UNIVERSITAS INDONESIA

ANALISA UNJUK KERJA DAN QUALITY OF SERVICE DARI APLIKASI SECURE VIDEO STREAMING PADA JARINGAN BERBASIS VPN (VIRTUAL PRIVATE NETWORK)

SKRIPSI

MUHAMMAD SALMON HARDANI
0706199621

FAKULTAS TEKNIK
PROGRAM STUDI TEKNIK ELEKTRO
DEPOK
DESEMBER 2009

UNIVERSITAS INDONESIA

ANALISA UNJUK KERJA DAN QUALITY OF SERVICE DARI APLIKASI SECURE VIDEO STREAMING PADA JARINGAN BERBASIS VPN (VIRTUAL PRIVATE NETWORK)

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Teknik

MUHAMMAD SALMON HARDANI
0706199621

FAKULTAS TEKNIK
PROGRAM STUDI TEKNIK ELEKTRO
DEPOK
DESEMBER 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	**: Muhammad Salmon Hardani**
NPM	**: 0706199621**
Tanda Tangan	**:**
Tanggal	**: 28 Desember 2009**

HALAMAN PENGESAHAN

Skripsi ini diajukan oleh :

Nama : Muhammad Salmon Hardani

NPM : 0706199621

Program Studi : Teknik Elektro

Judul Skripsi : ANALISA UNJUK KERJA DAN QUALITY OF SERVICE DARI APLIKASI SECURE VIDEO STREAMING PADA JARINGAN BERBASIS VPN (VIRTUAL PRIVATE NETWORK)

Telah berhasil dipertahankan dihadapan 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, MIT (_____)

Penguji : Dr. Ir. Anak Agung Putri Ratna, M.Eng (_____)

Penguji : Ir. Endang Sriningsih, MT, Si (_____)

Ditetapkan di : Depok

Tanggal : 28 Desember 2009

KATA PENGANTAR

Alhamdulillah, segala puji dan syukur saya panjatkan kepada Tuhan Yang Maha Esa, karena atas berkat dan rahmat-Nya saya dapat menyelesaikan skripsi ini. Penulisan skripsi ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Sarjana Teknik Jurusan Teknik 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. Muhammad Salman, ST. MIT, selaku dosen pembimbing yang telah menyediakan waktu, tenaga, dan pikiran untuk mengarahkan saya dalam penyusunan skripsi ini.
2. Kedua orang tua dan keluarga saya yang telah memberikan bantuan dukungan material dan moral.
3. Teman dan sahabat yang telah banyak membantu saya dalam menyelesaikan skripsi ini.

Akhir kata, saya berharap Tuhan Yang Maha Esa berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga skripsi ini membawa manfaat bagi pengembangan ilmu pengetahuan.

Depok, Desember 2009

Penulis

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI

TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Universitas Indonesia, saya yang bertanda tangan di bawah ini:

Nama : Muhammad Salmon Hardani

NPM : 0706199621

Program Studi : Elektro

Departemen : Elektro

Fakultas : Teknik

Jenis karya : Skripsi

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

ANALISA UNJUK KERJA DAN QUALITY OF SERVICE DARI APLIKASI SECURE VIDEO STREAMING PADA JARINGAN BERBASIS VPN (VIRTUAL PRIVATE NETWORK)

beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Indonesia berhak menyimpan, mengalihmedia / formatkan, 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 : 28 Desember 2009
Yang menyatakan

(Muhammad Salmon Hardani)

ABSTRAK

Nama : Muhammad Salmon Hardani
Program Studi : Teknik Elektro
Judul : Analisa Unjuk Kerja dan Quality of Service dari Aplikasi Secure Video Streaming Pada Jaringan Berbasis VPN (Virtual Private Network)

Aplikasi *video streaming* yang dijalankan pada jaringan dapat mempengaruhi *bandwidth* dari jaringan tersebut. Aplikasi ini dapat diterapkan pada perusahaan maupun dunia pendidikan yang memiliki kendala dalam hal jarak dan waktu sehingga aplikasi *video streaming* ini dapat menghubungkan dari satu client ke server.

Untuk pengiriman informasi yang bersifat rahasia diperlukan jaringan yang berada pada kondisi *top secret*, salah satu caranya dengan membangun Virtual Private Network (VPN). Pada teknologi VPN, aliran data di enkripsi dengan menggunakan protokol *tunneling* untuk membungkus protokol-protokol jaringan serta dapat mengamankan jalur yang digunakan.

Skripsi ini membahas tentang analisa unjuk kerja aplikasi *video streaming* saat dijalankan pada jaringan VPN. Pengukuran parameter *Quality of Service* (QoS) meliputi, *delay*, *throughput* dan *packet loss*. Nilai *video loss* yang diperoleh dari pengujian jaringan melalui VPN ini adalah berkisar antara 0,64% sampai 7,02% sedangkan nilai *voice loss* nya adalah berkisar antara 0,21% sampai 2,18%.

Kata kunci : VPN, tunneling, video streaming, delay, throughput, packet loss Quality of Service

ABSTRACT

Name : Muhammad Salmon Hardani
Study Program : Electrical Engineering
Title : Performance Analysis and Quality of Service (QoS) of Secure Video Streaming Application on VPN based Network

Video streaming application that run in network can influence bandwidth from network. this application applicable in company also education that has obstacle in the case of distance and time so that application of video streaming can connect from client to server.

For information delivery in secret need network that present in condition top secret, one of the way with build virtual private network (VPN). In VPN technology, data current will be encrypth by using protocol tunneling to wrap up network protocols with can protect stripe that used.

This research discusses about analysis procedure of application video streaming moment run in network vpn. measurement quality of service (QoS) cover, delay, throughput and packet loss. Video loss values obtained from measurements of the network through a VPN is range from 0,62% to 7,02 while the value of his voice is a loss range from 0,21% to 2,18%.

Key words : VPN, tunneling, video streaming, delay, throughput, packet loss Quality of Service

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR SINGKATAN

BRI	Basic Rate Interface
DSL	Digital Subscriber Line
HTTP	Hiper Text Transfer Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISDN	Integrated Service Digital Network
ISP	Internet Service Provider
LAN	Local Area network
PRI	Primary Rate Interface
PSTN	Public Switched Telephone Network
QoS	Quality of Service
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
UDP	Unit Datagram Protocol
WAN	Wide Area Network
VC	Virtual Circuit
VoIP	Voice over Internet Protocol
VSAT	Very Small Aperture Terminal
VPN	Virtual Private Network

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan bisnis yang sangat cepat dan melebar sekarang ini, membuat suatu perusahaan harus dapat melakukan pengolahan proses bisnisnya secara cepat, akan tetapi semua pemrosesan informasi tersebut sangat dipengaruhi oleh dukungan infrastruktur komunikasi yang dimiliki oleh suatu perusahaan. Bagi suatu perusahaan bisnis yang global, kebutuhan akan informasi yang terkini dan akurat sangat dibutuhkan untuk mendapatkan informasi yang aktual, cepat dan tepat yang akan menjadi kunci yang vital dalam persaingan pasar saat ini.

Saat ini dengan internet, manusia telah sangat mengurangi batasan jarak dan waktu.Dengan menggunakan teknologi jaringan komunikasi data WAN (*Wide Area Network*) maka dapat menghubungkan kantor pusat dengan seluruh kantor cabang. Seorang pimpinan perusahaan pusat dapat melakukan *video streaming* dengan pimpinan kantor cabang (*branch office*) dengan memanfaatkan jaringan komunikasi pubik yang sudah ada (dalam hal ini internet) hanya sekedar untuk bertatap muka.

Untuk alasan keamanan, implementasi jaringan WAN tersebut dapat dilakukan dengan menggunakan *leased line*. Namun biaya yang dibutuhkan untuk membangun infrastuktur jaringan yang luas dengan menggunakan *leased line* akan membutuhkan biaya yang cukup besar. Di sisi lain perusahaan ingin mengoptimalkan biaya untuk membangun jaringan mereka yang luas.

Oleh karena itu diperlukan suatu komunikasi yang aman dan murah untuk mengatasi masalah diatas, solusi VPN (*Virtual Private Network*) dapat menjawab permasalahan ini dimana kita bisa terkoneksi secara lokal ke jaringan intranet perusahaan dengan melalui jaringan internet. Dengan internet, maka biaya pengembangan yang dikeluarkan akan jauh relatif lebih murah dari pada harus membangun sebuah jaringan baru tertutup sendiri namun pengguna dapat menikmati fasilitas-fasilitas yang ada pada jaringan private seperti tingkat security yang tinggi, *Quality of Service* (QoS) serta kemudahan manajemen dan tingkat kepercayaan yang tinggi.

