UNIVERSITAS INDONESIA

ANALISA PERBANDINGAN QoS : PENGARUH IMPLEMENTASI ENKRIPSI 3DES DAN AES PADA MPLS-VPN UNTUK LAYANAN *IP-BASED* VIDEO *TELEPHONY*

SKRIPSI

GATOT S

0405030389

FAKULTAS TEKNIK

DEPARTEMEN ELEKTRO

DEPOK

JUNI 2009

UNIVERSITAS INDONESIA

ANALISA PERBANDINGAN QoS : PENGARUH IMPLEMENTASI ENKRIPSI 3DES DAN AES PADA MPLS-VPN UNTUK LAYANAN *IP-BASED* VIDEO *TELEPHONY*

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Teknik

GATOT S

0405030389

FAKULTAS TEKNIK

DEPARTEMEN ELEKTRO

DEPOK

JUNI 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 : Gatot S

NPM : 0405030389

Tanda Tangan :

Tanggal : 17 Juni 2009

Analisa perbandingan..., Gatot S., FT UI, 2009

LEMBAR PENGESAHAN

Skripsi ini diajukan oleh :

Nama : Gatot S

NPM : 0405030389

Program Studi : Teknik Elektro

Judul Skripsi : ANALISA PERBANDINGAN QoS: PENGARUH IMPLEMENTASI ENKRIPSI 3DES DAN AES PADA MPLS-VPN UNTUK LAYANAN 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

Analisa perbandingan..., Gatot S., FT UI, 2009

KATA PENGANTAR & UCAPAN TERIMA KASIH

Puji syukur saya panjatkan kepada Allah SWT, 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 Program Studi 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) Orang tua dan keluarga yang telah memberikan dukungan moral dan material
(2) Muhammad Salman, S.T, M.T, selaku dosen pembimbing yang telah menyediakan waktu, tenaga, dan pikiran serta solusi-solusi untuk mengarahkan dalam penyusunan skripsi ini;
(3) Pateru Yusuf, sebagai salah satu *Network* Engineer Datacomm yang telah memberikan jawaban-jawaban menarik tentang *MPLS*.
(4) Sofyan Nugraha, sebagai salah satu *Network* Engineer MULTIPOLAR yang telah mengenalkan GNS3.
(5) Rafdian, yang telah mengajarkan konfigurasi LVPN diatas GNS3 secara detil, sistematis dan terarah
(6) Faizal Firmansyah & I. Muhandhis, yang setia menemani dalam proses pembuatan skripsi dan memberikan masukan-masukan yang membangun
(7) Staff Mercator, yang telah mengijinkan menggunakan fasilitas.

Akhir kata, saya berharap Allah Subhanahuwata'ala berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga skripsi ini membawa manfaat bagi pengembangan ilmu.

Depok, 17 Juni 2009

Penulis

Analisa perbandingan..., Gatot S., FT UI, 2009

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

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

Nama : Gatot S
NPM : 0405030389
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 PERBANDINGAN QoS: PENGARUH IMPLEMENTASI ENKRIPSI 3DES DAN AES PADA MPLS-VPN UNTUK LAYANAN 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

(Gatot S)

Analisa perbandingan..., Gatot S., FT UI, 2009

Nama : Gatot S
Program studi : Teknik Elektro, S1 Reguler
Judul : ANALISA PERBANDINGAN QoS : PENGARUH IMPLEMENTASI ENKRIPSI 3DES DAN AES PADA MPLS-VPN UNTUK LAYANAN IP-BASED VIDEO TELEPHONY

ABSTRAK

Seiring dengan perkembangan teknologi tuntutan akan kualitas layanan dan sekuritas (keamanan) terhadap kerahasiaan informasi yang saling dipertukarkan tersebut semakin meningkat. Sehingga bermunculah berbagai macam cara untuk mengamankan paket yang dilewatkan pada suatu jaringan, diantaranya adalah IPSec, *MPLS*-VPN, *tunneling*, kombinasi dan sebagainya yang tidak melupakan QoS. Untuk pengiriman informasi yang bersifat rahasia diperlukan jaringan yang berada pada kondisi *top secret*, salah satu caranya dengan membangun *MPLS*-VPN yang di kombinasikan dengan IPSec. Skripsi ini membahas tentang hubungan antara perbandingan dari implementasi enkripsi AES & 3DES pada IPSec di atas *MPLS*-VPN terhadap parameter QoS yang meliputi *delay*, *jitter*, dan *throughput*. Traffic yang di jadikan acuan yaitu UDP dengan RTP yang berbasis *codec* G.723.1 (audio) dan *codec* H.263(video), yaitu dengan menggunakan Netmeeting. Pada pengujian diberikan paramater ketika jaringan tidak dibebani. Alasan pemilihan traffic yang digunakan *realtime* karena saat dan kedepan nanti banyak yang memanfaatkan *IP-BASED* video *Telephony*. Dari hasil pengujian didapatkan bahwa pada audio streaming 3DES memberikan QoS lebih baik sebesar 0.03% - 10.78%, sedangkan pada streaming video AES memberikan QoS lebih baik sebesar 2.56 % - 9.36 %, dan pada pengujian transfer data AES juga memberikan QoS lebih baik sebesar 5.24 % - 7.49%.

Kata kunci : *MPLS*-VPN, IPSec, AES, 3DES, kriptografi

Analisa perbandingan..., Gatot S., FT UI, 2009

Name : Gatot S
Study Programme : Electrical Engineering
Title : QoS COMPARISON ANALYSIS : IMPLEMENTATION IMPACT OF 3DES AND AES IN MPLS-VPN FOR IP-BASED VIDEO TELEPHONY

ABSTRACT

Along with the development of the technology, demands of the *quality* of *service* and *security* of the confidentiality of the information exchanged in the mutual increasing. So, appear various ways to secure the *packet* that cross on public *network*, such as IPSec, *MPLS*-VPN, *tunneling*, and so combination QoS. The information is confidential which required a *network* that is on *top secret* conditions, one can build with the *MPLS*-VPN on the combine with IPSec. It discusses the relationship between the comparison of the implementation of AES & 3DES *encryption* in IPSec on *MPLS*-VPN QoS parameters, such as *delay*, *delay jitter*, and *throughput*. Traffic in the reference is made to the UDP-based RTP *codec* G.723.1 (audio) *codec* and H.263 (video), with using Netmeeting. Those parameters are given in the test when the *network* is not burdened. Reason of election *realtime* traffic that is used as the fore later time and take advantage of the many *IP-BASED* video *Telephony*. From test results obtained in streaming audio 3DES is better 0.03% - 10.78%, in video streaming AES is better 2.56 % - 9.36 % than 3DES, in testing transfer file AES is better 5.24 % - 7.49% than 3DES.

*Key*word : *MPLS*-VPN, IPSec, AES, 3DES, Cryptography

Analisa perbandingan..., Gatot S., FT UI, 2009

DAFTAR ISI

Analisa perbandingan..., Gatot S., FT UI, 2009

Analisa perbandingan..., Gatot S., FT UI, 2009

DAFTAR GAMBAR

Analisa perbandingan..., Gatot S., FT UI, 2009

Analisa perbandingan..., Gatot S., FT UI, 2009

DAFTAR TABEL

Analisa perbandingan..., Gatot S., FT UI, 2009

DAFTAR LAMPIRAN

Analisa perbandingan..., Gatot S., FT UI, 2009

DAFTAR ISTILAH

Bandwith : lebar kanal jaringan dalam *bit*/s

Datagram : bentuk paket UDP yang dikirim oleh sebuah terminal

Delay : waktu antara pengiriman paket dengan pengiriman paket

Frame : bentuk paket yang diperoleh dari *network layer*, dan dienkapsulasi di data link *layer* untuk transmisi

Header : bagian paket yang diletakkan di depan data (pada *transport layer*) yang berfungsi untuk mengidentifikasi data dan melewatkan ke *network layer*

Host : terminal yang dapat mengirim atau menerima data dari/ ke terminal lain/ server

Interface : antarmuka pada sebuah alat atau media

Jitter : variasi *delay* antar paket satu dengan paket sebelumnya

Label : deretan *bit* informasi yang ditambahkan pada *header* suatu paket data dalam jaringan *MPLS*

Overhead : pembebanan paket yang berlebihan pada suatu jaringan

Path : jalur pengiriman data

Port : jalur komunikasi pada suatu terminal

Reliable : bersifat handal

Router : perangkat keras yang berfungsi mem*forward* paket dan mencari jalur terbaik

Throughput : kecepatan (*rate*) transfer data efektif, yang diukur dalam *bit*/s.

Analisa perbandingan..., Gatot S., FT UI, 2009

BAB I
PENDAHULUAN

1.1 Latar Belakang

Berkat perkembangan teknologi yang begitu pesat memungkinkan manusia dapat berkomunikasi dan saling bertukar informasi/data secara jarak jauh. Antar kota antar wilayah antar negara bahkan antar benua bukan merupakan suatu kendala lagi dalam melakukan komunikasi dan pertukaran data. Seiring dengan itu tuntutan akan sekuritas (keamanan) terhadap kerahasiaan informasi yang saling dipertukarkan tersebut semakin meningkat. Begitu banyak pengguna seperti departemen pertahanan, suatu perusahaan atau bahkan individu-individu tidak ingin informasi yang disampaikannya diketahui oleh orang lain atau kompetitornya atau negara lain. Oleh sebab itu munculah berbagai macam cara untuk mengamankan paket yang dilewatkan pada suatu jaringan, diantaranya adalah IPSec, *MPLS*-VPN, *tunneling* danlain sebagainya.

Saat ini orang semakin banyak yang menggunakan layanan video *telephony*, yaitu suatu layanan teknologi yang memungkinkan dua orang untuk berkomunikasi audio-visual secara *full-duplex* dan *real-time* tanpa harus betatap muka secara langsung, video *telephony* dapat diimplementasikan pada jaringan ISDN dan IP, aplikasi video *telephony* yang sering digunakan saat ini menggunakan jaringan IP karena perkembangan jaringan IP lebih pesat dibanding ISDN. Untuk aplikasi Video *telephony* ini protokol yang digunakan adalah *Realtime Transport* Protocl (RTP) sesuai dengan standart ITU-T. *standard* G.723.1 sebagai audio *codec* dan H.263 sebagai video *codec*nya.

Alasan utama berkembangnya video *telephony* adalah biaya yang diperlukan untuk melakukan percakapan relatif lebih murah dari pada percakapan menggunakan saluran telepon biasa, terutama untuk percakapan jarak jauh. Selain itu, dengan

Analisa perbandingan..., Gatot S., FT UI, 2009

teknologi ini dapat dilakukan videoconferencing, pemakaian dokumen bersama, serta pemakaian aplikasi dan *white-board* bersama.

Video *telephony* berbasis IP dapat dijalankan melalui jaringan IP yang bersifat publik maupun privat, untuk efisiensi dapat digunakan jaringan public. Agar data yang melewati jaringan publik terjamin keamanannya maka banyak *Service Provider* yang menggunakan teknologi *MPLS*, khususnya *MPLS*-VPN. Walau demikian untuk lebih menjamin kerahasiaan data tersebut dari sisi *client* dapat digunakan teknologi VPN pada jaringan tersebut.*MPLS*-VPN dan VPN (*Virtual Private Network*) memungkinkan terbentuknya sebuah jaringan data *private* pada jaringan public yang skalabilitasnya besar serta terjamin keamannya.

MPLS-VPN dan VPN (*Virtual Private Network*) merupakan suatu cara untuk membuat sebuah jaringan yang bersifat *private* dan aman dengan menggunakan jaringan publik misalnya internet. Sebuah jaringan *private* haruslah berada dalam kondisi VIP, dan *top secret*. Masalah keamanan data, ketertutupan transfer data dari akses ilegal yang tidak diharapkan serta skalabilitas jaringan menjadi standar utama sebuah *private network*. Pembangunan *private network* secara fisik, akan lebih mahal dari pada pembangunan sebuah VPN karena banyaknya perubahan atau penambahan jalur-jalur fisik baru pada sebuah *private network*.

Kebutuhan akan layanan *IP-BASED* Video *telephony* akhir-akhir ini menunjukkan peningkatan yang cukup signifikan baik untuk kegiatan bisnis, pendidikan maupun wawancara jarak jauh, meskipun videoconferencing sudah mulai banyak digunakan, bukan berarti tidak mempunyai kendala, yaitu masalah QoS (*Quality* of *Service*) yang juga masih menjadi perhatian yang cukup serius.

1.2 Perumusan Masalah

Permasalahan pada Tugas Akhir ini adalah mengetahui sejauh mana pengaruh pengimplementasian 2 buah algoritma IPSec yang berbeda yaitu 3DES dan AES di atas jaringan MPLS-VPN untuk layanan *IP-BASED* video *telephony*. Pada sistem tersebut akan dialirkan trafik UDP dari salah satu host untuk diketahui

Analisa perbandingan..., Gatot S., FT UI, 2009

performansi dan pengaruh trafik dan algoritma enkripsi terhadap sistem video *telephony* pada jaringan *MPLS*-VPN meliputi, *delay*, *jitter* dan *throughput*.

Perancangan topologi tersebut digunakan software opensource GNS3 sebagai komputer yang berperan sebagai Router dan 2 komputer sebagai host.

1.3 Tujuan

Tugas akhir ini bertujuan untuk mengetahui dan menganalisa parameter QoS seperti *delay*, *jitter* dan *throughput* pada implementasi enkripsi tipe 3DES/AES yang berbeda diatas jaringan *MPLS*-VPN serta pengaruh paramater-parameter QoS tersebut bila jaringan dalam keadaan terbebani traffic UDP dan TCP.

1.4 Batasan Masalah

Dalam pembahasan ini, ada beberapa batasan yaitu antara lain:

1 Sistem VPN yang digunakan adalah *MPLS*-VPN
2 Menggunakan *standard* G.723.1 sebagai audio *codec* dan H.263 sebagai video *codec*nya
3 Trafik UDP dibangkitkan melalui trafik generator
4 Pengambilan data bukan dengan metode *testbed* tetapi dengan pengimplementasian *MPLS*-VPN dengan menggunakan yang digunakan berbasis software
5 Parameter QoS yang digunakan *delay*, *jitter*, *throughput*
6 Pensimulasian jaringan dengan menggunakan software GNS3, bukan dengan *testbed*.
7 Menggunakan IPv4 sebagai pengalamatannya.

1.5 Metodologi

1. Studi literatur

   Mengumpulkan dan mempelajari referensi tentang jaringan *MPLS*-VPN, IPSec, software GNS3, Netmeeting.

Analisa perbandingan..., Gatot S., FT UI, 2009

2. Perancangan sistem

   Pada tugas akhir ini dirancang sistem *IP-BASED* Video *Telephony* pada *MPLS*-VPN untuk dilakukan implementasi IPSec.

3. Implementasi sistem

   Implementasi dilakukan dengan menghubungkan 3 buah komputer *directly-connected* dengan 2 buah komputer diujung sebagai *Testbed* used dan komputer yang terletak di tengah sebagai Topologi *MPLS*-VPN. Topologi tersebut berisi 5 buah router yaitu sebuah router CORE, 2 buah router PE, 2buah ruter CE.

   Semuanya terhubung langsung dengan media kabel UTP. Topologi *MPLS*-VPN dimaksudkan untuk membentuk VPN *Tunnel* antara *Testbed* user, sehingga terbentuk jaringan VPN lokal., trafik UDP dibangkitkan dari End-user . Pada sistem tersebut di atas akan diuji ketika sistem tak terbebani maupun terbebani trafik UDP pada saat router PE menggunakan 2 jenis enkripsi yang berbeda.

4. Pengambilan dan analisa data

   Setelah dilakukan implementasi, akan di catat data-data yang berhubungan dengan parameter QoS (*Quality* of *Service*) pada jaringan terbebani UDP/TCP, kemudian 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 *MPLS*-VPN.

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.

