

IMPLEMENTASI DAN ANALISIS PERFORMA MULTI PROTOCOL LABEL SWITCHING - VIRTUAL PRIVATE NETWORK (MPLS-VPN) DENGAN METODE GENERIC ROUTING ENCAPSULATION PADA LAYANAN BERBASIS FILE TRANSFER PROTOCOL (FTP)

IMPLEMENTATION AND ANALYSIS MULTI PROTOCOL LABEL SWITCHING-VIRTUAL PRIVATE NETWORK (MPLS-VPN) PERFORMANCE WITH GENERIC ROUTING ENCAPSULATION (GRE) METHOD ON FILE TRANSFER PROTOCOL (FTP) BASED SERVICES

Audy Septarindra¹, Rendy Munadi², Ridha Muldina Negara³

^{1,2,3}Program Studi S1 Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom

audysepta91@gmail.com¹, rendymunadi@telkomuniversity.ac.id², ridhanegara@telkomuniversity.ac.id³

Abstrak

Layanan berbasis IP semakin berkembang dan terintegrasi dengan baik. Untuk integrasi yang baik, salah satu faktor yang jadi bahasan adalah performa jaringan tersebut. *Generic Routing Encapsulation (GRE)* adalah salah satu mekanisme *tunneling* yang tersedia yang menggunakan IP sebagai protokol *transport* dan dapat digunakan untuk membawa banyak protokol penumpang yang berbeda. Terowongan bertindak sebagai jalur *virtual point-to-point* yang memiliki dua titik akhir yaitu *tunnel source* dan *tunnel destination* di setiap endpoint. Fitur ini menggunakan *MPLS* melalui *Generic Routing Encapsulation* untuk enkapsulasi paket *MPLS* dalam terowongan IP. Enkapsulasi *MPLS* paket dalam IP *tunnels* membuat *link virtual point-to-point* di seluruh jaringan *non-MPLS*. Parameter uji yaitu *throughput*, *RTT Delay*, dan *Packet Loss* menunjukkan penurunan performa dengan diberi *tunnel GRE*. Penurunan performa tersebut disebabkan oleh adanya penggunaan *resource* pada jaringan saat *interkey exchange* pada pembentukan *tunnel GRE*. Namun penurunan performa bisa saja tidak terjadi saat tidak adanya *background traffic* sehingga *resource* yang bisa digunakan masih tersedia.

Kata kunci: *Throughput, RTT Delay, Packet Loss, GRE, MPLS-VPN, FTP*

Abstract

IP based services is growing and well integrated. For good integration, one of the factors that important is network performance. *Generic Routing Encapsulation (GRE)* is a tunneling mechanism which uses IP as the transport protocol and can be used to carry many passengers with different protocols. Tunnel acts as a virtual lane point-to-point which has two end points, namely tunnel source and tunnel destination on each endpoint. This feature uses *MPLS* via *Generic Routing Encapsulation* to *MPLS* packet encapsulation in IP tunnels. Encapsulation of *MPLS* packets in IP tunnels to link virtual point-to-point across *non-MPLS* network. Test parameters are *throughput*, *RTT Delay*, and *Packet Loss* shows decreasing in performance when *GRE* tunnel is applied. The reduction in performance is caused by the use of the resource on the network when *interkey exchange* when network builds *GRE* tunnel. However, a decrease in performance may not occur when the absence of *background traffic* so that the resource still has much room to be used.