VPN sendiri merupakan sebuah teknologi komunikasi yang memungkinkan adanya koneksi dari dan ke jaringan publik serta menggunakannya menggunakan jaringan lokal dan juga bahkan bergabung dengan jaringan lokal itu sendiri. Dengan menggunakan jaringan publik ini, maka *user* dapat mengakses fitur-fitur yang ada di dalam jaringan lokalnya, mendapatkan hak dan pengaturan yang sama seolah-olah secara fisik berada di tempat dimana jaringan lokal itu berada. Hal yang perlu diingat adalah sebuah *private network* haruslah berada dalam kondisi diutamakan dan terjaga kerahasiaannya. Keamanan data dan ketertutupan transfer data dari akses ilegal serta skalabilitas jaringan menjadi standar utama dalam VPN ini pada jaringan lokal tersebut.

1.2 Perumusan Masalah

Permasalahan pada skripsi ini adalah bagaimana merancang sebuah jaringan dengan menggunakan aplikasi *OpenVPN* yang diaplikasikan pada WAN. Pada sistem tersebut akan dijalankan *video streaming* dengan menggunakan aplikasi *Netmeeting* dari salah satu client ke client yang lainnya untuk diketahui performansi dan pengaruh trafik terhadap sistem pada VPN meliputi *bandwidth*, *delay*, *throughput*, serta *packet loss.*

1.3 Tujuan Penulisan

Tujuan penulisan skripsi ini adalah untuk menganalisa unjuk kerja dan *quality of service* dari aplikasi *video streaming* pada jaringan berbasis VPN. Aplikasi yang akan dijalankan pada jaringan VPN ini adalah aplikasi video dari client ke server.

1.4 Batasan Masalah

Dalam skripsi ini ada beberapa pembatasan masalah, diantaranya yaitu :

1. Aplikasi VPN yang digunakan adalah perangkat lunak *OpenVPN.*
2. Sistem VPN yang digunakan adalah SSL (Secure Socket Layer)
3. Menggunakan IPv4 sebagai pengalamatan.
4. Router yang digunakan adalah router cisco seri 1800.
5. Pengukuran parameter yang dilakukan yaitu pada sisi client dan sisi server.

6. Aplikasi *video streaming* yang dipakai adalah perangkat lunak yang ada di windows yaitu *Netmeeting*.
7. Menganalisa kualitas dari sistem VPN yang dibangun, bukan tingkat keamanannya.

1.5 Sistematika Penulisan

Sistematika penulisan skripsi ini adalah sebagai berikut:

Bab 1 : Pendahuluan

Membahas tentang latar belakang penulisan, perumusan masalah, tujuan penulisan, batasan masalah serta sistematika penulisan.

Bab 2 : Jenis Layanan WAN dan konsep VPN

Penjelasan tentang dasar teori yang berkaitan dengan konsep jaringan keamanan, jenis-jenis teknologi WAN, konsep VPN dan metode tunneling serta protokol yang digunakan pada jaringan.

Bab 3 : Perancangan dan Implementasi

Bab ini menjelaskan topologi jaringan yang akan digunakan. Pembahasan meliputi instalasi dan konfigurasi jaringan baik di router maupun di client serta instalasi perangkat lunak yang dibutuhkan untuk mengukur parameter *throughput*, *delay* dan *packet loss*.

Bab 4 : Analisa Data dan Pembahasan

Pada bab ini akan dibahas analisa data untuk mengetahui performansi jaringan VPN saat aplikasi *video streaming* antara client dan server dijalankan yang meliputi parameter *throughput*, *delay* dan *packet loss*.

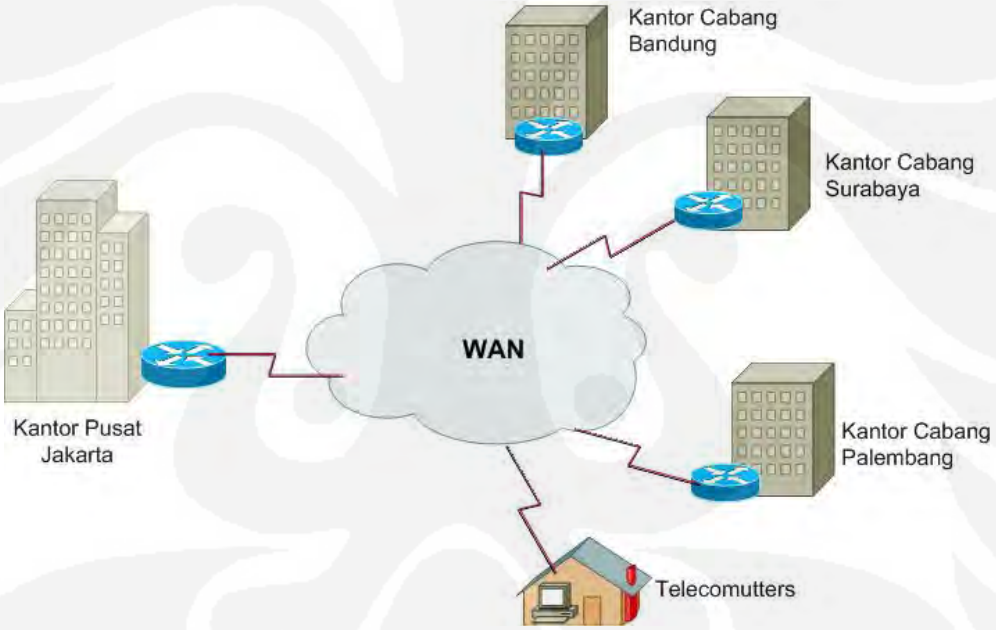
Bab 5 : Kesimpulan

Bab ini berisi kesimpulan dari hasil penulisan dan percobaan skripsi ini.

BAB II
JENIS LAYANAN WAN DAN KONSEP VPN

2.1 Jaringan Komunikasi Data WAN

Ada banyak solusi yang dapat digunakan untuk komunikasi data pada jaringan skala luas, saat ini terdapat beberapa solusi komunikasi data yang ditawarkan oleh provider telekomunikasi. WAN (*Wide Area Network*) adalah jaringan komunikasi yang meliputi area geograpis yang luas dan biasanya menggunakan fasilitas dari transmisi provider, seperti perusahaan telpon kabel atau perusahaan lainnya. Dalam jaringan WAN sangat sensitif dengan masalah lebar pita (*bandwidth*), para penyedia jasa biasanya menentukan biaya sewa dari layanan dan bandwidth yang digunakan.



Gambar 2.1 Contoh topologi Jaringan Skala Luas (WAN) [1]

Ada beberapa layanan WAN yang sering menjadi ukuran layanan perusahaan telekomunikasi terhadap pelanggannya, diantaranya yaitu :

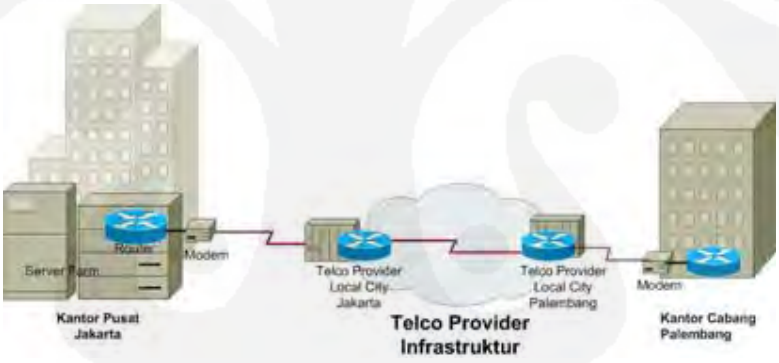
2.1.1 Leased Line

Solusi untuk menghubungkan jaringan dengan menyewa pada operator telekomunikasi untuk bandwidth tertentu, biasanya biaya dihitung dari banyaknya node, besarnya bandwidth yang digunakan dan jarak antara node tersebut, semakin besar bandwidth dan semakin jauh jarak antara satu node dengan yang

lain maka akan semakin mahal biayanya. Perusahaan telekomunikasi yang disewa biasanya perusahaan yang telah mempunyai infrastruktur ke seluruh Indonesia atau keluar negeri (tergantung kebutuhan), infrastruktur kebanyakan menggunakan Teresterial dan Metro-e yang rata-rata *backbone*-nya menggunakan Fiber Optic (FO).

