi Virtual yang bersifat *private*, disebut demikian karena pada dasarnya jaringan ini tidak ada secara fisik hanya berupa jaringan *Virtual*, dikatakan *private* karena tidak semua orang atau *user* bias mengakses, VPN menghubungkan computer dengan jaringan publikatau internet namun sifatnya private. *Virtual Private Network* (VPN) biasa digunakan untuk melakukan koneksi dengan jarak yang berjauhan yang diintergasikan dengan *tunnel* yang berfungsi sebagai jalur khusus melalui jalur publik, seperti hal nya instansi atau kantor yang memiliki cabang yang letak nya berjauhan, dengan menggunakan teknologi VPN dua kantor tersebut dapat terintergrasi atau dapat saling berkomunikasi meskipun dengan letak yang berbeda.

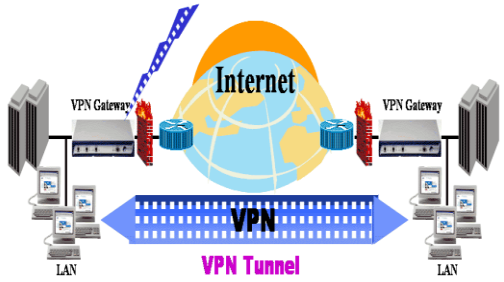
ISSN 2549-4805

Pada VPN metode ini disebut *Remote Access*VPN disebut juga *Virtual Private Dial-upNetwork* (VPDN). VPDN adalah jenis *user-to-LANconnection*. Artinya,*user* dapat melakukan koneksi ke *private network* dari manapun, apabila diperlukan. Pada jaringan VPN ini akan dilakukan perbandingan kualitas jaringan di mana jaringan nya tersebut menggunakan dua protocol yang berbeda, yaitu protocol PPTP dan L2TP. Dalam ha ini akan dilakukan pengujian untuk mengetahui perbedaannya dengan melakukan panggilan video call.

VPN merupakan sebuah jaringan private yang menghubungkan satu node jaringan ke *node* jaringan lainya dengan menggunakan jaringan *internet*. Data yang dilewatkan akan dienkapsulasi dan di enkripsi agar data tersebut terjamin kerahasiaannya(Rini, 2009).

Dapat disimpulkan bahwa *virtual private network* adalah suatu jaringan data *private* yang menggunakan infrastruktur telekomunikasi publik, yang menjamin keamanan data.

Adapun gambar yang mensimulasikan jaringan *Virtual Pivate Network* (VPN) dapat dilihat pada gambar 2.1 dibawah ini:



Gambar 2.1 Jaringan VPN

Menurut Iswan (2010) Protokol-protokol VPN yang paling banyak digunakan atau biasa diguanakan oleh *user* atau pengguna yang menggunakan jaringan VPN adalah : (dalam Rosidin, 2014, p.30).

1. *Poin to poin tunneling protocol* (PPTP)
2. *Layar 2 tunneling protocol* (L2TP)
3. *Internet protocol security* (IPSec)

Point-to-point Tuneling 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* (VPN) melalui jaringan data berbasis TCP/IP

Komunikasi yang aman dibuat dengan menggunakan protokol PPTP secara tipikal terdiri dari tiga proses, dimana membutuhkan keberhasilan penyelesaian dari proses sebelumnya. Ketiga proses tersebut adalah :

1. PPP *Connection and Communication*

Suatu *client* PPTP menggunakan PPP untuk koneksi ke sebuah ISP dengan memakai line telepon standar atau line ISDN. Koneksi ini memakai protokol PPP untuk membuat koneksi dan mengenkripsi paket data.

2. PPTP *Control Connection*

Penggunaan koneksi ke internet dibuat oleh protokolPPP, protokol PPTP membuat *control connection* dari client PPTP ke server PPTP pada internet.Koneksi ini memakai TCP untuk membuat koneksi yang disebut dengan PPTP tunnel.

3. PPTP Data *Tunneling*

Terakhir, protokol PPTP membuat IP datagram yang berisi paket PPP yang terenkripsi dan kemudian dikirim melalui PPTP tunnel ke *server* PPTP. *Server* PPTP memeriksa IP datagram dan mendekripsi paket PPP, dan kemudian mengarahkan paket yang terdekripsi ke jaringan private.