Keywords : *Throughput, RTT Delay, Packet Loss, GRE, MPLS-VPN, FTP*

1. Pendahuluan

Bahasan pokok mengenai layanan IP yang terintegrasi dengan baik ialah layanan yang mempunyai performa yang baik. Metode untuk meningkatkan performa itu salah satunya yang akan dibahas di tugas akhir ini adalah GRE (*Generic Routing Encapsulation*). *Tunneling* menyediakan mekanisme untuk mengangkut paket satu protokol dalam protokol lain. Protokol yang diangkut disebut sebagai protokol *passenger*, dan protokol yang digunakan untuk membawa protokol *passenger* disebut sebagai protokol *transport*. *Generic Routing Encapsulation* (GRE) adalah salah satu mekanisme *tunneling* yang tersedia yang menggunakan IP sebagai protokol *transport* dan dapat digunakan untuk membawa banyak protokol penumpang yang berbeda. Terowongan bertindak sebagai jalur *virtual point-to-point* yang memiliki dua titik akhir yaitu *tunnel source* dan *tunnel destination* di setiap endpoint. *MPLS-VPN* melalui fitur *GRE* menyediakan mekanisme untuk *tunneling Multiprotocol Label Switching (MPLS)* paket melalui jaringan non-*MPLS*. Fitur ini menggunakan *MPLS* melalui *Generic Routing Encapsulation* untuk enkapsulasi paket *MPLS* dalam terowongan IP. Enkapsulasi *MPLS* paket dalam IP tunnels membuat link virtual point-to-point di seluruh jaringan non-*MPLS*. Tugas akhir ini akan membahas mengenai implementasi *GRE* di dalam *MPLS-VPN* pada layanan berbasis *FTP*. Setelah dilakukan implementasi, performansi jaringan *MPLS* tersebut akan diuji dan dibandingkan dengan performansi tanpa *GRE*.

2. Dasar Teori

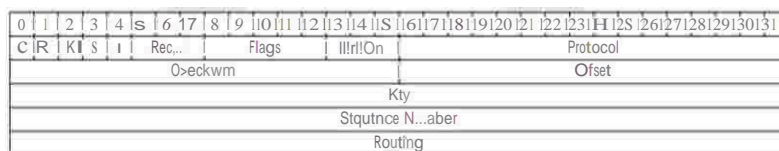
A. Generic Routing Encapsulation (GRE)^[4]

Tunneling adalah suatu mekanisme enkapsulasi *PDU (Packet Data unit)* dengan protokol yang lain dengan maksud untuk mengirimkan data pada *foreign network*. Tiga komponen utama dalam *tunneling* adalah :

- *Passenger Protocol*, yaitu protokol yang dienkapsulasi
- *Carrier Protocol*, yaitu protokol yang melakukan enkapsulasi
- *Transport Protocol*, yaitu protokol yang membawa (mengirim) *PDU* yang telah dienkapsulasi.

Generic Routing Encapsulation (GRE) merupakan sebuah metode *standard* yang dideskripsikan oleh IETF dan merupakan protokol *tunneling* yang memiliki kemampuan membawa lebih dari satu jenis protokol pengalamatan komunikasi. Bukan hanya paket beralamatkan *IP* saja yang dapat dibawanya, melainkan banyak paket protokol lain. Semua itu dibungkus atau dienkapsulasi menjadi sebuah paket yang bersistem pengalamatan *IP*. Kemudian paket tersebut didistribusikan melalui system *tunnel* yang juga bekerja di atas protokol komunikasi *IP*.

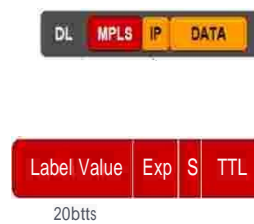
Aplikasi yang cukup banyak menggunakan bantuan protokol *tunneling* ini adalah menggabungkan jaringan-jaringan lokal yang terpisah secara jarak kembali dapat berkomunikasi. Atau dengan kata lain, *GRE* banyak digunakan untuk memperpanjang dan mengekspansi jaringan lokal yang dimiliki si penggunanya. Namun, pada mekanisme *GRE* tidak terdapat mekanisme keamanan untuk melindungi *PDU* dan pada mekanisme *GRE* akan terjadi penambahan 24 Byte header (20 Byte *IP header* dan 4 Byte *GRE header*) untuk *tunneling* paketnya.



