UNIVERSITAS INDONESIA

ANALISA PENGARUH ENKRIPSI TERHADAP QOS PADA GRE/IPSEC VPN UNTUK IMPLEMENTASI IP-BASED VIDEO TELEPHONY

SKRIPSI

Diajukan sebagai salah satu syarat untuk mendapatkan gelar sarjana Teknik

FAIZAL FIRMANSYAH

0405037073

FAKULTAS TEKNNIK

DEPARTEMEN ELEKTRO

DEPOK

JULI 2009

HALAMAN PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya saya sendiri,
dan semua sumber baik yang dikutip maupun dirujuk
telah saya nyatakan dengan benar.

Nama	: Faizal Firmansyah
NPM	: 0405037073
Tanda Tangan	: .....
Tanggal	: 7 Juli 2009

HALAMAN PENGESAHAN

Skripsi ini diajukan oleh :

Nama : Faizal Firmansyah

NPM : 0405037073

Program Studi : Teknik Elektro

Judul Skripsi : Analisa Pengaruh Enkripsi Terhadap QoS Pada GRE/IPSec VPN Untuk Implementasi *IP-Based Video telephony*.

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Teknik pada Program Studi Teknik Elektro, Fakultas Teknik, Universitas Indonesia.

DEWAN PENGUJI

Pembimbing : Muhammad Salman, ST, M.I.T ( )

Penguji : Dr. Ing. Kalamullah Ramli, M.Eng ( )

Penguji : Prof. Dr. Ir. Bagio Budiardjo, MSc. ( )

Ditetapkan di : Depok

Tanggal : 7 Juli 2009

UCAPAN TERIMA KASIH

Puji syukur saya panjatkan kepada Alloh 'Azza Wa Jalla, karena atas berkat dan rahmat-Nya, saya dapat menyelesaikan skripsi ini. Penulisan skripsi ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Sarjana Teknik Jurusan Elektro pada Fakultas Teknik Universitas Indonesia. Saya menyadari bahwa tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan skripsi ini, sangatlah sulit bagi saya untuk menyelesaikan skripsi ini. Oleh karena itu, saya mengucapkan terima kasih kepada:

(1) Bapak Muhammad Salman, S.T, M.IT, selaku dosen pembimbing yang telah menyediakan waktu, tenaga, dan pikiran untuk mengarahkan saya dalam penyusunan skripsi ini.

(2) Prof. Dr.-Ing. Dr. h.c (UKM) Axel Hunger, selaku pimpinan Lab Mercator yang telah memberikan izin pemakaian fasilitas.

(3) Orang tua dan keluarga yang telah memberikan bantuan dukungan materiil dan moril.

(4) "Adek" yang telah memberikan semangat dan senyum hari demi hari;

(5) Rekan-Rekan di Mercator Office, terutama Gatot Sungkono teman seperjuangan dalam mengerjakan skripsi ini;

(6) Teman-teman Elektro seangkatan dan ikhwah kajian selasar Selatan MUI atas apresiasi dan dukungan semangat;

Akhir kata, saya berharap Alloh 'Azza Wa Jalla berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga skripsi ini membawa manfaat bagi pengembangan ilmu.

Depok, 7 Juli 2009

Faizal Firmansyah

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai civitas akademik Universitas Indonesia, saya yang bertanda tangan dibawah ini:

Nama	:	Faizal Firmansyah
NPM	:	0405037073
Program Studi	:	Teknik Elektro
Departemen	:	Teknik Elektro
Fakultas	:	Teknik
Jenis Karya	:	Skripsi

demi perkembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Indonesia Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty-Free Right*) atas karya ilmiah saya yang berjudul :

Analisa Pengaruh Enkripsi Terhadap QoS pada GRE/IPSec VPN Untuk Implementasi *IP-based video telephony*

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Indonesia berhak menyimpan, mengalihmedia/format-kan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Depok

Pada tanggal : 14 Juli 2009

Yang menyatakan

(Faizal Firmansyah)

ABSTRAK

Nama : Faizal Firmansyah,
Program Studi : Teknik Elektro S1 Reguler
Judul :"Analisa Pengaruh Enkripsi terhadap QoS pada GRE/IPSec VPN untuk Implementasi *IP-based video telephony*",

Dengan menggunakan *tunneling* GRE, *router* yang ada pada ujung-ujung *tunnel* melakukan enkapsulasi paket-paket protokol lain di dalam header dari protokol IP. Dengan adanya kemampuan ini, maka protokol-protokol yang dibawa oleh paket IP tersebut dapat lebih bebas bergerak ke manapun lokasi yang dituju, asalkan terjangkau secara pengalamatan IP. GRE banyak digunakan untuk memperpanjang dan mengekspansi jaringan lokal yang dimiliki si penggunanya. Meski cukup banyak digunakan, GRE juga tidak menyediakan sistem enkripsi data. Sehingga perlu ditambahkan dengan IPSec dalam enkripsi datanya. Dengan menggunakan implementasi NetMeeting yang memiliki *codec* G.723.1 untuk audio dan H.232 untuk Video dapat ditunjukkan bahwa penambahan enkripsi pada GRE IPSec VPN mempengaruhi performa jaringan, namun demikian pengaruh tersebut sangat kecil sekali sehingga dapat ditoleransi dikarenakan perbedaan yang tidak signifikan. Jadi penambahan enkripsi pada suatu VPN adalah hal yang sudah merupakan kebutuhan bagi VPN dan tidak membebani performa dari suatu jaringan ataupun QoS di mana perbedaan antara yang terenkripsi dan yang tidak untuk audio rata-rata 0.05% untuk *delay*, 4.73% untuk *jitter*, dan 0.26% untuk *throughput*. Sementara pada video rata-rata 4.94% untuk *delay*, 13.14% untuk *jitter*, dan 2.59% untuk *throughput*. Adapun untuk *transfer* file perbedaannya adalah 25.7%

Kata Kunci : *jitter*, *delay*, GRE/IPSec, NetMeeting, *Throughput*, VPN, QoS

ABSTRACT

Nama : Faizal Firmansyah,
Study Programme : Teknik Elektro S1 Reguler

Title :"Analysis of Encryption towards QoS on GRE/IPSec VPN to Implement the IP-based video telephony",

By using GRE tunneling, the router is on the tip-end of the tunnel do encapsulation packets in the protocol's header in the IP protocol. With this capability, then the protocols carried by IP packets can be more free to move to any location destination, provided that the affordable IP addressing. GRE widely used to extend and expand network owned by the local users. Although quite a lot of use, the GRE does not provide data encryption system. So that should be added to the IPSec encryption in the data. Using implementing NetMeeting which has G.723.1 for audio codec and H.232 for video codec, in this simulations indicate that the addition of encryption in a VPN tunneling affect network performance. However, the different can be tolerated because of the differences are not significant. So the addition of encryption in a VPN is a need for VPN nowadays and not burdened network performance and QoS, where the difference between encrypted and not encrypted for audio which average 0.05% for delay, 4.73% for jitter, and 0.26% for throughput, where the difference between encrypted and not encrypted for video which average 4.94% for delay, 13.14% for jitter, and 2.59% for throughput. While for file transfer, the difference is 25.7%

Key words: jitter, delay, GRE/IPSec, NetMeeting, Throughput, VPN, QoS

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 LATAR BELAKANG

Dalam dunia internet dan intranet banyak sekali teknologi yang berkembang hingga saat ini baik itu dalam jaringan lokal maupun non lokal. Internet banyak digunakan perusahaan, kelompok pengguna bisnis, golongan maupun pribadi. Hal ini dikarenakan saat ini masyarakat umumnya sudah banyak menggunakan internet sebagai media informasi dan juga penyedia informasi. Namun perlu disadari juga dunia intranet juga tidak kalah menariknya dengan intranet khususnya bagi pelaku-pelaku bisnis dan para pengusaha yang meng-*online* kan bisnisnya dalam dunia internet. Salah satu teknologi yang digunakan dalam dunia intranet sendiri adalah VPN (*Virtual Private Network)*.

VPN dapat dibentuk dengan menggunakan teknologi *tunneling* dan *encryption* yang didasarkan pada suatu proses akses secara *remote* yang digunakan untuk mendapatkan koneksi ke jaringan dengan tujuan tertentu, baik itu ke jaringan publik atau internet, intranet maupun *extranet*, dimana koneksi tersebut dapat terjadi pada semua lapisan (*layer)* OSI dan dapat menggunakan media apa saja. VPN saat ini biasanya digunakan sebagai *Intranet* VPN dan *Extranet* VPN. Dalam Intranet VPN, koneksi VPN akan membentuk suatu *private link* yang menuju ke jaringan lokal melalui jaringan internet publik, sehingga kita dapat langsung mengakses data-data yang diperlukan dari manapun. Sedangkan extranet VPN biasanya diperuntukan bagi pihak ketiga atau mitra kerja suatu perusahaan yang memang memiliki kepentingan dan diberi hak untuk mengakses data di jaringan lokal.

Pada skripsi ini, penulis mencoba untuk mengangkat penggunaan enkripsi pada salah satu *tunneling* GRE/IPSec VPN terhadap parameter QoS, sehingga dapat diketahui apakah penggunaan enkripsi pada suatu jaringan VPN berpengaruh secara signifikan pada performa jaringan ataukah justru dengan enkripsi itu dapat lebih memberikan tingkat kehandalan dari suatu VPN tanpa harus menurunkan QoS.

1.2 PERUMUSAN MASALAH

Permasalahan pada Tugas Akhir ini adalah merancang sebuah sistem *IP-based video telephony* dengan melewati suatu topologi sederhana GRE/IPSec VPN secara virtual di mana pada sistem tersebut akan dialirkan trafik UDP berupa audio dan video dari salah satu *host* untuk diketahui performansi dan pengaruh trafik dan penggunaan algoritma enkripsi terhadap sistem *video telephony* pada jaringan GRE/IPSec VPN yang meliputi, *delay*, *jitter* dan *throughput*.

Perancangan topologi tersebut menggunakan software *open source* GNS3 sebagai emulator dan pada topologi tersebut divirtualisasikan pada sebuah komputer di mana ada dua buah komputer lagi sebagai *host* yang terhubung ke topologi tersebut.

1.3 TUJUAN PENULISAN

Skripsi ini ditulis dengan beberapa tujuan, yaitu :

1. Menunjukkan kinerja jaringan dan QoS baik yang terenskripsi ataupun tidak menggunakan GRE IPSec VPN.
2. Mengetahui parameter QoS yang dipengaruhi sebagai akibat adanya enkripsi pada suatu jaringan GRE/IPSec VPN

1.4 BATASAN MASALAH

Pada Skripsi ini, simulasi yang dirancang adalah simulasi GRE/IPSec VPN pada emulator GNS3, di mana aplikasi yang digunakan adalah Netmeeting yang dijalankan dari satu PC ke PC lain melewati sebuah PC yang divirtualisasikan sebagai jaringan GRE/IPSec VPN, dan parameter yang diukur adalah *Delay*, *Jitter*, dan *Throughput*.

1.5 METODOLOGI

1. Studi literatur

   Mengumpulkan dan mempelajari referensi tentang jaringan GRE/IPSec VPN, software GNS3, Netmeeting.

2. Perancangan sistem

   Pada tugas akhir ini dirancang sistem *IP-based video telephony* pada GRE/IPSec VPN untuk memperlihatkan QoS pada jaringan tersebut.

3. Implementasi sistem

   Implementasi dilakukan dengan menghubungkan tiga buah komputer direcly-connected dengan dua buah komputer diujung sebagai *end-to-end user* dan komputer yang terletak di tengah sebagai Topologi GRE/IPSec VPN. Topologi tersebut berisi tiga buah *router* yaitu sebuah *router* R0, ISP dan R1. Semuanya terhubung langsung dengan media kabel UTP. Topologi GRE/IPSec VPN dimaksudkan untuk membentuk VPN *Tunnel* antara *end-to-end user*, sehingga terbentuk jaringan VPN local. Trafik UDP dibangkitkan dari *end-to-end user*. Pada sistem tersebut di atas akan diuji ketika VPN menggunakan enkripsi dan mana yang tidak.

4. Pengambilan dan analisa data

   Setelah dilakukan implementasi, akan di catat data-data yang berhubungan dengan parameter QoS (*Quality of Service*) dengan menggunakan bantuan software wireshark dari sistem tersebut meliputi *delay*, *jitter*, *throughput* dan hasilnya akan dianalisa.

5. Penarikan kesimpulan

   Selanjutnya dari hasil analisa tersebut akan ditarik kesimpulan mengenai seberapa besar pengaruh implementasi kedua buah jenis enkripsi tersebut pada GRE/IPSec VPN dan juga ketika dilakukan pemindahan file.

6. Penulisan buku laporan

   Dalam penulisan laporan ini mengacu pada pedoman penulisan ilmiah dalam hal ini penulisan Tugas Akhir yang bentuk bakunya telah diatur oleh pihak Universitas Indonesia.

1.6 SISTEMATIKA PENULISAN

Sistematika penulisan skripsi ini adalah:

1. BAB I PENDAHULUAN

Bab ini berisi Latar Belakang, Tujuan Penulisan, Batasan Masalah, dan Sistematika Penulisan

2. BAB II GRE IPSec VPN

Pada Bab ini diperkenalkan tentang *routing protocol* EIGRP, *tunneling* GRE IPSec, dan jaringan VPN

3. BAB III PERANCANGAN *IP-BASED VIDEO TELEPHONY* MELALUI GRE IPSEC VPN

Pada Bab ini akan diperlihatkan bagaimana proses perancangan simulasi yang

4. BAB IV PENGUJIAN DAN ANALISA HASIL SIMULASI

Pada Bab ini akan dilakukan pengujian dan analisa dari hasil simulasi yang telah dibuat

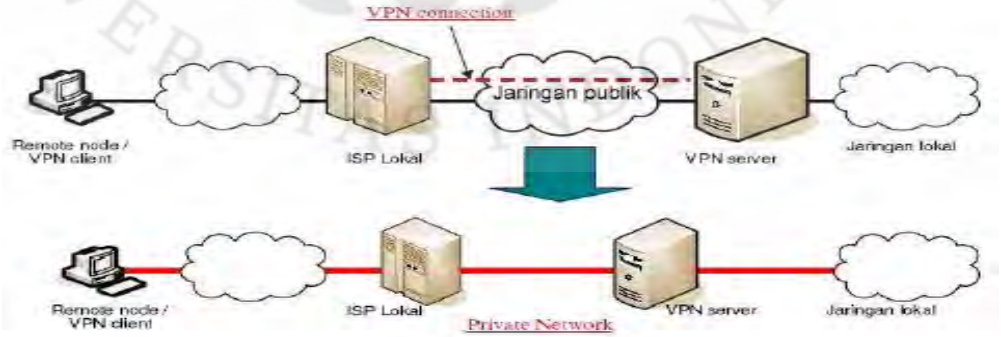
5. BAB V KESIMPULAN

BAB II
GRE/IPSEC VPN

2.1 VPN

Dalam dunia *IT networking*, istilah *virtual* yang berarti tidak memiliki wujud yang sebenarnya di antara *link* di kedua jaringan tersebut, tetapi menggunakan jaringan yang telah ada dan juga digunakan secara bersama. Demikian pula dengan istilah *private* yang berarti pribadi dalam membentuk suatu koneksi di antara dua jaringan atau lebih. Pada teknologi jaringan komputer tradisional untuk menghubungkan suatu jaringan komputer dengan jaringan komputer lain yang berbeda tempatnya akan digunakan *dedicated-line* atau *leased-line*, dimana akses seseorang akan menjadi sangat terbatas dan tidak dapat melakukan pekerjaan secara *remote.*

Teknologi ini memang tidak mendukung seseorang yang memiliki pekerjaan secara *mobile* yang memerlukan akses data dimana saja dan kapan saja, sehingga solusi yang dapat diberikan disini adalah dengan menyediakan modem sebagai fasilitas *dial-up*. Sedangkan pada teknologi VPN yang secara umum merupakan suatu teknologi yang memungkinkan seseorang terkoneksi ke jaringan lokal melalui jaringan komputer publik dan membentuk suatu jaringan pribadi, sehingga dapat dimanfaatkan untuk mendapatkan hak dan pengaturan yang sama seperti ketika berada di kantor. Prinsip kerja layanan VPN seperti yang diilustrasikan dalam gambar berikut:



Gambar 2. 1 Ilustrasi VPN [1]

2.1.1 Kriteria *VPN*

Ada beberapa criteria VPN yang menjadikannya sebuah solusi untuk akses *private,* yaitu [2]:

1. User Authentication

VPN harus mampu mengklarifikasi identitas klien serta membatasi hak akses user sesuai dengan otoritasnya. VPN juga dituntut mampu memantau aktifitas klien tentang masalah waktu, kapan, di mana dan berapa lama seorang klien mengakses jaringan serta jenis resource yang diaksesnya.