Tabel 2.1 Line Type dan Bandwidth [2]

Line Type	Bit Rate Capacity	Line Type	Bit Rate Capacity
56	56 kb/s	OC-9	466.56 Mb/s
64	64 kb/s	OC-12	622.08 Mb/s
T1	1.544 Mb/s	OC-18	933.12 Mb/s
E1	2.048 Mb/s	OC-24	1244.16 Mb/s
J1	2.048 Mb/s	OC-36	1866.24 Mb/s
E3	34.064 Mb/s	OC-48	2488.32 Mb/s
T3	44.736 Mb/s	OC-96	4976.64 Mb/s
OC-1	51.84 Mb/s	OC-192	9953.28 Mb/s
OC-3	155.54 Mb/s	OC-768	39813.12 Mb/s

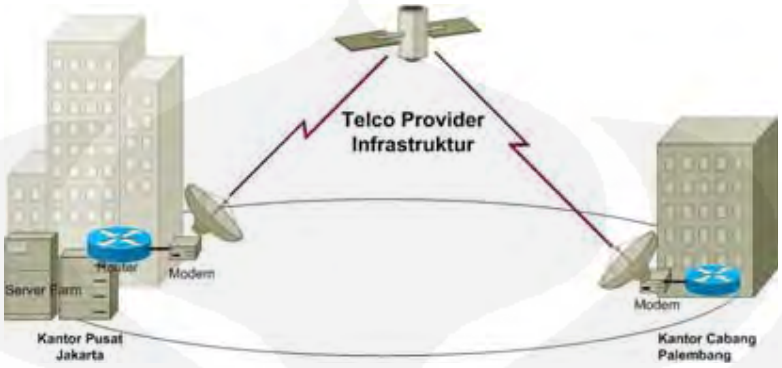


Gambar 2.2 Solusi Leased Channel pada Jaringan Skala Luas (WAN) [3]

2.1.2 VSAT (*Very Small Aperture Terminal*)

VSAT merupakan komunikasi yang menggunakan media *satellite* diluar muka bumi sebagai transmitter dan receivernya dari tempat yang berada di permukaan bumi ke tempat lain selama masih dalam *coverage area* (hotspot area) dari satelit tersebut. Solusi ini sering digunakan perusahaan minyak lepas pantai, kehutanan jauh didalam hutan, riset di pegunungan atau gurun, yang jauh dari coverage area layanan. Namun VSAT biasanya digunakan sebagai solusi terakhir jika layanan lain tidak tersedia dikarenakan latency yang besar dan sangat rentan

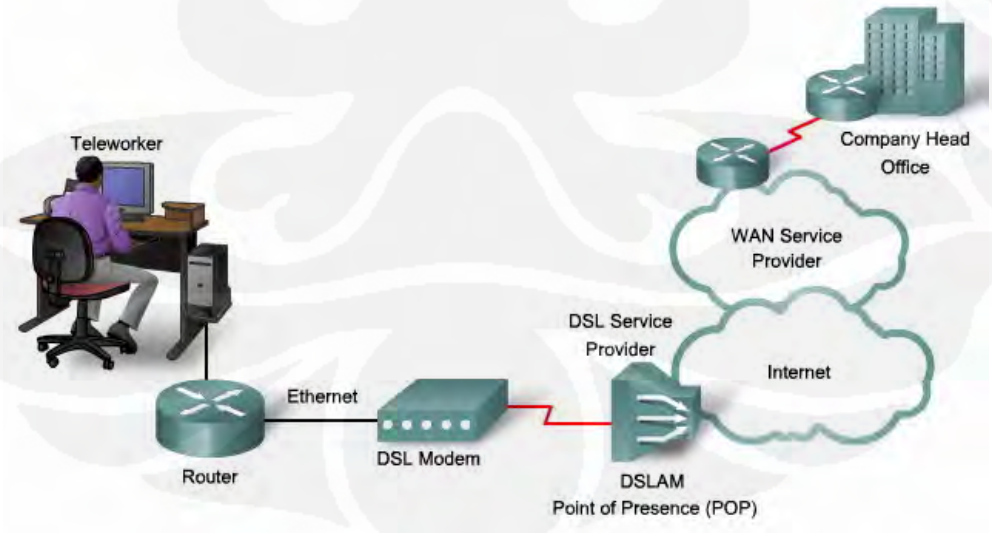
terhadap gejala alam, VSAT sangat tidak sesuai untuk solusi komunikasi data dan suara yang memerlukan kualitas yang prima dan reliable.



Gambar 2.3 Solusi VSAT pada Jaringan Skala Luas (WAN)

2.1.3 DSL (Digital Subscriber Line)

DSL sering menjadi solusi telekomunikasi untuk menghubungkan ke *end user*. Ada banyak varian DSL yang sering disebut XDSL (ADSL, SDSL, VDSL, dan lain-lain). *Asymmetric DSL* yang paling banyak saat ini digunakan karena versi ekonomis dari DSL, teknologi ini memungkinkan transfer data untuk download dengan kecepatan tinggi namun berbeda dengan uploadnya yang kecepatan transfernya lebih kecil dari download. ADSL adalah teknologi yang menggunakan jaringan line telpon *twister-pair* yang ada untuk mengalirkan data dengan kecepatan tinggi seperti multimedia dan video.



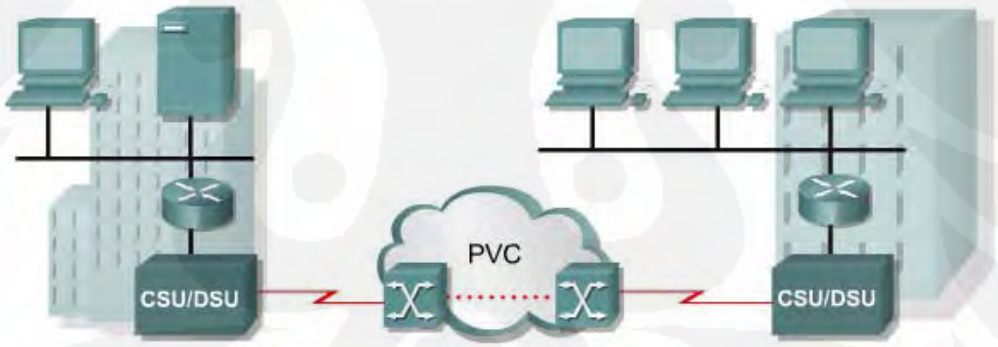
Gambar 2.4 Layanan DSL [2]

Keuntungan lainnya adalah ADSL dapat menggunakan fixed cable yang existing seperti PSTN (*Public Switched Telephone Network*) tanpa menggangu komunikasi suara. Namun kelemahannya adalah jarak yang pendek, rata-rata berjalan dengan baik dibawah jarak 5 km.

2.1.4 Frame Relay

Suatu skema teknologi WAN yang dibuat untuk memperbaiki dari teknologi X.25. Frame Relay menjadi pilihan utama dahulu karena jaringan ini dapat diimplementasikan dengan interkoneksi perangkat pasaran. Frame Relay dirancang berdasarkan konsep *Virtual Circuit* (VC). VC merupakan sebuah jalur sambungan dua arah didalam jaringan yang didefinisikan oleh *software*.

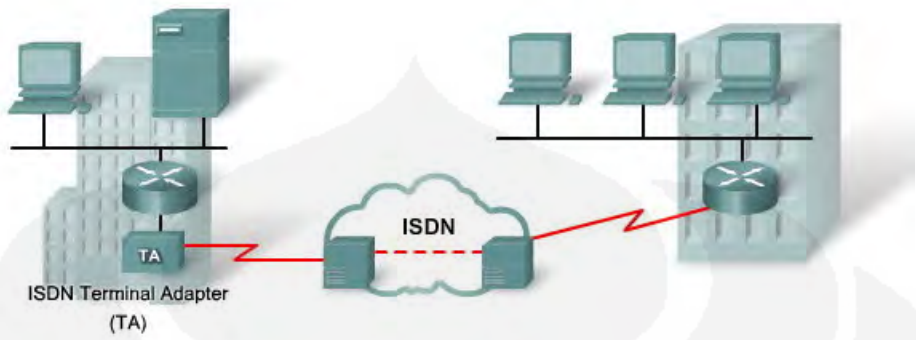
Frame relay dapat dapat menangani error dan pengalamatan di jaringan, namun sangat rentan terhadap ganggunan pengiriman paket data (*drop*) dan keterlambatan (*delay*) karena Frame Relay tidak dapat memilah paket yang lewat di jaringan, hal ini sangat tidak diinginkan dengan kondisi pengiriman data saat ini yang menginginkan jaringan yang reliable dan stabil.



Gambar 2.5 Solusi Frame Relay untuk Jaringan Skala Luas [4]

2.1.5 ISDN (Integrated Service Digital Network)

ISDN dirancang untuk membawa data, suara dan video. Teknologi yang memungkinkan membawa data digital pada kabel analog dengan membawa data lebih besar dan proses komunikasi lebih cepat dari *dial-up* biasa. ISDN menjadi trend pada era tahun 90-an dikarenakan teknologi yang dapat membawa paket data dengan kecepatan yang tinggi namun dahulu cocok dengan infrastruktur *last miles* di Indonesia. ISDN menyediakan dua tingkatan pelayanan, *Basic Rate Interface* (BRI) dan *Primary Rate Interface* (PRI).



Gambar2. 6 Solusi ISDN untuk Jaringan Skala Luas [4]

2.2 Model Arsitektur TCP/IP

Tujuan dari TCP/IP adalah untuk membangun suatu komunikasi antar jaringan (*network*), dimana biasa disebut *internetwork* atau *internet*, yang menyediakan pelayanan komunikasi antar jaringan dan memiliki bentuk fisik yang beragam. Tujuan yang jelas adalah menghubungkan *host* pada jaringan yang berbeda, atau mungkin terpisahkan secara geografis pada area yang luas.