Gambar 1 GRE Header^[4]

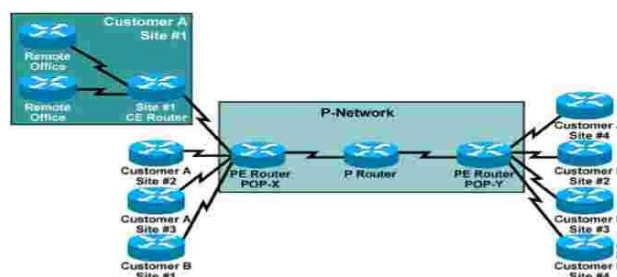
B. Multi Protocol Label Switching-Virtual Private Network (MPLS-VPN)^[2]

Multi Protocol Label Switching merupakan teknologi yang memberikan alternatif baru dalam proses pengiriman paket pada jaringan. Arsitektur MPLS memberikan solusi tentang mekanisme pemberian label *switching*, hal ini merupakan gabungan dari kelebihan kecepatan pengiriman paket pada *switching layer 2* dengan kelebihan-kelebihan dari proses *routing* dengan skalabilitas *layer 3* ^[2]. Seperti pada jaringan-jaringan *layer 2* (*frame relay* atau *ATM*), MPLS memberikan label pada tiap paket agar dapat melewati sebuah jaringan. Proses pengiriman melalui suatu jaringan disebut dengan *packet swapping*. Perbedaan mendasar antara MPLS dengan teknologi IP biasa adalah pemberian label-label pada paket dan pada *label stack* yang disisipkan pada paket. Konsep dari *label stack* dapat memperbaharui aplikasi-aplikasi baru seperti *traffic engineering*, *virtual private network* dan *fast rerouting*. Label MPLS dipropagasikan dari router ke router lainnya sehingga terbentuk sebuah pemetaan label ke label. Dalam prosesnya paket diteruskan berdasarkan *label switching* dan bukan menggunakan *IP Switching*. Label tersebut dimuat bersama dengan paket IP, yang selanjutnya router akan meneruskan trafik dengan melihat label, bukan berdasarkan alamat IP.



Gambar 2 Format MPLS header^[8]

MPLS VPN membagi keseluruhan jaringan ke dalam *customer-controlled part* (jaringan-C) dan *provider-controlled part* (jaringan-P). Bagian yang berdekatan dari jaringan-C dinamakan *site* dan terhubung dengan jaringan-P via router CE. Router CE terhubung ke router PE, yang bertindak sebagai perangkat bagian tepi dari jaringan-P. Perangkat *core* di jaringan-P yaitu router P menyediakan transit *transport* melewati jaringan utama (*backbone*) dari *Service Provider* tanpa membawa rute pelanggan ^[3].



Gambar 3 Arsitektur MPLS VPN^[6]

C. File Transfer Protocol

File Transfer Protocol atau FTP adalah salah satu services jaringan / protokol yang menyediakan layanan untuk transfer data antara client dengan server . FTP berjalan diatas protokol transport TCP (Transmission Control Protocol) yang bersifat *connection-oriented*. FTP menggunakan dua port dalam operasinya, antara lain :