Analisa perbandingan..., Gatot S., FT UI, 2009

1.6 Sistematika Pembahasan

Sistematika pembahasan tiap bab untuk tugas akhir ditunjukkan sebagai berikut:

Bab I : PENDAHULUAN

Bab ini berisi penjelasan singkat mengenai latar belakang, permasalahan, batasan masalah, tujuan, metodologi, sistematika pembahasan.

Bab II : TEORI PENUNJANG

Bab ini berisi penjelasan mengenai konsep MPLS-VPN, VPN, IPSec, kriptograpi, AES, 3DES.

Bab III : PERENCANAAN DAN IMPLEMENTASI

Bab ini berisi penjelasan mengenai cara mengimplementasikan *IP-Based Video Telephony* pada MPLS-VPN. Pembahasannya meliputi instalasi dan konfigurasi router dan instalasi software yang dibutuhkan untuk mengukur *delay, jitter, throughput.*

Bab IV : PENGUJIAN DAN ANALISA DATA

Pada bab ini akan membahas proses analisa data untuk mengetahui performansi *AES/3DES* pada MPLS-VPN yang meliputi *delay, jitter, throughput.*

Bab V : PENUTUP

Bab ini berisi kesimpulan dan saran

Analisa perbandingan..., Gatot S., FT UI, 2009

BAB II

Prinsip dan Cara Kerja MPLS-VPN dan IPSec

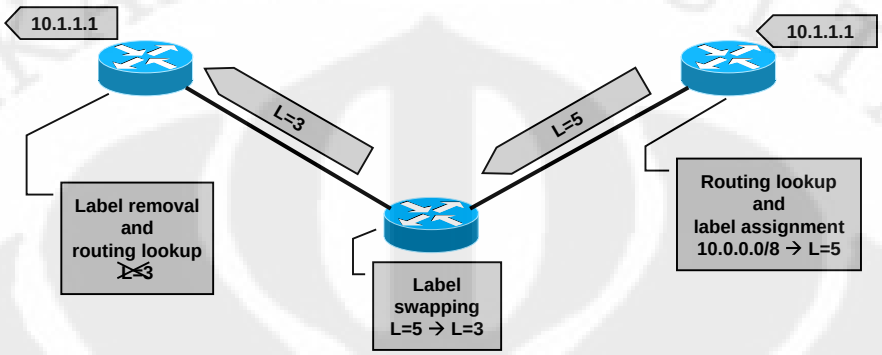
2.1 *MPLS*

Multi *Protocol* Label Switching (*MPLS*) adalah suatu metode *forward*ing paket yang melalui suatu jaringan dengan menggunakan informasi label yang dilekatkan pada paket IP. Dan merupakan perkembangan terbaru dari *multilayer* switch yang diusahakan oleh IETF (*Internet Engineering Task Force*). Hal ini dilakukan agar terdapat standar untuk *multilayer* switch dan mendukung interoperabilitas. Disebut multiprotokol karena tekniknya dapat diterapkan pada semua protokol *layer* jaringan. Dasar teknologi label switching mampu meningkatkan performansi *routing*, memperbaiki jangkauan *layer* jaringan, dan menyediakan fleksibilitas yang lebih besar dalam pengiriman pelayanan *routing*. *MPLS* menerapkan komponen *control* yang mirip dengan *multilayer* switch. Untuk mendukung interoperabilitas, *MPLS* mendefinisikan pensinyalan IP dan protokol distribusi label yang baru. Sedangkan komponen *forward*ingnya berdasarkan algoritma label swapping.

Network MPLS terdiri atas sirkit yang disebut *label-switched path* (LSP), yang menghubungkan titik-titik yang disebut *label-switched router* (LSR). LSR pertama dan terakhir disebut ingress dan egress. Setiap LSP dikaitkan dengan sebuah *forward*ing *equivalence class* (FEC), yang merupakan kumpulan paket yang menerima perlakukan *forward*ing yang sama di sebuah LSR. FEC diidentifikasikan dengan pemasangan label. Untuk membentuk LSP, diperlukan suatu protokol persinyalan. Protokol ini menentukan *forward*ing berdasarkan label pada paket. Label yang pendek dan berukuran tetap mempercepat proses *forward*ing dan mempertinggi fleksibilitas pemilihan path. Hasilnya adalah *network* datagram yang bersifat lebih connection-oriented. Untuk memperjeas tentang MPLS lihat Gambar 2.1, router paling kanan adalah ingress, router tengah

Analisa perbandingan..., Gatot S., FT UI, 2009

adalah LSR, dan yang paling kiri adalah egress. L=3 dan L=5 adalah proses label *swapping*.



Gambar 2. 1 *MPLS* Router [1]

2.1.1 Keunggulan *MPLS*

MPLS memiliki banyak keuntungan pada *network* berbasis IP. *Forward*ing *packet* berdasarkan label bukan berbasarkan *routing* dari *header packet-packet* terserbut. Ini menimbulkan beberapa keuntungan :

1. Sejak paket diasosiasikan pada sebuah FEC, maka *packet* dapat dipisahkan berdasarkan sumber, QoS, dan sebagainya.
2. *Packet* dapat diasosiasikan dengan prioritas label, sehingga membuat frame-relay ataupun ATM dapat terjamin QoSnya. Ini merupakan fungsi dari COS *(Class of Service*).
3. Menyediakan pelayanan ISP yang baru yang tidak bisa dilakukan dengan teknik *routing* IP yang lama
4. *MPLS* mendukung fleksibilitas perkembangan fungsi komponen *control* tanpa mengubah mekanisme *forward*ing. Sehingga *MPLS* dapat meningkatkan kemampuan *forward*ing yang dibutuhkan untuk mengantisipasi perkembangan internet yang sangat pesat. *MPLS*

menggabungkan teknologi switching/*forward*ing *layer* 2 dengan teknologi *routing layer* 3 pada standar OSI (*Open System Interconnection*)

5. *Forwarding* pada MPLS lebih cepat dibandingkan pada *traditional* IP *forwarding* karena pada MPLS menggunakan label. Apabila dahulu melakukan lookup tujuan yang kompleks, sedangkan dengan menggunakan label hanya menggunakan lookup tujuan yang sederhana.

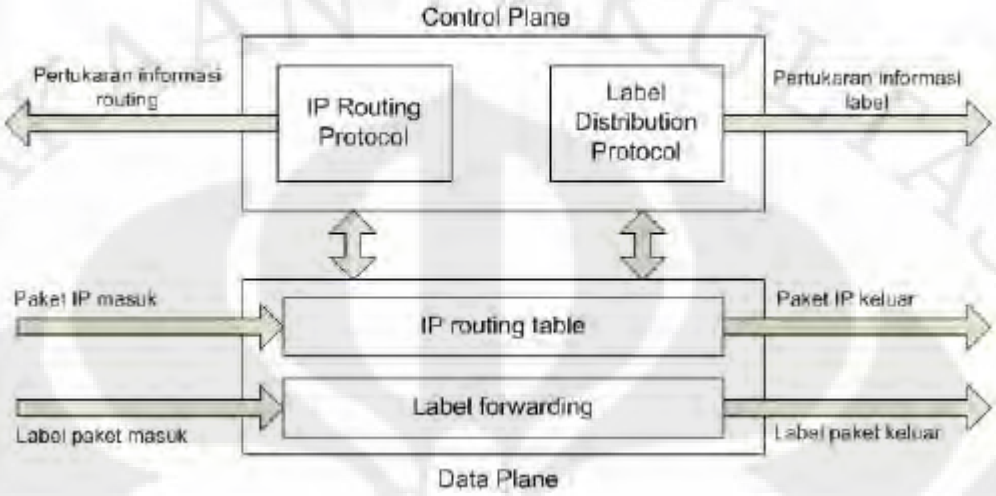
.

2.1.2 KOMPONEN *MPLS*

1. Pada Semua switch *multilayer*, termasuk *MPLS*, terdiri dari dua komponen fungsional yang berbeda yaitu sebuah komponen kontrol dan sebuah komponen *forward*ing. Komponen *control* membentuk fungsi yang berkaitan dengan pengidentifikasian reachability ke *prefix* tujuan. Sehingga bagian kontrol terdiri dari semua informasi *routing layer* 3 berserta proses yang berjalan di dalamnya yang berkaitan dengan pertukaran informasi reachbility untuk suatu prefi *layer* 3 tertentu, sebagai contoh dari fungsi ini adalah digunakannya OSPF, IS-IS, atau BGP-4. Komponen kontrol juga membentuk suatu fungs pensinyalan yang menerapkan LDP, CR-LDP, atau RSVP-TE untuk mempertukarkan atau mendistribusikan informasi dengan router yan lain dengan tujuan membangun dan mengurusi Tabel *forward*ing. Ketika paket tiba, komponen penerus mencari Tabel *forward*ing yang diurus oleh komponen kontrol untuk membuat suatu keputusan *routing* bagi setiap paket. Secara spesifik, komponen *forward*ing memeriksa informasi didalam *header* paket, menelusuri table *forward*ing, dan menghubungkan paket dariantarmuka input ke antarmuka output melintasi router (*system*'s switching *fabric*). Dengan total memisahkan komponen *control* dengan komponen *forward*ing, setiap komponen dapat secara bebas dikembangkan dan dimodifikasi. Yang dibutuhkan dari pemisahan komponen ini adalah komunikasi yang terus menerus antara komponen kontrol (*Control* Plane) dan komponen *forward*ing

Analisa perbandingan..., Gatot S., FT UI, 2009

(Data Plane) dalam mengatur Tabel *forward*ing paket. Untuk memperjelas konsep komponen MPLS ini lihat Gambar 2.2



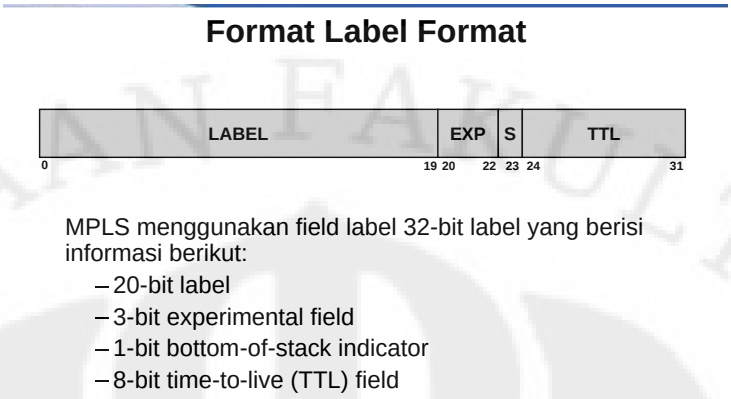
Gambar 2. 2Komponen LSR [2]

2. Algoritma penerusan label-swapping (penukaran label). Komponen *forward*ing *MPLS* (Data Plane) membentuk fungsi yang berkaitan dengan penerusan paket data. Paket ini dapat berupa paket IP *layer* 3 atau paket IP berlabel. Bila paket IP *Layer* 3 memasuki komponen ini, maka akan diteruskan berdasarkan Tabel FIB (*Forwarding Information Base*), sedangkan bila paket IP berlabel, penerusan pada setiap router backbone *MPLS* didasarkan pada algoritma label-swaping berdasarkan Tabel LFIB (Label *Forwarding Information Base*) yang mirip dengan yang digunakan oleh Frame Relay

2.1.3 Label Format

Gambar 2.3 adalah format label yang disisipkan diantara *frame header* dan IP *header*.

Analisa perbandingan..., Gatot S., FT UI, 2009



Gambar 2. 3 Format label [1]

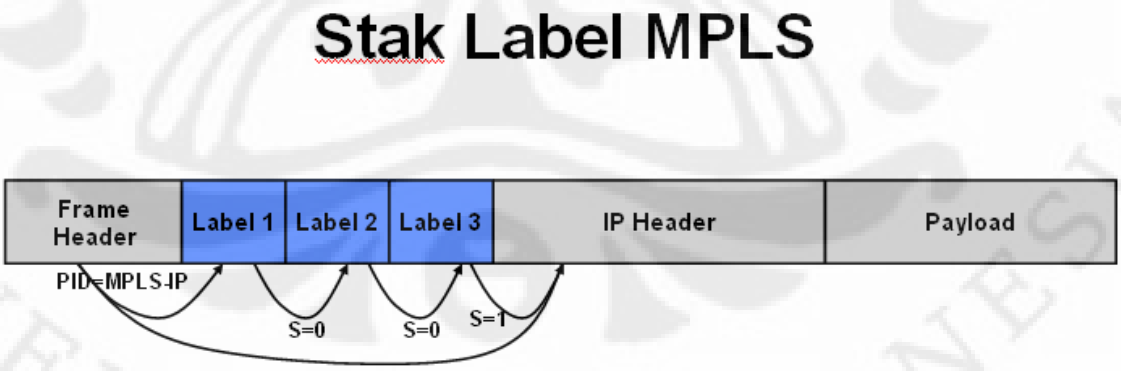
Biasanya hanya satu label digunakan untuk satu paket.Untuk fungsi berikut dapat digunakan lebih dari satu label.

1 *MPLS* VPNs (dua—label pertama menunjukkan egress router dan label kedua merupakan identitas VPN)

2. *MPLS* TE (dua atau lebih label—label pertama menunjukkan ujung dari suatu *tunnel* TE dan label kedua menunjukkan tujuan)

3. Kombinasi VPN *MPLS* dengan TE (tiga atau lebih label)

Pada Gambar 2.4 terlihat *stack*/urutan label MPLS bila menggunakan lebih dari satu label.

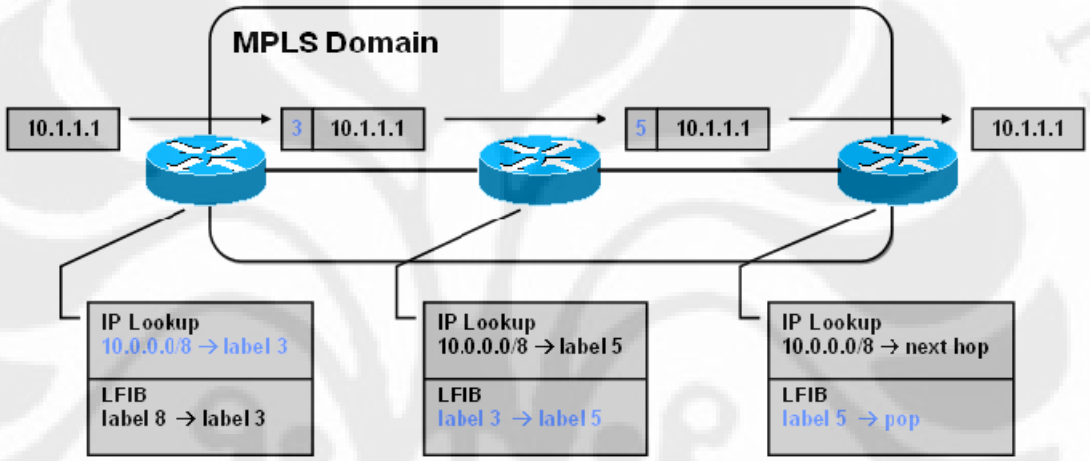


Gambar 2. 4 Stack Label [1]

2.1.4 Proses *MPLS forward*ing

Gambar 2.4 mnggambarkan proses *forwarding* pada MPLS. Sedangkan penjelasannya adalah sebagai berikut :

- Pada ingress suatu label ditetapkan dan disisipkan dengan proses IP *routing*.
- LSR di core, melakukan swap label berdasarkan isi Tabel label *forward*ing.
- Di egress, label dibuang dan *routing* lookup digunakan untuk mem-*forward*kan paket.