2. Address Management

VPN harus dapat mencantumkan alamat klien pada intranet dan memastikan alamat/*address* tersebut tetap rahasia.

3. Data Encryption

Data yang melewati jaringan harus dibuat agar tidak dapat dibaca oleh pihak-pihak atau klien yang tidak berwenang.

4. Key Management

VPN harus mampu membuat dan memperbarui *encryption key* untuk klien dengan klien yang lain.

5. Multiprotocol Support

VPN harus mampu menangani berbagai macam protokol dalam jaringan publik seperti IP, IPX dan sebagainya.

Perkembangan intranet yang cepat menawarkan solusi untuk membangun sebuah VPN. Di lain pihak, kekuatan suatu industri juga berkembang dan menuntut terpenuhinya lima kebutuhan dalam intranet, yaitu [3] :

1. *Kerahasiaan*, dengan kemampuan *scramble* atau *encript* pesan ketika sepanjang jaringan tidak aman.
2. *Kendali akses*, menentukan siapa yang diberikan akses ke suatu sistem atau jaringan, sebagaimana informasi apa dan seberapa banyak seseorang dapat menerima.

3. *Authentication*, menguji indentitas dari dua perusahaan yang mengadakan transaksi
4. *Integrity*, menjamin bahwa *file* atau pesan tidak berubah dalam perjalanan
5. *Non-repudiation*, mencegah dua perusahaan saling menyangkal bahwa mereka telah mengirim atau menerima *file*.

2.1.2 Mode Pemakaian pada VPN

VPN saat ini banyak digunakan untuk diterapkan pada jaringan extranet ataupun intranet perusahaan-perusahaan besar. VPN harus dapat mendukung paling tidak 3 mode pemakaian [1] :

- Koneksi *client* untuk akses jarak jauh
- LAN-to-LAN internetworking,
- Pengontrolan akses dalam suatu intranet

Oleh karena infrastruktur VPN menggunakan infrastruktur telekomunikasi umum, maka dalam VPN harus menyediakan beberapa komponen,

- Konfigurasi, harus mendukung skalabilitas platform yang digunakan, mulai dari konfigurasi untuk kantor kecil sampai tingkat *enterprise* (perusahaan besar).
- Keamanan, antara lain dengan *tunneling* (pembungkusan paket data), enkripsi, otentifikasi paket, otentifikasi pemakai dan kontrol akses.
- Layanan-layanan VPN, antara lain fungsi *Quality of Services* (QoS),Layanan routing VPN yang menggunakan BGP, OSPF dan EIGRP.
- Untuk perangkat, antara lain *Firewall*, pendeteksi pengganggu, dan auditing keamanan.
- Manajemen untuk memonitor jaringan VPN.

2.1.3 Protokol VPN

Terdapat lima protokol yang hingga saat ini paling banyak digunakan untuk VPN. Kelima protokol tersebut antara lain sebagai berikut [3]:

1. PPTP (Point to Point Tunneling Protocol)

PPTP memberikan sarana selubung *(tunneling)* untuk berkomunikasi melalui internet. Salah satu kelebihan yang membuat *PPTP* ini terkenal adalah karena protokol ini mendukung protokol non-IP seperti *IPX/SPX*, *NETBEUI*, *Appletalk* dan sebagainya. Protokol ini merupakan protokol standar pada *enkapsulasi VPN* yang digunakan oleh *Windows Virtual Private Network*. Protokol ini bekerja berdasarkan *PPP protokol* yang digunakan pada *dial-up connection*.

2. L2TP (Layer Two Tunneling Protocol)

L2TP memberikan sarana enkripsi dan selubung untuk berkomunikasi melalui internet. L2TP merupakan kombinasi dari dua protokol Cisco yaitu L2F dan PPTP. Seperti PPTP, L2TP juga mendukung protokol-protokol non-IP. L2TP lebih banyak digunakan pada VPN *non-internet* (*frame relay*, *ATM*, dsb).

3. IPSec (Internet Protocol Security)

IPSec merupakan protokol standar yang digunakan untuk memberikan keamanan untuk berkomunikasi melalui jaringan IP dengan menggunakan layanan enkripsi keamanan *(Cryptographic Security Services)*. Protokol ini merupakan protokol populer kedua setelah PPTP. *IPSec* sebenarnya merupakan kumpulan dari beberapa protokol yang berhubungan dan mendukung format enkripsi yang lebih kuat dibandingkan dengan PPTP. Kunci kekuatan *IPSec* terletak pada metode enkripsi yang terstandarisasi serta koordinasi enkripsi yang baik antara *endpoint* VPN. Fitur ini tidak didukung oleh PPTP dan L2TP.

4. PPTP Over L2TP

PPTP *Over* L2TP memberikan sarana *PPTP* menggunakan protokol *L2TP*.

5. IP in IP

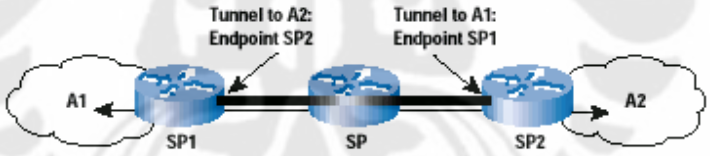
IP in IP menyelubungi *IP datagram* dengan *IP* header tambahan. *IP in IP* berguna untuk meneruskan paket data melalui jaringan dengan *policy* yang berbeda.

IP ini IP juga dapat digunakan untuk meneruskan *multicast audio dan video* data melalui *router* yang tidak mendukung *multicast routing*.

Protokol-protokol ini menekankan pada *authentikasi* dan enkripsi dalam VPN. Authentikasi mengizinkan klien dan server untuk menempatkan identitas orang dalam jaringan secara benar. Enkripsi mengizinkan data yang berpotensi sensitif untuk tersembunyi dari publik secara umum dengan cara membuat sandi.

Dua buah protokol yang paling sering digunakan adalah PPTP dan IPSec. Pemilihan protokol ini lebih banyak ditentukan oleh kondisi yang dihadapi saat men-*setting* VPN dari pada kebutuhan. Misalnya, jika pada *setting VPN* menggunakan *NT Server*, maka protokol yang digunakan tentunya *PPTP* karena protokol ini adalah *default NT*. Sedangkan jika *setting VPN* menggunakan *router* dengan VPN *endpoint built*, maka protokol yang digunakan biasanya IPSEC karena protokol inilah yang biasanya ter*install* secara *default* pada *router* tersebut.

2.2 *Tunneling*



Gambar 2. 2 *Tunneling* [1]

Tunneling merupakan metode untuk *transfer* data dari satu jaringan ke jaringan lain dengan memanfaatkan jaringan internet secara terselubung. Disebut *tunnel* atau saluran karena aplikasi yang memanfaatkannya hanya melihat dua end point atau ujung, sehingga paket yang lewat pada *tunnel* hanya akan melakukan satu kali lompatan atau hop. Data yang akan di*transfer* dapat berupa frame (atau paket) dari protokol yang lain [3].

Protokol *tunneling* tidak mengirimkan frame sebagaimana yang dihasilkan oleh node asalnya begitu saja melainkan membungkusnya (meng-enkapsulasi) dalam header tambahan. Header tambahan tersebut berisi informasi routing sehingga data (frame) yang dikirim dapat melewati jaringan internet. Jalur yang dilewati data dalam

internet disebut *tunnel*. Saat data tiba pada jaringan tujuan, proses yang terjadi selanjutnya adalah dekapsulasi, kemudian data original akan dikirim ke penerima terakhir. *Tunneling* mencakup keseluruhan proses mulai dari enkapsulasi, transmisi dan dekapsulasi.

2.2.1 Teknologi *Tunneling*

Agar saluran atau *tunnel* dapat dibuat, maka antara klien dan server harus menggunakan protokol yang sama. Teknologi *tunneling* dapat dibuat pada layer 2 atau layer 3 dari protokol *tunneling*. Layer-Layer ini mengacu pada model OSI (Open System Interconnection). Layer 2 mengacu kepada layer datalink dan menggunakan frame sebagai media pertukaran.

PPTP dan L2TP adalah protokol *tunneling* layer 2. Keduanya mengenkapsulasi data dalam sebuah frame PPP untuk kemudian dikirim melewati jaringan internet. Layer 3 mengacu kepada layer Network dan menggunakan paket-paket. IPSEC merupakan contoh protokol *tunneling* layer 3 yang mengenkapsulasi paket-paket IP dalam sebuah header IP tambahan sebelum mengirimkannya melewati jaringan IP[3].

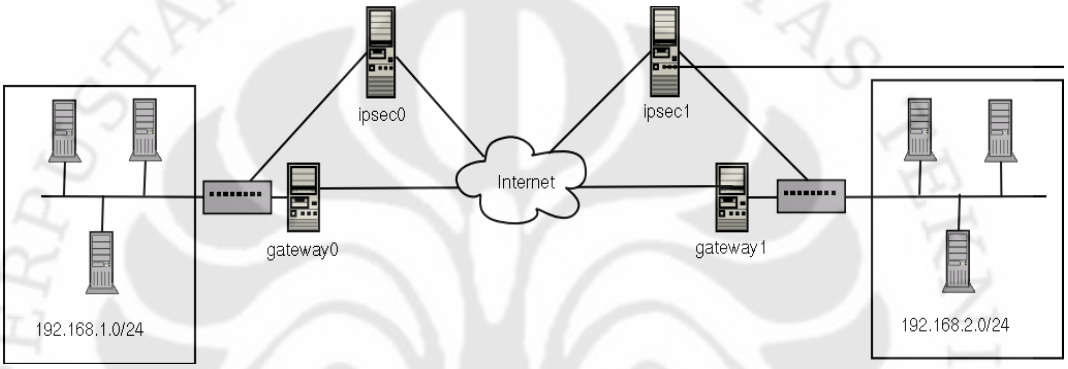
2.2.2 Prinsip Kerja *Tunneling*

Untuk *teknologi tunneling Layer 2*, seperti *PPTP* dan *L2TP*, sebuah *tunnel* mirip dengan sebuah sesi, kedua ujung *tunnel* harus mengikuti aturan *tunnel* dan menegosiasikan variabel-variabel *tunnel* seperti pengalamatan, parameter enkripsi atau parameter kompresi. Pada umumnya data yang dikirim melalui *tunnel* menggunakan protokol berbasis datagram, sedangkan protokol maintenance dari *tunnel* digunakan sebagai mekanisme untuk mengatur *tunnel*. Jadi, teknologi Layer 2 dan membuat *tunnel*, mengaturnya dan memutuskannya bila tidak diperlukan[3].

Untuk teknologi Layer 3, seluruh parameter konfigurasi telah ditentukan sebelumnya secara manual. Teknologi ini tidak memiliki protokol maintenance. Seteleh *tunnel* tercipta, proses *transfer* data siap dilangsungkan. Apabila *tunnel* klien ingin mengirim data kepada *tunnel* server, atau sebaliknya, maka klien harus

menambahkan data *transfer* protokol header pada data (proses enkapsulasi). Klien kemudian mengirim hasil dari enkapsulasi ini melalui internet untuk kemudian akan di routing kepada *tunnel* server. Setelah *tunnel* server menerima data tersebut, kemudian *tunnel* server memisahkan header data *transfer* protokol (proses dekapsulasi), dan memforward data ke jaringan tujuan [3].

2.2.2 IPSecurity



Gambar 2. 3 Ilustrasi IPSecurity [2]

IPSec didesain untuk menyediakan interoperabilitas, kualitas yang baik, sekuriti berbasis kriptografi untuk IPv4 dan IPv6. layanan yang disediakan meliputi kontrol akses, integritas hubungan, otentifikasi data asal, proteksi jawaban lawan, kerahasiaan (enkripsi), dan pembatasan aliran lalulintas kerahasiaan. Layanan-layanan ini tersedia dalam IP layer, memberi perlindungan pada IP dan layer protokol berikutnya. IP Security menyediakan sederet layanan untuk mengamankan komunikasi antar komputer dalam jaringan. Selain itu juga menambah integritas dan kerahasiaan, penerima jawaban optional (penyortiran jawaban) dan otentifikasi data asal (melalui manajemen kunci SA), IP Security juga menyediakan kontrol akses untuk lalulintas yang melaluinya. Tujuan-tujuan ini dipertemukan dengan dipertemukan melalui penggunaan dua protokol pengamanan lalulintas yaitu AH (Authentication Header) dan ESP (Encapsulating Security Payload) dan dengan penggunan prosedur dan protokol manajemen kunci kriptografi. Jika mekanisme ini

diimplementasikan sebaiknya tidak merugikan pengguna, *host* dan komponen internet lainnya yang tidak mengguankan mekanisme ini untuk melindungi lalulintas data mereka.

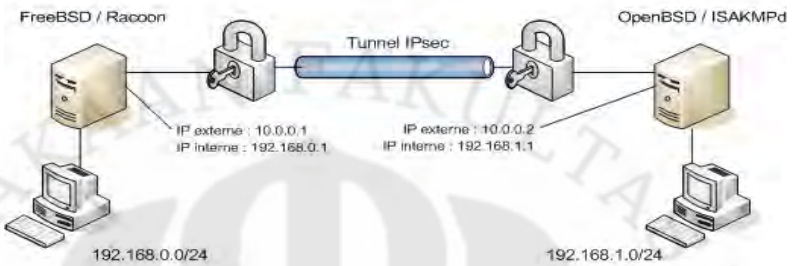
2.2.2.1 Definisi IPSec

IPSec (singkatan dari *IP Security*) adalah sebuah protokol yang digunakan untuk mengamankan transmisi *datagram* dalam sebuah *internetwork* berbasis TCP/IP. IPSec mendefiniskan beberapa standar untuk melakukan enkripsi data dan juga integritas data pada lapisan kedua dalam DARPA Reference Model (*internetwork layer*). IPSec melakukan enkripsi terhadap data pada lapisan yang sama dengan protokol IP dan menggunakan teknik *tunneling* untuk mengirimkan informasi melalui jaringan Internet atau dalam jaringan Intranet secara aman. IPSec didefinisikan oleh badan Internet Engineering Task Force (IETF) dan diimplementasikan di dalam banyak sistem operasi. Windows 2000 adalah sistem operasi pertama dari Microsoft yang mendukung IPSec.