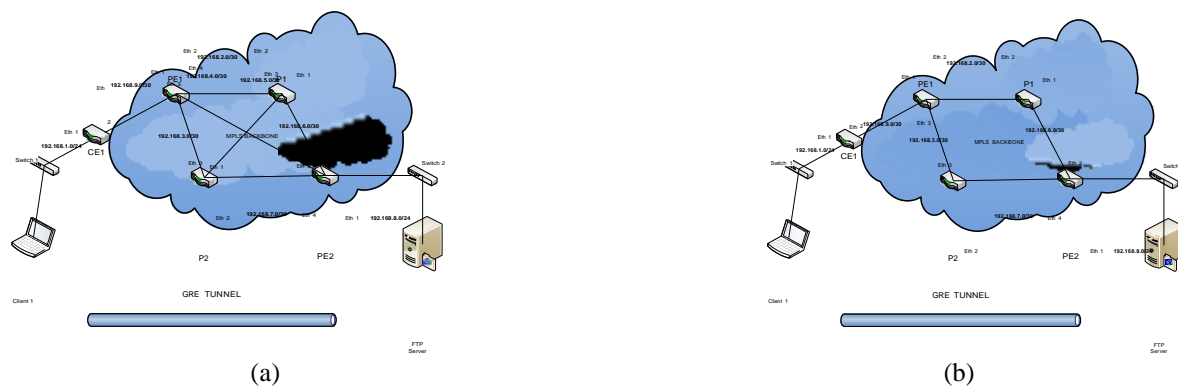
- Jalur kontrol (port 21) : jalur yang dipakai FTP untuk mengirimkan perintah (request) dari client atau menerima respon dari server. Username dan password dari FTP client juga dikirimkan melalui jalur ini.
- Jalur data (port 20) : jalur yang dipakai FTP untuk mengirimkan data berupa file yang ditransfer. Selain data berupa file, jalur data juga digunakan untuk mengirimkan data *directory listing* atau

melihat direktori FTP. Pembukaan jalur data dipicu oleh permintaan *directory listing*, upload atau download dari FTP client.

3. Perancangan Dan Implementasi

A. Implementasi Sistem

Perencanaan topologi jaringan dengan mengkonfigurasi MPLS-VPN dan server FTP. Tugas akhir ini menggunakan 4 router mikrotik rb750 difungsikan sebagai 2 router Provider Edge (PE1 dan PE2), dan 2 router Provider (P1 dan P2), serta menggunakan satu buah router mikrotik virtual melalui GNS3 di sisi Customer Edge (CE1). Setelah dikonfigurasi keempat router fisik tersebut dan satu router virtual tersebut, konfigurasi GRE tunnel dilakukan di CE1 dan PE2. Setelah semua komponen berjalan dan terkoneksi dengan baik, akan dilanjutkan ke konfigurasi *server* dan *client*. Konfigurasi *server* dan *client* sudah berjalan, maka akan dilakukan pengujian sesuai desain skenario untuk mengukur performansi jaringan MPLS, layanan yang dilakukan adalah *file sharing*.



Gambar 4 Topologi Mesh (a) dan Topologi Ring (b)

B. Perangkat Implementasi

Pada tabel dibawah terdapat beberapa perangkat lunak yang dibutuhkan dalam rencana implementasi tugas akhir ini.

Tabel 1 Perangkat lunak pada implementasi Tugas Akhir

No	Perangkat	Jumlah	Keterangan
1	Winbox	1	Perangkat yang digunakan untuk konfigurasi router mikrotik
2	Wireshark	1	Perangkat yang digunakan untuk analisis trafik
3	GNS3	1	Perangkat yang digunakan untuk membuat router virtual pada <i>Customer Edge</i>
4	Filezilla	1	Perangkat yang digunakan sebagai <i>File Sharing</i>
5	Vmware	1	Software untuk instalasi PC Virtual yang digunakan sebagai <i>Client</i>
6	TfGen	1	Software untuk membangkitkan <i>Background Traffic</i>
1	Personal Computer (PC)	Intel Core i3 3Ghz, Memory 4GB DDR3, Hardisk 500GB, Ethernet 10/100 Mbps	1 Digunakan sebagai FTP server
2	Router	Mikrotik RB750	4 Router yang digunakan pada infrastruktur MPLS.

3	Laptop	Intel Core i3 1.9 Ghz. Memory 4GB, Hardisk 1TB, Ethernet 10/100 Mbps	1	Digunakan sebagai client FTP dan sebagai router virtual
4	Kabel UTP	Kategori 5	Menyesuaikan	Link penghubung pada implementasi tugas akhir ini.