Gambar 2. 5 Proses *Forward*ing [1]

2.1.5 *MPLS* Fitur

Dengan cara kerja yang berbeda dengan *routing protocol* biasanya menyebabkan *MPLS* memiliki banyak keuntungan sehingga *MPLS* sendiri dapat dibagi menjadi 3 :

1. *MPLS Virtual Private Network*s (VPNs) - memberikan "*MPLS*-enabled IP *network*s" untuk koneksi *Layer* 3 dan *Layer* 2. Berisi 2 komponen utama :
    1. *Layer* 3 VPNs (menggunakan *Border Gateway Protocol*.)
    2. *Layer* 2 VPNs *Any Transport over MPLS* (AToM)
2. *MPLS Traffic Engineering* (TE) - menyediakan peningkatan utilisasi dari bandwidth jaringan yang ada dan untuk "*protection services*".

3. *MPLS Quality* of *Service* (QoS) - menggunakan mekanisme IP QoS existing, dan menyediakan perlakuan istimewa untuk type trafik tertentu, berdasarkan atribut QoS (seperti *MPLS* EXP)

2.1.6 *MPLS*-VPN

VPN atau *Virtual Private Network* adalah suatu jaringan *private* yang mempergunakan sarana jaringan komunikasi publik (dalam hal ini Internet) dengan memakai *tunneling protocol* dan prosedur pengamanan. Dengan memakai jaringan publik yang ada, dalam hal ini Internet, maka biaya pengembangan yang dikeluarkan akan jauh relatif lebih murah daripada harus membangun sebuah jaringan internasional tertutup sendiri namun pengguna dapat menikmati fasilitas-fasilitas yang ada pada jaringan privat seperti tingkat *security* yang tinggi, *quality* of *service* (QoS), kemudahan manajemen dan tingkat kepercayaan yang tinggi.

Sedangkan *MPLS*-VPN merupakan VPN yang dibentuk oleh jaringan SP yang berbasis MLPS. Di dalam VPN, *customer* dapat membentuk hubungan antar lokasi. Konektivitas dapat terbentuk dari titik mana pun ke titik mana pun (banyak arah sekaligus), tanpa harus melewati semacam titik pusat, dan tanpa harus menyusun serangkaian link dua arah. Ini dapat digunakan sebagai *platform* intranet yang secara efisien melandasi jaringan IP sebuah perusahaan. Ini juga dapat digunakan sebagai extranet yang menghubungkan perusahaan-perusahaan yang terikat perjanjian.

Mekanisme pembentukan VPN telah tercakup dalam konfigurasi *MPLS*, sehingga tidak diperlukan perangkat tambahan di *site customer*. Bahkan, jika diinginkan, konfigurasi VPN sendiri dapat dilakukan dari *site provider*.

Salah satu feature *MPLS* adalah kemampuan membentuk *tunnel* atau *virtual circuit* yang melintasi *network*nya. Kemampuan ini membuat *MPLS* berfungsi sebagai *platform* alami untuk membangun *virtual private network* (VPN).

VPN yang dibangun dengan *MPLS* sangat berbeda dengan VPN yang hanya dibangun berdasarkan teknologi IP, yang hanya memanfaatkan enkripsi data. VPN

Analisa perbandingan..., Gatot S., FT UI, 2009

pada *MPLS* lebih mirip dengan *virtual circuit* dari FR atau ATM, yang dibangun dengan membentuk isolasi trafik. Trafik benar-benar dipisah dan tidak dapat dibocorkan ke luar lingkup VPN yang didefinisikan. Lapisan pengamanan tambahan seperti IPSec dapat diaplikasikan untuk data *security*, jika diperlukan. Namun tanpa metode semacam IPSec pun, VPN dengan *MPLS* dapat digunakan dengan baik.

Ada beberapa rancangan yang telah diajukan untuk membentuk VPN berbasis IP dengan *MPLS*. Belum ada satu pun yang dijadikan bakuan. Namun ada dua rancangan yang secara umum lebih sering diacu, yaitu *MPLS*-VPN dengan BGP, dan explicitly routed VPN. *MPLS*-VPN dengan BGP saat ini lebih didukung karena alternatif lain umumnya bersifat propriertary dan belum menemukan bentuk final.

Panduan implementasi *MPLS*-VPN dengan BGP adalah RFC-2547. BGP mendistribusikan informasi tentang VPN hanya ke router dalam VPN yang sama, sehingga terjadi pemisahan trafik. E-LSR dari *provider* berfungsi sebagai *provider-edge* router (PE) yang terhubung ke *customer-edge* router (CE). PE mempelajari alamat IP dan membentuk sesi BGP untuk berbagi info ke PE lain yang terdefinisikan dalam VPN. BGP untuk *MPLS* berbeda dengan BGP untuk paket IP biasa, karena memiliki ekstensi multi-protokol seperti yang didefinisikan dalam RFC-2283.

Pada prinsipnya penerapan ***MPLS* VPN** berfungsi untuk menekan biaya operasi, menunjang overlapping IP, mempercepat proses switching, meningkatkan keamanan, dan mempermudah implementasi jaringan.

2.1.6.1 L3VPN

Layer 3 VPNs atau BGP VPNs, teknologi *MPLS* yang paling banyak digunakan. *Layer* 3 VPNs menggunakan "*Virtual Routing* instances" untuk membuat sebuah pemisahan table *routing* untuk tiap-tiap pelanggan/*subscriber*, dan menggunakan BGP untuk membentuk koneksi (peering relations) dan signal VPN-berlabel dengan masing-masing router *Provider Edge* (PE) yang sesuai. Hasilnya sangat *scalable* untuk diimplementasikan, karena router core (P) tidak memiliki informasi tentang VPNs.

Analisa perbandingan..., Gatot S., FT UI, 2009

BGP VPNs sangat berguna ketika pelanggan menginginkan koneksi *Layer* 3 (IP), dan lebih menyukai untuk membuang *overhead routing* ke *Service Provider*. Hal ini menjamin bahwa keanekaragaman interface *Layer* 2 dapat digunakan pada tiap sisi/site VPN. Contoh, *Site* A menggunakan interface Ethernet, sementara *Site* B menggunakan interface ATM; *Site* A dan *Site* B adalah bagian dari single VPN.

Relatif sederhana untuk penerapan "*multiple topologies*" dengan "router *filter*ing ", Hub & Spoke atau Full Mesh:

- Hub and Spoke - "*central site*" dikonfigurasi untuk "learn/mempelajari" semua "routes" dari seluruh *remote site*s, sementara *remote site*s dibatasi untuk "learn/mempelajari" routes, hanya khusus dari central *site*.
- Topology Full Mesh akan menciptakan semua *site*s mempunyai kemampuan "learn/mempelajari" atau mengimpor routes dari tiap *site* lainnya.

Layer 3 VPNs telah dikembangkan dalam jaringan yang mempunyai router PE sebanyak 700. Saat ini terdapat *Service Provider* yang memiliki sampai 500 VPNs, dengan masing-masing VPN berisi *site* sebanyak 1000. Banyak ragam *routing protocol* yang digunakan pada link akses pelanggan (yaitu link CE ke PE); Static Routes, BGP, RIP dan *Open Shortest Path First* (OSPF). VPNs paling banyak menggunakan Static Routes, diikuti dengan *Routing* BGP.

Layer 3 VPNs menawarkan kemampuan lebih, seperti Inter-AS dan *Carrier Supporting Carrier* (CSC). Hierarchical VPNs, memungkinkan *Service Provider* menyediakan koneksi melewati *"multiple administrative network*s". Saat ini, penerapan awal dari fungsi seperti ini sudah tersebar luas.

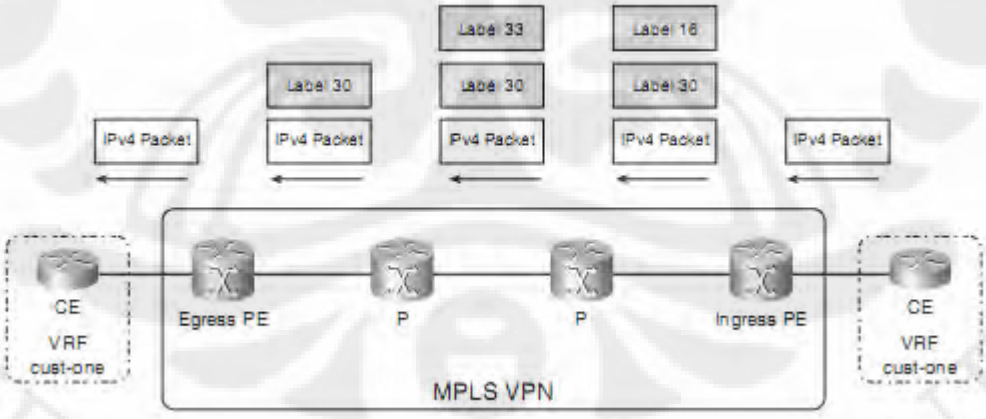
2.1.6.2 *Layer* 2 VPNs

Layer 2 VPNs mengacu pada kemampuan dan kebutuhan dari pelanggan *Service Provider* untuk menyediakan *Layer* 2 *Circuit*s melalui "*MPLS*-enabled IP backbone". Penting untuk memahami 3 komponen utama dari *Layer* 2 VPNs:

Analisa perbandingan..., Gatot S., FT UI, 2009

1. *Layer* 2 *Transport* over over *MPLS* - *Layer* 2 *circuit* - membawa data secara transparent - melalui *MPLS* enabled IP backbone (juga dikenal sebagai AToM).
2. *Virtual Private Wire Service*s - Kemampuan untuk menambahkan signalling ke AToM, dan untuk fitur-fitur seperti auto-*discovery* perangkat CE.
3. *Virtual Private* LAN *Service*s - Kemampuan menambahkan *Virtual* Switch Instances (VSIs) pada router PE untuk membentuk "LAN based *service*s" melalui *MPLS*-enabled IP backbone. *Circuit*s *Layer* 2 yang dominan adalah Ethernet, ATM, Frame Relay, PPP, dan HDLC. AToM dan *Layer* 3 VPNs didasarkan pada konsep yang sama, tetapi AToM menggunakan sebuah "directed LDP session" untuk mendistribusikan Labels VC (analogy dengan BGP VPN Label). Oleh karena itu, router core tidak perlu mengetahui per-subscriber basis, hasilnya sebuah architecture yang sangat "*scalable*".

MPLS-VPN menggunakan 2 stak label, yang paling atas adalah label IGP label, dan label dibawahnya VPN label. Pada Gambar 2.6 terlihat penambahan dan pengurangan, serta proses sawpping label pada MPLS-VPN.



Gambar 2. 6 Proses *forward*ing *MPLS*-VPN [3]

Analisa perbandingan..., Gatot S., FT UI, 2009

Sebelum ada AToM, *Service Provider* harus membangun jaringan yang berbeda untuk menyediakan koneksi *Layer* 2. Contoh, *Service Provider* harus membangun sebuah ATM dan sebuah Frame Relay *Network*, hasilnya peningkatan biaya operasional dan "*capital expenses*". Saat ini, *Layer* 2 VPNs *MPLS* memungkinkan *Service Provider* untuk menggabungkan jenis jaringan yang berbeda ini, sehingga menghemat biaya operasional dan "*capital expenses*" secara signifikan.

Layer 2 VPNs dan *Layer* 3 VPNs dapat dikonfigurasi dalam single/satu box dan dapat difungsikan untuk meningkatkan keuntungan dari pelanggan. *Layer* 2 dan *Layer* 3 VPNs saling melengkapi satu sama lain. Dengan berjalannya waktu, permintaan akan *Layer* 2 VPNs bisa jadi lebih tinggi dibandingkan dengan *Layer* 3 VPNs.

2.2 IPSec

IPSec adalah kependekan dari IP *Security*, sekumpulan pengembangan protokol oleh IETF untuk menunjang keamanan pertukaran *packet* pada *layer* IP. IPSec telah dikembangakan secara luas untuk mengimplementasikan VPN(*Virtual Private Network*).

IPSec memiliki 2 buah enkripsi mode : yaitu *Transport* Mode dan *Tunnel* Mode. *Transport* Mode hanya mengenkripsi data dari setiap paket, sedangkan headernya tidak dienkripsi. *Tunnel* Mode memberikan keamanan yang lebih karena tidak hanya data saja yang dienkripsi tetapi *header* paket juga ikut dienkripsi. Pendekprisian akan dilakukan di jaringan tujuan.

Supaya IPSec dapat bekerja, divais pengirim dan penerima harus berbagi sebuah *Public key*. Ini dikerjakan pada sebuah *framework* protokol yang dikenali sebagai Internet *Security* Assosiation and *Key* Management/Oakley) yang mengizinkan penerima mendapatkan *Public key* dan mengautentikasi pengirim menggunakan *digital certificates*. Framework tersebut mencakup beberapa algoritma kriptografi yang telah ditentukan sebelumnya, dan juga dapat diperluas

Analisa perbandingan..., Gatot S., FT UI, 2009

dengan menambahkan beberapa sistem kriptografi tambahan yang dibuat oleh pihak ketiga.

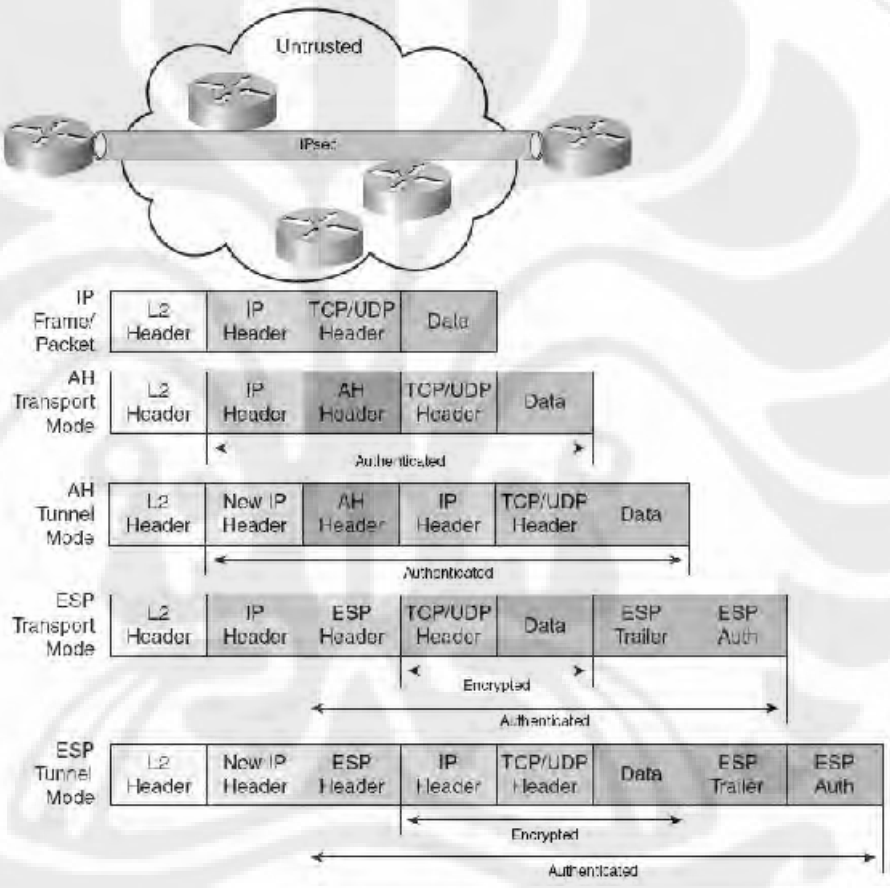
IPSec diimplementasikan pada lapisan *transport* dalam OSI Reference Model untuk melindungi protokol IP dan protokol-protokol yang lebih tinggi dengan menggunakan beberapa kebijakan keamanan yang dapat dikonfigurasikan untuk memenuhi kebutuhan keamanan pengguna, atau jaringan. IPSec umumnya diletakkan sebagai sebuah lapisian 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 kelakuan yang dikaitkan dengannya akan diaplikasikan terhadap paket IP tersebut.