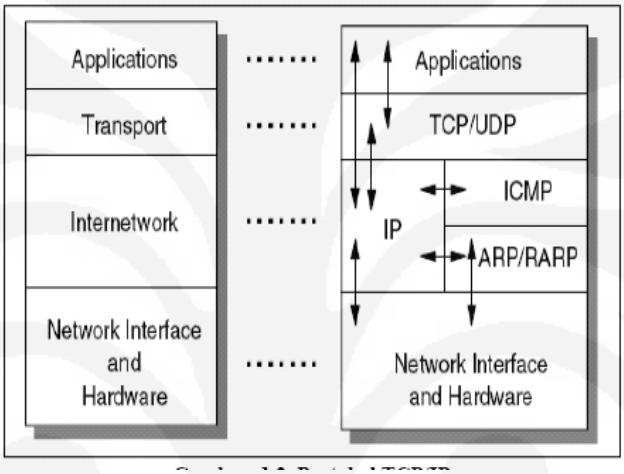
Aspek lain yang penting dari TCP/IP adalah membentuk suatu standarisasi dalam komunikasi. Tiap-tiap bentuk fisik suatu jaringan memiliki teknologi yang berbeda-beda, sehingga diperlukan pemrograman atau fungsi khusus untuk digunakan dalam komunikasi. TCP/IP memberikan fasilitas khusus yang bekerja diatas pemrograman atau fungsi khusus tersebut dari masing-masing fisik jaringan. Sehingga bentuk arsitektur dari fisik jaringan akan tersamarkan dari pengguna dan pembuat aplikasi jaringan. Dengan TCP/IP, pengguna tidak perlu lagi memikirkan bentuk fisik jaringan untuk melakukan sebuah komunikasi.

Untuk dapat berkomunikasi antar jaringan, diperlukan komputer yang terhubung dalam suatu perangkat yang dapat meneruskan suatu paket data dari jaringan yang satu ke jaringan yang lain. Perangkat tersebut disebut *Router*. Selain itu router juga digunakan sebagai pengarah jalur (*routing*). Untuk dapat mengidentifikasikan host diperlukan sebuah alamat, disebut alamat IP (*IP address*). Apabila sebuah host memiliki beberapa perangkat jaringan (*interface*), seperti router, maka setiap interface harus memiliki sebuah IP address yang unik. IP address terdiri dari 2 bagian, yaitu :

IP address = <alamat jaringan><alamat host>

2.2.1 Lapisan (Layer) TCP/IP

Seperti pada perangkat lunak, TCP/IP dibentuk dalam beberapa lapisan (*layer*). Dengan dibentuk dalam layer, akan mempermudah untuk pengembangan dan pengimplementasian. Antar layer dapat berkomunikasi ke atas maupun ke bawah dengan suatu penghubung interface. Tiap-tiap layer memiliki fungsi dan kegunaan yang berbeda dan saling mendukung layer diatasnya. Pada protokol TCP/IP dibagi menjadi 4 layer, tampak pada gambar berikut.



Gambar 2.7 Protokol pada lapisan TCP/IP [5]

Fungsi masing-masing layer atau lapisan protokol serta aliran data pada layer TCP/IP, dapat dicontohkan dengan mengggunakan analogi yang sangat sederhana. Seperti analogi pengiriman surat seperti berikut ini :

1. Langkah pertama yaitu harus menulis dahulu isi surat tersebut lalu mengambil selembar kertas dengan pena untuk menulis berita.
2. Setelah langkah ini terselesaikan, maka setelah itu mengambil amplop surat agar terlindung dari kerusakan.
3. Selanjutnya memilih amplop yang tertutup (TCP) atau amplop yang terbuka (UDP).
4. Barulah menulis alamat yang dituju dengan jelas, serta nama pengirim dan alamat pengirim.
5. Maka selesailah sudah pengiriman surat tersebut dengan menitipkan surat itu pada kantor pos.

Tabel 2.2 Fungsi beserta contoh layer TCP/IP

Nama Layer	Kegunaan	Contoh
Aplikasi	Layer aplikasi digunakan pada program untukberkomunikasi menggunakan TCP/IP, interface yang digunakan untuk saling berkomunikasi adalah nomer port dan socket.	FTP, Telnet
Transport	Layer transport memberikan fungsi pengiriman data secara *end-to-end* ke sisi remote. Aplikasi yang beragam dapat melakukan komunikasi secara serentak (simultaneously).	TCP, UDP,
Internetwork	Layer internetwork biasa disebut juga layer internet atau layer network, dimana memberikan "vitual network" pada internet	IP, ICMP, IGMP, ARP, RARP
Network Interface	Layer network interface disebut juga layer link atau layer datalink, yang merupakan perangkat keras pada jaringan.	IEEE802.2, X.25, ATM, FDDI.

Cara kerja TCP/IP dalam satu komputer adalah sangat mirip dengan cerita diatas. Mengirimkan e-mail terlebih dahulu diolah di TCP. Saat diolah TCP memberi amplop untuk melindungi data-data yang hendak dikirim, yang berupa data tambahan (no.urut), 16 bit *source port number* (nama pengirim dan penerima).

Komputer dengan protokol TCP/IP dapat berhubungan dengan komputer lain dan jaringan lain karena bantuan peralatan jaringan komputer. Peralatan ini biasanya disebut *network interface*. Selain peralatan tersebut masih diperlukan peralatan lain yang disebut dengan *device* penghubung jaringan, yang secara umum dibagi menjadi beberapa kategori :

1. Repeater

   Fungsinya adalah menerima sinyal dari satu segment kabel LAN dan memancarkan kembali dengan kekuatan yang sama dengan sinyal aslinya. Repeater hanya berfungsi membantu menguatkan sinyal yang melemah akibat jarak, sehingga sinyal dapat ditransmisikan ke jarak yang lebih jauh.

2. Bridge

   Bridge adalah "*intelligent repeater*". Bridge menguatkan sinyal yang ditransmisikannya, tetapi tidak seperti repeater, Brigde mampu menentukan tujuan.

3. Hub

   Hub menghubungkan semua komputer yang terhubung ke LAN. Hub adalah repeater dengan jumlah port banyak (*multiport repeater*). Hub tidak mampu menentukan tujuan. Hub hanya mentransmisikan sinyal ke setiap line yang terhubung dengan menggunakan mode *half-duplex*.

4. Switch

   Switch menghubungkan semua komputer yang terhubung ke LAN, sama seperti hub. Perbedaannya adalah switch dapat beroperasi dengan mode *full-duplex* dan mampu mengalihkan jalur dan memfilter informasi ke dan dari tujuan yang spesifik.

5. Router

   Router adalah peningkatan kemampuan dari bridge. Router mampu menunjukkan rute/jalur (*route*) dan memfilter informasi pada jaringan yang berbeda. Beberapa router mampu secara otomatis mendeteksi masalah dan mengalihkan jalur informasi dari area yang bermasalah.

2.2.2 Internet Protocol (IP)

Internet Protocol didesain untuk interkoneksi sistem komunikasi komputer pada jaringan *paket switched.* Pada jaringan TCP/IP, sebuah komputer diidentifikasi dengan alamat IP. Tiap-tiap komputer memiliki alamat IP yang unik, masing-masing berbeda satu sama lainnya. Hal ini dilakukan untuk mencegah kesalahan pada transfer data. Terakhir, protokol data akses berhubungan langsung dengan media fisik. Secara umum protokol ini bertugas untuk menangani pendeteksian kesalahan pada saat transfer data. Untuk komunikasi datanya, *Internet Protokol* mengimplementasikan dua fungsi dasar yaitu *addressing* dan *fragmentasi.*

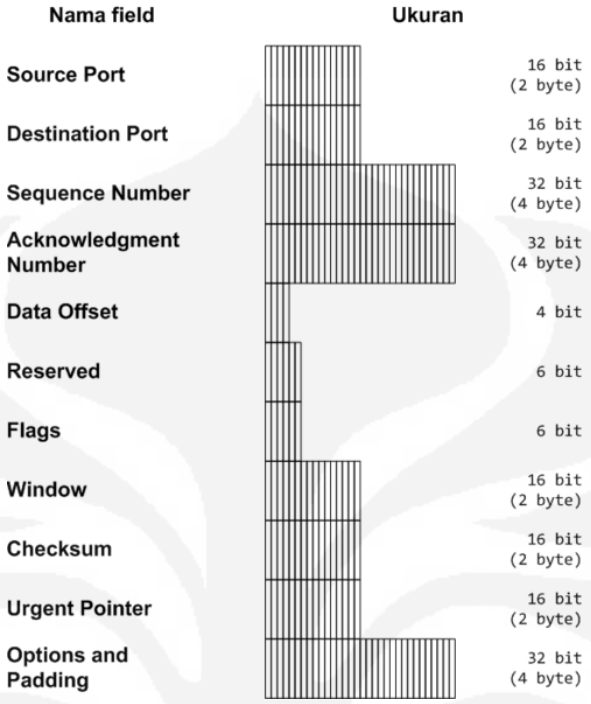
Salah satu hal penting dalam IP dalam pengiriman informasi adalah metode pengalamatan pengirim dan penerima. Saat ini terdapat standar pengalamatan yang sudah digunakan yaitu IPv4 dengan alamat terdiri dari 32 bit. Jumlah alamat yang diciptakan dengan IPv4 diperkirakan tidak dapat mencukupi kebutuhan pengalamatan IP sehingga sekarang sudah tersedia sistem pengalamatan yang baru yaitu IPv6 yang menggunakan sistem pengalamatan 128 bit.