IPSec diimplementasikan pada lapisan transport dalam OSI Reference Model untuk melindungi protokol IP dan protokol-protokol yang lebih tinggi dengan menggunakan beberapa kebijakan keamanan yang dapat dikonfigurasikan untuk memenuhi kebutuhan keamanan pengguna, atau jaringan. IPSec umumnya diletakkan sebagai sebuah lapsian tambahan di dalam stack protokol TCP/IP dan diatur oleh setiap kebijakan keamanan yang diinstalasikan dalam setiap mesin komputer dan dengan sebuah skema enkripsi yang dapat dinegosiasikan antara pengirim dan penerima. Kebijakan-kebijakan keamanan tersebut berisi kumpulan filter yang diasosiasikan dengan kelakuan tertentu. Ketika sebuah alamat IP, nomor port TCP dan UDP atau protokol dari sebuah paket datagram IP cocok dengan filter tertentu, maka kelakukan yang dikaitkan dengannya akan diaplikasikan terhadap paket IP tersebut

Layanan dari sekuritas yang disediakan oleh IPSec meliputi kontrol akses, integritas dan lain-lain seperti tesebut dibagian atas bekerja pada IP layer oleh karena

itu layanan ini dapat digunakan oleh layer protokol yang lebih tinggi seperti TCP, UDP, ICMP, BGP dan lain-lain. IPSec DOI juga mendukung kompresi IP [SMPT 98] dimotivasi dari pengamatan bahwa ketika kompresi diterapkan dalam IPSec, hal ini akan mencegah kompresi efektif pada protokol yang lebih rendah.



Gambar 2. 4 Ilustrasi Pengamanan pada *Tunnel* IPSec [2]

2.2.2.2 Cara Kerja IPSec

Untuk membuat sebuah sesi komunikasi yang aman antara dua komputer dengan menggunakan IPSec, maka dibutuhkan sebuah *framework* protokol yang disebut dengan ISAKMP/Oakley. *Framework* tersebut mencakup beberapa algoritma kriptografi yang telah ditentukan sebelumnya, dan juga dapat diperluas dengan menambahkan beberapa sistem kriptografi tambahan yang dibuat oleh pihak ketiga. Selama proses negosiasi dilakukan, persetujuan akan tercapai dengan metode autentikasi dan kemanan yang akan digunakan, dan protokol pun akan membuat sebuah kunci yang dapat digunakan bersama (shared key) yang nantinya digunakan sebagi kunci enkripsi data. IPSec mendukung dua buah sesi komunikasi keamanan, yakni sebagai berikut:

- Protokol Authentication Header (AH):

Protokol ini menawarkan autentikasi pengguna dan perlindungan dari beberapa serangan (umumnya serangan *man in the middle*), dan juga menyediakan fungsi autentikasi terhadap data serta integritas terhadap data. Protokol ini mengizinkan penerima untuk merasa yakin bahwa identitas si pengirim adalah benar

adanya, dan data pun tidak dimodifikasi selama transmisi. Namun demikian, protokol AH tidak menawarkan fungsi enkripsi terhadap data yang ditransmisikannya. Informasi AH dimasukkan ke dalam *header* paket IP yang dikirimkan dan dapat digunakan secara sendirian atau bersamaan dengan protokol *Encapsulating Security Payload*.

- Protokol Encapsulating Security Payload (ESP):

Protokol ini melakukan enkapsulasi serta enkripsi terhadap data pengguna untuk meningkatkan kerahasiaan data. ESP juga dapat memiliki skema autentikasi dan perlindungan dari beberapa serangan dan dapat digunakan secara sendirian atau bersamaan dengan *Authentication Header*. Sama seperti halnya AH, informasi mengenai ESP juga dimasukkan ke dalam *header* paket IP yang dikirimkan.

IPSec mengizinkan pengguna (administrator sistem) untuk mengontrol bagian-bagian terkecil dimana layanan keamanan diberikan. Sebagai contoh, salah satu dapat membuat *tunnel* enkripsi tunggal untuk membawa semua lalulintas antara dua sekurity gateway atau membuat *tunnel* enkripsi terpisah yang dibuat di masing-masing hubungan TCP antara sepasang *Host* yang berkomunikasi melintasi gateway tersebut. Manajemen IPSec harus menggabungkan fasilitas untuk menspesifikasikan:

- Layanan keaman apa yang digunakan dan dengan kombinnasi yang seperti apa.
- bagian Sekecil apa proteksi keamanan diterapkan.
- Algoritma yang digunakan untuk mempengaruhi keamanan berbasis kriptografi

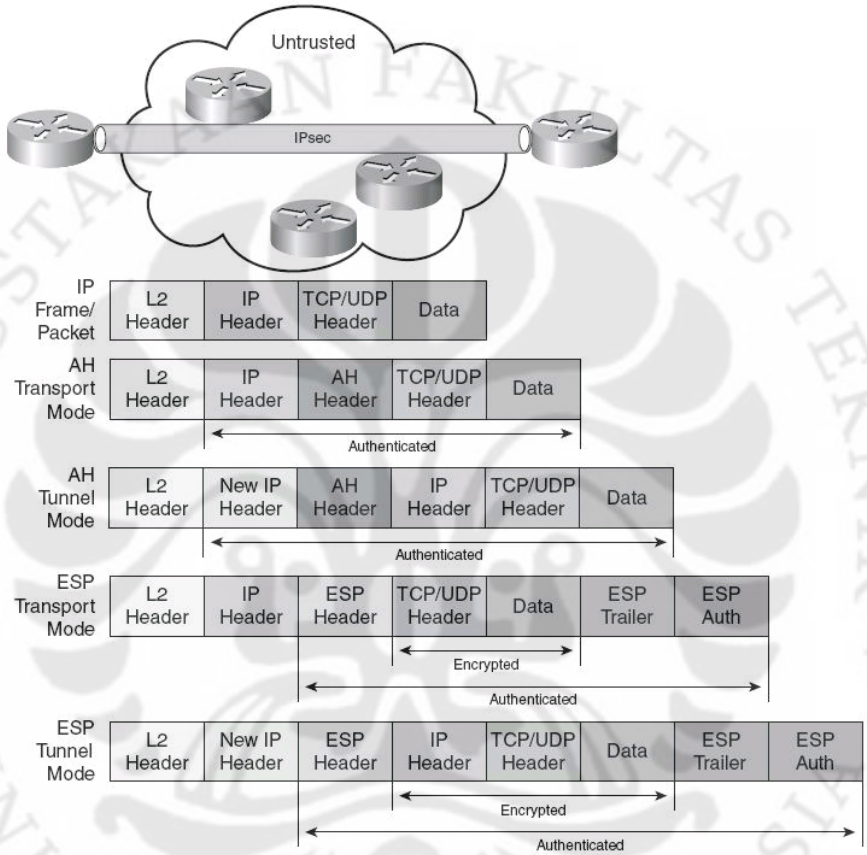
IPSec di design untuk memberikan keamanan trafik pada *network layer* dengan memberikan layanan utama yaitu[3]:

- *Confidentially* : Menjamin kerahasiaan data.
- *Integrity* : Menjamin integritas data dalam proses *transfer* data.
- *Authenticity* : Menjamin keaslian bahwa data berasal dari pengirim yang sebenarnya.

- *Anti Reply* : Menjamin tidak akan terjadi transaksi berulang-ulang

  Bagan di bawah ini menggambarkan tentang perbedaan Autentikasi dan Enkripsi pada algoritma AH dan ESP

Figure 12-2 *AH and ESP Headers*



Gambar 2. 5 Perbandingan Enkripsi dan Autentikasi pada IPSec [6]

Dalam mode transport protokol menyediakan proteksi terutama untuk layer protokol berikutnya. Sedangkan dalam mode *tunnel* protokol diterapkan untuk meneruskan paket IP.

2.2.3 GRE

Generic Routing Encapsulation (GRE) adalah Protokol *tunneling* yang memiliki kemampuan membawa lebih dari satu jenis protokol pengalamatan komunikasi. Bukan hanya paket beralamat IP saja yang dapat dibawanya, melainkan

banyak paket protokol lain seperti CNLP, IPX, dan banyak lagi. Namun, semua itu dibungkus atau dienkapsulasi menjadi sebuah paket yang bersistem pengalamatan IP. Kemudian paket tersebut didistribusikan melalui sistem *tunnel* yang juga bekerja di atas protokol komunikasi IP. Dengan menggunakan *tunneling* GRE, *router* yang ada pada ujung-ujung *tunnel* melakukan enkapsulasi paket-paket protokol lain di dalam header dari protokol IP. Hal ini akan membuat paket-paket tadi dapat dibawa ke manapun dengan cara dan metode yang terdapat pada teknologi IP. Dengan adanya kemampuan ini, maka protokol-protokol yang dibawa oleh paket IP tersebut dapat lebih bebas bergerak ke manapun lokasi yang dituju, asalkan terjangkau secara pengalamatan IP.

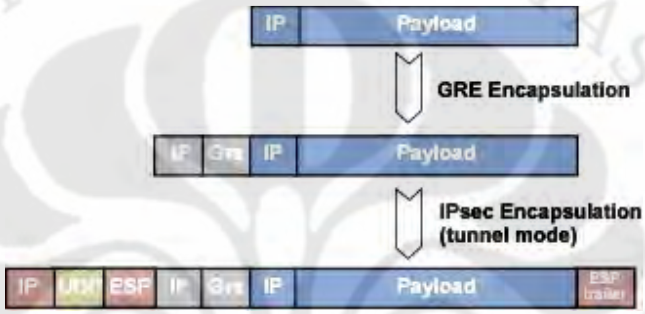
Aplikasi yang cukup banyak menggunakan bantuan protokol *tunneling* ini adalah menggabungkan jaringan-jaringan lokal yang terpisah secara jarak kembali dapat berkomunikasi. Atau dengan kata lain, GRE banyak digunakan untuk memperpanjang dan mengekspansi jaringan lokal yang dimiliki si penggunanya. Meski cukup banyak digunakan, GRE juga tidak menyediakan sistem enkripsi data yang lalu-lalang di *tunnel*-nya, sehingga semua aktivitas datanya dapat dimonitor menggunakan protocol analyzer biasa saja.

OSI model layer	Protocol
5. Application	RADIUS
4. Transport	UDP
3. Network (GRE-encapsulated)	IPv6
Encapsulation	**GRE**
3. Network	IPv4
2. Data Link	Ethernet
1. Physical	Ethernet physical layer

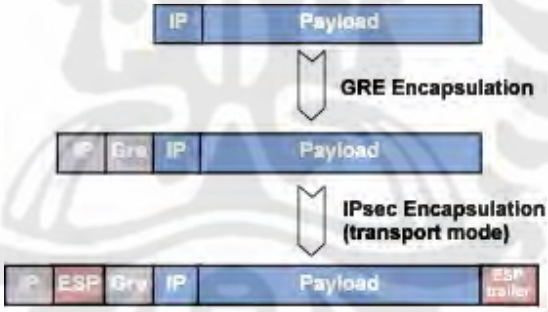
Tabel 2. 1 Protokol GRE pada OSI Model Layer[7]

Bits 0–4					5–7	8–12	13–15	16–31
C	R	K	S	s	Recur	Flags	Version	Protocol Type
Checksum *(optional)*								Offset *(optional)*
Key *(optional)*								
Sequence Number *(optional)*								
Routing *(optional)*								

Gambar 2. 6 Struktur Paket Header GRE [7]



Gambar 2. 7 Enkapsulasi GRE IPSec *Tunnel* Mode[10]



Gambar 2. 8 Enkapsulasi GRE IPSec Transport Mode[10]

2.3 EIGRP

EIGRP (*Enhanched Interior Gateway Routing Protocol*) adalah routing protocol yang hanya diadopsi oleh *router* cisco atau sering disebut sebagai proprietary protocol pada cisco, dimana EIGRP ini hanya bisa digunakan sesama *router* cisco. EIGRP menggunakan formula berbasis bandwidth dan *delay* untuk menghitung metric yang sesuai dengan suatu rute. EIGRP melakukan konvergensi secara tepat ketika menghindari loop. EIGRP tidak melakukan perhitungan-

perhitungan rute seperti yang dilakukan oleh protocol *link state*. Hal ini menjadikan EIGRP tidak membutuhkan desain ekstra, sehingga hanya memerlukan lebih sedikit memori dan proses dibandingkan protocol *link state[*11*]*.

Konvergensi EIGRP lebih cepat dibandingkan dengan protocol *distance vector*. Hal ini terutama disebabkan karena EIGRP tidak memerlukan fitur *loop-avoidance* yang pada kenyataannya menyebabkan konvergensi protocol *distance vector* melambat. Hanya dengan mengirim sebagian dari *routing update* (setelah seluruh informasi routing dipertukarkan). EIGRP mengurangi pembebanan di jaringan.

EIGRP sering disebut juga *hybrid- distance-vector* routing protocol, karena EIGRP ini terdapat dua tipe routing protocol yang digunakan, yaitu *distance vector* dan *link state*. Dalam perhitungan untuk menentukan jalur manakah yang terpendek, EIGRP menggunakan algoritma DUAL (*Diffusing Update Algorithm*) dalam menentukannya.

2.3.1 **Tabel dalam EIGRP**

EIGRP mempunyai 3 tabel dalam menyimpan informasi jaringannya[11]

1. Neighbor table : di table ini menyimpan list tentang *router- router* tetangganya. Setiap ada *router* baru yang dipasang, *address* dan *interface* langsung dicatat pada table ini.
2. Topology table : Tabel ini dibuat untuk memenuhi kebutuhan dari routing table dalam suatu *autonomous system* (AS). DUAL mengambil informasi dari table tetangga dan table topologi untuk melakukan kalkulasi *lowest cost router to each destination.*
3. Routing table : *the best routes* ke tujuan. Informasi tersebuit diambil table topologi.

EIGRP akan mengirimkan hello packet untuk mengetahui apakah *router-router* tetangganya masih hidup atau mati. Pengiriman *hello packet* tersebut bersifat simultan, dalam *hello packet* tersebut mempunyai *hold time*, bila dalam jangka waktu *hold time router* tetangga tidak membalas, maka *router* tersebut

dianggap mati.

Internal Route : Route-route yang berasal dari dalam suatu autonomous system dari *router-router* yang menggunakan routing protocol EIGRP, yang menjadi anggota dari *autonomous system* adalah yang mempunyai AND dari EIGRP yang sama dan mempunyai *autonomous system* yang sama juga. AND internal route adalah 90.

External Route : Route-route yang muncul dari luar *autonomous system*, baik *redistribution* secara manual maupun otomatis.