IPSec mendukung dua buah sesi komunikasi keamanan, yakni sebagai berikut:

- Protokol Authentication *Header* (AH): 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

Analisa perbandingan..., Gatot S., FT UI, 2009

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. Untuk melihat pebedaan antara transport mode dan tunnel mode lihat Gambar 2.7. pada Gambar 2.7 juga terlihat bahwa IPSec merupakan salah satu bentuk dari *tunneling.*



Gambar 2. 7 Perbandingan Enkripsi dan Autentikasi pada IPSec [16]

Beberapa perangkat keras serta perangkat lunak dapat dikonfigurasikan untuk mendukung IPSec, yang dapat dilakukan dengan menggunakan enkripsi kunci publik yang disediakan oleh Certificate Authority (dalam sebuah *public key*

Analisa perbandingan..., Gatot S., FT UI, 2009

infrastructure) atau kunci yang digunakan bersama yang telah ditentukan sebelumnya (skema Pre-Shared *Key*/PSK) untuk melakukan enkripsi secara privat.

IPSec digunakan bila user tidak mempercayai tingkat keamanan yang ditawarkan oleh *service provider*, bahkan di atas *MPLS*-VPN sekalipun. Karena mungkin saja terjadi saat konfigurasi dari SP yang menyebabkan tidak terjaminnya *packet* yang melewati jaringannya. Selain itu IPSec juga dapat digunakan untuk memperkuat tingkat keamanan pada *MPLS*-VPN, sehingga terjadi kombinasi yang baik antara *MPLS*-VPN dengan IPSec. Bila konfigurasi *MPLS* dilakukan oleh pihak *ServiceProvider*, maka IPSec dilakukan dari sisi user, sehingga kedua belah pihak memegang peranan penting terhadap keamanan data. Kombinasi tersebut dapat terlihat pada Tabel 2..1 :

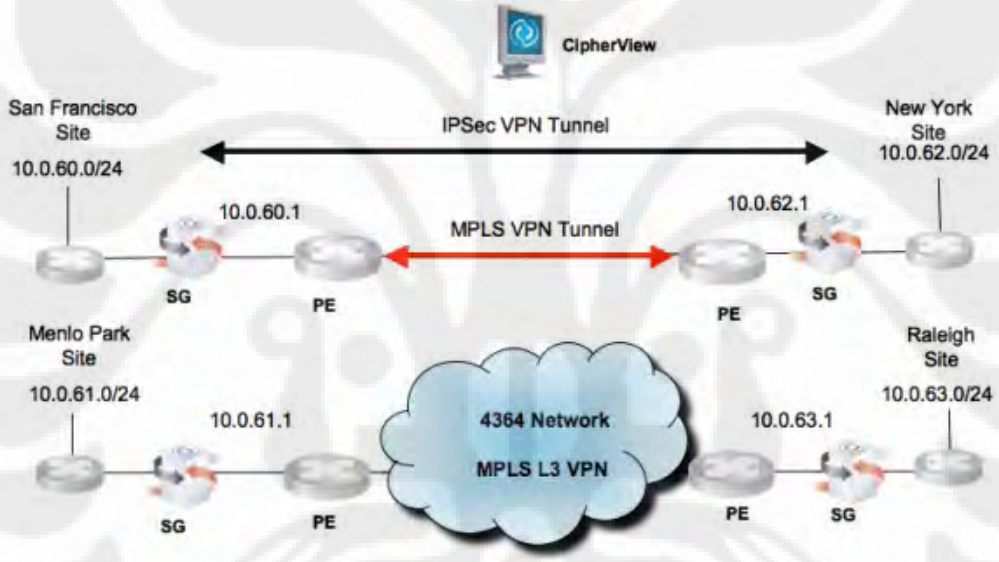
	MPLS VPNs	**IPSec Data Protection**	**IPSec Data Protection Over the MPLS VPNs**
Services	Provide Ethernet and IP VPNs	Provide encryption and authentication	MPLS provides the VPN service, IPSec secures the IP traffic
Deployment	Within the service provider metro and core networks	At the edge of the enterprise network	MPLS is deployed by the service provider, IPSec is deployed by the enterprise network
Management	One time provisioning of the service provider PEs to support the MPLS service	One time provisioning of the security policies between the enterprise sites on each IPSec appliance	The service provider manages its MPLS network, the enterprise manages its IPSec network
Transparency	Transparent to the traffic and applications	Transparent to the traffic and applications	Transparent to the traffic and applications
Scalability	Design limited by tunnels hierarchy	Limited to point-to-point network design	Limited by IPSec scalability
Resiliency	Through fast re-route provided at the link and node layers	Left to the underlying IP network design, limited by IKE connection-oriented nature	Need to be integrated into the network design

Analisa perbandingan..., Gatot S., FT UI, 2009

Security	None	Secure IP traffic	Provided by IPSec
Multicast	No support yet but in the process of being defined by the IETF	No standard support for multicast	No support
QoS	Enable Class of Service (CoS) and Differentiated Services (DiffServ)	Transparent to IP ToS and DiffServ	Provided by MPLS

Tabel 2. 1 Kombinasi *MPLS*-VPN & IPSec [4]

Kombinasi *MPLS*-VPN (L3VPN) dengan IPSec dapat dilihat pada Gambar 2.8:



Gambar 2. 8 IPSec pada *MPLS*-VPN [4]

2.3 Kriptograpi

Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga. Menurut Bruce Scheiner dalam bukunya "*Applied Cryptography*", kriptografi adalah ilmu pengetahuan dan seni menjaga *message-message* agar tetap aman *(secure)* [13].

Dalam kriptografi terdapat dua konsep utama yakni enkripsi dan dekripsi. Enkripsi adalah adalah proses pengubahan plain text "tak tersembunyi" menjadi cryptext "tersembunyi" untuk mengamankan data tersebut dari pencuri [11] atau disebut pula proses dimana informasi/data yang hendak dikirim diubah menjadi bentuk yang hampir tidak dikenali sebagai informasi awalnya dengan menggunakan algoritma tertentu. Dekripsi adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awal.

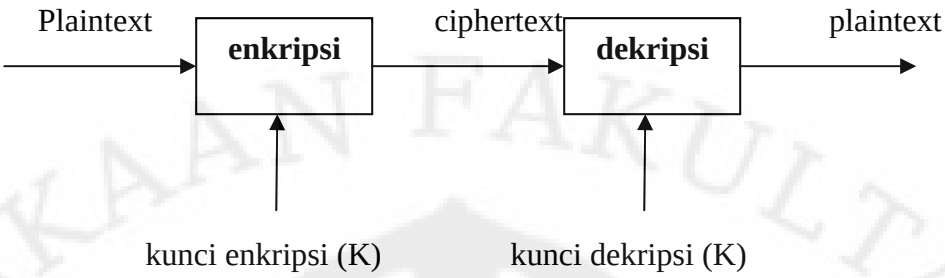
Konsep kriptografi sendiri telah lama digunakan oleh manusia misalnya pada peradaban Mesir dan Romawi walau masih sangat sederhana. Prinsip-prinsip yang mendasari kriptografi yakni:

1. *Confidelity* (kerahasiaan) yaitu layanan agar isi pesan yang dikirimkan tetap rahasia dan tidak diketahui oleh pihak lain (kecuali pihak pengirim, pihak penerima / pihak-pihak memiliki ijin). Umumnya hal ini dilakukan dengan cara membuat suatu algoritma matematis yang mampu mengubah data hingga menjadi sulit untuk dibaca dan dipahami.
2. *Data integrity* (keutuhan data) yaitu layanan yang mampu mengenali/ mendeteksi adanya manipulasi (penghapusan, pengubahan atau penambahan) data yang tidak sah (oleh pihak lain).
3. *Authentication* (keotentikan) yaitu layanan yang berhubungan dengan identifikasi. Baik otentikasi pihak-pihak yang terlibat dalam pengiriman data maupun otentikasi keaslian data/informasi.
4. *Non-repudiation* (anti-penyangkalan) yaitu layanan yang dapat mencegah suatu pihak untuk menyangkal aksi yang dilakukan sebelumnya (menyangkal bahwa pesan tersebut berasal dirinya).

2.3.1 Algoritma simetris

Dimana kunci yang digunakan untuk proses enkripsi dan dekripsi adalah kunci yang sama atau disebut juga disebut juga sebagai single-*key* algorithm. Lihat Gambar 2.9 untuk memperjelas konsep dari algoritma simetris.

Analisa perbandingan..., Gatot S., FT UI, 2009



Gambar 2. 9 Enkripsi dan dekripsi algoritma simetris

Sebelum melakukan pengiriman pesan, pengirim dan penerima harus memilih suatu suatu kunci tertentu yang sama untuk dipakai bersama, dan kunci ini haruslah rahasia bagi pihak yang tidak berkepentingan sehingga algoritma ini disebut juga algoritma kunci rahasia (secret-*key* algorithm).

Kelebihan :

- Kecepatan operasi lebih tinggi bila dibandingkan dengan algoritma asimetrik.
- Karena kecepatannya yang cukup tinggi, maka dapat digunakan pada sistem *realtime*

Kelemahan :

- Untuk tiap pengiriman pesan dengan pengguna yang berbeda dibutuhkan kunci yang berbeda juga, sehingga akan terjadi kesulitan dalam manajemen kunci tersebut.
- Permasalahan dalam pengiriman kunci itu sendiri yang disebut "*key* distribution problem"

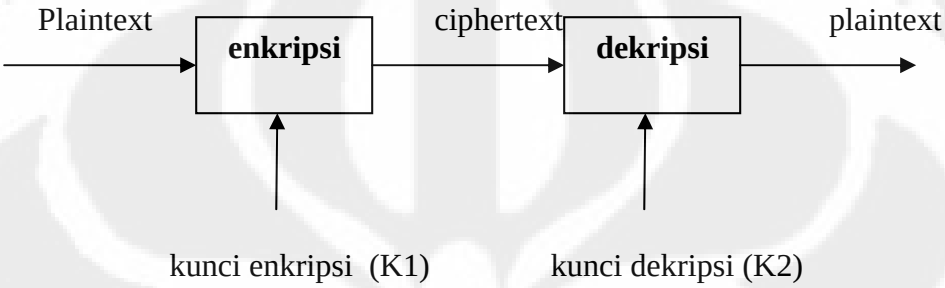
Contoh algoritma : TwoFish, Rijndael, Camellia

2.3.2 Algoritma Asimetris

Dimana kunci yang digunakan untuk proses enkripsi dan dekripsi menggunakan kunci yang berbeda.

Analisa perbandingan..., Gatot S., FT UI, 2009

Pada algoritma ini menggunakan dua kunci yakni kunci publik (*public key*) dan kunci privat (*private key*). Kunci publik disebarkan secara umum sedangkan kunci privat disimpan secara rahasia oleh si pengguna. Walau kunci publik telah diketahui namun akan sangat sukar mengetahui kunci privat yang digunakan. Untuk lebih jelasnya lihat Gambar 2.10



Gambar 2. 10 enkripsi dan dekripsi algoritma asimetris

Pada umumnya kunci publik (*public key*) digunakan sebagai kunci enkripsi sementara kunci privat (*private key*) digunakan sebagai kunci dekripsi.

Kelebihan :

- Masalah keamanan pada distribusi kunci dapat lebih baik
- Masalah manajemen kunci yang lebih baik karena jumlah kunci yang lebih sedikit

Kelemahan :

- Kecepatan yang lebih rendah bila dibandingkan dengan algoritma simetris
- Untuk tingkat keamanan sama, kunci yang digunakan lebih panjang dibandingkan dengan algoritma simetris.

  Contoh algoritma : RSA, DSA, ElGama

Sedangkan berdasarkan besar data yang diolah dalam satu kali proses, maka algoritma kriptografi dapat dibedakan menjadi dua jenis yaitu :

1. Algoritma *block* cipher

Analisa perbandingan..., Gatot S., FT UI, 2009

Informasi/data yang hendak dikirim dalam bentuk blok-blok besar (misal 64-*bit*) dimana blok-blok ini dioperasikan dengan fungsi enkripsi yang sama dan akan menghasilkan informasi rahasia dalam blok-blok yang berukuran sama.

2. Algoritma stream cipher

   Informasi/data yang hendak dikirim dioperasikan dalam bentuk blok-blok yang lebih kecil (byte atau *bit*), biasanya satu karakter persatuan persatuan waktu proses, menggunakan tranformasi enkripsi yang berubah setiap waktu.

2.3.2 AES

AES (Advanced *Encryption Standard*) diperkenalkan pada Desember 2001 yang merupakan algoritma yang lebih efisien dibanding algoritma sebelumnya. Ia mempunyai 10, 12 atau 14 kitaran untuk kunci 128 *bit*, 192 dan 256 *bit*.

Deskripsi dari algoritma AES sebagai berikut :

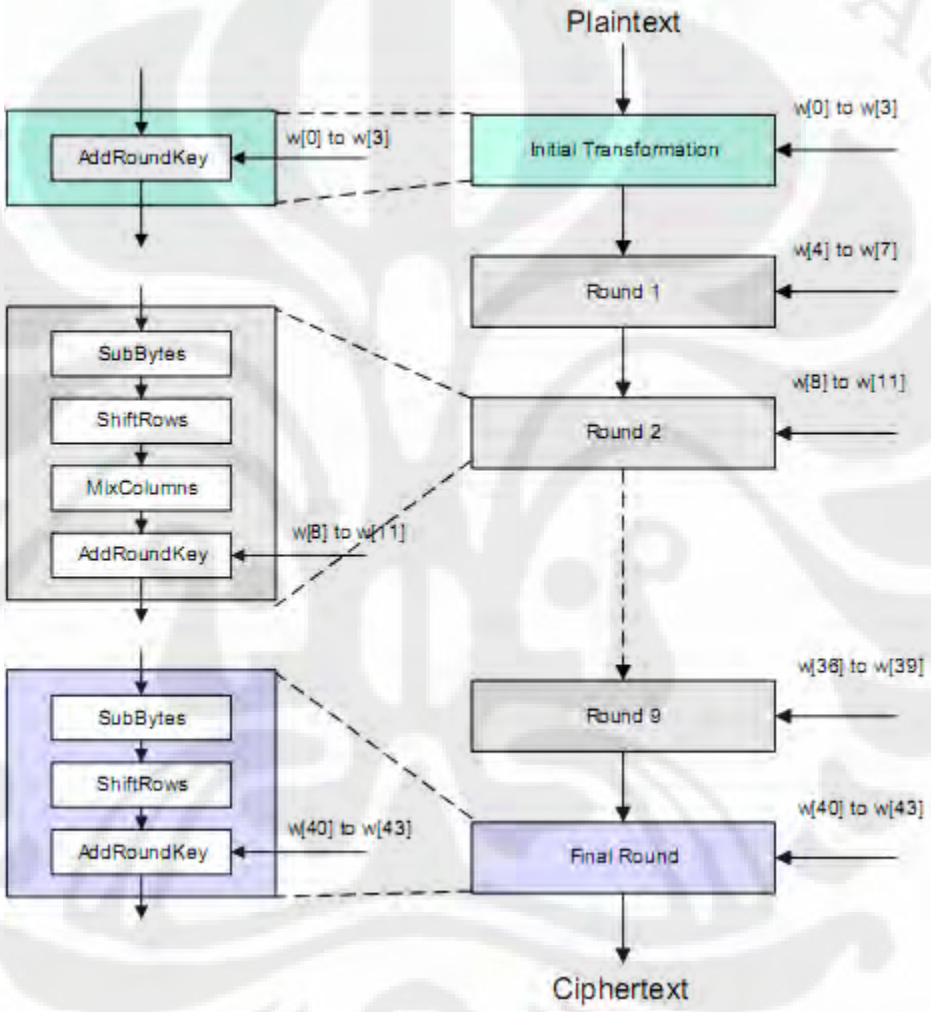
1. *Key*Expansion using Rijndael's *key* schedule
2. Initial Round
   a. AddRound*Key*
3. Rounds
   a. SubBytes—sebuah substitusi non-linear dimana setiap byte dipindahkan dengan sebuah byte yang lain berdasarkan lookup
   b. ShiftRows—sebuah pergantian tempat dari byte dimana setiap baris dari setiap *state* di shifting rotasi berdasarkan ketentuan
   c. *Mix*Columns— operasi pencampuran kolom dari sebuah *state* dengan cara di XOR-kan dengan hasil dari operasi
   d. AddRound*Key*—setiap byte dari setiap *state* dikombinasikan dengan round*key*. Masing-masing roud*key* dipisahkan dari cipher *key* yang menggunakan *key*
4. Final Round (no *Mix*Columns)
   a. SubBytes

Analisa perbandingan..., Gatot S., FT UI, 2009

b. ShiftRows

c. AddRound*Key*

Skematik sekuensial dari algoritma enkripsi AES 128 dengan menggunakan 12 ronde terdapat pada Gambar 2.11 :



Gambar 2. 11 skema algoritma AES [5]

128 *bit* AES menawarkan total 3,4 x 10^38 individu kunci. Hal ini diperkirakan jika DES kunci generator mampu menemukan kunci DES 1 per detik, ia akan mengambil 149 ribu-milyar (149 triliun) tahun menmbuka satu kunci AES

Analisa perbandingan..., Gatot S., FT UI, 2009

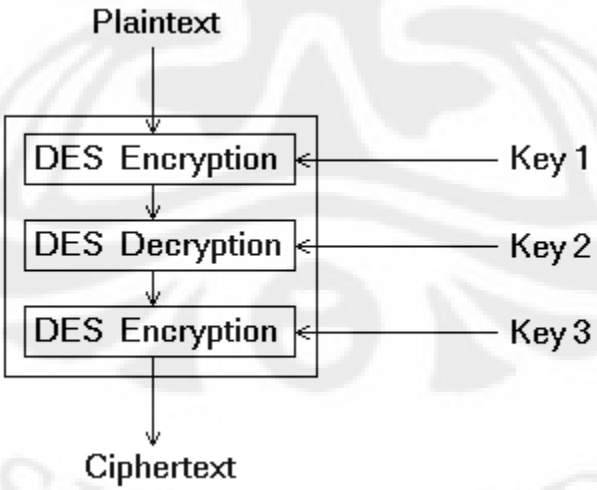
128*bit*[g]. Saat ini, teknologi ini tidak tersedia. AES menawarkan 3 macam pilihan yaitu 128 *bit*, 192 *bit*, dan 256 *bit*. Tetapi 192*bit* jarang dipakai.