4. Pengukuran dan Analisis

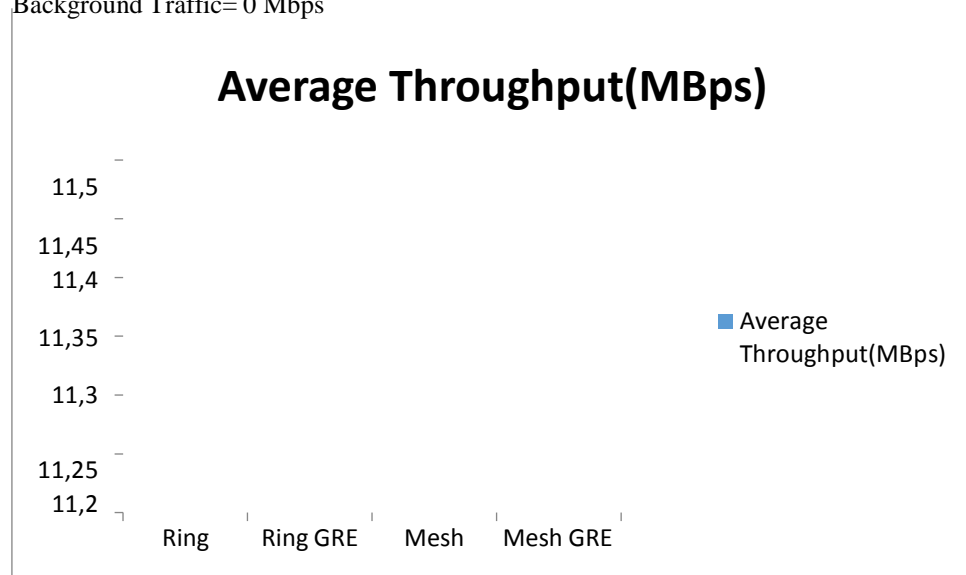
A. Pengukuran *Throughput*

Background Traffic= 0 Mbps

Topologi Jaringan	Average Throughput(MBps)
Ring	11,3125
Ring GRE	11,2875
Mesh	11,4625
Mesh GRE	11,3375

Tabel 3 *Average Throughput* pada background traffic 0 Mbps

Background Traffic= 0 Mbps



Gambar 5 Grafik *Throughput* rata-rata pada setiap topologi dengan background traffic 0 Mbps

Seperti yang terlihat di Gambar 4.3 di atas setiap topologi baik mesh dan ring, begitu diaplikasikan *tunnelling GRE* mengalami penurunan performa. Skenario ring menunjukkan

adanya penurunan performa sebesar 0,025 MBps, sedangkan scenario mesh menunjukkan penurunan performa sebesar 0,125 MBps. Hasil yang didapat dari pengukuran menunjukkan bahwa *throughput* pada mesh sebesar 11,4625 MBps sedangkan ring 11,3125 MBps. Angka ini tidak berbeda jauh, hal ini disebabkan oleh belum adanya background traffic yang dilakukan, kapasitas jaringan masih penuh resource untuk digunakan.