2.3.2 Kelebihan dan kekurangan EIGRP

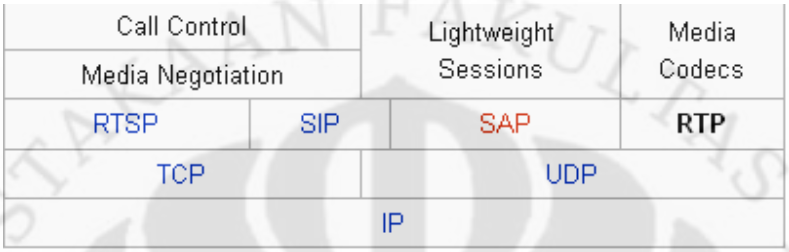
Kelebihan-kelebihan EIGRP[11]

- Satu-satunya protokol routing yang menggunakan route backup. Selain memaintain table routing terbaik, EIGRP juga menyimpan backup terbaik untuk setiap route sehingga setiap kali terjadi kegagalan pada jalur utama, maka EIGRP menawarkan jalur alternative tanpa menunggu waktu convergence.
- Mudah dikonfigurasi semudah RIP.
- Summarization dapat dilakukan dimana saja dan kapan saja. Pada OSPF summarization hanya bisa dilakukan di ABR dan ASBR.
- EIGRP satu-satunya yang dapat melakukan unequal load balancing.
- Kombinasi terbaik dari protokol distance vector dan link state.
- Mendukung multiple protokol network (IP, IPX, dan lain-lain).

Kelemahan utama EIGRP adalah protocol *Cisco-propritary,* sehingga jika diterapkan pada jaringan multivendor diperlukan suatu fungsi yang disebut *route redistribution.* Fungsi ini akan menangani proses pertukaran rute *router* di antara dua protocol *link state* (OSPF dan EIGRP), selain itu juga jika ada routing table boundednya putus maka semua bounded sehingga bandwith bnyak yang putus.

2.4 **RTP**

Real-time Transport Protocol (RTP) adalah standar untuk menyampaikan paket format audio dan video., protocol ini terdapat di atas UDP sebagaimana yang digambarkan di bawah ini :



Gambar 2. 9 Protokol RTP [8]

RTP digunakan secara luas pada komunikasi dan hiburan yang melibatkan streaming, video conference, dan telepon.

2.5 QoS

QoS adalah hasil kolektif dari berbagai kriteria performansi yang menentukan tingkat kepuasa penggunaan suatu layanan. Umumnya QoS dikaji dalam kerangka pengoptimalan kapasitas network untuk berbagai jenis layanan, tanpa terus menerus menambah dimensi network.

Berbagai aplikasi memiliki jenis kebutuhan yang berbeda. Misalnya transaksi data bersifat sensitif terhadap distorsi tetapi kurang sensitif terhadap *delay*. Sebaliknya, komunikasi suara bersifat sensitif terhadap tundaan dan kurang sensitif terhadap kesalahan. Tabel berikut [Dutta-Roy 2000] memaparkan tingkat kepekaan performansi yang berbeda untuk jenis layanan network yang berlainan. Parameter QoS. Bandwidth adalah rating transmisi data atau total maksimum(bit/sec) informasi yang dapat dikirimkan sepanjang channel.

LAYANAN	KEPEKAAN PERFORMANSI			
	BAND WIDTH	LOSS	DELAY	JITTER
Voice	Rendah	Medium	Tinggi	Tinggi
Transaksi Data	Rendah	Tinggi	Tinggi	Rendah
Email	Rendah	Tinggi	Rendah	Rendah
Browsing Biasa	Rendah	Medium	Medium	Rendah
Browsing Serius	Medium	Tinggi	Tinggi	Rendah
Transfer File	Tinggi	Medium	Rendah	Rendah
Video Conference	Rendah	Medium	Tinggi	Tinggi
Multicasting	Tinggi	Tinggi	Tinggi	Tinggi

Tabel 2. 2 Kepekaan Performansi untuk berbagai macam layanan [12]

IP tidak memiliki mekanisme pemeliharaan QoS. Protokol seperti TCP memang memungkinkan jaminan validitas data, sehingga suite TCP/IP selama ini dianggap cukup ideal bagi *transfer* data. Tetapi verifikasi data mengakibatkan tundaan antaran paket. Lagipula mekanisme ini tidak dapatdigunakan untuk paket dengan protocol UDP, seperti suara dan video *Throughput* adalah sejumlah data yang di*transfer* dibagi durasi engiriman paket tersebut, biasanya diekspresikan dalam satuan bytes/sec.

Performansi jaringan merujuk ke tingkat keceptan dan kehandalan penyampaian berbagai jenis beban data di dalam suatu sistem komunikasi. Performansi merupakan kumpulan dari berbagai besaran teknis, antara lain :

1. Availibiltas, yaitu persentase hidupnya sistema tau subsistem telekomunikasi. Idealnya, availibilitas harus mencapi 100%. Nilai availibilitas yang diakui cukup baik adalah 99,9999% yang menunjukkkan tingkat kerusakan sebesar 2,6 detik per bulan.
2. Thruoghput, yaitu kecepatan *transfer* data efektif yang diukur dalam bit/s. header-header dalam paket-paket data mengurangi nilai *throughput*. Maka penggunaan sebuah saluran secara bersama-sama juga mengurangi nilai ini
3. Packet loss, adalah jumlah paket yang hilang. Umumnya perangkat jaringan memiliki buffer untuk menampung data yang diterima. Jika

terjadi kongesti yang cukup lama, buffer akan penuh, dan data baru tidak diterima. Paket yang hilang ini harus diretransmisi, yang akan membutuhkan waktu tambahan. Umumnya packet loss diharuskan kurang dari 1% dalam waktu misalnya satu bulan

4. Latency, adalah waktu yang dibutuhkan data untuk menempuh jarak dari asal ke tujuan, *Delay* ini bisa dipengaruhi oleh jarak, kongesti, ataupun waktu olah
5. *Jitter*, atau variasi dalam latency, diakibatkan oleh variasi-variasi dalam panjang antrian, dalam waktu pengolahan data, dalam waktu yang dibutuhkan untuk retransmisi data (karena jalur yang digunakan mungkin berbeda), dan juga waktu dalam penghimpunan ulang paketpaket di akhir perjalanan.

Beberapa hal penyebab *throughput* yang didapat tidak sebesar bandwidth :

1. Routing protocol
2. Broadcast traffic
3. Collision
4. Header, dsb

Delay adalah waktu yang dibutuhkan oleh sebuah paket untuk mencapai tujuan.

Delay jitter adalah variasi *delay*.

2.6 NetMeeting Windows

NetMeeting merupakan aplikasi sederhana yang bisa digunakan pada versi windows 95 hingga XP di mana menggnakan standar H.263 untuk melakukan konferensi multimedia berbasis IP/Ethernet LAN [9]

- Audio *codec* menggunakan ITU G.723 dan memberikan bit-rates antara 4.8 kbit/s dan 64 kbit/s.
- Video *codec* menggunakan ITU H.263 dan mendukung 30 fps.
- *Codec* audio dan video NetMeeting menggunakan RTP yang berjalan di atas koneksi UDP/IP.

- Whiteboard, Chat, dan *Transfer* file menggunakan standar *data conferencing* ITU T.120 di atas koneksi TCP/IP.

2.6.1 Protokol Audio

NetMeeting menggunakan *codec* G.723.1 untuk protokol audio, di mana G.723.1 adalah *codec* audio untuk suara yang melakukan kompresi pada 30ms frame. Sebuah algoritma yang memiliki durasi 7.5 ms berarti total algoritma *delay*nya adalah 37.5 ms. Ada dua jenis jenis transmisi Dual rate speech coder untuk komunikasi multimedia yaitu 5.3 dan 6.3 kbps. Perlu diperhatikan bahwa *codec* ini berbeda dengan G.723 [9]

2.6.2 Protokol Video

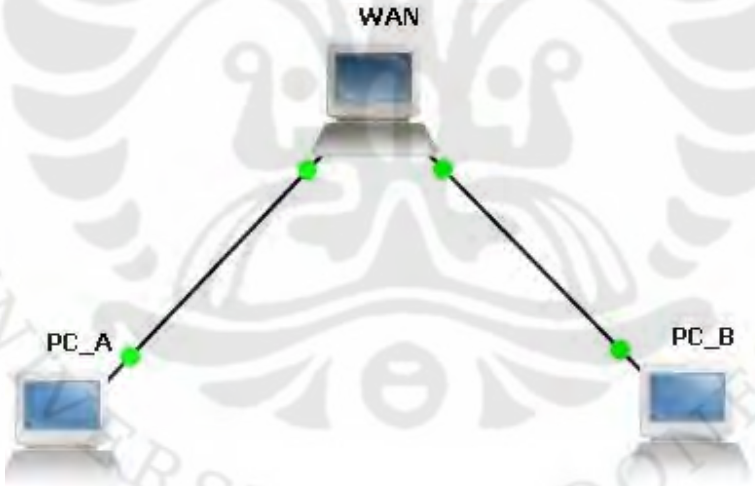
NetMeeting menggunakan H.263 yang merupakan standar *codec* video yang dirancang untuk kompresi bitrate yang rendah untuk videoconferencing. *Codec* ini dikembangkan oleh ITU-T Video Coding Experts Group (VCEG) pada sebuah project di akhir tahun 1995/1996 sebagai salah satu keluarga dari standar kode video H.26x pada domain ITU-T.[9]

BAB III
PERANCANGAN DAN SIMULASI

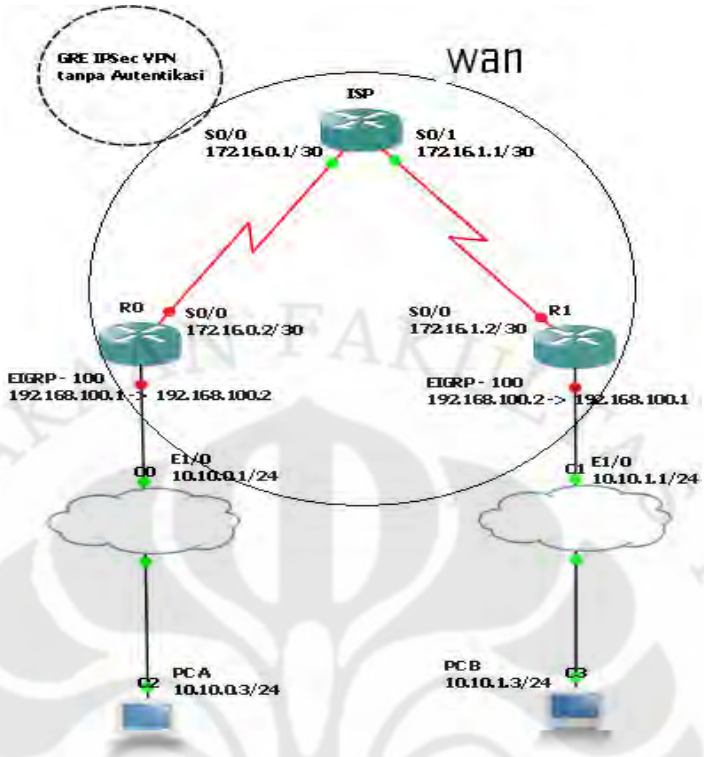
Pada bab ini akan dibahas perancangan sistem *IP-based video telephony* peer to peer pada topologi GRE/IPSEC VPN, dimulai dengan perencanaan topologi di GNS3, instalasi dan persiapan software dan hardware yang diperlukan, jaringan, konfigurasi, serta persiapan pengujian.

3.1 Perencanaan topologi jaringan

Model topologi jaringan yang digunakan pada pengujian untuk skripsi ini terdiri dari tiga buah komputer dimana satu komputer berperan sebagai topologi *router* WAN yang terletak di tengah dan dua komputer lain sebagai end-to-end device yang menjalankan aplikasi net meeting di mana saling terhubung langsung dengan kabel RJ45 cross-over, seperti pada gambar 3.1 berikut :



Gambar 3. 1 Topologi Jaringan *IP-based video telephony* pada VPN



Gambar 3. 2 Topologi GRE/IPSec VPN [1]

3.2 Kebutuhan pendukung simulasi

Kebutuhan akan infrastruktur terbagi menjadi dua macam, yaitu software dan hardware, dimana keduanya saling mendukung satu sama lain.

3.2.1 Kebutuhan Hardware

Kebutuhan hardware pada tugas akhir ini terdiri dari beberapa perangkat keras meliputi kabel RJ 45 cross over, NIC (Network Interface Card), Webcam/PC Camera, headset, 2 PC untuk menjalankan aplikasi netmeeting dan satu PC sebagai virtualisasi topologi VPN.

Headset

Pada aplikasi *IP-based video telephony*, headset memegang peranan yang sangat penting. Headset yang digunakan disini adalah headset yang terdiri dari mic dan speaker untuk komunikasi dua arah. Tidak diperlukan spesifikasi khusus untuk

headset agar bisa digunakan dalam komunikasi. Headset yang kami gunakan adalah Sonic Gear dan Creative, untuk aplikasi normal, kedua headset ini berfungsi sangat baik

NIC (Network Interface Card)

NIC atau yang lebih kenal dengan LAN Card merupakan komponen utama dalam sebuah jaringan lokal, NIC digunakan pada PC yang dijadikan virtualisasi topologi sebanyak dua buah dan dua PC lain masing-masing dipasangi 1 NIC. NIC yang digunakan ada yang onboard dengan merek Realtek dan LAN Card yang lain dengan merek 3Com

Webcam/PC Camera

Dalam aplikasi *IP-based video telephony*, Webcam/PC Camera memegang peranan yang paling penting. PC Camera digunakan untuk mengambil input berupa gambar untuk diolah dalam komputer dan kemudian dikompresi serta di transmisikan pada jaringan.

Pada saat ujicoba digunakan 2 buah PC Camera dengan merek Creative Webcam Pro.