AES adalah kecil, cepat, sulit untuk crack enkripsi standar dan sangat cocok untuk berbagai perangkat atau aplikasi. Telah ditetapkan sebagai yang terbaik kompromi antara kombinasi keamanan, kinerja, efisiensi, kemudahan dan fleksibilitas pelaksanaan.

2.3.3 3DES

DES merupakan *symmetric encryption* algoritm yang menggunakan 64 *bit*, *Block* yang efektif digunakan yaitu hanya 56 *bit*, sisanya digunakan sebagai parity check yang terletak di paling kanan. Ini berarti bahwa kekuatan kunci efektif untuk Triple DES 168 *bit* sebenarnya adalah karena masing-masing berisi tiga tombol 8 paritas *bit* yang tidak digunakan selama proses enkripsi.

Prosedur enkripsi pada 3DES adalah persis sama seperti biasa DES, tetapi diulang tiga kali, untuk lebih jelasnya lihat Gambar 2.12 sebagai gambaran umum dari 3DES. Sedangkan untuk penggambaran secara detil lihat Gambar 2.13. Oleh karena itu dinamakan Triple DES. Data dienkripsi dengan kunci pertama, didekrip dengan kedua kunci, dan akhirnya dienkripsi lagi dengan kunci yang ketiga.



Gambar 2. 12 Enkripsi pada 3DES [6]

Struktur algoritma DES yaitu pada Gambar di bawah terdapat proses sebanyak 16 ronde. Terdapat juga *Initial Permutation* (IP) dan *Final Permutation* (FP). IP dan FP tidak signifikan mengenkripsi plaintext teapi digunakan untuk memfasilitasi dalam hal loading *block*.

Sebelum ronde utama dimulai, 64-*bit block* dibagi menjadi dua yang masing-masing 32-*bit block* dan diproses secara bergantian, proses selang-seling ini yang disebut dengan Feisel-Function. Feisel Function digunakan untuk memastikan bahwa enkripsi dan dekripsi memiliki proses yang dentik. Perbedaannya hanylah bahwa sub*key* diberikan secara terbalik pada proses dekripsi. Terlihat jelas bahwa algoritma ini adalah algoritma yang sederhana sehingga mudah pula dalam pengimplementasian di dalam hardware karena tidak dibutuhkan algoritma yang terpisah antara enkripsi dan dekripsi.

Feisel-function menggabungkan dengan cara meng-XOR kan 32*bit block* tadi dengan *key* yang muncul pada sub*key* schedule. Kemudian output fungsi-F tersebut dicampur lagi dengan setengah *block* yang lain dan kemudian setengah *block* itu diganti sebelum ronde selanjutnya. Pada final ronde setengah *block* tidak diganti, ini adalah yang membuat fungsi-F memiliki proses yang sama antara enkripsi dan dekripsi.

Feistel (F) function

Fungsi-F mengoperasikan setengah *block* (32*bit*) setiap waktu yang terdiri dari 4 proses :

1. Expansion — setengah *block* (32-*bit*) di expand menjadi 48-*bit* dengan menggunakan expand permutation yaitu dengan menduplikasi beberapa *bit* dan ini disimbolkan dengan lambing E pada Gambar.
2. *Key mix*ing — Hasil proses pertama tadi dikombinasikan dengan sub*key* dengan menggunakan operasi XOR. Karena untuk memproses sebuah blok meelalui 16 ronde maka dibutuhkan pula 16 sub*key*. Ke 16 sub*key* ini didapatkan dengan memasukkan *key* utama pada *key* schedule.

Analisa perbandingan..., Gatot S., FT UI, 2009

3. Substitution — setelah mencampurkan sub*key* sebuah blosk dipecah menjadi 8 buah kotak yang disebut sebagai S-box. Masing –masing kotak terdiri dari 6-*bit*. Kemudian isi dari S-box saling dipertukarkan dengan 4 output dari setiap box dengan transformasi nonlinear. Transformasi ini dapat dilihat pada lookup table. S-box inilah inti dari keamanan pada DES, tanpa S-box cipher akan linear dan mudah untuk di bongkar.
4. Permutation — Akhirnya, 32 output dari S-box disusun kembali dengan menggunakan permutasi tetap yang menghasilkan P-box.

Penggambaran dari keempat langkah di atas dapat diilustrasikan pada Gambar 2.14. Sedangkan sebagai perbandingan antara AES(128-bit) dengan 3DES dapat dilihat pada Gambar 2.15

AES vs. Triple-DES[1]		
	AES	**Triple-DES**
Description	Advanced Encryption Standard	Triple Data Encryption Standard
Timeline	Official standard since 2001	Standardized 1977
Type of algorithm	Symmetric	Symmetric
Key size (in bits)	192	168
Speed	High	Low
Time to crack (assume a machine could try 255 keys per second - NIST)	149 trillion years	4.6 billion years
Resource consumption	Low	Medium

Gambar 2. 13 AES vs 3DES [9]

Penjelasan mengenai algoritma AES dapat dilihat pada Gambar 2.13 dan Feisel-Function pada Gambar 2.14 :

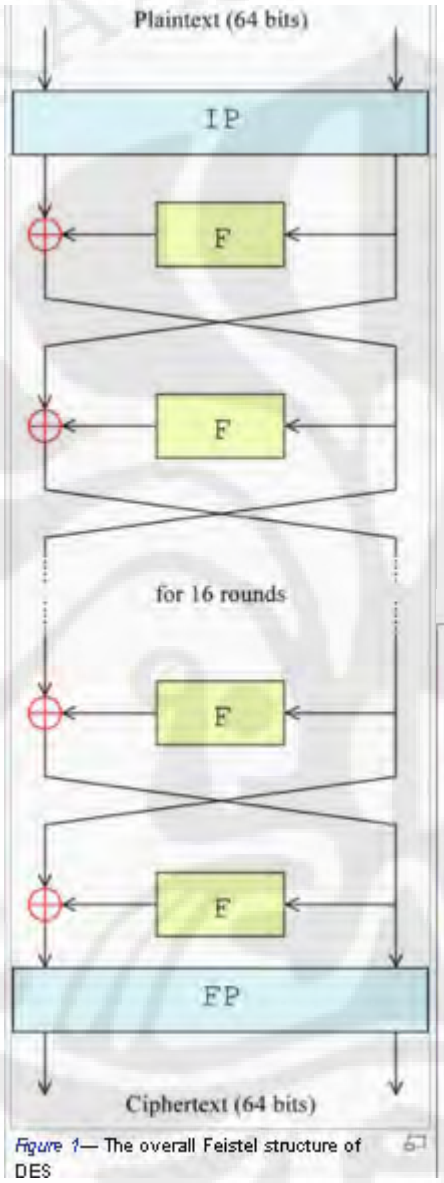
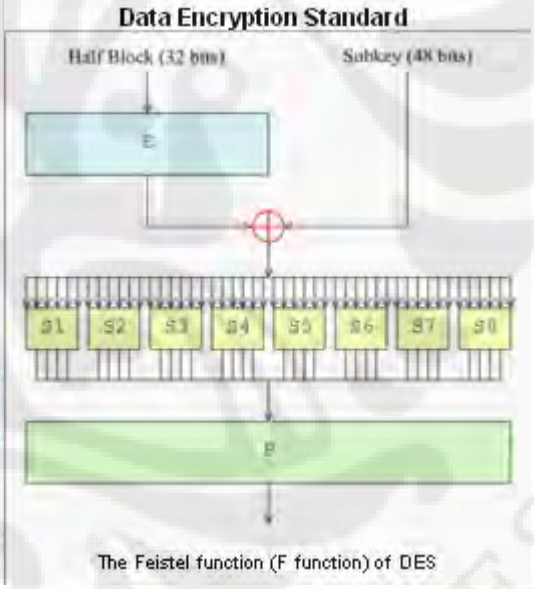


Figure 1— The overall Feistel structure of DES



The Feistel function (F function) of DES

C

Gambar 2. 14 Skema algoritma DES [7] Gambar 2. 15 Feisel-Function [7]

Rumus 3DES dengan 3key : C= EK3(EK2(EK1(P))) [8]

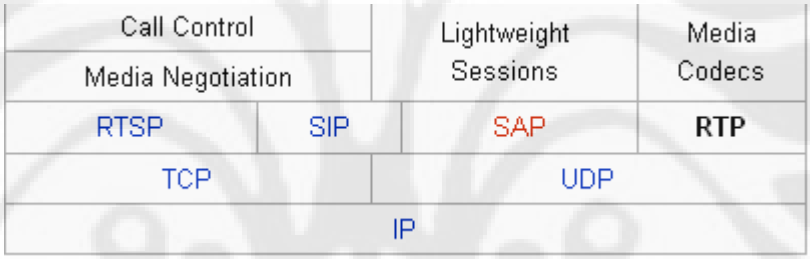
2.4 NetMeeting

Netmeeting adalah program IP-*telephony* yang telah terintegrasi pada OS windows, netmeeting ini pula dapat digunakan sebgai media teleconference

NetMeeting *Protocol* Architecture [15]:

1. Menggunakan Audio *Codec* ITU G.723.1 dan menyediakan *bit*-rates antara 4.8kbps s.d 64 kbps
2. Menggunakan Video *Codec*ITU H.263 dengan kemampuan 30fps
3. Netmeeting audio dan video *codec* menggunakan RTP diatas UDP connection

The *Real-time Transport Protocol* (RTP) adalah standar untuk menyampaikan paket format audio dan video., *protocol* ini terdapat di atas UDP sebagaimana yang digambarkan pada Gambar 2.16 :



Gambar 2. 16 RTP di atas UDP [10]

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

2.5 Qualitas Layanan (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

Analisa perbandingan..., Gatot S., FT UI, 2009

terhadap kesalahan. Tabel 2.2 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 Tipe Layanan QoS [1]

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 ditransfer dibagi durasi engiriman paket tersebut, biasanya diekspresikan dalam satuan bytes/sec.

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

1. Availabilitas, yaitu persentase hidupnya sistem atau subsistem telekomunikasi. Idealnya, availabilitas harus mencapai 100%. Nilai availabilitas yang diakui cukup baik adalah 99,9999% (*six nines*), yang menunjukkan tingkat kerusakan sebesar 2,6 detik per bulan [6].

Analisa perbandingan..., Gatot S., FT UI, 2009

2. *Throughput*, yaitu kecepatan (*rate*) 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 akan 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 nilai *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 (misalnya akibat pemakaian satelit), atau kongesti (yang memperpanjang antrian), atau bisa juga akibat waktu olah yang lama (misalnya untuk *digitizing* dan kompresi data).
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 juga berbeda), dan juga dalam waktu penghimpunan ulang paket-paket di akhir perjalanan.

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

1. *Routing protocol*
2. *Broadcast traffic*
3. *Collision*
4. *Header*
5. dan sebagainya

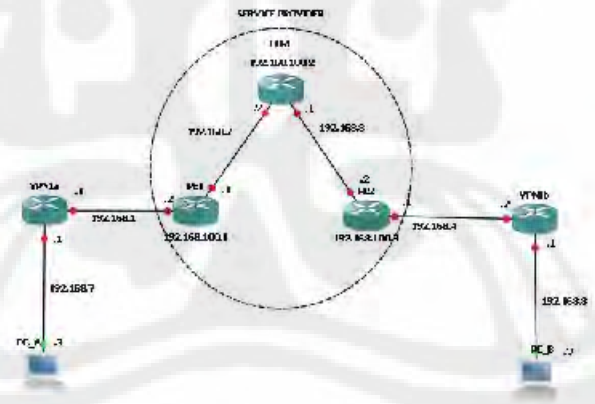
Analisa perbandingan..., Gatot S., FT UI, 2009

BAB III
PERANCANGAN DAN SIMULASI

Pada bab ini akan dibahas perancangan sistem *IP-BASED* video *telephony* peer to peer pada topologi *MPLS* VPN dengan menggunakan, 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 *testbed device* yang menjalankan aplikasi net meeting di mana saling terhubung langsung dengan kabel RJ45 cross-over, seperti pada Gambar 3.1:



Gambar 3. 1 Topologi Pengujian

3.2 Kebutuhan pendukung simulasi

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

Analisa perbandingan..., Gatot S., FT UI, 2009

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 *virtual*isasi 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 *virtual*isasi 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.

Analisa perbandingan..., Gatot S., FT UI, 2009

Komputer

Nama Komputer	: WAN
Processor	: Intel Core2Duo 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	: N-Vidia, GeForce 7300 GS 256 Mb
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	: N-Vidia, GeForce 7300 GS 256 Mb
Memory	: DDR PC 2700 1 GB
Sound Card	: C-Media
NIC	: Realtek RTL 8139/810X
Operating *System*	: Microsoft Windows XP SP2

Analisa perbandingan..., Gatot S., FT UI, 2009

3.2.2 Kebutuhan Software

Software yang digunakan pada skripsi ini adalah Wireshark, Netmeeting, GNS3, BES 1.3.6(CPU Limiter), 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 web*site* 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.

Analisa perbandingan..., Gatot S., FT UI, 2009

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 192.168.8.3/24 dan 192.168.7.3/24
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 wireshar, perlu didownload 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 A dan PC B

Analisa perbandingan..., Gatot S., FT UI, 2009

3.3.3 Instalasi PC *testbed*

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 192.168.7.3/24 dan 192.168.8.3/24
5. Melakukan instalasi program GNS3
6. Menambahkan IOS CISCO versi 7200
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 192.168.7.3/24 (PC_A) dan 192.168.8.3/24 (PC_B).

3.3.4 Instalasi Netmeeting pada End-toEnd PC

Program Netmeeting ini merupakan aplikasi yang menjembatani *testbed* 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.