2.2.3 Transmission Control Protocol (TCP)

TCP adalah suatu protokol yang berada di lapisan transport dari TCP/IP model yang berorientasi sambungan (*connection-oriented*) serta dapat diandalkan (*reliable*) dimana sebelum data dapat ditransmisikan antar host, dua proses yang berjalan pada lapisan aplikasi harus melakukan negosiasi untuk membuat sesi komunikasi terlebih dahulu. Koneksi TCP ditutup dengan menggunakan proses terminasi TCP.

TCP juga sudah mendukung *full-duplex* dimana data dapat secara simultan diterima dan dikirim. *Header* TCP berisi nomor urut (*TCP sequence number*) dari data yang ditransmisikan dan sebuah *acknowledgment* dari data yang masuk. Data yang dikirimkan ke sebuah protokol TCP akan diurutkan dengan sebuah nomor urut paket dan akan mengharapkan paket *positive acknowledgment* dari penerima. Jika tidak ada paket *acknowledgment* dari penerima, maka segmen TCP akan ditransmisikan ulang. Pada pihak penerima, segmen-segmen duplikat akan diabaikan dan segmen-segmen yang datang tidak sesuai dengan urutannya akan diletakkan di belakang untuk mengurutkan segmen-segmen TCP. Untuk menjamin integritas setiap segmen TCP, TCP mengimplementasikan penghitungan TCP Checksum.

TCP juga memiliki layanan *flow control* untuk mencegah data terlalu banyak dikirimkan pada satu waktu yang akhirnya membuat "macet" jaringan internetwork IP. TCP mengimplementasikan layanan *flow control* yang dimiliki oleh pihak pengirim yang secara terus menerus memantau dan membatasi jumlah data yang dikirimkan pada satu waktu. Untuk mencegah pihak penerima untuk memperoleh data yang tidak dapat disangganya (*buffer*), TCP juga mengimplementasikan *flow control* dalam pihak penerima, yang mengindikasikan jumlah *buffer* yang masih tersedia dalam pihak penerima.

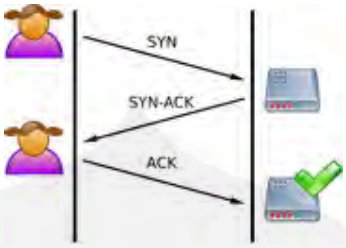


Gambar 2.8 Format Header TCP [5]

Proses pembuatan komunikasi TCP disebut juga dengan "*Three-way Handshake*". Tujuan metode ini adalah agar dapat melakukan sinkronisasi terhadap nomor urut dan nomor *acknowledgement* yang dikirimkan oleh kedua pihak dan saling bertukar ukuran TCP Window. Prosesnya dapat digambarkan sebagai berikut:

- Host pertama (yang ingin membuat komunikasi) akan mengirimkan sebuah segmen TCP dengan *flag* SYN diaktifkan kepada host kedua (yang hendak diajak untuk berkomunikasi).
- Host kedua akan meresponsnya dengan mengirimkan segmen dengan *acknowledgment* dan juga SYN kepada host pertama.
- Host pertama selanjutnya akan mulai saling bertukar data dengan host kedua.

TCP menggunakan proses jabat tangan yang sama untuk mengakhiri komunikasi yang dibuat. Hal ini menjamin dua host yang sedang terhubung tersebut telah menyelesaikan proses transmisi data dan semua data yang ditransmisikan telah diterima dengan baik. Itulah sebabnya, mengapa TCP disebut dengan komunikasi yang *reliable*.

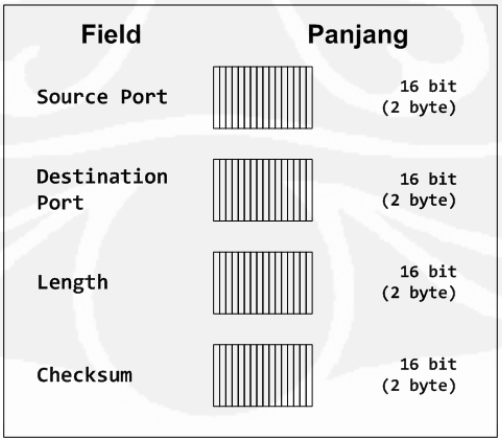


Gambar 2.9 Proses pembuatan komunikasi (TCP Three way handshake) [6]

2.2.4 User Datagram Protocol (UDP)

UDP yang merupakan salah satu *protocol* utama diatas IP yang merupakan *transport protocol* yang lebih sederhana dibandingkan dengan TCP. UDP digunakan untuk situasi yang tidak mementingkan mekanisme reliabilitas. *Header* UDP hanya berisi empat *field* yaitu *source port*, *destination port*, *length* dan UDP *checksum* dimana fungsinya hampir sama dengan TCP, namun fasilitas *checksum* pada UDP bersifat opsional.

UDP bersifat tanpa hubungan (c*onnectionless)* dimana pesan-pesan UDP akan dikirimkan tanpa harus dilakukan proses negosiasi komunikasi antar host yang hendak berukar informasi. UDP juga bersifat *unreliable* (tidak andal) dimana pesan-pesan UDP akan dikirimkan sebagai datagram tanpa adanya nomor urut atau pesan *acknowledgment*. Protokol lapisan aplikasi yang berjalan di atas UDP harus melakukan pemulihan terhadap pesan-pesan yang hilang selama transmisi. Umumnya, protokol lapisan aplikasi yang berjalan di atas UDP mengimplementasikan layanan keandalan mereka masing-masing, atau mengirim pesan secara periodik atau dengan menggunakan waktu yang telah didefinisikan.



Gambar 2.10 Format Header TCP [5]

UDP pada VoIP digunakan untuk mengirimkan *audio stream* yang dikrimkan secara terus menerus. UDP digunakan pada VoIP karena pada pengiriman *audio streaming* yang berlangsung terus menerus lebih mementingkan kecepatan pengiriman data agar tiba di tujuan tanpa memperhatikan adanya paket yang hilang walaupun mencapai 50% dari jumlah paket yang dikirimkan.

Karena UDP mampu mengirimkan data *streaming* dengan cepat, maka dalam teknologi VoIP UDP merupakan salah satu protokol penting yang digunakan sebagai *header* pada pengiriman data selain RTP dan IP. Untuk mengurangi jumlah paket yang hilang saat pengiriman data maka pengiriman data banyak dilakukan pada *private network*.

2.3. VPN (Virtual Private Network)

Virtual Private Network (VPN) adalah komunikasi jaringan terenkripsi yang menggunakan *tunnel* yang aman di antara ujung ke ujung komunikasi melalui internet atau jaringan lain, seperti WAN. Pada VPN, komunikasi *dial-up* pada *remote user* dan *leased line* atau komunikasi *frame relay* pada *remote site* digantikan dengan komunikasi lokal ke *Internet Service Provider* (ISP) atau *point of presence* dari service provider yang lain.

VPN memungkinkan masing-masing remote user dari jaringan dapat berkomunikasi dalam jalur yang aman dan dapat diandalkan dengan menggunakan internet sebagai perantara untuk terhubung ke LAN pribadi. VPN dapat dikembangkan untuk mengakomodasi lebih banyak pengguna dan tempat-tempat lain secara lebih mudah daripada *leased line*.

2.3.1 Cara kerja VPN

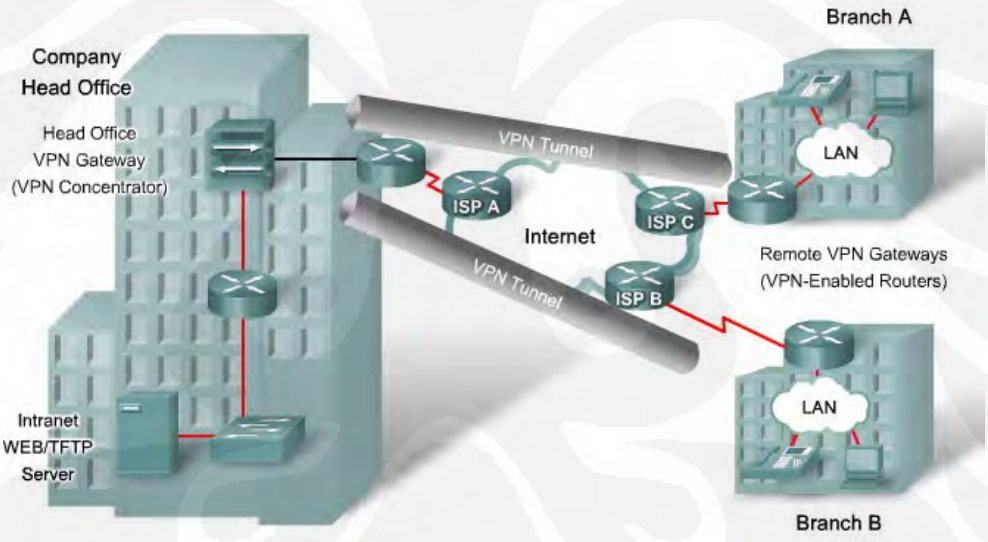
Secara sederhana dapat dikatakan VPN hanyalah membuat tunneling yang aman antara 2 buah *node* atau lebih melewati jaringan terbuka (internet/intranet). VPN dapat menghubungkan dua network yang kecil (maupun yang lebih besar) untuk membangun sebuah jaringan tunggal yang sebelumnya terpisah baik secara fisik maupun logika, traffic VPN antara dua network/end point dilindungi/enkripsi oleh kunci spesial, dan hanya komputer atau seseorang yang mempunyai kunci ini yang dapat membuka dan melihat data yang dikirimkan, semua data yang dikirimkan dienkripsi terlebih dahulu dan didekripsi setelah transmisi.