Nama Komputer	: WAN
Processor	: Intel Core2Dua E4500 2.2 GHz
Motherboard	: ECS 945PT-A2
Graphic Card	: N-Vidia, GeForce 7300 GS 256 Mb
Memory	: DDR2 PC 6400 2GB Vgen
Sound Card	: Realtek Onboard
NIC	: Realtek Onboard, dan 3Com
Operating System	: Microsoft Windows XP SP2

Nama Komputer	: PC A
Processor	: Intel Pentium 4 3 GHz HT
Motherboard	: Asus P4i65GV

Graphic Card	: Intel 82865G
Memory	: DDR PC 2700 758 MB
Sound Card	: C-Media
NIC	: Realtek RTL 8139/810X
Operating System	: Microsoft Windows XP SP2

Nama Komputer	: PC B
Processor	: Intel Pentium 4 3 GHz HT
Motherboard	: Asus P4i65GV
Graphic Card	: Intel 82865G
Memory	: DDR PC 2700 1 GB
Sound Card	: C-Media
NIC	: Realtek RTL 8139/810X
Operating System	: Microsoft Windows XP SP2

3.2.2 Kebutuhan Software

Software yang digunakan pada skripsi ini adalah Wireshark, Netmeeting, GNS3, Secure CRT

Wireshark

Wireshark merupakan software yang digunakan untuk melakukan analisa jaringan komputer, wireshark dapat menganalisa beberapa parameter QoS seperti ,*jitter*, *delay*, *throughput*, dan packet loss dan lain lain serta dapat meng*capture* protocol yang sedang berjalan dalam jaringan tersebut, versi wireshark yang digunakan untuk pengujian adalah wireshark 0.99.5 dan dapat didownload secara gratis pada website www.wireshark.org

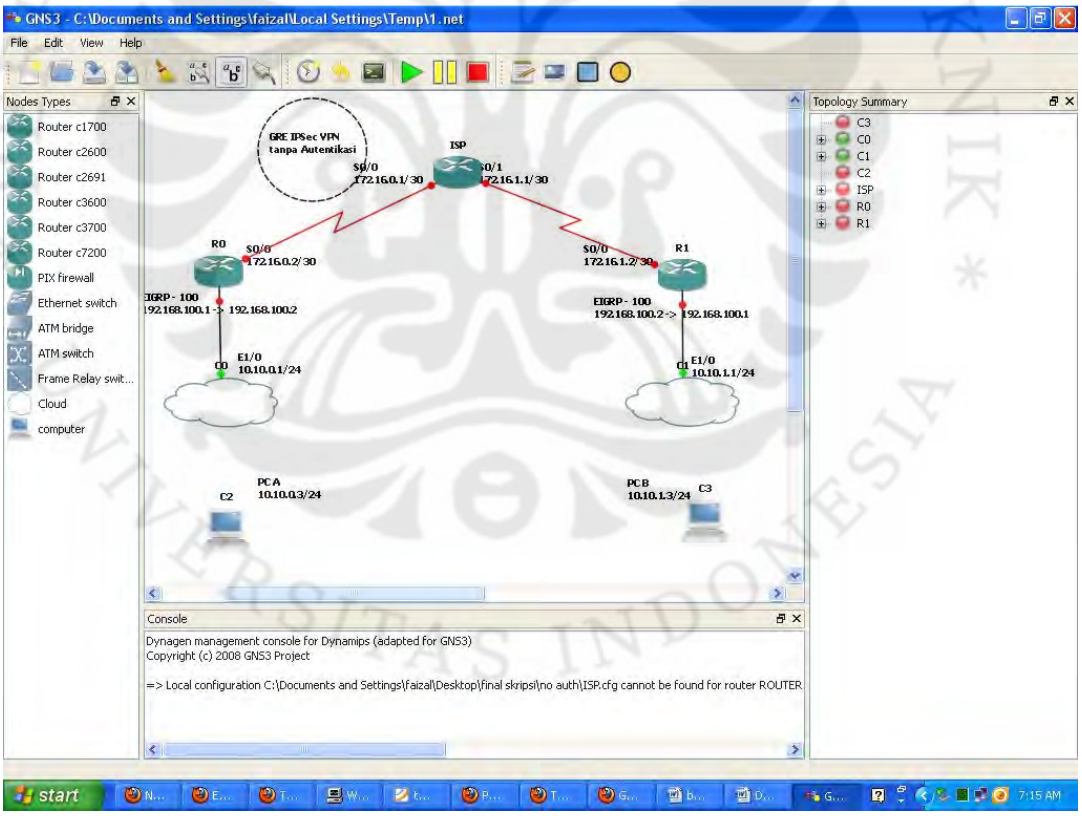
GNS3

GNS3 adalah sebuah aplikasi simulasi jaringan yang bersifat *open source*. Bagi Anda yang selama ini terbiasa menggunakan Packet Tracer untuk melakukan

simulasi jaringan dalam mempelajari jaringan di dunia Cisco juga bisa menggunakan GNS3 ini, karena GNS3 juga bisa melakukan hal yang sama seperti yang dilakukan oleh Packet Tracer dan bahkan bisa mensimulasi jaringan yang kompleks sekalipun. GNS3 juga cocok bagi yang sedang mengambil sertifikasi CCNA, CCNP, CCSP, dan beberapa sertifikasi Cisco yang lainnya.

GNS3 tersedia untuk platform Linux, Windows, dan MacOS X. Saat ini GNS3 telah mencapai versi 0.5, dan perkembangan GNS3 ini bisa dilihat di sourceforge maupun di situs resminya.

Fitur-fitur dari GNS3 ini antara lain : mendesain topologi jaringan berkualitas tinggi dan kompleks, emulasi dari berbagai macam platform *router* Cisco dan firewall PIX, simulasi jaringan Ethernet, ATM, dan Frame Relay, menghubungkan jaringan simulasi dengan jaringan di dunia nyata, dan meng-capture packet dengan Wireshark.



Gambar 2. 10 Fitur-fitur yang terdapat pada GNS3

3.3 Instalasi Infrastruktur

Pada bagian ini akan dibahas mengenai proses instalasi hardware dan software sistem *IP-based video telephony*.

3.3.1 Instalasi Komputer WAN

Untuk dapat menjadi virtual WAN maka computer perlu untuk di konfigurasi, adapun langkah-langkah konfigurasinya adalah sebagai berikut :

1. Memasang Interface Jaringan/LAN Card pada slot PCI selain dari LAN Card Onboard
2. Instalasi Sistem Operasi Windows XP Proffesional Service Pack 2
3. Instalasi driver-driver hardware yang diperlukan
4. Pemberian alamat IP pada komputer server sesuai dengan interface NIC masing-masing yaitu 10.10.0.1/24 dan 10.10.1.1/24
5. Melakukan instalasi program GNS3
6. Menambahkan IOS CISCO versi c3640-jk9s-mz.124-16a dan *router* yang digunakan adalah *router* 3640
7. Instalasi Secure CRT

3.3.2 Instalasi Wireshark

Sebelum melakukan instalasi wireshark kita perlu mendownload program wireshark dari alamat http://www.wireshark.org, untuk instalasi kita tinggal mengeklik double program wireshark-setup-0.99.5.exe dan ikuti petunjuk selanjutnya, pada program wireshark juga diperlukan program WinpCap untuk mengcapture protocol yang sudah terintegrasi pada wireshark-setup-0.99.8.exe. Wireshark diinstal pada PC B

3.3.3 Instalasi PC end-to-end

Untuk dapat menjadi virtual WAN maka computer perlu untuk di konfigurasi, adapun langkah-langkah konfigurasinya adalah sebagai berikut :

1. Memasang Interface Jaringan/LAN Card pada slot PCI selain dari LAN Card Onboard
2. Instalasi Sistem Operasi Windows XP Proffesional Service Pack 2
3. Instalasi driver-driver hardware yang diperlukan
4. Pemberian alamat IP pada PC_A dan PC_Bsesuai dengan interface NIC masing-masing secara berurutan yaitu 10.10.0.3/24 dan 10.10.1.3/24
5. Melakukan instalasi program GNS3
6. Menambahkan IOS CISCO versi 3640
7. Install Netmeeting
8. Instalasi Secure CRTP ada PC_A dn PC_B masing-masing dijalankan Netmeeting untuk melakukan komunikasi dua arah, dan wireshark diaktifkan pada salah satu PC untuk mengcapture packet yang diterima. Pengaturan IP untuk masing-masing PC adalah 10.10.0.3/24 (PC_A) dan 10.10.1.3/24 (PC_B).

3.3.4 Instalasi Netmeeting pada End-toEnd PC

Program Netmeeting ini merupakan aplikasi yang menjembatani end-to-end user untuk dapat berkomunikasi secara real time baik audio,video, chatbox, file *transfer*,whiteboard, dan sharing video.

Secara default program Netmeeting tidak muncul pada menu>all program tetapi kita harus mencari dan menginstal sendiri aplikasi tersebut dari directory : C:\Program Files\NetMeeting\conf.exe

Double klik pada file tersebut dan isikan data yang diminta oleh program tersebut. Abaikan apabila kita diminta untuk menceklist, next>next.dan akhirnya Netmeeting siap untuk digunakan.

3.3.4 Instalasi Webcam pada masing-masing client

Webcam perlu diinstall pada masing-masing client agar tampilan visual dapat di masing-masing user dapat ditampilkan pada netmeeting, instalasi dilakukan dengan memasukkan cd driver webcam pada cdrom dan pilih type dari webcam, serta lakukan instalasi sesuai dengan petunjuk.

3.3.5 Konfigurasi Topologi Pada computer WAN

Hal yang terpenting dalam simulasi ini yaitu komfigurasi computer WAN yang berisi lima buah *router* cisco yang terdiri dari sebuah *router* ISP, sebuah *router* R0, dan sebuah R1.

Secara umum pada computer wan terdiri dari ISP, R0 dan R1. ISP dimiliki oleh Service provider dan R0 dan R1 dimiliki oleh customer. Pada ISP di-configure GRE/IPSec VPN dengan menggunakan, dan EIGRP untuk Internal Gateway Protokolnya.

Sedangkan pada sisi R0 dan R1, routing protokol yang digunakan hanyalah static routing. Implementasi dari GRE/IPSec pada sisi R0 dan R1 yaitu dengan menggunakan enkripsi AES dan tanpa enkripsi.Untuk lebih lengkap dan detilnya file config dari tiap *router* tersebut terdapat pada lampiran.

3.4 Uji coba dan Pengambilan data

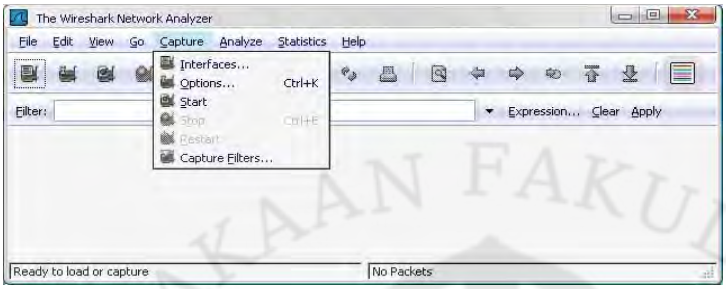
Uji coba dilakukan dengan menjalankan aplikasi NetMeeting pada PC_A dan PC_B, kemudian dari hasil uji coba tersebut di ambil data dengan bantuan software wireshark, adapun data-data yang diambil saat ujicoba meliputi :

a. Data ujicoba video
b. Data ujicoba audio
c. Data ujicoba *transfer* file

Langkah-langkah pengambilan data menggunakan wireshark adalah sebagai berikut :

i. Menjalankan software wireshark dari server pada menu start → wireshark →wireshark

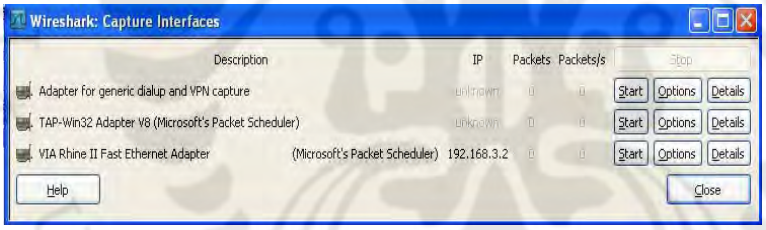
ii. mengcapture protokol yang sedang berjalan pada videoconference dengan bantuan wireshark, dengan mengklik Capture → interfaces



Gambar 3. 3 Langkah mengcapture protokol pada wireshark

iii. Klik option pada interface dan pilih interface NIC yang kita gunakann

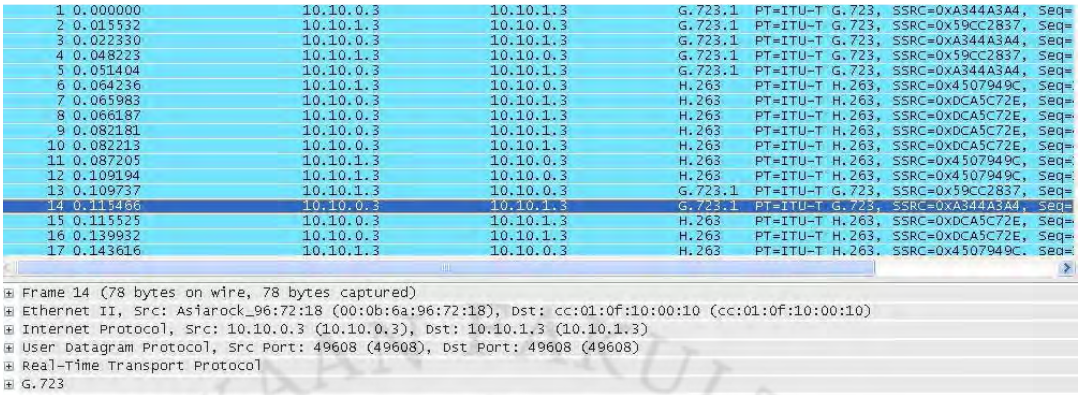
iv. Pada menu stop capture pilih after dan isi dengan 2 menit untuk menentukan lama proses capture



Gambar 3. 4 Memulai mengcapture trafik paket data

v. Proses capture data berjalan, pada tugas akhir ini pengambilan data pada masing-masing kondisi dilakukan selama 30 detik.

vi. Setelah proses capture selesai dengan mengklik stop maka akan muncul protokol-protokol yang muncul pada saat proses capture untuk di analisa



Gambar 3. 5 Protokol yang tercapture pada ujicoba

vii. Menyimpan file hasil capture dengan memilih menu file → save as kemudian beri nama untuk dilakukan proses analisa selanjutnya.

Gambar 3. 6 Tampilan Netmeeting setelah terjadi komunikasi dua arah

3.5 Pembuktian Keberhasilan Pengujian

Ada beberapa hal yang dapat dijadikan acuan bila simulasi GNS3 berhasil, di antaranya:

3.5.1 Interface Up untuk setiap Device

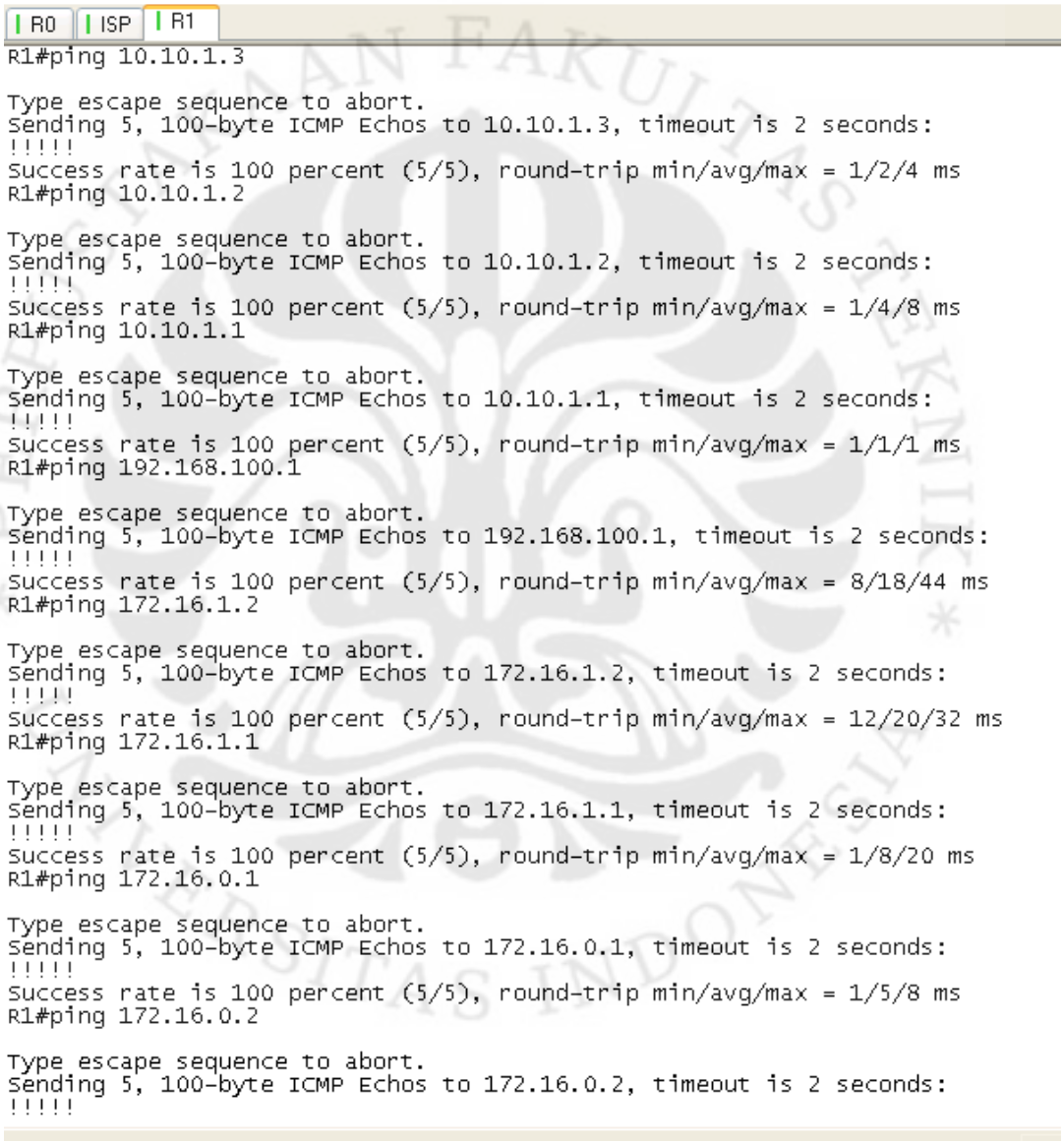
Pada Gambar 3.7 diperlihatkan interface up pada GNS3. Sebagai contoh interface up pada salah satu *router*, di mana yang up adalah interface serial yang menghubungkan ke *router* lain dan interface ethernet yang menghubungkan ke *client*, sementara interface *Tunnel* yang merupakan enkapsulasi dari VPN itu sendiri

```
*Mar  1 00:10:59.823: %SYS-5-CONFIG_I: Configured from console by consolep int b
Interface                  IP-Address      OK? Method Status                Protocol
Serial0/0                  172.16.1.2      YES manual up                    up
Serial0/1                  unassigned      YES manual administratively down down
Serial0/2                  unassigned      YES manual administratively down down
Serial0/3                  unassigned      YES manual administratively down down
Ethernet1/0                10.10.1.1       YES manual up                    up
Ethernet1/1                unassigned      YES manual administratively down down
Ethernet1/2                unassigned      YES manual administratively down down
Ethernet1/3                unassigned      YES manual administratively down down
Tunnel0                    192.168.100.2   YES manual up                    up
R1#
```