2. METODE

Fungsi VPN

ISSN 2549-4805

Adapun fungsi utama yang dimiliki *Virtual Private Network*(VPN) yaitu[10].

1. *Confidentially*

Teknologi VPN mempunyai sistem kerja mengenkripsi semua data yang lewat melaluinya. Dengan adanya teknologi *enkripsi*, maka kerahasiaan klien menjadi lebih terjaga walaupun ada pihak yang dapat menyadap data klien yang lalu-lalang, tapi belum tentu bisa dibaca dengan mudah karena memang sudah diacak.

2.Data Integrity

Ketika melewati jaringan Internet, data yang ada pada sisi *client* sebenarnya sudah berjalan sangat jauh melintasi berbagai negara. Ditengah perjalanannya, apapun bisa terjadi terhadap paket data yang dikirim.

1.*Authentication*

Teknologi VPN memiliki kemampuan untuk melakukan autentikasi terhadap sumber pengirim data yang akan diterimanya.

Protokol VPN

Menurut [3] Protokol-protokol VPN yang paling banyak digunakan atau biasa diguanakan oleh *user* atau pengguna yang menggunakan jaringan VPN adalah : [7]

***Poin to poin tunneling protocol* (PPTP)**

Point-to-Point TunnelingProtocol (PPTP) adalah suatu protokol jaringan yang memungkinkan pengiriman data secara aman dari *remote client* kepada server perusahaan swasta dengan membuat suatu *Virtual Private Network* (VPN) melalui jaringan data berbasis TCP/IP .

Komunikasi yang aman dibuat dengan menggunakan protokol PPTP secara tipikal terdiri dari tiga proses, dimana membutuhkan keberhasilan penyelesaian dari proses sebelumnya. Ketiga proses tersebut adalah :

4. PPP *Connection and Communication*

Suatu *client* PPTP menggunakan PPP untuk koneksi ke sebuah ISP dengan memakai line telepon standar atau line ISDN.

5. PPTP *Control Connection*

Penggunaan koneksi ke internet dibuat oleh protokol PPP, protokol PPTP membuat *control connection* dari client PPTP ke server PPTP pada internet.

6. PPTP Data *Tunneling*

Terakhir, protokol PPTP membuat IP datagram yang berisi paket PPP yang terenkripsi dan kemudian dikirim melalui PPTP tunnel ke *server* PPTP.

***Layar 2 tunneling protocol* (L2TP)**

L2TP adalah suatu standar IETF (RFC 2661) pada layer 2 yang merupakan kombinasi dari keunggulan-keunggulan fitur dari protokol L2F (dikembangkan oleh Cisco) dan PPTP (dikembangkan oleh Microsoft), yang didukung oleh vendor-vendor : Ascend, Cisco, IBM, Microsoft dan 3 Com. Untuk mendapatkan tingkat keamanan yang lebih baik. Terdapat dua model tannel yang dikenal, yaitu compulsory dan voluntary. Pebedaan utama keduanya terletak pada endpoint tunnel. Pada compulsory tunnel, ujung tunnel berada pada ISP sedangkan pada voluntary ujung tunnel berada pada client berada pada client remote. L2TP murni hanya membentuk jaringan tunnel, oleh karena itu L2TP sering dikombinasikan dengan IPsec sebagai metode enkripsi.

PengertianQoS (*Quality of Service*)

QoS (Quality of Service) merupakan sekumpulan teknik dan mekanisme yang menjamin performansi dari jaringan komputer (terutamanya di Internet) di dalam penyediaan layanan kepada aplikasi-aplikasi di dalam jaringan komputer. QoS (Quality of Service) dilihat dan diukur dari sudut pandang penyedia layanan. Berbeda dengan QoE (Quality of Experience) di mana penilaian dilakukan dari sudut pandang pengguna [6].

QoS (Quality of Service) adalah kemampuan suatu jaringan untuk menyediakan layanan yang lebih baik pada trafik data tertentu pada berbagai jenis platform teknologi. QoS (Quality of Service) tidak diperoleh langsung dari infrastruktur yang ada, melainkan diperoleh dengan mengimplementasikannya pada jaringan yang bersangkutan.