Dengan menggunakan VPN maka komputer client yang berada di internet seolah-olah berada pada jaringan lokal, proses diawali dengan client melakukan remote menuju VPN Server untuk mendapatkan IP VPN selanjutnya akan dilakukan negosiasi sertifikat. Dan apabila sertifikat sesuai maka akan dilakukan proses enkripsi pada saat paket dikirimkan dan dilakukan dekripsi saat paket sampai pada tujuan.

2.3.2 Tipe-Tipe VPN

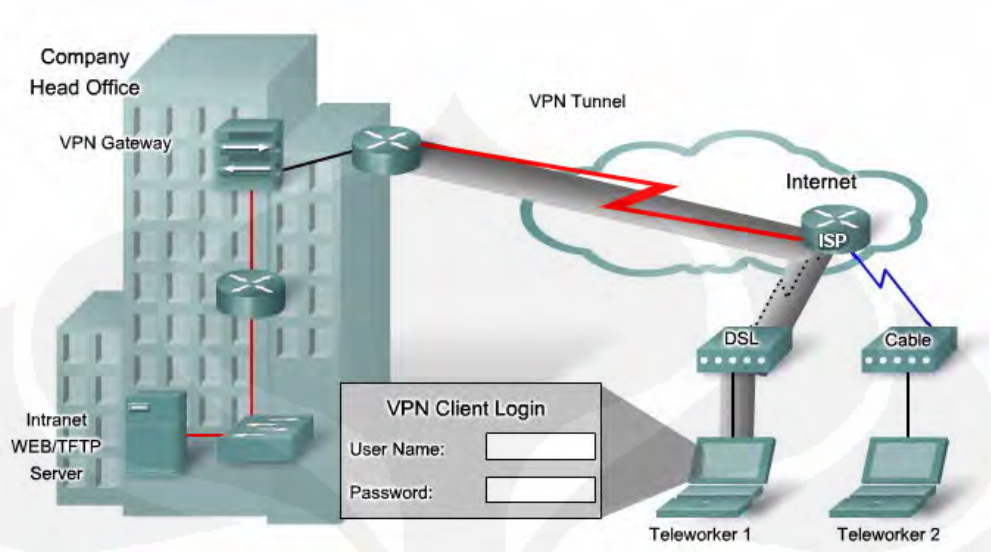
Ada 2 macam tipe implementasi dari VPN, yaitu :

1. *Site-to-site VPN*, dapat menghubungkan seluruh jaringan ke jaringan lainnya. Sebagai contoh, site-to-site VPN dapat menghubungkan kantor cabang (*branch office*) ke jaringan kantor pusat (*head office*) seperti ditunjukkan pada gambar 7. Setiap *site* dilengkapi dengan sebuah VPN *gateway* seperti router, *firewall*, VPN concentrator atau peralatan keamanan lainnya.



Gambar 2.11 Site-to-site VPN [2]

2. *Remote-access VPN*, memungkinkan setiap host secara individu berdiri sendiri. Setiap teleworker dapat mengakses jaringan kantor pusat perusahaan nya kapan pun dan dimana pun ia berada dengan melewati jalur publik seperti internet. Setiap host akan dilengkapi dengan *software* yang disebut dengan *VPN client*.



Gambar 2.12. Remote-access VPN

2.3.3 Authentikasi Pada VPN

Autentikasi adalah suatu proses untuk memastikan bahwa kedua ujung komunikasi nya adalah merupakan benar usernya sesuai dengan yang diberikan kewenangan untuk mengakses suatu server. Sedangkan enkripsi berfungsi untuk melakukan pengacakan terhadap suatu data agar tidak dapat dibaca oleh orang lain. Meskipun baik autentikasi dan enkripsi memiliki cara kerja sendiri-sendiri namun keduanya sering kali dipadukan agar didapatkan suatu sistem keamanan yang lebih baik.

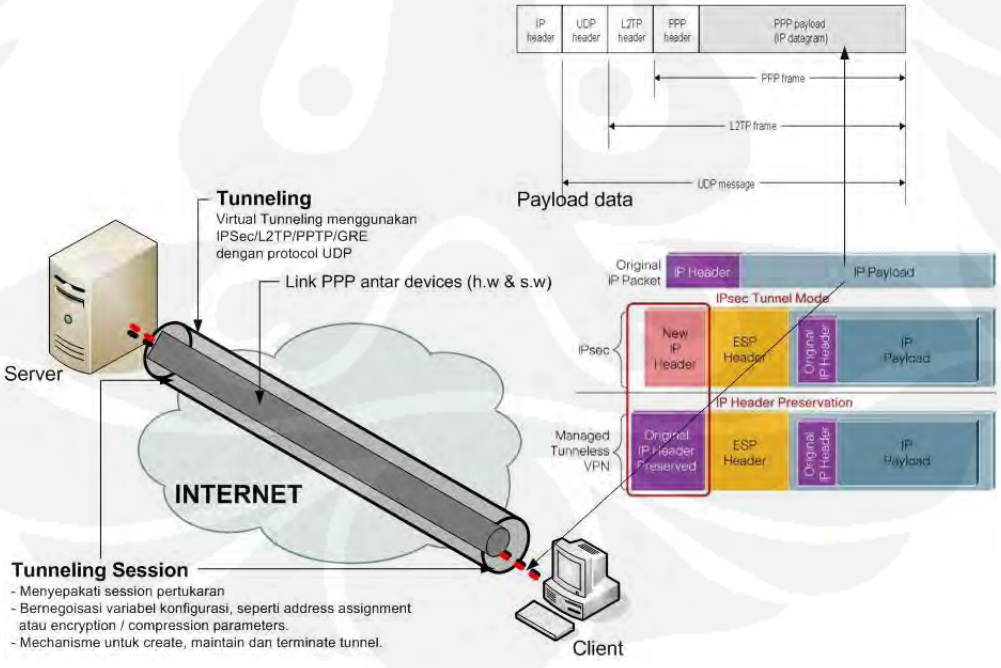
Pada umunya jenis autentikasi yang paling mudah dan banyak digunakan orang adalah menggunakan *Login Password* dimana untuk dapat melakukan akses maka seorang user harus memasukkan *username* dan *password* yang benar baru kemudian dapat melakukan akses ke server. Namun demikian hal tersebut belumlah cukup untuk memberikan keamanan yang baik mengingat hal tersebut hanya dilakukan di awal *session* saja. Permasalahan dapat saja terjadi ketika ada *attacker* yang berada di tengah antara server dan client tersebut yang kemudian mengambil alih *session* sehingga client yang sebenarnya telah terputus sessionnya sementara *attacker* berhasil menguasai *session* tersebut dan dianggap user yang benar oleh server. Saat ini kebutuhan akan authentikasi tidaklah cukup hanya menggunakan form login saja, tipe authentikasi yang saat ini mulai banyak

digunakan adalah penggunaan sertifikat dan *digital signature* atau tanda tangan digital.

2.3.4 Metode Tunneling Pada VPN

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

Protokol *tunneling* tidak mengirimkan *frame* sebagaimana yang dihasilkan oleh node asalnya begitu saja melainkan membungkusnya *(mengenkapsulasi*) dalam *header* tambahan. *Header* tambahan tersebut berisi informasi routing sehingga data (frame) yang dikirim dapat melewati jaringan internet. Jalur yang dilewati data dalam internet disebut *tunnel*. Saat data tiba pada jaringan tujuan, proses yang terjadi selanjutnya adalah *dekapsulasi*, kemudian data original akan dikirim ke penerima terakhir. *Tunneling* mencakup secara keseluruhan mulai dari enkapsulasi, transmisi dan dekapsulasi.