Gambar 3. 7 Interface UP

3.5.2 Hasil PING

Pada Gambar 3.8 diperlihatkan hasil PING untuk GRE IPSec yang tidak terenkripsi di mana Ping dilakukan dari R1 ke beberapa interface lain. Berikut sebagian contohnya, dan dari Gambar dapat diperlihatkan bahwa PING berhasil ke semua interface.



Gambar 3. 8 Hasil PING

3.5.2 Algoritma Enkripsi yang digunakan

Pada Gambar 3.9 diperlihatkan enkripsi yang digunakan pada GRE IPSec yang terenkripsi, di mana algoritma enkripsi yang digunakan adalah AES 128 bit. Adapun yang tidak terenkripsi maka *default*nya adalah DES 56 bit

```
RO#sh crypto isakmp key
Keyring              Hostname/Address                Preshared Key

default              172.16.1.2                      cisco
RO#sh crypto isakmp peers
Peer: 172.16.1.2 Port: 500 Local: 172.16.0.2
 Phase1 id: 172.16.1.2
RO#sh crypto isakmp policy

Global IKE policy
Protection suite of priority 1
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit
RO#sh crypto isakmp profile

RO#sh crypto isakmp sa
dst             src             state          conn-id slot status
172.16.0.2      172.16.1.2      QM_IDLE              1    0 ACTIVE

RO#
```

Gambar 3. 9 Algoritma Enkripsi yang digunakan pada GRE IPS VPN

BAB IV
ANALISA DATA HASIL SIMULASI DAN PEMBAHASAN

Proses Pengambilan data audio dan video dilakukan dengan menggunakan Wireshark ketika terjadi komunikasi dua arah antara *host*-to-*host* selama setengah menit, dan dilakukan sebanyak lima kali dan dipilih empat yang terbaik. Berikut adalah skema pengambilan data dan pengolahan data

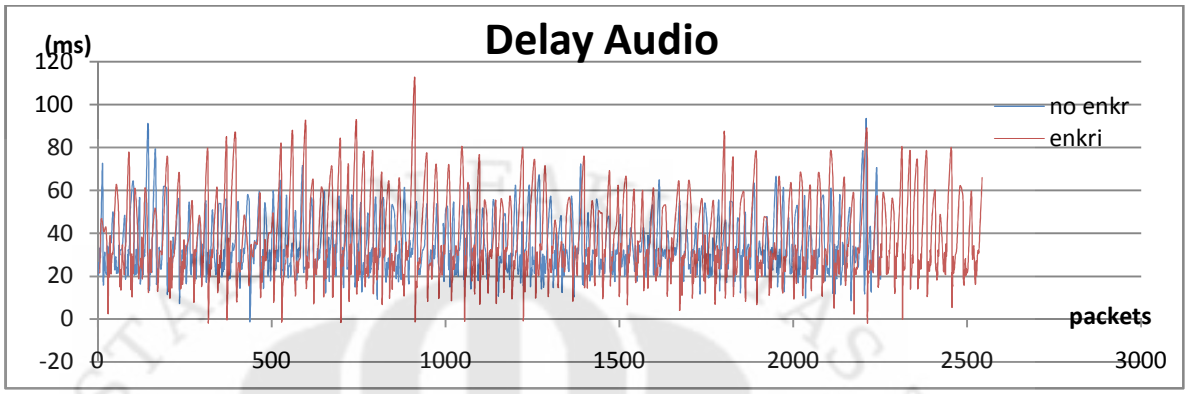
1. *Capturing* dalam bentuk .pcap
2. Ubah ke CSV untuk *stream analyze* dari protokol H.263 dan G.723.1 untuk paket yang diterima oleh PC B sehingga akan didapatkan file CSV,
3. Buka file CSV dengan menggunakan Microsoft Excel, untuk kemudian diklasifikan berdasarkan parameter yang hendak diperhatikan, yaitu *delay*, *jitter*, dan *throughput*
4. Dari kelima pengambilan data, untuk masing-masing dicari rata-rata, Kemudian disajikan dalam bentuk table

Proses pengambilan data *transfer* file dilakukan dengan menggunakan wireshark ketika terjadi pemindahan file dari PC B ke PC A hingga file selesai dikirim, file yang dikirimkan ada 6 jenis yaitu flv, mp3, doc, exe, pdf, dan zip. Pengambilan dilakukan sebanyak lima kali dan dipilih empat yang terbaik. Berikut skema pengambilan data dan pengolahan data

1. Capturing dalam bentuk .pcap
2. Kemudian catat *throughput* data pada setiap pengambilan melalui opsi Statistic-> summary
3. Olah dalam excel dan cari rata-rata serta buat dalam bentuk grafik

4.1 Analisa Grafik Audio

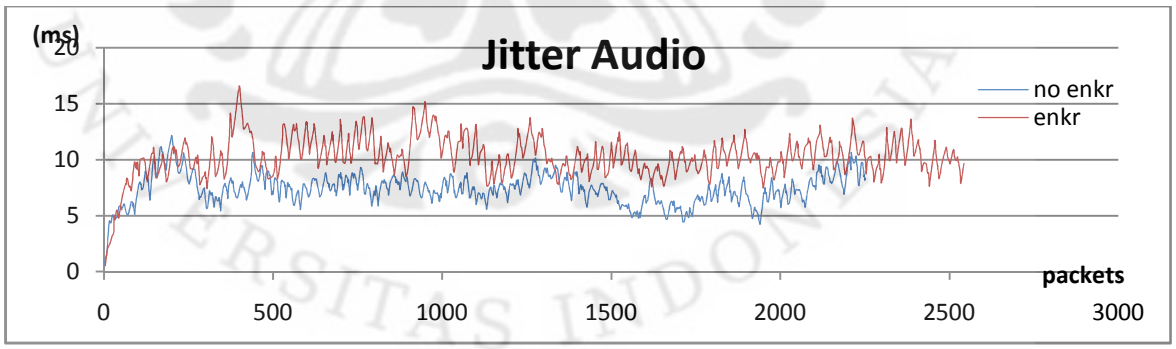
4.1.1 *Delay*



Gambar 4. 1 Perbandingan *Delay* Audio pada terenkripsi dan tidak terenkripsi

Dari Grafik 4.1, terlihat perbedaan *delay* antara yang tidak terenkripsi dan terenkripi tidak terlalu signifikan perbedaannya, hanya saja terlihat untuk yang terenkripsi lebih lebar jangkauan batas atas dan batas bawahnya bila dibandingkan dengan yang tidak terenkripsi. Hal ini dikarenakan, latency yang dihasilkan pada terenkripsi memiliki rentang yang cukup lebar sebagai akibat dari rata-rata *jitter* pada terenkripsi yang lebih besar dibandingkan tidak terenkripsi.

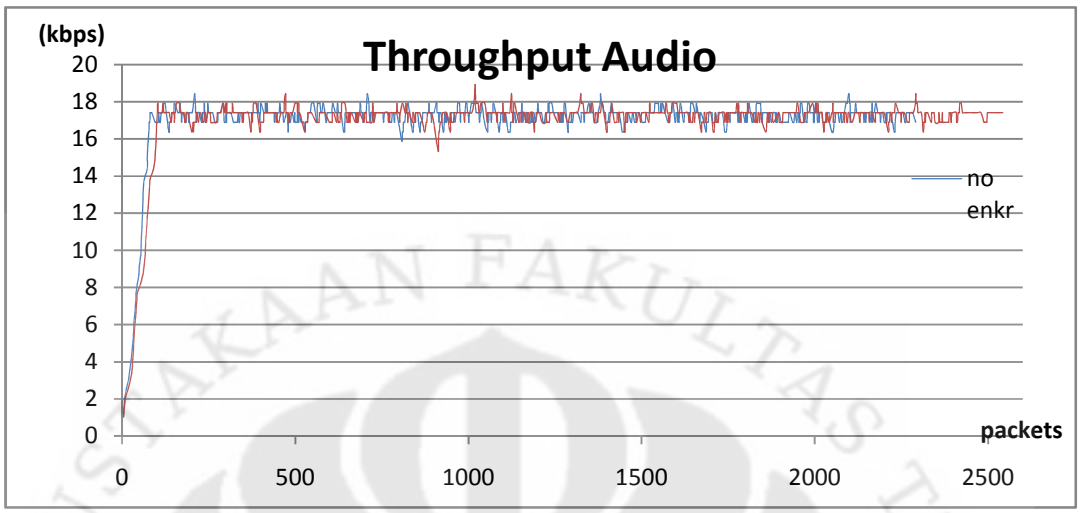
4.1.2 *Jitter*



Gambar 4. 2 Perbandingan *Jitter* Audio pada terenkripsi dan tidak terenkripsi

Dari Grafik 4.2, terlihat perbedaan *jitter* yang cukup signifikan, dikarenakan perbedaan *jitter* yang bervariasi antara 2-7 ms antara yang terenkripsi dan tidak terenkripsi. Hal ini juga mempengaruhi *delay* pada grafik sehingga dapat dilihat pada Grafik 4.1, rentangan *delay* pada terenkripsi lebih besar bila dibandingkan dengan yang tidak terenkripsi

4.1.3 *Throughput*

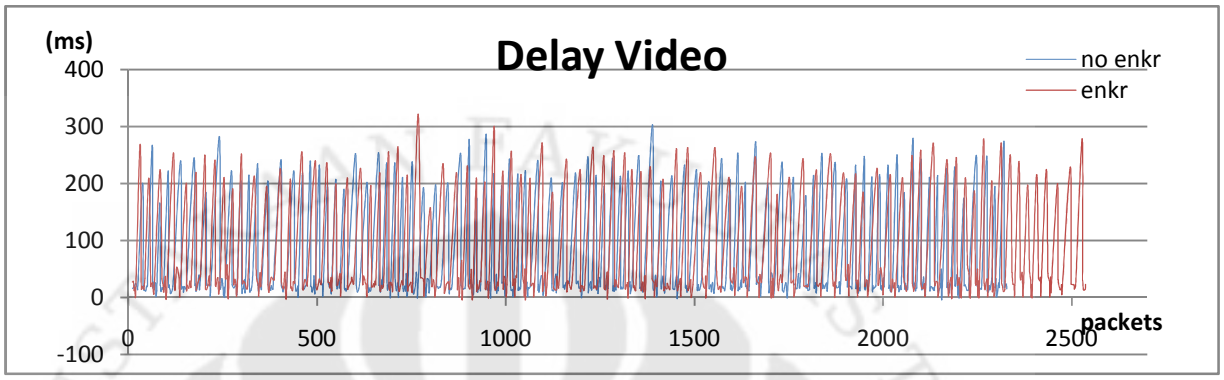


Gambar 4. 3 Perbandingan *Throughput* Audio pada terenkripsi dan tidak terenkripsi

Dari grafik *Throughput* dapat terlihat bila perbedaan antara yang terenkripsi dan yang tidak terenkripsi bisa dikatakan hampir sama, hal ini disebabkan oleh besar paket yang dilewatkan berupa audio cukup kecil dikarenakan panjang frame untuk audio sebesar 78 bytes (statis), sehingga pengaruh dari enkripsi tidak terlalu besar.

4.2 Analisa Grafik Video

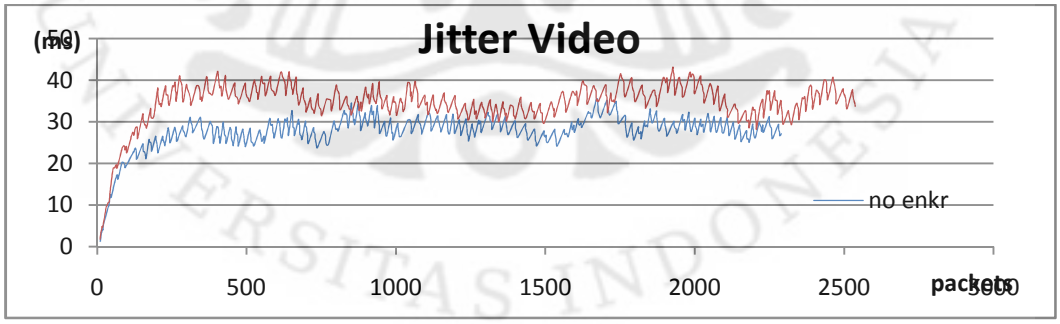
4.2.1 *Delay*



Gambar 4. 4 Perbandingan *Delay* Video pada terenkripsi dan tidak terenkripsi

Dari Grafik 4.4, terlihat perbedaan *delay* antara yang tidak terenkripsi dan terenkripi tidak terlalu signifikan perbedaannya, hanya saja terlihat untuk yang terenkripsi lebih lebar jangkauan batas atas dan batas bawahnya bila dibandingkan dengan yang tidak terenkripsi. Hal ini dikarenakan, latency yang dihasilkan pada terenkripsi memiliki rentang yang cukup lebar sebagai akibat dari rata-rata *jitter* pada terenkripsi yang lebih besar dibandingkan tidak terenkripsi.