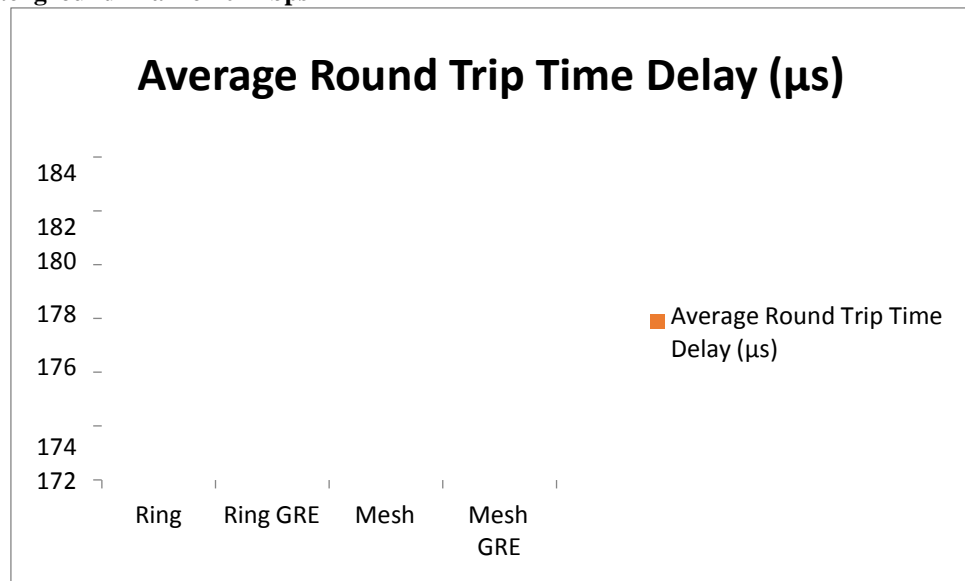
B. Pengukuran *RTT Delay*

Background Traffic= 0 Mbps

Topologi Jaringan	Average Round Trip Time Delay (μ s)
Ring	180
Ring GRE	183
Mesh	176
Mesh GRE	176

Tabel 4 Average *RTT Delay* pada Background Traffic 0 Mbps

Background Traffic= 0 Mbps



Gambar 6 Grafik *Round Trip Time Delay* rata-rata pada setiap topologi dengan background traffic 0 Mbps

Seperti yang terlihat di Gambar 4.6 di atas pada topologi Ring begitu diaplikasikan *tunnelling GRE* mengalami penurunan performa, sedangkan topologi mesh tidak mengalami perubahan performa ketika *tunnelling GRE* yang dapat disebabkan oleh belum adanya pengaruh dari *Background Traffic* sehingga resource masih tersedia. Skenario ring

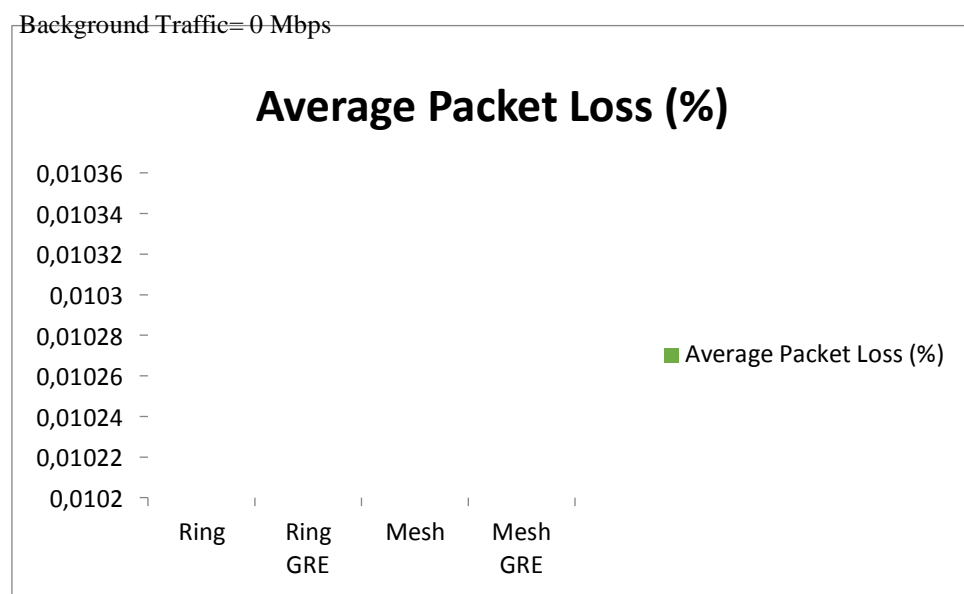
menunjukkan adanya penambahan delay sebesar $3\mu\text{s}$, sedangkan skenario mesh tidak mengalami perubahan.