ISSN 2549-4805

Qos dapat di lihat secara subjektif dan objektif. Secara subjektif, tingkat kualitas dari suatu layanan diukur berdasarkan subjektifitas masing-masing pengguna. Setiap pengguna dapat memberikan nilai yang berbeda untuk suatu aplikasi yang sama. Metode pengukuran QoS secara subjektif ini umumnya dilakukan dengan menggunakan nilai MOS, dimana dilakukan uji coba langsung suatu layanan Video Conference oleh beberapa pengguna, yang kemudian akan memberikan penilaian terhadap kualitas Video Conference tersebut. Range nilai yang diberikan adalah anatara 1 sampai 5, 1 untuk kualitas terburuk sedangkan 5 untuk kualitas terbaik seperti yang ada pada tabel [14].

Delay

Delay adalah waktu tunda saat paket yang diakibatkan oleh proses transmisi dari satu titik menuju titik lain yang menjadi tujuannya. *Delay* diperoleh dari selisih waktu kirim antara satu paket TCP dengan paket lainnya yang direpresentasikan dalam satuan *seconds* Rumus untuk menghitung nilai *delay* adalah:

$$\text{Delay (sec) Tx} = \frac{\text{Duration (s)}}{\text{Total RTP Packets}}$$

Sumber : [1]

Tabel 2.2 Standar *delay* berdasarkan ITU-T G.114

***Delay* (ms)**	**Kualitas**
0 – 150	Baik
150 - 400	Cukup, masih dapat diterima
>400	Buruk
>400	Buruk

Sumber: [2]

Jitter

Jitter disebabkan oleh bervariasinya waktu penerimaan paket-paket data dari pengirim ke penerima. Parameter ini dapat ditangani denganmengatur metode antrian pada *router* saat terjadi kongesti atau saat perubahan kecepatan terjadi. Hanya saja *jitter* tidak mungkin dihilangkan sebab metode antrian yang paling baik tetap saja tidak dapat menangani semua kasus antrian.

PacketLoss

Packet Loss adalah banyaknya paket yang hilang pada suatu jaringan paket yang disebabkan oleh tabrakan (*collision*), penuhnya kapasitas jaringan, dan penurunan paket yang disebabkan oleh habisnya TTL (*TimetoLive*).

Rumus untuk menghitung *packetloss*:

Packet Loss = (data yang dikirim – paket data yang dikirim) / paket data yang dikirim x 100 %

Throughput

Throughput adalah kecepatan rata-rata yang diterima oleh suatu node dalam selang waktu pengamatan tertentu. *Throughput* merupakan *bandwith* actual saat itu juga dimana kita sedang melakukan koneksi. Satuan yang dimiliki sama dengan *bandwith* yaitu bps.Rumus untuk menghitung nilai *throughput* adalah:

$$\textit{Throughput} = \frac{\text{Jumlah data yang dikirim}}{\text{Waktu pengiriman data}}$$

Pengertian Video Call

Video Call merupakan suatu layanan yang dapat digunakan untuk mentransmisikan gambar serta suara dalam bentuk video sehingga terlihat seperti nyata (real-time). Hal ini bisa sama sederhananya dengan percakapan yang dilakukan oleh dua orang di tempat yang sama. Saat ini video call sangat berguna bagi

ISSN 2549-4805

orang tuli dan bisu karena mereka tetap dapat melakukan komunikasi dengan menggunakan bahasa isyarat [4].

Analisis Data

Analisa merupakan upaya yang dilakukan guna untuk mengetahui tentang apa yang diteliti sehingga bisa dijadikan sebagai bahan acuan oleh penulis dalam penelitian ini.

1. Protokol VPN yang paling banyak digunakan yaitu PPTP, L2TP dan IPsec, namun pada penelitian ini akan dibahas mengenai VPN PPTP dan L2TP.
2. Dalam implementasinya VPN dibagi menjadi dua jenis yaitu *remote access* dan *site-to-site*, dalam penelitian yang akan dilakukan maka akan digunakan jenis implementasi *site-to-site* yang berfungsi untuk menghubungkan letak yang berjauhan dalam halnya instansi atau kantor yang memiliki cabang yang letaknya berjauhan
3. Menentukan parameter apa saja yang akan dianalisis untuk video call pada jaringan VPN.