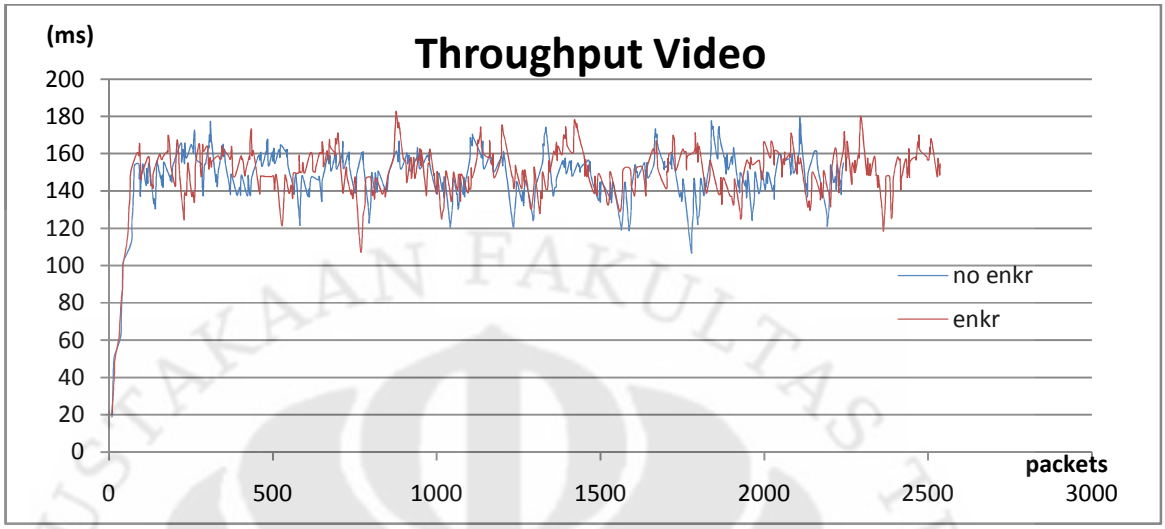
4.2.2 *Jitter*



Gambar 4. 5 Perbandingan *Jitter* Video pada terenkripsi dan tidak terenkripsi

Dari Grafik 4.5, terlihat perbedaan *jitter* yang cukup signifikan, dikarenakan perbedaan *jitter* yang bervariasi antara 1-7 ms antara yang terenkripsi dan tidak terenkripsi. Hal ini juga mempengaruhi *delay* pada grafik sehingga dapat dilihat pada Grafik 4.4, rentangan *delay* pada terenkripsi lebih besar bila dibandingkan dengan yang tidak terenkripsi

4.2.3 *Throughput*



Gambar 4. 6 Perbandingan *Throughput* Video pada terenkripsi dan tidak terenkripsi

Dari grafik *Throughput* dapat terlihat bila perbedaan antara yang terenkripsi dan yang tidak terenkripsi bisa dikatakan cukup berbeda, hal ini disebabkan oleh besar paket yang dilewatkan berupa video cukup besar dikarenakan panjang frame untuk video berbeda-beda (dinamis), sehingga pengaruh dari enkripsi walaupun ada tapi secara rata-rata tidak berbeda terlalu jauh.

4.3 Analisa Data Audio

JENIS (AUDIO)	PARAMETER	PENGAMBILAN			RATA-RATA		
		1	2	3	*Delay*	*Jitter*	*Throughput*
NO ENCRYP	*delay* (ms)	30.16	30.08	30.08	**30.11**		
	jitter (ms)	11.33	9.46	8.74		**9.84**	
	throughput (kbps)	17.03	17.03	17.05			**17.04**
ENCRYP	*delay* (ms)	30.16	30.13	30.08	**30.12**		
	jitter (ms)	10.27	10.49	10.18		**10.31**	
	throughput (kbps)	16.98	16.97	17.02			**16.99**
Persentase Perbedaan Encry terhadap No Encry (%)					**0.05**	**4.73**	**0.26**

Tabel 4. 1 Persentase Perbedaan antaraRata-rata *Delay*, *Jitter*, pada inputan AUDIO

Pada Tabel 4.1, terlihat bahwa besar rata-rata *delay* pada terenkripsi sebesar 30.12 ms dan yang tidak terenkripsi adalah 30.11 ms, sehingga didapatkan perbedaan persentase sebesar 0.05 %. Perbedaan yang sangat kecil bisa diabaikan sehingga kita bisa mengetahui pengaruh enkripsi pada audio untuk *delay* tidak berpengaruh sama sekali.

Adapun untuk rata-rata *jitter*, pada terenkripsi sebesar 10.31 ms dan yang tidak terenkripsi sebesar 9.84 ms. Perbedaan persentase mencapai 4.73 %, hal ini terjadi dikarenakan pada enkripsi, paket tersebut mengalami perlakuan enkripsi terlebih dahulu sehingga perbedaan *delay* paket yang satu dengan paket yang lain dapat terlihat. Hal ini berbeda dengan yang tidak terenkripsi yang memiliki rata-rata *jitter* lebih kecil.

Untuk *Throughput*, pada terenkripsi sebesar 16.99 kbps sementara pada yang tidak terenkripsi sebesar 17.04 kbps. Perbedaan persentase mencapai 0.26%, *throughput* yang tidak terenkripsi lebih besar dikarenakan *delay* yang lebih kecil bila dibandingkan dengan yang terenkripsi, walaupun sebenarnya perbedaannya sangatlah kecil, jadi pengaruh enkripsi sangat kecil sekali pada *throughput* audio.

4.4 Analisa Data Video

JENIS (VIDEO)	PARAMETER	PENGAMBILAN			RATA-RATA		
		1	2	3	*Delay*	*Jitter*	*Throughput*
NO ENCRYP	*delay* (ms)	54.42	48.19	48.08	**50.23**		
	jitter (ms)	26.77	25.57	25.82		**26.05**	
	throughput (kbps)	147.53	153.94	156.65			**152.70**
ENCRYP	*delay* (ms)	52.33	55.28	50.54	**52.71**		
	jitter (ms)	29.78	29.85	28.79		**29.48**	
	throughput (kbps)	147.34	148.86	150.07			**148.76**
Persentase Perbedaan Encry terhadap No Encry (%)					**4.94**	**13.14**	**2.59**

Tabel 4. 2Persentase Perbedaan antaraRata-rata *Delay*, *Jitter*, pada inputan Video

Pada Tabel 4.1, terlihat bahwa besar rata-rata *delay* pada terenkripsi sebesar 52.71 ms dan yang tidak terenkripsi adalah 50.23 ms, sehingga didapatkan perbedaan persentase sebesar 4.94 %. Perbedaan ini cukup besar dikarenakan pada video, paket yang dilewatkan cukup besar di samping itu juga karena faktor ukuran paket yang dinamis, walaupun demikian perbedaan 2.48 ms masih tidak terlalu berpengaruh terhadap performansi jaringan.

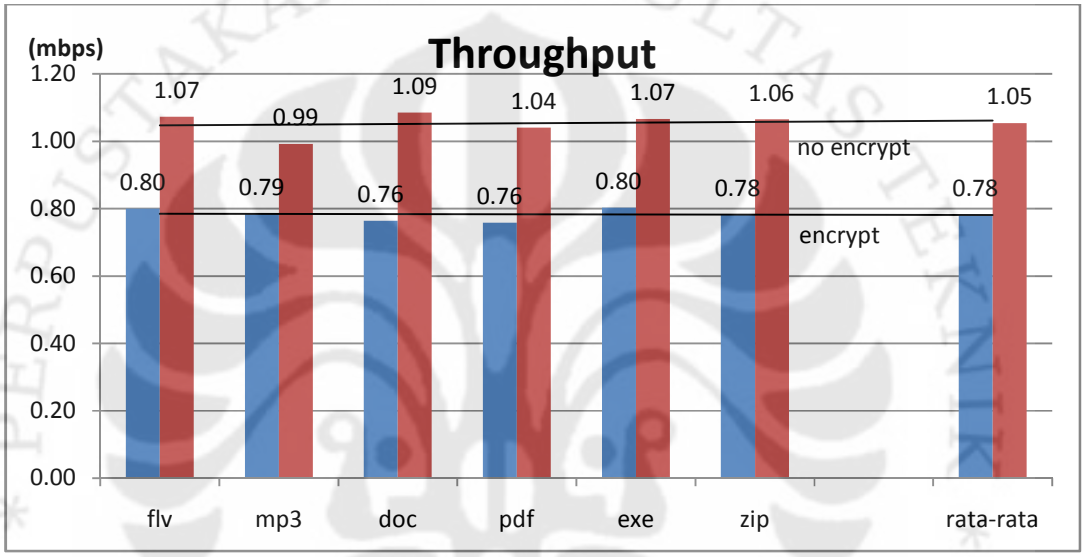
Adapun untuk rata-rata *jitter*, pada terenkripsi sebesar 29.48 ms dan yang tidak terenkripsi sebesar 26.05 ms. Perbedaan persentase mencapai 13.14 %, hal ini terjadi dikarenakan pada enkripsi, paket tersebut mengalami perlakuan enkripsi terlebih dahulu sehingga perbedaan *delay* paket yang satu dengan paket yang lain dapat terlihat. Hal ini berbeda dengan yang tidak terenkripsi yang memiliki rata-rata *jitter* lebih kecil.

Untuk *Throughput*, pada terenkripsi sebesar 148.76 kbps sementara pada yang tidak terenkripsi sebesar 152.70 kbps, perbedaannya mencapai 2.59%. *Throughput* yang tidak terenkripsi lebih besar dikarenakan *delay* yang lebih kecil bila dibandingkan dengan yang terenkripsi, walaupun sebenarnya perbedaannya sangatlah kecil, jadi pengaruh enkripsi sangat kecil sekali pada *throughput* video. *Throughput* dan *delay* berbanding terbalik

4.4 Analisa Data *Transfer* File

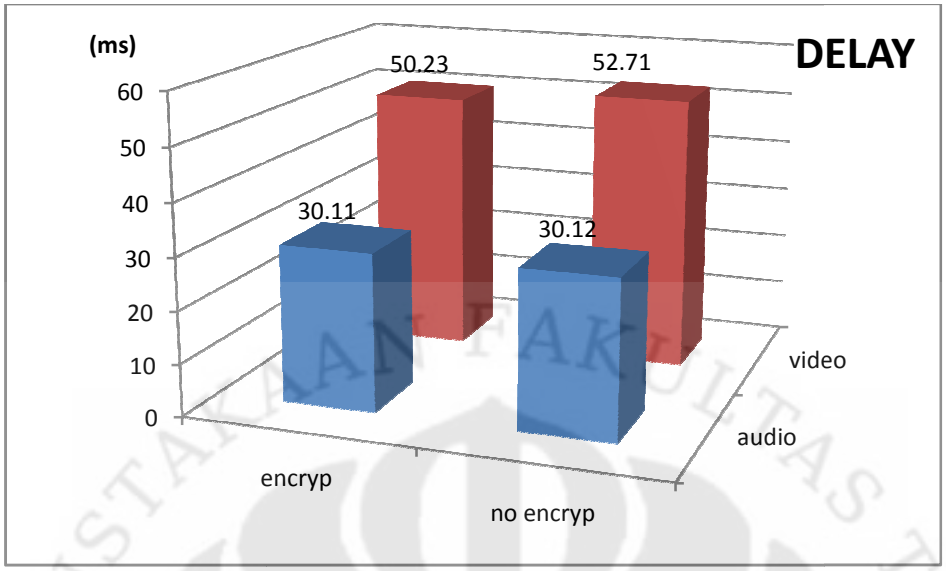
JENIS	TIPE FILE						RATA-RATA (mpbs)
	flv	mp3	doc	pdf	exe	zip	
Encry	0.80	0.79	0.76	0.76	0.80	0.78	0.78
No Encry	1.07	0.99	1.09	1.04	1.07	1.07	1.05

Tabel 4. 3 Rata-rata *Throughput* pada *transfer* file

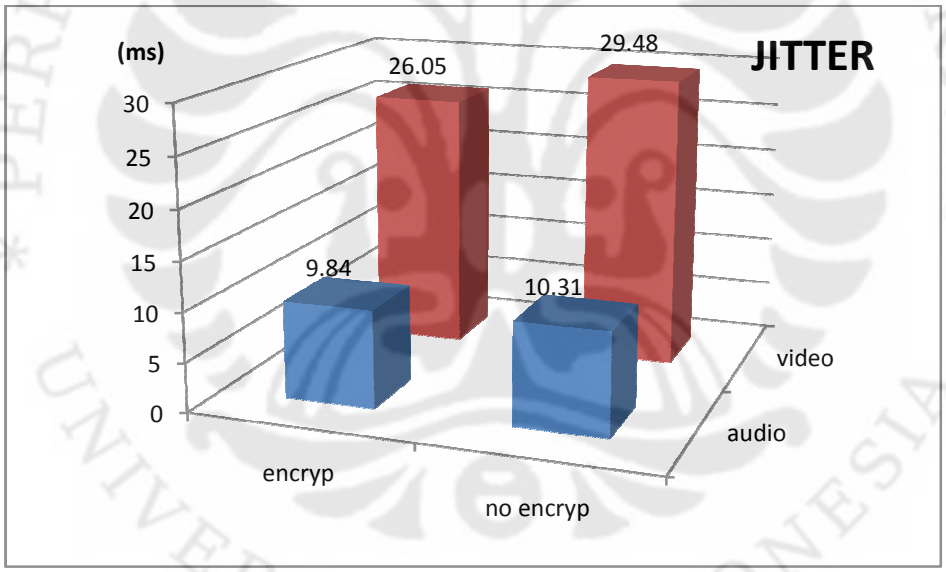


Gambar 4. 6 Rata-rata *Throughput* pada *transfer* file

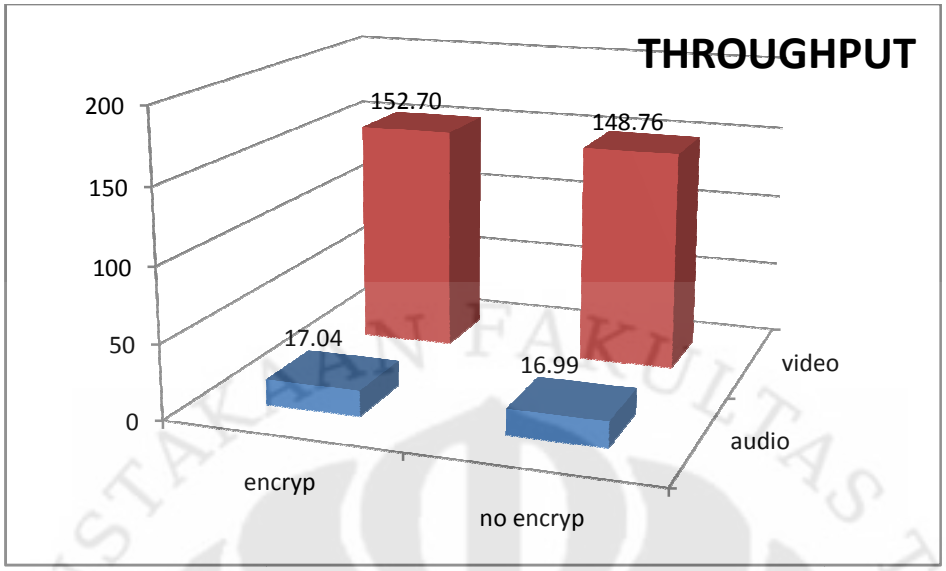
Dari tabel 4.3, terlihat bahwa perbedaan *throughput* yang terenkripsi dengan yang tidak terenkripsi cukup besar di mana rata-rata *throughput* yang tidak terenkripsi sebesar 1.05 mpbs sementara yang terenkripsi sebesar 0.78 mbps, dan persentase perbedaannya adalah 25.7 %. Pengaruh enkripsi sangat berpengaruh pada *transfer* file, dikarenakan ukuran file yang cukup besar dan bervarisi sehingga perbedaannya lumayan besar.