C. Pengukuran Packet Loss

Background Traffic= 0 Mbps

Topologi Jaringan	Average Packet Loss (%)
Ring	0,010262188
Ring GRE	0,010336368
Mesh	0,010270072
Mesh GRE	0,010355744

Tabel 5 Average Packet Loss pada Background Traffic 0Mbps



Gambar 7 Grafik *Packet Loss* rata-rata pada setiap topologi dengan *background traffic* 0 Mbps

Seperti yang terlihat pada Gambar 4.9 diatas, *tunnelling GRE* menyebabkan kenaikan *Packet Loss*, pada topologi *Ring Packet Loss* naik sebesar 0,093101493% dari 0,010262188% ke 0,010336368% setelah *tunnelling GRE* dilakukan dan pada topologi *mesh Packet Loss* naik sebesar 0,00085672% dari 0,010270072% ke 0,010355744%.

5. Kesimpulan

Kesimpulan yang diambil dari hasil penelitian dan analisis yang pada implementasi tugas akhir adalah dengan dibentuknya *Tunnel GRE*, kedua topologi mengalami penurunan performa jaringan terlihat pada nilai *throughput*, *RTT Delay*, dan *Packet Loss*. Penurunan performa tersebut dialami karena adanya penggunaan resource pada jaringan dalam bentuk *interkey exchange* pada saat pembentukan *tunnel GRE*. Namun penurunan performa tersebut nilainya sangat kecil dan bisa tidak terjadi penurunan performa untuk mempengaruhi kinerja jaringan untuk sisi *client* jika *background traffic* tidak ada, karena resource yang bisa digunakan jaringan masih tersedia.

Daftar Pustaka

- [1] A. Purnomo, Reisa (2012). "Implementasi dan Analisis Performansi Tunneling Secure GRE (Generic Routing Encapsulation) pada Layanan VoIP dan VoD Berbasis IMS (IP Multimedia Subsystem)". Fakultas Elektro dan Komunikasi. IT Telkom.
- [2] Ahn, Gaeil. Chun, Woojik (2009). "*Overview Of MPLS Network Simulator: Design And Implementation*". Department of Computer Engineering. Chungnam National University.
- [3] Cisco Corporation (2002). "MPLS-VPN Technology". Cisco System
- [4] D. Farrinacci, dkk. *RFC 2784 Generic Routing Encapsulation (GRE)*. Internet Engineering Task Force, 2000.
- [5] M. Fazar, Eka (2011). "Analisis Perbandingan Performansi dan Keamanan File Transfer Protocol over SSH Tunneling (Secure FTP) dengan File Transfer Protocol over SSL (FTPS)". Fakultas Elektro dan Komunikasi. IT Telkom
- [6] Mende, Daniel. Rey, Enno dan Schmidt, Hendrik (2011). "*Practical Attacks Against MPLS or Carrier Ethernet Networks*". ERNW Providing Security
- [7] Mountaino, Ramavito (2012). "Implementasi dan Analisis Secured Personalized Internet Protocol Television (IPTV) Menggunakan VPN Gateway dan Enkripsi SSL dan SRTP". Fakultas Teknik Informatika. Universitas Telkom
- [8] Q Shawl, Rashed. Thaher, Rukhsana. Singh, Jasvinder. A Review : Multi Protocol Label Switching (MPLS). Buest
- [9] Safitri, Ellen (2013). "Implementasi dan Analisis Performansi Multi Protocol Label Switching Virtual Private Network pada Layanan Berbasis IP Multimedia Subsystem". Fakultas Elektro. IT Telkom
- [10] Sari, Anisa (2011). "Analisis Pengaruh Keamanan IP Security (IPSec) pada Implementasi Interkoneksi Jaringan IPv4-IPv6 di layanan VoIP". Fakultas Elektro. IT Telkom