3. HASIL DAN PEMBAHASAN

Pada bab ini akan membahas bagaimana langkah atau tahapan-tahapan instalasi, konfigurasi, dan menganalisa, perbandingan hasil dari konfigurasi dan analisa yang telah dilakukan

3.1 Hasil Implementasi Video Call

Untuk bisa melakukan *video call* pertama,buka server trixbox yang telah terinstall pada vmware login dengan menggunakan root dengan password 123456 seperti pada gambar dibawah ini :

Gambar 4.34 Tampilan *Video Call*

1. Perbandingan Nilai *Delay*

Untuk mendapatkan selisih *delay* jaringan VPN yang menggunakan protocol PPTP dengan jaringan VPN yang menggunakan protocol L2TP yaitu dengan mengurangi nilai rata-rata *delay pada masing-masing* jaringan VPN Maka didapatkan selisih seperti pada tabel 4.29 berikut

Tabel 4.29 Perbandingan *Delay*

jenis codec	Rata-rata Delay (ms) jaringan VPN		Selisih Delay (ms)
	PPTP	L2TP	
H263	3,88	3,59	0,29
H263+	4,02	4,09	0,07

Berdasarkan tabel 4.29 selisih *delay* jaringan VPN yaitu terlihat dominan perbandingan nya pada jaringan VPN yang menggunakan codec H263 yaitu sebesar 0,29 ms.

2. Perbandingan Nilai *Throughput*

Untuk mendapatkan selisih *Throughput* jaringan VPN yang menggunakan protocol PPTP dengan jaringan VPN yang menggunakan protocol L2TP yaitu dengan mengurangi nilai rata-rata

ISSN 2549-4805

Throughput pada masing-masing jaringan VPN Maka didapatkan selisih seperti pada tabel 4.31 berikut.

Tabel 4.31. Perbandingan *Throughput*

jenis codec	Rata-rata Throughput (Mbit/s) jaringan VPN		Selisih Throughput (Mbit/s)
	PPTP	L2TP	
H263	0,649	0,874	0,225
H263+	0,586	0,574	0,012

Analisa Pada Jaringan VPN dengan Protokol PPTP

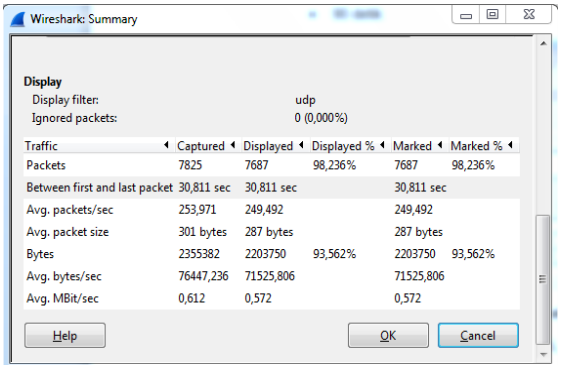
3.2.1 Parameter Delay

Delay adalah waktu tunda saat paket yang diakibatkan oleh proses transmisi dari satu titik menuju titik lain yang menjadi tujuannya. *Delay* diperoleh dari selisih waktu kirim antara satu paket dengan paket lainnya yang direpresentasikan dalam satuan *seconds*.Rumus untuk menghitung nilai delay adalah:

$$\text{Delay (sec)} = \frac{\text{Duration (s)}}{\text{Total RTP Packets}}$$

1. Analisa parameter delay menggunakan *Code*c h263

- 30 detik



Gambar. 4.35 Analisa Delay

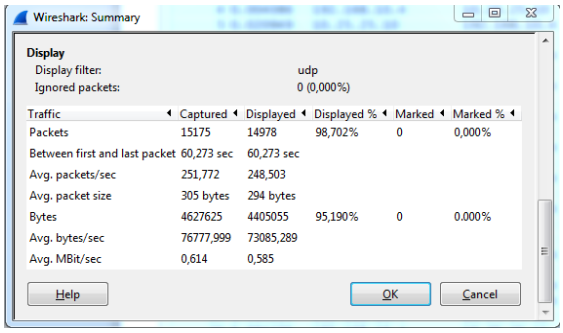
Pada gambar diatas waktu pengirimannya= 30,811 *second*, dan total paket yang diterima adalah 7825, sehingga jika hitung sesuai dengan rumus didapatkan.