Gambar 4. 7 Gambar Perbandingan *Delay*



Gambar 4. 8 Gambar Perbandingan *Jitter*



Gambar 4. 9 Gambar Perbandingan *Throughput*

4.5 Analisa Keseluruhan

Setelah membandingkan hasil yang diperoleh baik yang berupa grafik line maupun bar serta tabel, maka dapat dilihat bahwa secara umum perbedaan *delay* dan *jitter* pada terenkripsi lebh besar dibandingkan yang tidak terenkripsi, namun *throughput* lebih kecil. Walaupun demikian, perbedaan tersebut sangatlah kecil sehingga bisa diabaikan. Hal ini berlaku pula baik yang video maupun yang audio. Perbedaan tersebut walaupun kecil dipengaruhi oleh enkripsi pada data sehingga membutuhkan waktu yang banyak agar *router* memproses setiap pay load yang dilewatkan, penggunaan daya, adanya block size pada enkripsi.

Selain itu juga, *jitter* pada audio lebih kecil dikarenakan untuk data yang memiliki prioritas lebih tingi maka *jitter* dan paket loss akan semakin kecil. Sehingga audio datang terlebih dahulu, hal ini bisa dilihat dari Tabel 4.2 di mana *delay* audio dan *jitter* audio selalu lebih kecil bila dibandingkan dengan *delay* dan *jitter* pada video.

Berdasarkan grafik *Delay*, *Jitter* dan *Throughput*, terlihat bahwa untuk data audio memiliki kecenderungan yang hampir sama baik yang terenkripsi dan yang tidak terenkripsi, adapun pada video, cukup memiliki perbedaan. Hal ini disebabkan

oleh penggunaan pay load yang berbeda untuk audio dan video, dikarenakan pay load dari audio statis, sementara pada video dinamis, sehingga kecenderungan pada audio lebih stabil bila dibandingkan pada video.

Data-data yang disajikan untuk *delay*, *jitter* dan *throughput* masih reliable dikarenakan masih berada di bawah 150 ms untuk *delay* dan 50 ms untuk *jitter*

BAB V
KESIMPULAN

Setelah melakukan serangkaian simulasi dan pengujian, maka dapat disimpulkan bila pada pengujian ini:

1. GRE IPSec VPN Terenkripsi pada audio memiliki perbedaan *delay* 0.05% , dan *jitter* 4.73% lebih besar serta *throughput* lebih kecil 0.26%, bila dibandingan dengan yang tidak menggunakan enkripsi,
2. GRE IPSec VPN Terenkripsi pada video memiliki perbedaan *delay* 4.94% , dan *jitter* 13.14% lebih besar serta *throughput* lebih kecil 2.59%, bila dibandingan dengan yang tidak menggunakan enkripsi,,
3. Perbedaan *Throughput* pada *transfer* file untuk GRE IPSec VPN yang tidak terenkripsi lebih besar 0.27 mbps dengan persentase 25.7 % bila dibandingkan dengan yang terenkripsi
4. Enkripsi menyebabkan terjadinya penurunan QoS yang sangat kecil untuk konfigurasi jaringan yang sama. Toleransi Error yang diberikan ketika adanya enkripsi tidak terlalu signifikan bila dibandingkan dengan tanpa enkripsi sehingga pada dasarnya penggunaan enkripsi tidak membebani performa jaringan VPN.
5. Paket Audio memiliki prioritas yang lebih tinggi sehingga memiliki *jitter* dan *delay* yang lebih kecil.
6. Penggunaan Enkripsi cukup signifikan pada *transfer* data, dikarenakan ukuran tiap paket yang dikirimkan jauh lebih besar bila dibandingkan *transfer* audio ataupun video

DAFTAR ACUAN

[1] As Tawa, I Gede. *Analisis Implementasi Manajemen Bandwidth IP DSLAM.* Diakses 30 Juni 2009 http://www.ittelkom.ac.id/library/index.php?option=com_content&view=article&id=629:vpn&catid=10:jaringan&Itemid=15.

[2] Widiastuti. *Implementasi Vpn Server Pada Jaringan Program Rofesional ITt Telkom Bandung.* Diakses 1 Juli 2009 http://www.ittelkom.ac.id/library/index.php?option=com_content&view=article&id=407:vpn-server-&catid=10:jaringan&Itemid=15

[3] Wendy, Aris dan Ahmad SS Ramadhana. *Membangun VPN Linux Secara Cepat*. Penerbit Andi. Yogyakarta. 2005

[4] Topology: BlindHogs' *EIGRP Over GRE-IPSec VPN With No Authentication Lab Configs*. Diakses 20 Juni 2009 http://www.gns3-labs.com/2008/06/02/topology-blindhogs-greipsec-vpn-no-authentication-lab-configs/

[5] Topology: BlindHogs' *EIGRP Over GRE-IPSec VPN Tunnel Part-2 With AUTHENTICATION*. Diakses 20 Juni 2009 http://www.gns3-labs.com/2008/06/02/topology-blindhogs-eigrp-over-gre-ipsec-vpn-*tunnel*-part-2-w-authentication/

[6] _____, Diakses tanggal 6 Juli 2009

http://blogimg.chinaunix.net/blog/upfile2/080106135559.jpg

[7] _____, *Generic Routing Encapsulation*. Diakses 25 Juni 2009 http://en.wikipedia.org/wiki/Generic_Routing_Encapsulation

[8] _____, *Real-time Transport Protocol*. Diakses 25 Juni 2009 http://en.wikipedia.org/wiki/Real-time_Transport_Protocol

[9]_____, *NetMeeting protocol architecture.* Diakses 27 Juni 2009 http://www.ensc.sfu.ca/~ljilja/cnl/presentations/milan/milan_thesis/tsld029.htm

[10]_____, Designing Site-to-Site IPsec VPNs - Part 2. Diakses 7 Juli 2009 http://www.nil.si/ipcorner/IPsecVPN2/

[11]_____, EIGRP FAQ. Diakses 7Juli 2009 http://www.secev.com/support/networking/eigrp.htm

[12]_____, Multi Protocol Label Switch. Telkom.co.id. mpls.ppt

DAFTAR PUSTAKA

Wendy, Aris dan Ahmad SS Ramadhana. *Membangun VPN Linux Secara Cepat*. Penerbit Andi. Yogyakarta. 2005

Chadda, Ankur. *Quality of Service Testing Methodology.* University of Bombay. India. 2004

Henmi, Anne(ed.) ; Lucas, Mark; Singh, Abhishek; Cantrell, Chris. *Firewall Policies and VPN Configurations.* Syngress Publishing. Boston. 2004

Slice, Don. *EIGRP for IP*. Addison Wesley Professional, Boston. 2008

Hutapea, Tommy P.M. *Virtual Private Network (VPN) Dynamic, Jawaban Keamanan untuk Intranet Pada Suatu Perusahaan.*Diakses 1 Juli 2009. http://ikc.cbn.net.id/populer/tommy/tommy-vpn.zip

LAMPIRAN A

Enkripsi GRE/IPSec VPN

Konfigurasi ISP

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ISP
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
no aaa new-model
memory-size iomem 5
!
!
ip cef
no ip domain lookup
!
!
interface Serial0/0
 description = menuju R0 =
 ip address 172.16.0.1 255.255.255.252
 serial restart-delay 0
!
interface Serial0/1
 description = menuju R1 =
 ip address 172.16.1.1 255.255.255.252
 serial restart-delay 0
!
interface Serial0/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial0/3
 no ip address
 shutdown
 serial restart-delay 0
!
interface Ethernet1/0
 no ip address
 shutdown
 half-duplex
!
interface Ethernet1/1
 no ip address
```

```
 shutdown
 half-duplex
!
interface Ethernet1/2
 no ip address
 shutdown
 half-duplex
!
interface Ethernet1/3
 no ip address
 shutdown
 half-duplex
!
ip http server
no ip http secure-server
!
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 password cisco
 login
!
!
End
```

Konfigurasi *Router* 0

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R0
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$jHc8$0OkRLcV8BRALqjp4/lVSE1
!
no aaa new-model
memory-size iomem 5
!
!
ip cef
ip host R0 172.16.0.2
ip host R1 172.16.1.2
ip host ISP 172.16.0.1
!
crypto isakmp policy 1
```

```
 encr aes
 authentication pre-share
 group 5
crypto isakmp key cisco address 172.16.1.2
!
!
crypto ipsec transform-set aes-sha esp-aes esp-sha-hmac
!
crypto map vpn 10 ipsec-isakmp
 description VPN menuju R1
 set peer 172.16.1.2
 set transform-set aes-sha
 match address 101
!
!
interface Tunnel0
 description = GRE Tunnel menuju R1
 ip address 192.168.100.1 255.255.255.0
 ip mtu 1500
 ip tcp adjust-mss 1400
 keepalive 10 3
 tunnel source 172.16.0.2
 tunnel destination 172.16.1.2
!
interface Tunnel2
 no ip address
!
interface Tunnel12
 no ip address
!
interface Serial0/0
 description = menuju ISP
 ip address 172.16.0.2 255.255.255.252
 serial restart-delay 0
 crypto map vpn
!
interface Serial0/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial0/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial0/3
 no ip address
 shutdown
 serial restart-delay 0
!
interface Ethernet1/0
 description = menuju LAN R0 =
 ip address 10.10.0.1 255.255.255.0
```

```
 half-duplex
!
interface Ethernet1/1
 no ip address
 shutdown
 half-duplex
!
interface Ethernet1/2
 no ip address
 shutdown
 half-duplex
!
interface Ethernet1/3
 no ip address
 shutdown
 half-duplex
!
router eigrp 100
 network 10.0.0.0
 network 192.168.100.0
 no auto-summary
!
ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 172.16.0.1
!
access-list 101 permit gre host 172.16.0.2 host 172.16.1.2
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
!
End
```

Konfigurasi *Router* 1

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
```

```
boot-start-marker
boot-end-marker
!
enable secret 5 $1$UYYK$D5sCGXN9ymQA7VRhDvC4W1
!
no aaa new-model
memory-size iomem 5
!
!
ip cef
no ip domain lookup
ip host R0 172.16.0.2
ip host R1 172.16.1.2
ip host ISP 172.16.0.1
!
!
crypto isakmp policy 1
 encr aes
 authentication pre-share
 group 5
crypto isakmp key cisco address 172.16.0.2
!
!
crypto ipsec transform-set aes-sha esp-aes esp-sha-hmac
!
crypto map vpn 10 ipsec-isakmp
 description = VPN dari R1 menuju R0 =
 set peer 172.16.0.2
 set transform-set aes-sha
 match address 100
!
!
interface Tunnel0
 description = GRE Tunnel menuju R0
 ip address 192.168.100.2 255.255.255.0
 ip mtu 1500
 ip tcp adjust-mss 1400
 keepalive 10 3
 tunnel source 172.16.1.2
 tunnel destination 172.16.0.2
!
interface Serial0/0
 ip address 172.16.1.2 255.255.255.252
 serial restart-delay 0
 crypto map vpn
!
interface Serial0/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial0/2
 no ip address
 shutdown
```

```
 serial restart-delay 0
!
interface Serial0/3
 no ip address
 shutdown
 serial restart-delay 0
!
interface Ethernet1/0
 description = menuju LAN R1 =
 ip address 10.10.1.1 255.255.255.0
 half-duplex
!
interface Ethernet1/1
 no ip address
 shutdown
 half-duplex
!
interface Ethernet1/2
 no ip address
 shutdown
 half-duplex
!
interface Ethernet1/3
 no ip address
 shutdown
 half-duplex
!
router eigrp 100
 network 10.0.0.0
 network 192.168.100.0
 auto-summary
!
ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 172.16.1.1
!
access-list 100 permit gre host 172.16.1.2 host 172.16.0.2
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
!
End
```

Tanpa Enkripsi GRE/IPSec VPN

Konfigurasi ISP

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ISP
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
!
!
ip cef
!
interface Serial0/0
 description = menuju R0 =
 ip address 172.16.0.1 255.255.255.252
 serial restart-delay 0
!
interface Serial0/1
 description = menuju R1 =
 ip address 172.16.1.1 255.255.255.252
 serial restart-delay 0
!
interface Serial0/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial0/3
 no ip address
 shutdown
 serial restart-delay 0
!
interface Ethernet1/0
 no ip address
 shutdown
 half-duplex
!
interface Ethernet1/1
 no ip address
 shutdown
 half-duplex
!
interface Ethernet1/2
 no ip address
```

```
 shutdown
 half-duplex
!
interface Ethernet1/3
 no ip address
 shutdown
 half-duplex
!
ip http server
no ip http secure-server
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
 password cisco
 login
!
!
End
```

Konfigurasi *Router* 0

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R0
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$jHc8$0OkRLcV8BRALqjp4/lVSE1
!
no aaa new-model
memory-size iomem 5
!
ip cef
ip host R0 172.16.0.2
ip host R1 172.16.1.2
ip host ISP 172.16.0.1
!
interface Tunnel0
 description = GRE Tunnel menuju R1
 ip address 192.168.100.1 255.255.255.0
 tunnel source 172.16.0.2
 tunnel destination 172.16.1.2
!
```

```
interface Tunnel2
 no ip address
!
interface Tunnel12
 no ip address
!
interface Serial0/0
 description = menuju ISP =
 ip address 172.16.0.2 255.255.255.252
 serial restart-delay 0
!
interface Serial0/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial0/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial0/3
 no ip address
 shutdown
 serial restart-delay 0
!
interface Ethernet1/0
 description = menuju LAN R1 =
 ip address 10.10.0.1 255.255.255.0
 half-duplex
!
interface Ethernet1/1
 no ip address
 shutdown
 half-duplex
!
interface Ethernet1/2
 no ip address
 shutdown
 half-duplex
!
interface Ethernet1/3
 no ip address
 shutdown
 half-duplex
!
router eigrp 100
 network 10.0.0.0
 network 192.168.100.0
 no auto-summary
!
ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 172.16.0.1
```

```
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
!
End
```

Konfigurasi *Router* 1

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$UYYK$D5sCGXN9ymQA7VRhDvC4W1
!
no aaa new-model
memory-size iomem 5
!
!
ip cef
ip host R0 172.16.0.2
ip host R1 172.16.1.2
ip host ISP 172.16.0.1
!
interface Tunnel0
 description = GRE Tunnel menuju R0 =
 ip address 192.168.100.2 255.255.255.0
 tunnel source 172.16.1.2
 tunnel destination 172.16.0.2
!
interface Serial0/0
 ip address 172.16.1.2 255.255.255.252
 serial restart-delay 0
!
interface Serial0/1
 no ip address
 shutdown
 serial restart-delay 0
```

```
!
interface Serial0/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial0/3
 no ip address
 shutdown
 serial restart-delay 0
!
interface Ethernet1/0
 description = menuju LAN R1 =
 ip address 10.10.1.1 255.255.255.0
 half-duplex
!
interface Ethernet1/1
 no ip address
 shutdown
 half-duplex
!
interface Ethernet1/2
 no ip address
 shutdown
 half-duplex
!
interface Ethernet1/3
 no ip address
 shutdown
 half-duplex
!
router eigrp 100
 network 10.0.0.0
 network 192.168.100.0
 auto-summary
!
ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 172.16.1.1
!
control-plane
!

line con 0
line aux 0
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
!
end
```