Gambar 2.13 Skema Tunneling dan Enkapsulasi VPN [1]

2.3.5 Mekanisme Enkripsi VPN

Secara sederhana enkripsi adalah sebuah proses melakukan perubahan sebuah kode dari yang dapat dimengerti menjadi sebuah kode yang tidak dapat dimengerti. Enkripsi juga dapat diartikan sebagai *cipher.* Terdapat beberapa enkripsi yang sering dilakukan yaitu IPSec dan SSL.

SSL (*Secure Socket Layer*) adalah salah satu protokol enkripsi dalam komunikasi data yang dibuat oleh *Nestcape Communication Corporation* yang bekerja pada *application layer* dan umum digunakan pada komunikasi aman berbasis web pada internet [7]. SSL dapat , menciptakan saluran enkripsi yang aman untuk data, dan dapat mengenkripsi banyak tipe data. biasanya digunakan untuk keamanan pada aplikasi *HTTP*, *IMAP, POP3* dan lain-lain . ketika SSL bekerja dibelakang *firewall*, port tidak akan terbuka sampai proses negosiasi antara *firewall* dan SSL berhasil. Port yang digunakan untuk mode server adalah *HTTPS 443/TCP* sedangkan untuk mode client bebas.

IPSec adalah sebuah *framework* standar terbuka yang dikembangkan oleh *Internet Engineering Task Force* (IETF). IPSec menyediakan keamanan untuk transmisi informasi yang bersifat sensitif melalui jaringan yang tanpa proteksi seperti internet. IPSec dijalankan pada layer network pada jaringan, berfungsi untuk melindungi dan melakukan authentikasi paket IP antara device IPSec ("*peer*") [8].

IPsec didesain untuk menyediakan keamanan berbasis kriptografi yang memiliki karakteristik *interoperable* dan berkualitas. Layanan keamanan yang disediakan mencakup *access control*, *connectionless integrity*, *data origin authentication*, proteksi dari *replay attack* (*sequence integrity*), *data confidentiality* dan *traffic flow confidentiality*. Layanan tersebut disediakan pada IP *layer* sehingga mendukung proteksi untuk *IP layer* dan *layer* lain di atasnya.

2.4 Program OpenVPN

OpenVPN mempunyai fitur penuh yang mendukung VPN SSL yang mengakomodasi konfigurasi yang fleksibel dan luas termasuk *remote accses, site to site VPN, Wifi security* dan skala *remote acces* yang bersifat *enterprise*.

OpenVPN mengimplentasikan model OSI layer dua atau tiga untuk keamanan jaringan yang mempunyai standar protokol SSL, mendukung

autentikasi *client* yang menggunakan sertifikat dan autentikasi yang mengijinkan user untuk mengakses melalui *firewall* yang dipasang pada VPN.

OpenVPN dapat berjalan diatas system operasi *Linux, Windows 2000/XP/Vista, OpenBSD, FreeBSD, NetBSD, Mac OS X*, dan *Solaris*. Layanan yang disediakan diantaranya :

- Menyediakan *tunneling* dengan banyak *IP subnetwork* atau *virtual Ethernet adapter* dengan menggunakan single *UDP* dan *TCP port*.
- Konfigurasinya *scalable*, bervariasi sesuai dengan kebutuhan dan dapat dihubungkan dengan banyak *client* sebagai *VPN client*
- Menggunakan enkripsi, autentikasi dan sertifikat yang ada pada *OpenSSL* yang dapat melindungi jaringan *privat* pada saat terhubung dengan internet.
- Menggunakan banyak *cipher*, ukuran *key* yang beragam, *HMAC digest* (untuk intgritas dalam hal pengecekan data) yang didukung penuh oleh *OpenSSL.*
- Menyediakan *static key* dan *public key* pada enkripsinya.
- Menyediakan kompresi untuk menghemat *bandwitdth.*

2.5 Aplikasi *Video Streaming*

Video merupakan gambar-gambar yang bergerak. Didalam video menampilkan sejumlah gambar atau *frame* dengan kecepatan tertentu yang disebut dengan istilah *frame rate*, dihitung dalam skala *frame per second* (fps). Seperti halnya dengan jenis data yang lain, data video juga dapat disimpan, diedit, ataupun dikirim melalui jaringan.

Video streaming merupakan suatu metode yang memanfaatkan suatu *streaming* untuk mentransmisikan *digital video* melalui suatu jaringan data sehingga *video playback* dapat langsung dilakukan tanpa harus menunggu proses *download* selesai terlebih dahulu ataupun menyimpannya terlebih dahulu disisi PC *client*. Sistem *video streaming* melibatkan proses *encoding* terhadap isi dari data *video*, dan kemudian mentransmisikan *video streaming* melalui suatu jaringan (*wired* atau *wireless*), sehingga *client* tujuan dapat mengakses, melakukan *decoding*, dan menampilkan video tersebut secara *real-time*.

Teknologi *streaming* cenderung bersifat *bandwidth-dependent*, sehingga sangat bergantung pada kondisi jaringan. Agar *data stream* dapat di-*playback*

secara baik, perlu diperhatikan beberapa pertimbangan supaya *data stream* memiliki *bit rate/data transfer rate* yang cukup rendah, karena dengan mengurangi *bit rate* berarti sama saja dengan mengirimkan lebih sedikit data. Mengurangi *bit rate* dapat dilakukan dengan cara antara lain membuat dimensi *frame* video menjadi lebih kecil, membuat jumlah *frame per second* (fps) *video* menjadi lebih rendah serta mengurangi jumlah informasi yang ada di setiap *frame* video melalui proses kompresi. [9]

Suatu jaringan dapat disebut ideal apabila mampu mengirimkan informasi apapun, tidak terbatas jumlah dan ukuran, serta tanpa menimbulkan *delay* ataupun *loss*. Akan tetapi dalam prakteknya akan sangat sulit untuk menciptakan jaringan dengan karakteristik seperti itu, karena *bit error*, *bit loss*, *delay*, *latency*, dan terbatasnya *bandwidth* merupakan hal-hal yang bersifat temporal. Faktor performansi dari sistem *video streaming* dalam hubungannya dengan jaringan dapat dijelaskan sebagai berikut :

a. *Throughput*

Throghput atau biasa disebut *actual bandwidth* adalah jumlah data yang dapat melalui suatu jaringan, atau bagian dari jaringan, untuk setiap waktu tertentu. [9] *Bandwidth* pada jaringan bersifat terbagi, terbatas, dan berubah terhadap waktu. Suatu jaringan tidak mampu menjamin *bandwidth* yang dibutuhkan untuk mentransmisikan *video streaming* akan selalu tersedia.

b. *Delay*

Secara umum *delay* adalah waktu tunda yang disebabkan oleh proses transmisi dari satu titik ke titik lain yang menjadi tujuannya. Nilai *delay* maksimal yang diperbolehkan untuk mencapai *quality of service* adalah sebesar 150 ms [13].

c. *Packet loss*

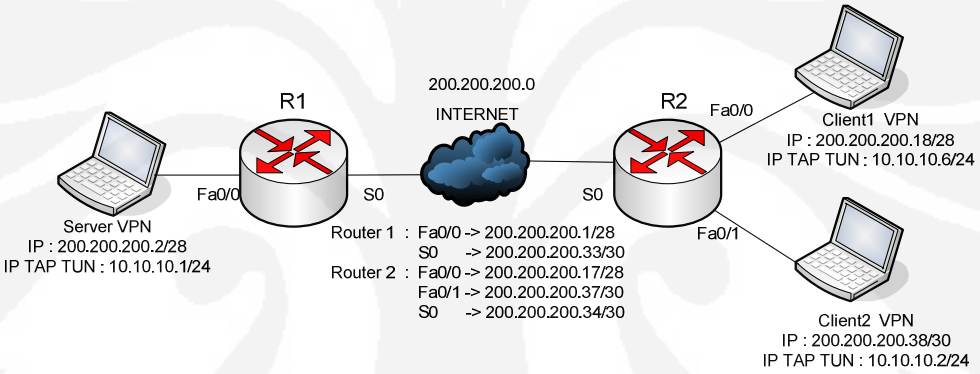
Packet loss adalah satu atau lebih paket yang gagal melewati jaringan untuk mencapai tujuan. Jumlah maksimal *packet loss* yang diperbolehkan adalah sekitar 1% [13].

BAB III
PERANCANGAN DAN IMPLEMENTASI

Pada bab ini akan dibahas perancangan sistem *video streaming* pada jaringan berbasis virtual private network menggunakan perangkat lunak openvpn, dimulai dengan perencanaan topologi, persiapan perangkat lunak dan perangkat keras yang diperlukan, instalasi jaringan, konfigurasi, serta persiapan pengujian.

3.1 Perencanaan topologi jaringan

Model topologi jaringan yang digunakan pada skripsi ini terdiri dari sebuah laptop sebagai server VPN, 2 komputer/laptop client VPN dan 2 buah router dengan bentuk topologi seperti pada gambar 3.1 berikut :



Gambar 3.1 Topologi Jaringan

Pada gambar 3.1 VPN Server terhubung langsung dengan Router 1 pada interface ethernet dengan menggunakan kabel UTP type *crossover*, sedangkan interface ethernet lain nya pada Router R1 terhubung dengan interface Router R2 melalui kabel serial. Selanjutnya Router R2 akan terhubung dengan client1 dan client2 dengan menggunakan kabel UTP type *crossover*, pengalamatan IP address sesuai dengan gambar topologi di atas.