Analisa perbandingan..., Gatot S., FT UI, 2009

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 satu buah router core, dua buah router PE, dan dua buah router CE.

Secara umum pada computer wan terdiri dari CE,Core, dan PE. Core dan PE dimiliki oleh *Service provider* dan CE dimiliki oleh *customer*. Pada C dan CE di-configure *MPLS*-VPN dengan menggunakan BGP-MP untuk exterior gateway *protocol*, dan OSPF untuk Internal Gateway *Protocol*nya.

Sedangkan pada sisi CE *routing protocol* yang digunakan hanyalah static *routing*. Implementasi dari IPSec pada sisi CE yaitu dengan menggunakan enkripsi 3DES dan AES. 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 pada kondisi jaringan tanpa beban maupun pada kondisi jaringan terbebani oleh paket UDP, kemudian dari hasil uji coba tersebut di ambil data dengan bantuan software wireshark, adapun data-data yang diambil saat ujicoba meliputi :

a. Data ujicoba streaming video *telephony* dengan enkripsi AES
b. Data ujicoba streanming video *telephony* dengan enkripsi 3DES
c. Data ujicoba streaming audio *telephony* dengan enkripsi AES
d. Data ujicoba streaming audio *telephony* dengan enkripsi 3DES

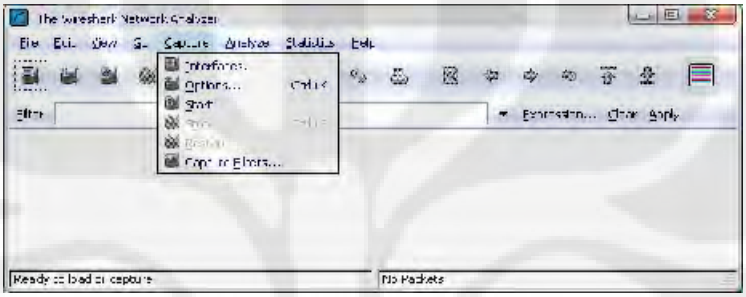
Analisa perbandingan..., Gatot S., FT UI, 2009

e. Data ujicoba transfer file yang berukuran 5MB.

Langkah-langkah pengambilan data menggunakan wireshark adalah sebagai berikut :

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

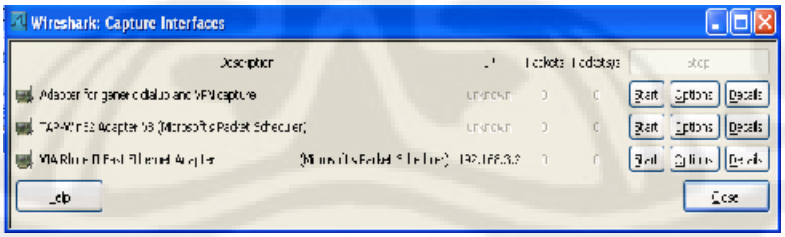
ii. mengcapture protokol yang sedang berjalan pada videoconference dengan bantuan wireshark, dengan mengklik Capture → interfaces. Lihat Gambar 3.2



Gambar 3. 2 Langkah mengcapture protokol pada wireshark

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

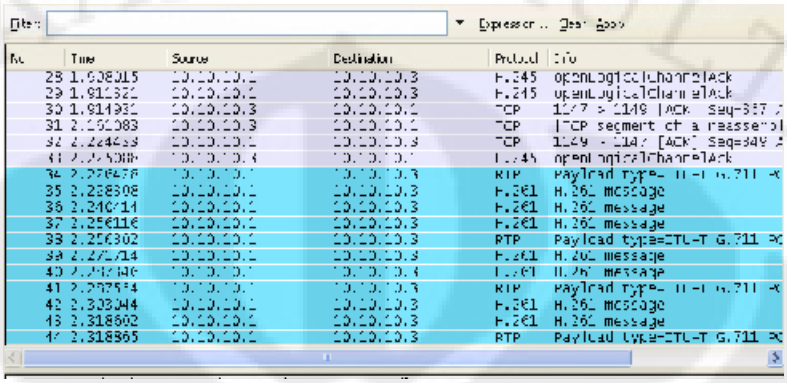
iv. Pada menu stop capture pilih after dan isi dengan 2 menit untuk menentukan lama proses capture. Lihat Gambar 3.3



Gambar 3. 3 Memulai mengcapture trafik paket data

v. Proses capture data berjalan, pada tugas akhir ini pengambilan data pada masing-masing kondisi dilakukan selama 1 menit.

vi. Setelah proses capture selesai dengan mengklik stop maka akan muncul protokol-protokol yang muncul pada saat proses capture untuk di analisa. Lihat Gambar 3.4



Gambar 3. 4 Protokol yang tercapture pada ujicoba

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

Langkah-langkah untuk melakukan komunikasi dari PC_A ke PC_B atau sebaliknya :

i. klik icon netmeeting pada desktop

ii. masukkan IP PC tujuan yanng akan dihubungi, kemudian klik icon telepon di samping IP tersebut. Lihat Gambar 3.5

Gambar 3. 5 Tatap muka Netmeeting

iii. Maka proses calling pun akan segera berjalan.

iv. Di PC satunya lagi akan muncul pesan bahwa ada host yang sedang berusaha menguhungi PC tersebut.

v. Klik accept. Maka komunikasipun telah berlangsung.

Proses calling dan capture terus diulang sebanyak lima kali dengan keadaan wan menggunakan AES/3DES .

BAB IV
ANALISA DATA DAN PEMBAHASAN

Pada bab IV ini akan dilakukan analisa perbandingan penggunaan tiap enkripsi 3DES dan AES terhadap performansi suatu *IP-BASED* video *telephony* di atas jaringan *MPLS*-VPN. Pada *streaming* Audio dan Video parameter yang diukur meliputi *delay, jitter,* dan *throughput,* sedangkan pada transfer file, parameter yang diukur hanya parameter *throughput* saja. Nilai yang terdapat pada diagram adalah nilia pada tiap kali pengujian sebanyak 5 kali dan setelah itu dihitung rata-ratanya.

Berikut adalah skema pengambilan data :

1. Capture paket-paket dengan menggunakan wireshark
2. Save *packet* yang ter-capture dengan file .pcap
3. Decode *packet* tersebut sebagai RTP
4. Export data hasil analisa RTP ke dalam format CSV menggunakan program pengolah sheet.
5. Ubah format CSV tersebut ke dalam kolom-kolom supaya mudah dalam penghitungan nilai rata-rata
6. Hitung nilai rata-rata dari tiap scenario pengujian dengan parameter-parameter yang telah ditentukan sebelumya.

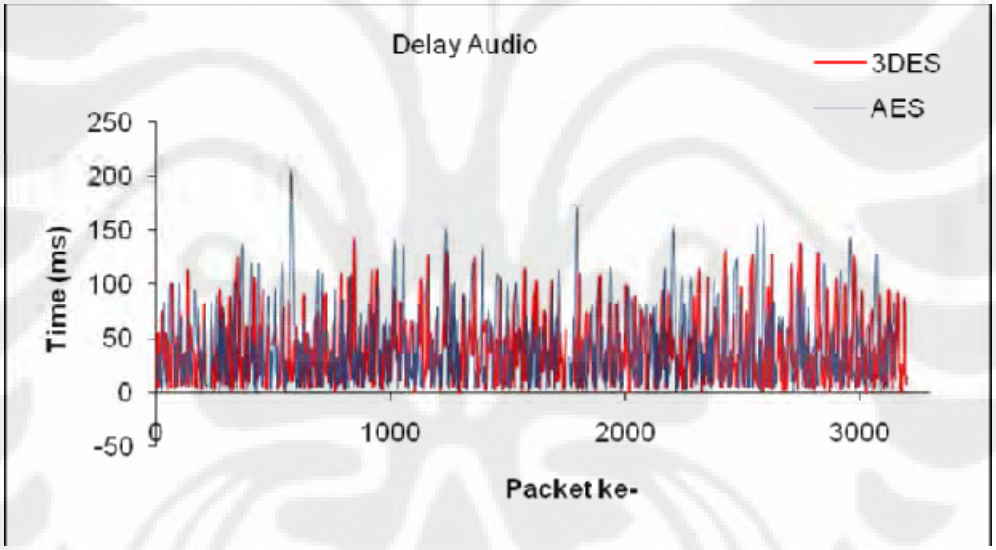
Analisa perbandingan..., Gatot S., FT UI, 2009

4.1 *Analisa Audio*

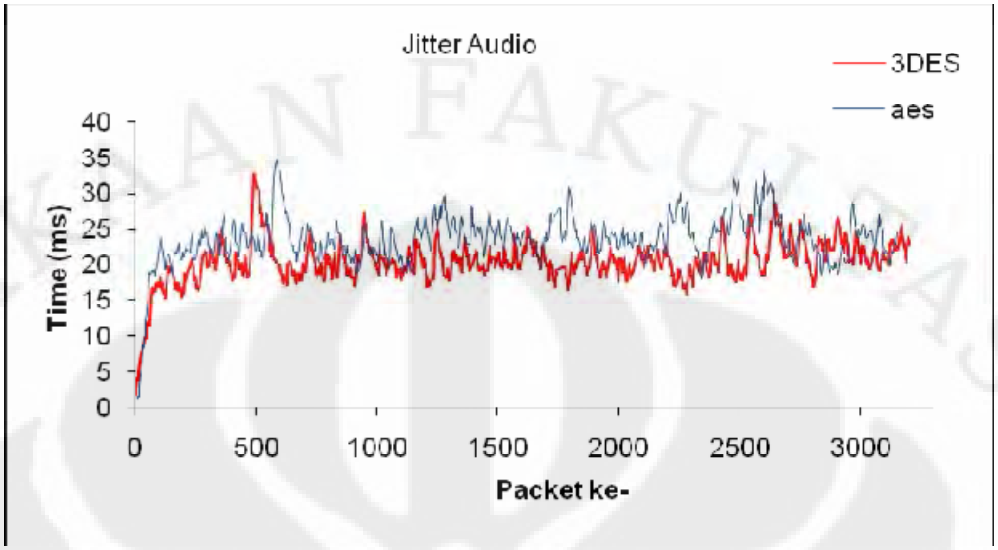
Tabel 4.1 adalah hasil pengolahan data pada pengujian *streaming* audio :

AUDIO						
	3DES			AES		
Pengambilan data ke-	*Delay* (ms)	*Jitter* (ms)	*Throughput* (kbps)	*Delay* (ms)	*Jitter* (ms)	*Throughput* (kbps)
1	30.63	18.85	16.77	30.80	20.04	16.67
2	31.05	20.47	16.61	31.00	23.45	16.50
3	31.06	20.82	16.57	31.00	23.55	16.56
4	31.02	21.17	16.64	31.05	23.92	16.50
5	29.58	20.32	16.77	30.01	22.94	16.70
Rata-rata	**30.67**	**20.33**	**16.67**	**30.77**	**22.78**	**16.58**

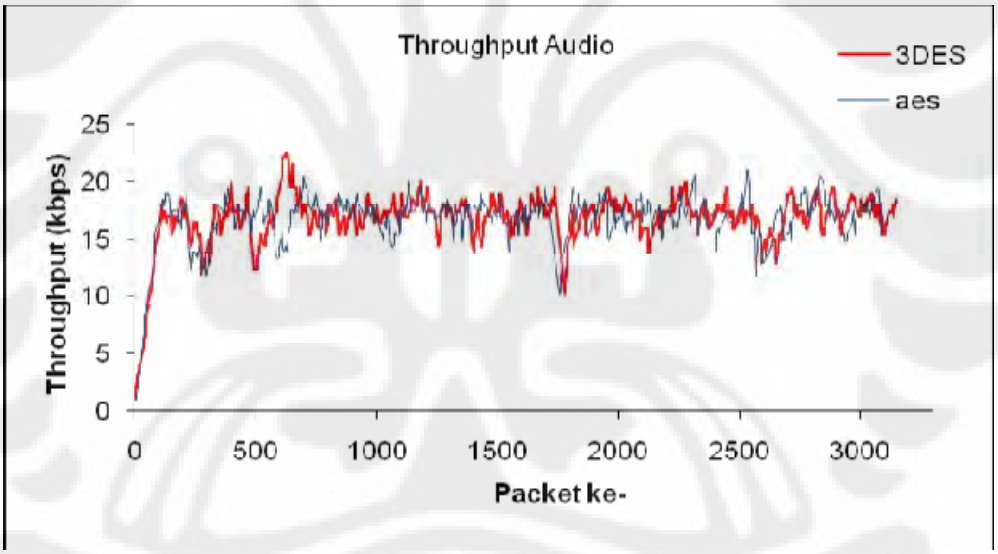
Tabel 4. 1 Perbandingan QoS pada paket *streaming* audio



Gambar 4. 1 *Delay* Audio



Gambar 4. 2 *Jitter* Audio



Gambar 4. 3 *Throughput* Audio

Pada pengujian streaming audio menurut Tabel 4.1 diperoleh nilai *delay*, *jitter*, dan *throughput* pada 3DES lebih baik dibandingkan dengan AES dengan selisih 0.1 ms (0.33%), 2.46 ms(10.78%), dan 0.09 kbps(0.53%). Dari Gambar 4.1 terlihat rentang min-max AES lebih besar dibandingkan 3DES. Nilai rentang

Analisa perbandingan..., Gatot S., FT UI, 2009

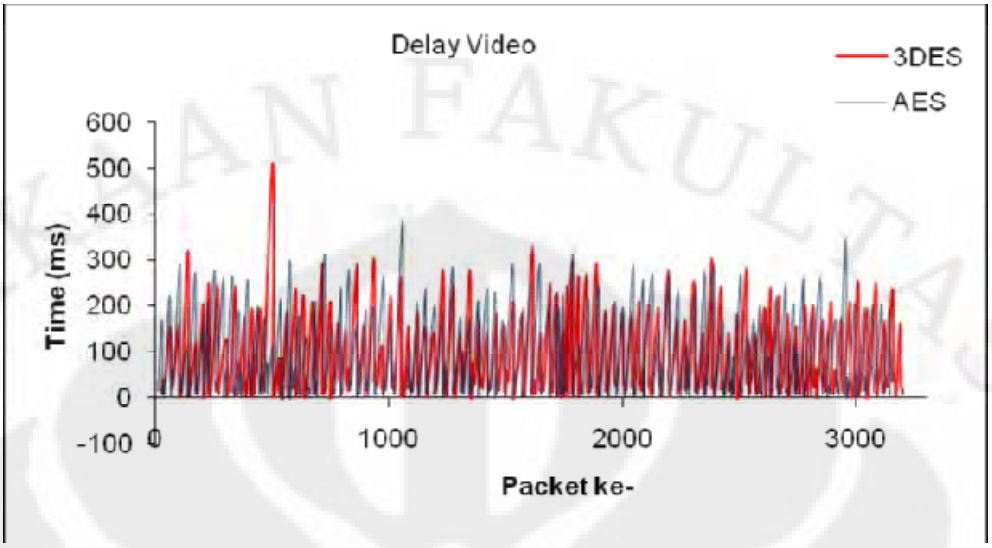
tersebut merupakan akibat dari pengaruh *jitter* AES yang lebih besar, ini bisa terlihat pada grafik *jitter* audio. Sedangkan pada data maupun grafik *throughput* audio tidak terlihat perbedaan yang mencolok. Nilai ini berbeda dengan nilai pada streaming video yang parameter QoS pada AES lebih baik dibandingkan dengan 3DES. Memang tidak dipungkiri bahwa AES seharusnya lebih baik dibandingkan dengan 3DES dengan alasan AES ditujukan untuk menggantikan 3DES serta alasan-alasan yang telah dikemukakan pada analisa video nanti. Perbedaan tersebut yang secara kasat mata tidak terlalu signifikan ini disebabkan pula karena pada streaming audio *bit*rate-nya relatif sangat kecilkecil sehingga tidak terlalu membebani prosesor. Walaupun demikian, pada streaming audio kualitas layanan yang diberikan 3DES lebih baik dibandingkan AES

4.2 Analisa Video

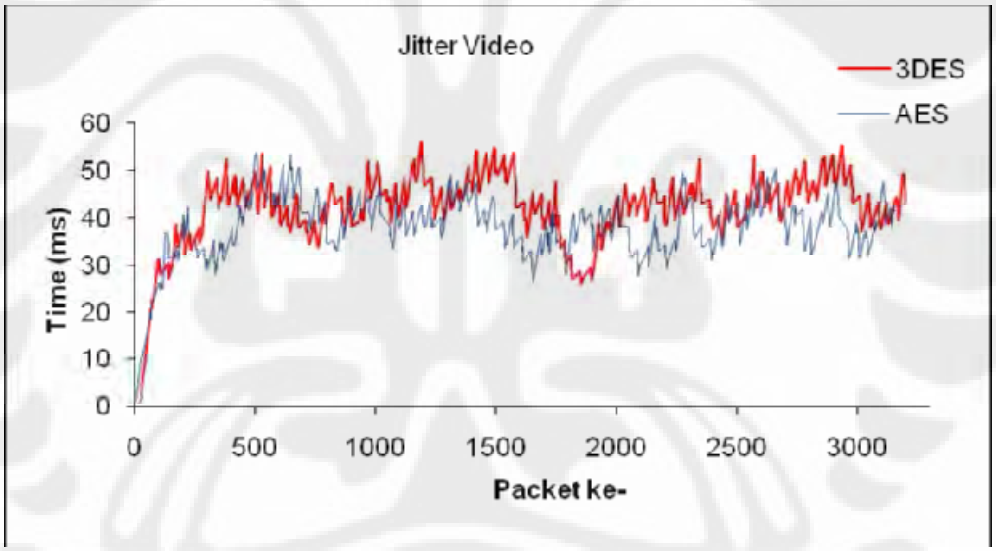
Tabel 4.2 adalah data hasil pengujian *streaming* video yang dilakukan sebanyak 5 kali dan berisi parameter *delay*, *jitter*, dan *throughput*.