$$\text{Delay (sec)} = \frac{\text{Duration (s)}}{\text{Total RTP Packets}}$$

= 30,811 s / 7825 paket
= 0,0039375079s
= 3,94 ms

- 60 detik

ISSN 2549-4805

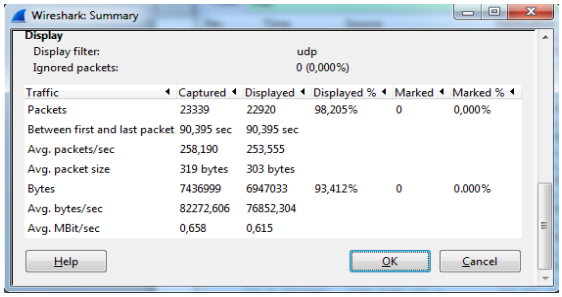


Gambar. 4.36 Analisa Delay

Pada gambar diatas waktu pengirimannya= 60,273*second*, dan total paket yang diterima adalah 15175, sehingga jika hitung sesuai dengan rumus didapatkan.

Delay (sec)=Duration (s)
Total RTP Packets
= 60,273 s / 15175 paket
= 0,0039718616s
= 3,97 ms

- 90 detik



Gambar. 4.37 Analisa Delay

Pada gambar diatas waktu pengirimannya= 30,395 *second*, dan total paket yang diterima adalah 23339, sehingga jika hitung sesuai dengan rumus didapatkan.

Delay (sec)=Duration (s)
Total RTP Packets
= 90,395 s / 23339 paket
= 0.0038731308 s
= 3.87 ms

Tabel 4.1 Hasil Analisa Parameter *Delay* Pada Pengujian Ke-1

Waktu video call	Total RTP Packets	Duration (s)	Delay (ms)
30 detik	7825	30,811	3,94
60 detik	15175	60,273	3,97
90 detik	23339	90,395	3.87

ISSN 2549-4805

Berdasarkan perhitungan *delay* secara matematis pada pengujian pertama seperti hasil *delay* pada tabel 4.1, maka hasil delay pada pengujian ke-2 sampai ke-5 bila dihitung dengancara yang sama diperoleh hasil seperti pada tabel 4.2.

Tabel 4.2 Hasil Analisa Parameter *Delay* Pada Pengujian Ke 1-5

Pengujian	Waktu Pengujian			Rata-rata Delay (ms)
	30 detik	60 detik	90 detik	
1	3,94	3,97	3,87	3,92
2	3,85	3,91	3,64	3,8
3	3,80	3,91	3,90	3.87
4	3,88	3,80	3,76	3,81
5	4,11	4,00	3,97	4,02
Total Rata-rata	3,91	3,91	3,82	3,88

Dari tabel 4.2 diperoleh nilai rata-rata *delay*pada saat melakukan *video call*30 detik, 60 detik, dan 90 detik pada pengujian 1-5 sebesar 3,88 ms.Namun nilai tersebut tidak begitu berpengaruh besar karena nilai rata-rata delay yang terjadi masih terhitung bagus untuk melakukan *video call*.