	3DES			AES		
Pengambilan data ke-	*Delay* (ms)	*Jitter* (ms)	*Throughput* (kbps)	*Delay* (ms)	*Jitter* (ms)	*Throughput* (kbps)
1	54.31	42.89	172.92	55.40	43.09	170.23
2	54.25	38.13	171.71	55.70	44.67	167.97
3	53.46	41.11	169.55	56.11	42.54	165.85
4	52.16	36.89	172.58	55.97	44.55	165.29
5	53.80	39.33	170.82	55.61	42.07	166.25
Rata-rata	**53.60**	**39.67**	**171.52**	**55.76**	**43.39**	**167.12**

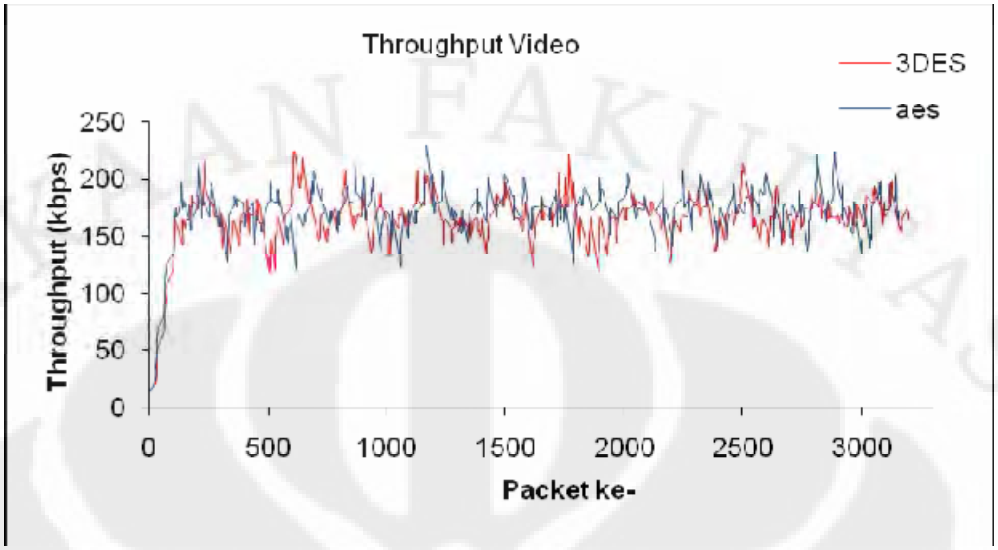
Tabel 4. 2 Perbandingan QoS pada paket *streaming* audio



Gambar 4. 4 *Delay* Video



Gambar 4. 5 *Jitter* Audio



Gambar 4. 6 *Throughput* Video

Pada pengujian streaming video diperoleh nilai *delay*, *jitter*, dan *throughput* pada AES lebih baik dibandingkan dengan 3DES dengan selisih 2.16 ms (4.03%), 3.71 ms (9.36%), dan 4.4 kbps (2.56%). Dari Gambar 4.4 terlihat rentang min-max 3DES lebih besar dibandingkan AES. Nilai rentang tersebut merupakan akibat dari pengaruh *jitter* 3DES yang lebih besar 3.71 ms, ini bisa terlihat pada Gambar 4.5 video. Sedangkan pada Tabel 4.2 maupun Gambar 4.6, *throughput* video secara umum lebih baik AES. Pada grafik-grafik tersebut terlihat kurang stabil dibandingakan dengan paket audio karena pada video menggunakan *framesize* yang berbeda untuk tiap paketnya. Sehingga waktu untuk memproses tiap paket tersebut berbeda-beda, tergantung dari *framesize* yang sedang dienkripsi/dekripsi. Dengan nilai yang demikian yaitu AES memberikan layanan yang lebih baik dibandingkan dengan 3DES menunjukkan percobaan telah berhasil dan telah membuktikan algoritma Rijndael memiliki performa yang lebih baik dibandingakn dengan algoritma Data Encyption Standard.

Ada beberapa penyebab 3DES lebih rendah performanya dibandingkan dengan enkripsi AES pada *streaming* video :

1. Ronde

   3DES memiliki ronde yang lebih banyak dibandingkan AES. Enkripsi 3DES harus melalui proses sebanyak 16 ronde sedangkan pada AES hanya 10, 12, dan 14 ronde. Tetapi pada pengujian kali ini mengguakan 12 ronde karena *keyspace* yang digunakan 192-*bit*.

2. *Block size*

   3DES menggunakan 64-*bit block size*, dan itupun akan dipecah lagi menjadi dua yang masing-masing sebesar 32-*bit*. Sehingga untuk sebuah paket yang berukuran 128 *bit* akan dipecah menjadi 4 yang setiap pecahan itu akan dimuat secara terpisah. Sedangkan pada AES memakai *block size* 128-*bit*. Sehingga sebuah paket yang berukuran 128-*bit* hanya akan dimuat hanya satu kali.

3. Banyak proses

   Data yang di enkripsi menggunakan 3DES akan diproses sebanyak 3x sedangkan AES hanya 1x.

4. Paralel proses

   Karena DES muncul di tahun 1977 sedangkan AES muncul tahun 1999, menyebabkan AES didisain untuk bisa diproses secara paralel yaitu pada proses SubBytes dan ShiftRows bisa diparalelkan dengan proses *Mix*Columns.

5. DES menggunakan sub*key* yang *dependent* pada setiap ronde sedangkan AES menggunakan sub*key* yang *independent*.

4.3 Analisa Throughput Transfer Data

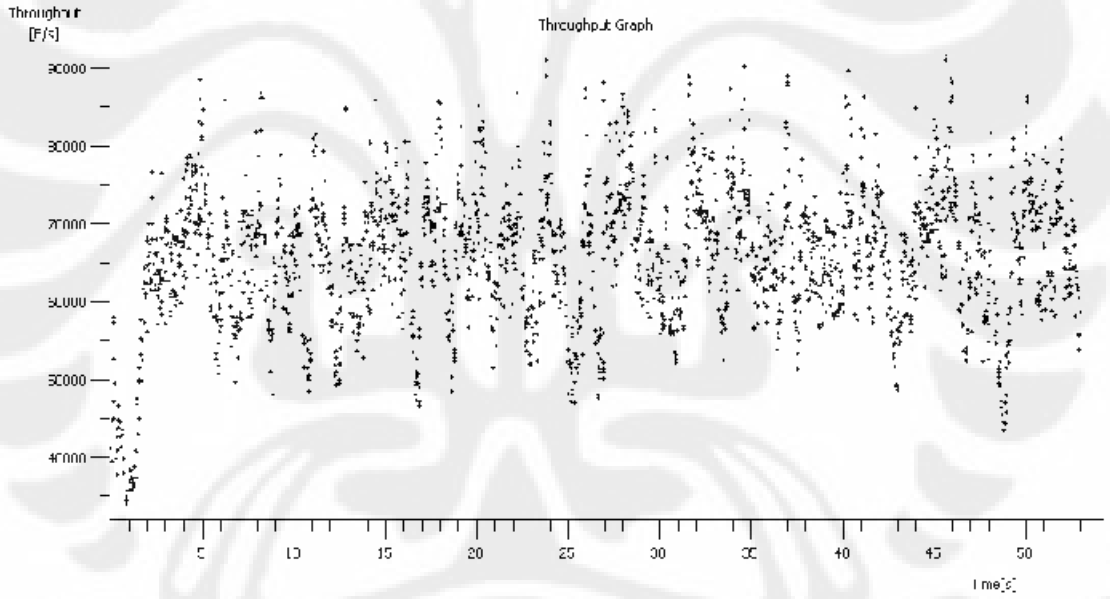
Pada pengujian kali ini yaitu mengukur *throughput* pada jenis pengujian transfer file MP3, FLV, dan DOC dengan mengguakan TCP, sedangkan sebelumnya ketika pengujian *streaming* menggunakan UDP. Masing-masing file tersebut

Analisa perbandingan..., Gatot S., FT UI, 2009

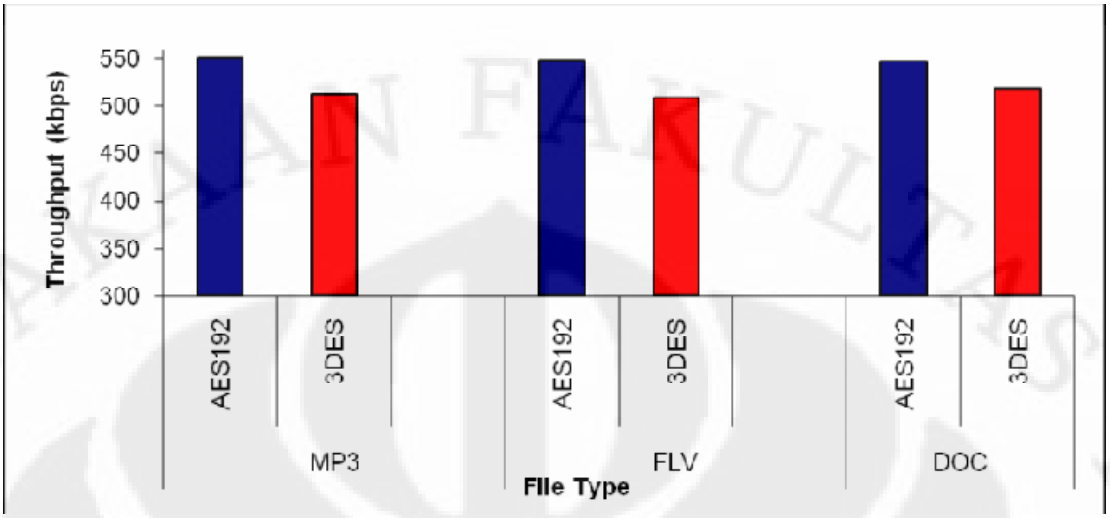
berukuran 5MB. Pengujian dilakukan sebanyak 5 kali, kemudian diambil rata-ratanya. Tabel 4.3 adalah Tabel hasil pengukurannya :

Pengambilan data ke-	MP3		FLV		DOC	
	AES192	**3DES**	**AES192**	**3DES**	**AES192**	**3DES**
1	551	557	554	506	517	482
2	532	548	556	524	559	528
3	559	424	527	509	572	538
4	549	517	558	501	535	529
5	559	523	546	510	550	520
Rata-rata (kbps)	**550**	**513.8**	**548.2**	**510**	**546.6**	**519.4**

Tabel 4. 3 *Throughput* transfer file



Gambar 4. 7 *Throughput* transfer file



Gambar 4. 8 *Throughput* transfer file

Terlihat jelas baik dari Tabel 4.3 ataupun Gambar 4.8 menunjukkan *throughput* pada AES selalu lebih baik dibandingkan 3DES dengan perbedaan 36.2 kbps, 38.2 kbps, 27.2 atau 7.05%, 7.49%, dan 5.24% untuk file jenis MP3, FLV, dan DOC.

Pada pengujian transfer file hanya digunakan parameter *throughput* saja karena grafik dan data yang disediakan untuk TCP hanya *throughput* dan round trip. Round trip sengaja tidak dimasukkan karena untuk mendapatkan Gambaran parameter yang sama antara UDP dan TCP.

Pada Gambar 4.8 hanya ditampilkan satu grafik *throughput* karena data-data nya tidak bisa di eksport untuk bisa dijadikan grafik seperti pada grafik *delay*, *jitter throughput* pada streaming audio dan video. Dan perbedaan *throughput* tidak terlihat secara jelas karena skala yang digunakan cukup besar sehingga penyajian 1 buah grafik dinilai cukup mengGambarkan keadaan data-data yang lain. Terlihat jelas bahwa enkripsi AES memberikan *throughput* yang lebih baik dibandingkan dengan 3DES. Untuk alasannya tidak jauh berbeda dengan analisa pada sub bab 4.2 Analisa Video.

Analisa perbandingan..., Gatot S., FT UI, 2009

4.4 Analisa Perbandingan Audio, Video, Transfer File

Terdapat 3 jenis pengujian yaitu *streaming* audio, *streaming* video, dan transfer file, apabila dilihat lebih dalam menggunakan wireshark maka akan ditemui bahwa secara berurutan *framesize* dari ketiga jenis pengujian tersebut yaitu 78 bytes, 700-1300 bytes, 1433 bytes. Dan bila diambil data persentase selisih *throughput* antara 3DES dan AES yaitu 0.53%, 2.56%, dan 5.24% -7.49%. Akan terlihat bahwa semakin besar *framesize*-nya maka akan semakin jelas pula perbedaan performa dari 3DES dan AES. Ini terjadi karena semakin besar frame *size* maka akan semakin lama pula sebuah router untuk memproses tiap framenya, bila frame *size*nya kecil maka router akan relatif lebih mudah memprosesnya. Walaupun terlihat selisih diantara 3DES dan AES pada *streaming* audio relatif kecil, tidak serta merta nilai tersebut dapat diabaikan begitu saja karena prosesor yang bekerja dengan clock yang relatif tinggi dibandingkan dengan selisih yang berkisar pada satuan mili second. Prosesor yang digunakan pada PC wan yaitu 2.2GHz sedangkan kemampuan dari router cisco seri 7200 berkisar 263MHz.

Pada pengujian *streaming* audio dan *streaming* video didapatkan nilai *delay*, *jitter*, dan *throughput* pada *streaming* video selalu lebih baik daripada audio. Ini terjadi karena data yang dikirimkan pada *streaming* video lebih besar dibandingkan pada *streaming* audio.

Ketika conference berlangsung suara datang lebih cepat dibandingkan video, ini terjadi karena *jitter* audio lebih kecil dibandingkan *jitter* pada *streaming* video. Ini terjadi secara alamiah karena semakin variasi *delay* lebih rendah maka dia yang akan sampai dahulu dibandingkan yang memiliki *jitter* yang lebih besar.

Berdasarkan grafik *delay*, *jitter*, dan *throughput* terlihat bahwa grafik audio lebih stabil dibandingkan grafik video. Bila diperhatikan dengan menggunakan wireshark yang menyebabkan ketidak stabilannya yaitu pada audio menggunakan *framesize* yang statis sedangkan pada video menggunakan *framesize* yang dinamis.

Pengujian tersebut cukup *reliable* karena nilai *delay* dan *jitter*-nya masih berada di bawah angka standar yaitu dibawah 150ms (*delay*) dan 50ms (*jitter*).

Analisa perbandingan..., Gatot S., FT UI, 2009

Dalam sebuah paper disebutkan bahwa kecepatan 3DES yaitu 3x lebih lama dibandingkan dengan DES karena 3DES menggunakan algoritma yang sama dengan DES, yang membedakannya yaitu 3DES mengulangi 2x proses DES lagi. Dan disebutkan pula bahwa kecepatan AES sebanding dengan DES. Tetapi berdasarkan pada data-data hasil pengolahan data tidak menunjukkan nilai demikian, tidak didapatkan nilai *delay* 3DES 3x lebih besar dibandingkan AES. Yang dimaksud 3x lebih cepat itu yaitu apabila proses enkripsi berjalan pada sistem *stand alone*, sedangkan yang diujicobakan yaitu berjalan pada jaringan. Sehingga nilai *delay*, dan *jitter* dapatkan adalah nilai *jitter* total rata-rata dari *delay* setiap *device* yang dilaluinya.

Analisa perbandingan..., Gatot S., FT UI, 2009

BAB V
KESIMPULAN

Setelah melakukan serangkaian simulasi dengan menggunakan GNS3 untuk membangun MPLS-VPN yang ditambahkan enkripsi AES dan 3DES didapat beberapa kesimpulan berikut :

1. Pada pengujian *streaming* audio, *delay* 3DES lebih baik 0.1 ms (0.33%), *jitter* 3DES lebih baik 2.46 ms (10.78%), dan *throughput* 3DES lebih baik 0.09 kbps (0.53%) dibanding AES. Hal yang menyebabkan tidak terlalu signifikan perbedaan antara AES dan 3DES ini adalah bitrate pada streaming audio relatif sangat kecil sehingga tidak terlalu membebani prosesor.
2. Pada pengujian *streaming* video, *delay* AES lebih baik 2.16 ms (4.03%),, *jitter* AES lebih baik 3.71 ms (9.36%), dan *throughput* AES lebih baik 4.4 kbps (2.56%) dibanding DES
3. Pada pengujian *throughput* Transfer file, menunjukkan AES lebih baik dibandingkan 3DES sebesar 27.2 kbps (5.24%) – 38.2 kbps (7.49%)
4. Pada streaming video dan transfer file AES menawarkan kualitas layanan lebih baik dibandingkan dengan 3DES(168-*bit*) walaupun AES(192-*bit*) menggunakan *keyspace* yang lebih besar. Hal ini disebabkan : Ronde AES lebih sedikit dibanding 3DES; block size AES lebih besar, dan efektif untuk file berukuran besar; AES didisain untuk menjalankan proses secara paralel, sedangkan 3DES tidak; AES menggunakan subkey *independent*, sehingga tidak menunggu antrian subkey sebelumnya, sedangkan 3DES menggunakan subkey yang *dependent*

Analisa perbandingan..., Gatot S., FT UI, 2009

DAFTAR ACUAN

[1] _____"*Multi Protocol Label Switch*" , Diakses juli 2008 telkom.co.id *MPLS*.ppt

[2] _____*MultiProtocol Label Switching (MPLS),* diakses tanggal 22 Juni 2009 http://www.ittelkom.ac.id/library/index.php?view=article&catid=15:pemrosesan-sinyal&id=338:multi*protocol*-label-switching-pls&option=com_content&Itemid=15

[3] Luch the Ghein CCIE, *MPLS Fundamental*, Cisco Press : 2007

[4] *"white paper of MPLS"* www.CipherOptics.com/wp-*MPLS*/

[5] S.Hirani, *"Energy Consumption of Encryption Schemes in Wireless Devices Thesis,"* university of Pittsburgh, April 9,2003. Retrieved October 1, 2008,

[6] _____"*3DES",* Diakses tanggal 20 Juni 2009 www.tropsoft.com/strongenc/des3.htm

[7] _____ *"Data Encryption Standard",* diakses tangggal 1 Juni 2009 en.wikipedia.org/wiki/Data_*Encryption_Standard*

[8] Vijay Bollapragada, Mohamed Khalid, Scott Wainner, *IPSec VPN Design* Cisco Press, April 07, 2005

[9] _____"*Encryption: AES versus Triple-DES"* , diakses tanggal 25 Juni 2009 http://www.icommcorp.com/downloads/Comparison%20AES%20vs%203DES.pdf

[10] _____ *"Real-time Transport Protocol",* diakses tanggal 25 Juni 2009 http://en.wikipedia.org/wiki/*Real-time_Transport_Protocol*

[11] Abdel-Karim Al Tamimi, *"Performance Analysis of Data Encryption Algorithms"* Diakses tanggal 15 juni 2009 http://www.cs.wustl.edu/~jain/cse567-06/ftp/*encryption*_perf.pdf

[12] _____"*Encryption: AES versus Triple-DES*", diakses tanggal 20 juni 2009 http://www.nexiondata.com/products/options/encrypt/howgood.htm

[13] Schneier, Bruce. *Applied Cryptography*. John Wiley & Sons, 1996

[14] Ralph, C Merkle "*On the Security of Multiple Encryption*", standford University
http://www.cs.purdue.edu/homes/ninghui/courses/Spring04/homeworks/p465-merkle.pdf

[15] _____ "*Netmeeting Protocol Architecture*", diakses tanggal 27 Juni 2009
http://www.ensc.sfu.ca/people/faculty/ljilja/cnl/presentations/milan/milan_thesis/sld029.htm

[16] _____, diakses tanggal 27 Juni 2009
http://blogimg.chinaunix.net/blog/upfile2/080106135559.jpg

Analisa perbandingan..., Gatot S., FT UI, 2009

DAFTAR REFERENSI

A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996

Luch the Ghein CCIE, *MPLS* Fundamental, Cisco Press, 2007

Jim, Ivan. *MPLS* and VPN Architectures Jim CCIE #2069 Guichard, Ivan CCIE #1354 Pepelnjak, October 31, 2000

Michael H. Behringer, Monique J. Morrow ,, *MPLS* VPN *Security*, Cisco Press

Vijay Bollapragada, Mohamed Khalid, Scott Wainner, IPSec VPN Design Cisco Press, April 07, 2005

Schneier, Bruce. Applied Cryptography. John Wiley & Sons, 1996

"*Encryption*: AES versus Triple-DES"
http://www.icommcorp.com/downloads/Comparison%20AES%20vs%203DES.pdf

http://www.ietf.org/rfc/rfc1889.txt

http://www.ietf.org/rfc/2547.txt

http://csrc.nist.gov/

"On the *Security* of Multiple *Encryption*"
http://www.cs.purdue.edu/homes/ninghui/courses/Spring04/homeworks/p465-merkle.pdf

"Performance Evaluation of *Symmetric Encryption* Algorithms"
http://paper.ijcsns.org/07_book/200812/20081240.pdf

LAMPIRAN A

----------CORE----------

```
mpls label protocol ldp
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Loopback0
 ip address 192.168.100.2 255.255.255.255
!
interface FastEthernet0/0
 description ***connection to PE1***
 ip address 192.168.2.2 255.255.255.0
 duplex auto
 speed auto
 mpls ip
!
interface FastEthernet0/1
 description ***connection to PE2***
```


Analisa perbandingan..., Gatot S., FT UI, 2009

```
 ip address 192.168.3.1 255.255.255.0
 duplex auto
 speed auto
 mpls ip
!
router ospf 100
 log-adjacency-changes
 network 192.168.2.0 0.0.0.255 area 100
 network 192.168.3.0 0.0.0.255 area 100
 network 192.168.100.2 0.0.0.0 area 100
!
ip classless
no ip http server
no ip http secure-server
!
!
!
logging alarm informational
!
!
!
mpls ldp router-id Loopback0 force
```

----------PE1----------

```
ip vrf vpn1
 rd 100:1
 route-target export 100:1
 route-target import 100:1
!
ip vrf vpn2
 rd 100:2
 route-target export 100:2
 route-target import 100:2
!
no ip domain lookup
```


Analisa perbandingan..., Gatot S., FT UI, 2009

```
!
mpls label protocol ldp
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Loopback0
 ip address 192.168.100.1 255.255.255.255
!
interface FastEthernet0/0
 description ***connection to CORE***
 ip address 192.168.2.1 255.255.255.0
 duplex auto
 speed auto
 mpls ip
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
```


Analisa perbandingan..., Gatot S., FT UI, 2009

```
 speed auto
!
interface FastEthernet1/0
 description ***connection to VPN1a***
 ip vrf forwarding vpn1
 ip address 192.168.1.2 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet1/1
 ip vrf forwarding vpn2
 ip address 192.168.6.2 255.255.255.0
 duplex auto
 speed auto
!
router ospf 100
 log-adjacency-changes
 network 192.168.2.0 0.0.0.255 area 100
 network 192.168.100.1 0.0.0.0 area 100
!
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 neighbor 192.168.100.3 remote-as 100
 neighbor 192.168.100.3 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
 neighbor 192.168.100.3 activate
 neighbor 192.168.100.3 send-community both
 exit-address-family
 !
 address-family ipv4 vrf vpn2
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
```


Analisa perbandingan..., Gatot S., FT UI, 2009

```
 exit-address-family
 !
 address-family ipv4 vrf vpn1
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 exit-address-family
!
ip classless
ip route vrf vpn1 192.168.7.0 255.255.255.0 192.168.1.1
ip route vrf vpn1 202.147.192.1 255.255.255.255 192.168.1.1
ip route vrf vpn2 202.147.192.1 255.255.255.255 192.168.6.1
```

----------PE2----------

```
ip vrf vpn1
 rd 100:1
 route-target export 100:1
 route-target import 100:1
!
ip vrf vpn2
 rd 100:2
 route-target export 100:2
 route-target import 100:2
!
no ip domain lookup
!
mpls label protocol ldp
!
!
!
!
!
!
!
```


Analisa perbandingan..., Gatot S., FT UI, 2009

```
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Loopback0
 ip address 192.168.100.3 255.255.255.255
!
interface FastEthernet0/0
 description ***connection to CORE***
 ip address 192.168.3.2 255.255.255.0
 duplex auto
 speed auto
 mpls ip
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet1/0
 description ***connection to VPN1b***
 ip vrf forwarding vpn1
 ip address 192.168.4.1 255.255.255.0
 duplex auto
 speed auto
!
```


Analisa perbandingan..., Gatot S., FT UI, 2009

```
interface FastEthernet1/1
 description ***connection to VPN2b***
 ip vrf forwarding vpn2
 ip address 192.168.5.1 255.255.255.0
 duplex auto
 speed auto
!
router ospf 100
 log-adjacency-changes
 network 192.168.3.0 0.0.0.255 area 100
 network 192.168.100.3 0.0.0.0 area 100
!
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 neighbor 192.168.100.1 remote-as 100
 neighbor 192.168.100.1 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
 neighbor 192.168.100.1 activate
 neighbor 192.168.100.1 send-community both
 exit-address-family
 !
 address-family ipv4 vrf vpn2
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv4 vrf vpn1
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 exit-address-family
```


Analisa perbandingan..., Gatot S., FT UI, 2009

```
!
ip classless
ip route vrf vpn1 192.168.8.0 255.255.255.0 192.168.4.2
ip route vrf vpn1 202.147.192.2 255.255.255.255 192.168.4.2
ip route vrf vpn2 202.147.192.2 255.255.255.255 192.168.5.2
no ip http server
no ip http secure-server
!
!
!
logging alarm informational
!
!
!
mpls ldp router-id Loopback0 force
```

----------VPN1A FOR AES----------

```
crypto isakmp policy 1
 encr aes
 hash md5
 authentication pre-share
 group 2
crypto isakmp key cisco address 192.168.4.2
!
!
crypto ipsec transform-set esp-aes-md5 esp-aes esp-md5-hmac
!
crypto map vpn 10 ipsec-isakmp
 set peer 192.168.4.2
 set transform-set esp-aes-md5
 match address 102
!
!
!
```


Analisa perbandingan..., Gatot S., FT UI, 2009

```
!
!
interface Loopback0
 ip address 202.147.192.1 255.255.255.255
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
 crypto map vpn
!
interface FastEthernet0/1
 ip address 192.168.7.1 255.255.255.0
 duplex auto
 speed auto
!
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.1.2
no ip http server
no ip http secure-server
!
!
!
logging alarm informational
access-list 102 permit ip 192.168.7.0 0.0.0.255 192.168.8.0 0.0.0.255
!
!
```

----------VPN1B FOR AES----------

```
crypto isakmp policy 1
 encr aes
 hash md5
 authentication pre-share
 group 2
crypto isakmp key cisco address 192.168.1.1
```


Analisa perbandingan..., Gatot S., FT UI, 2009

```
!
!
crypto ipsec transform-set esp-aes-md5 esp-aes esp-md5-hmac
!
crypto map vpn 10 ipsec-isakmp
 set peer 192.168.1.1
 set transform-set esp-aes-md5
 match address 102
!
!
!
!
!
interface Loopback0
 ip address 202.147.192.2 255.255.255.255
!
interface FastEthernet0/0
 ip address 192.168.4.2 255.255.255.0
 duplex auto
 speed auto
 crypto map vpn
!
interface FastEthernet0/1
 ip address 192.168.8.1 255.255.255.0
 duplex auto
 speed auto
!

!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.4.1
no ip http server
no ip http secure-server
!
!
!
logging alarm informational
```


Analisa perbandingan..., Gatot S., FT UI, 2009

```
access-list 102 permit ip 192.168.8.0 0.0.0.255 192.168.7.0 0.0.0.255
!
```

----------VPN1A FOR 3DES----------

```
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key cisco address 192.168.4.2
!
!
crypto ipsec transform-set esp-3des-md5 esp-3des esp-md5-hmac
!
crypto map vpn 10 ipsec-isakmp
 set peer 192.168.4.2
 set transform-set esp-3des-md5
 match address 102
!
!
!
!
!
interface Loopback0
 ip address 202.147.192.1 255.255.255.255
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
 crypto map vpn
!
interface FastEthernet0/1
 ip address 192.168.7.1 255.255.255.0
 duplex auto
```


Analisa perbandingan..., Gatot S., FT UI, 2009

```
 speed auto
!
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.1.2
no ip http server
no ip http secure-server
!
!
!
logging alarm informational
access-list 102 permit ip 192.168.7.0 0.0.0.255 192.168.8.0 0.0.0.255
```

----------VPN1B FOR 3DES----------

```
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key cisco address 192.168.1.1
!
!
crypto ipsec transform-set esp-3des-md5 esp-3des esp-md5-hmac
!
crypto map vpn 10 ipsec-isakmp
 set peer 192.168.1.1
 set transform-set esp-3des-md5
 match address 102
!
!
!
!
!
interface Loopback0
```

```
 ip address 202.147.192.2 255.255.255.255
!
interface FastEthernet0/0
 ip address 192.168.4.2 255.255.255.0
 duplex auto
 speed auto
 crypto map vpn
!
interface FastEthernet0/1
 ip address 192.168.8.1 255.255.255.0
 duplex auto
 speed auto
!
interface Ethernet1/0

!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.4.1
no ip http server
no ip http secure-server
!
!
!
logging alarm informational
access-list 102 permit ip 192.168.8.0 0.0.0.255 192.168.7.0 0.0.0.255
!
!
```


Analisa perbandingan..., Gatot S., FT UI, 2009

This document was created with Win2PDF available at http://www.daneprairie.com.
The unregistered version of Win2PDF is for evaluation or non-commercial use only.