4. KESIMPULAN

Berdasarkan penelitian atau analisa yang telah dilakukan oleh peneliti terhadap analisa dan perbandingan PPTP dan L2TP menggunakan video call melalui jaringan VPN , maka diperoleh kesimpulan berdasarkan hasil ujicoba sebagai berikut:

1. Lamanya waktu video call mengakibatkan jumlah paket dari jenis trafik yang dikirimkan akan semakin besar.
2. Dapat dilihat perbandingan nilai delay dari pengukuran dengan durasi panggilan 30 detik,60 detik dan 90 detik diperoleh delay pada jaringan VPN yang menggunakan protocol L2TP lebih kecil dibandingkan dengan jaringan VPN yang menggnakan protocol PPTP.
3. Untuk jitter pada jaringan VPN PPTP maupun jaringan VPN L2TP pada saat melakukan panggilan video call menggunakan codec yang berbeda yaitu codec h-263 dan codec h-263+ tidak terlalu jauh berbeda (relative konstan), bergantung dari delay yang dihasilkan.
4. Pada saat *video call* 30 detik, 60 detik, dan 90 detik pada VPN sebesar 0 %, yang artinya paket yang dikirim dan diterima oleh masing-masing *user* tidak ada paket yang mengalami *broken* (rusak) ataupun hilang (*lost*) pada saat pengiriman ataupun penerimaan data.
5. Penggunaan protokol PPTP pada codec H263 memiliki nilai throughput lebih besar dibandingkan protokol L2TP dengan codec H263+.
6. Kualitas QOS jaringan VPN yang menggunakan protocol L2TP lebih baik daripada jaringan VPN yang menggunakan protocol PPTP karena paket data yang diterima pada waktu yang sama lebih besar pada jaringan VPN L2TP dengan codec h-263 sehingga nilai troughputnya lebih besar.

DAFTAR PUSTAKA

[1] Alfarizi Gunawan. (2013). *Menghitung Throughput, Delay Dan Packet Loss Menggunakan Wireshark dan Rumus.* Retrieved 28 July 2016 From *http://gunawan-alfarizi.blogspot.com/2013/11/menghitung-throughput-delay-dan-packet.html.*

[2] Cahyadi, dkk. (2013). *Analisa Quality of Service Pada Jaringan Lokal Session Initiation Protocol (SIP) Menggunakan GNS3.* Jurusan Teknik Elektro Universitas Diponegoro Semarang.

[3] Iswan. L. M. (2010). *implementasi virtual private network(VPN) remote acces dengan linux openswan*. Skripsi. Fakultas sains dan teknologi universitas islam negeri syarif hidayatullah jakarta.

ISSN 2549-4805

[4] Nuzul. L. dkk (2014). *Analisis Kualitas Layanan Video Call menggunakan Codec H.263 Dan H.264 Terhadap Lebar Pita Jaringan Yang Tersedia*. Fakultas Teknik, Universitas Sumatera Utara (USU).

[5] Prasetya, Aditya. (2011). *Perancangan dan Penerapan Teknologi VPN (Virtual Private Network) Untuk Komunikasi Data.* (Studi Kasus: Gardanet Corporation)

[6] Pratama, Eka. (2014). *Handbook Jaringan Komputer*. Bandung:Informatika.

[7] Rosidin, B. (2014). *Konfigurasi virtual private network (vpn) dengan mengkombinasikan pptp/ipsec pada router mikrotik. Skripsi* , 8-9

[8] Roseno, M. T. (n.d.).(2012). *Analisis perbandingan protokol virtual private network (vpn) -pptp, l2tp, ipsec- sebagai dasar perancangan vpn pada politeknik negeri sriwijaya palembang*.

[9] Rudiansyah.dkk (2013). *perancangan voice over internet protocol (voip)menggunakan virtual private network(vpn) pada PT care technologies.Jurusan*. Teknik Informatika, STMIK Nusa Mandiri Jakarta.

[10] Sahari. (2008). *Perancangan Dan Implementasi Virtual Private Network (VPN) Pada Jaringan Nirkabel (Study Kasus :UPY-YPTK Paang)*. *Poli Rekayasa* , 47.

[11] Sofana, I.(2012) *cisco ccna & jaringan komputer.Informatika Bandung*,p 130-

[12] Sugiri and Saputro, Haris. (2006).*VMware Solusi Menjalankan Beberapa Sistem Operasi*.Yogyakarta:CV Andi Offset.

[13] Sugeng, Winarno.(2008). *Membangun Telepon berbasis VoIP*. Bandung:Informatika

[14] Wulandari,Henannda. (2010). *Pembangunan Simulasi Dan Analisa Kinerja Optimalisasi VoIP – SIP Dengan Resource Reservation Protocol (RSVP*)