3.2 Kebutuhan pendukung infrastruktur

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

3.2.1 Kebutuhan Hardware

Kebutuhan hardware pada skripsi ini terdiri dari beberapa perangkat keras meliputi NIC (Network Interface Card), Switch, Webcam/PC Camera, headset, serta beberapa laptop sebagai server dan client, PC sebagai client dan router sebagai penerus paket antar jaringan.

Laptop dan PC

Disini digunakan 2 buah laptop dan 1 buah PC dengan spesifikasi sebagai berikut :

1. Laptop Axioo dengan processor Intel Core 2 Duo 1,73 GHz dan memory 1 Gb yang digunakan sebagai server VPN. Server VPN pada saat pengujian memegang peranan ganda yaitu bertindak sebagai server VPN yang bertugas membentuk tunnel, melakukan validitas certificate, dan sebagai gateway antar VPN client.
2. Laptop Compaq Presario dengan processor Intel Core 2 Duo 1,66 GHz dan memory 1Gb yang digunakan sebagai client 1.
3. PC Intel Pentium 4 dengan processor 2,2 GHz dan memori 512 Mb yang digunakan sebagai client 2.

Headset

Pada aplikasi *video streaming*, 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 dapat digunakan dalam komunikasi *video streaming*.

Webcam/PC Camera

Dalam aplikasi *video streaming* Webcam/PC Camera memegang peranan yang paling penting. Webcam digunakan untuk mengambil input berupa gambar untuk diolah dalam komputer dan kemudian dikompresi serta di transmisikan pada jaringan. Pada saat ujicoba digunakan 2 laptop yang sudah terintegrasi dengan webcam dengan resolusi 1,3 Megapixel.

Router

Router adalah sebuah alat jaringan komputer yang mengirimkan paket data melalui sebuah jaringan atau internet menuju tujuannya, melalui sebuah proses yang dikenal sebagai routing. Proses routing terjadi pada layer 3 pada OSI

layer. Router berfungsi sebagai penghubung antar dua atau lebih jaringan untuk meneruskan data dari satu jaringan ke jaringan lainnya. Router berbeda dengan switch. Switch merupakan penghubung beberapa alat untuk membentuk suatu *Local Area Network* (LAN). Dalam perancangan ini router yang digunakan adalah router Cisco seri 1800.

3.2.2 Kebutuhan Software

Software yang digunakan pada skripsi ini meliputi openvpn, dan wireshark.

Openvpn

Openvpn merupakan software yang digunakan untuk membentuk tunnel antara server dan client, dan menciptakan public key serta sertifikat yang diperlukan dalam VPN, type VPN yang digunakan pada openvpn adalah VPN SSL. Openvpn juga merupakan software yang dapat bertindak sebagai server VPN maupun client VPN tergantung pada konfigurasinya, pada skripsi ini versi openvpn yang digunakan adalah *openvpn-2.0.9-gui-1.0.3-install* dengan ukuran file 1,06 MB yang didownload secara gratis pada website www.openvpn.se [10].

Wireshark

Wireshark merupakan software yang digunakan untuk melakukan analisa jaringan komputer, wireshark dapat menganalisa beberapa parameter QoS seperti, *delay*, *throughput*, dan *packet loss* dan lain lain serta dapat mengcapture protokol yang sedang berjalan dalam jaringan tersebut, versi wireshark yang digunakan untuk pengujian adalah *wireshark-setup-1.0.10* dan dapat didownload secara gratis pada website www.wireshark.org [11].

3.3 Instalasi Infrastruktur

Pada bagian ini akan dibahas mengenai proses instalasi hardware dan software sistem *video streaming* pada virtual private network.

3.3.1 Instalasi Server

Untuk dapat berkomunikasi dengan komputer klien maka komputer server perlu untuk di konfigurasi, adapun langkah-langkah konfigurasinya adalah sebagai berikut :

1. Memasang interface jaringan/LAN Card pada slot PCI.
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 topologi yang telah direncanakan, yaitu IP Address 200.200.200.1 dengan netmask 255.255.255.240

3.3.2 Instalasi Wireshark

Sebelum melakukan instalasi wireshark kita perlu mendownload program wireshark dari alamat http://www.wireshark.org, untuk instalasi kita tinggal mengklik double program *wireshark-setup-1.0.10*.exe dan ikuti petunjuk selanjutnya, pada program wireshark juga diperlukan program WinpCap untuk mengcapture protokol yang sudah terintegrasi pada wireshark.

3.3.3 Instalasi Client

Pada dasarnya urutan instalasi pada sisi client sama dengan sisi server, perbedaannya hanya pada setting IP Address, untuk client1 diberikan IP Address 200.200.200.18 dengan subnetmask 255.255.255.240 dan untuk client2 diberikan IP Address 200.200.200.38 dan subnetmask 255.255.255.252 sesuai topologi yang telah direncanakan.

3.3.4 Instalasi Webcam pada masing-masing client

Webcam perlu diinstall pada masing-masing client agar wajah masing-masing user dapat tercapture 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 Instalasi Router

Router digunakan untuk meneruskan paket menuju network yang berbeda dalam hal ini adalah dari network 200.200.200.0/28 menuju 200.200.200.16/28 dan 200.200.200.36/30 ataupun sebaliknya, hal ini dimaksudkan untuk mensimulasikan kondisi di internet dimana komunikasi di internet melewati network yang berbeda. pada skripsi ini router yang digunakan adalah router cisco seri 1800.

3.3.6 Instalasi Openvpn pada server dan client

Program openvpn dapat didownload dengan gratis pada alamat http://www.openvpn.se, setelah proses download selesai, kita tinggal menjalankan program *openvpn-2.0.9-gui-1.0.3-install.exe* dengan mengeklik double dan ikuti petunjuk instalasi.

3.3.7 Konfigurasi Openvpn

Agar Virtual Private Network dapat terbentuk antara server dan client, maka software openvpn perlu dikonfigurasi dengan langkah-langkah sebagai berikut [12] :

1. Menciptakan certificate
   - Klik start → Run → ketik cmd lalu tekan enter sehingga halaman console tampil.
   - Masuk ke directory C:\Program Files\Openvpn\easy rsa dengan mengetikkan cd C:\Program Files\OpenVPN\easy-rsa pada C:\>
   - Ketik init-config lalu tekan enter untuk menciptakan konfigurasi awal pada openvpn
   - Edit file pada C:\Program Files\OpenVPN\easy-rsa\vars.bat dengan konfigurasi sebagai berikut :

```
set HOME=%ProgramFiles%\OpenVPN\easy-rsa
set KEY_CONFIG=openssl.cnf
set KEY_DIR=keys
set KEY_SIZE=1024
set KEY_COUNTRY=ID
set KEY_PROVINCE=Jabar
set KEY_CITY=Depok
set KEY_ORG=FTUI
set KEY_EMAIL=mhd.salmon@ui.ac.id
```

   - Menciptakan Certificate Authority (CA) dengan perintah sebagai berikut:
     - Ketik vars.bat → enter
     - Ketik clean-all → enter
     - Ketik build-ca → enter
   - Menciptakan private key untuk server dengan mengetik perintah build-key-server.bat server →enter pada komputer server

- Menciptakan private key untuk client dengan mengetik perintah build-key.bat client pada
- Menciptakan Diffie Hellman parameters dengan mengetikkan perintah build-dh
- Menciptakan file konfigurasi untuk server dan client pada folder C:\Program Files\OpenVPN\Config menggunakan software editor seperti notepad
- File konfigurasi untuk server diberi nama server.ovpn dengan konfigurasi :

```
dev tap
port 5000
verb 4
mode server
duplicate-cn
ifconfig 10.10.10.1 255.255.255.0
ifconfig-pool 10.10.10.1 10.10.10.11 255.255.255.0
tls-server
ca ca.crt
cert server.crt
key server.key
dh dh1024.pem
cipher AES-128-CBC
tls-cipher DHE-RSA-AES256-SHA
auth SHA1
key-method 2
comp-lzo
status openvpn-status.log
push "route 200.200.200.0 255.255.255.240"
```

- File konfigurasi untuk client diberi nama client.ovpn dengan konfigurasi :

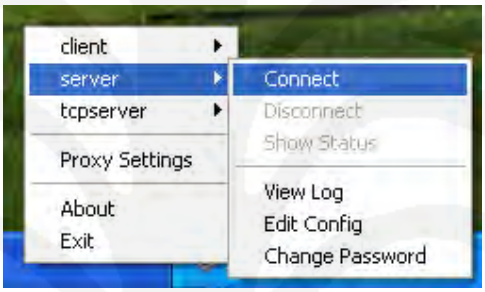
```
dev tap
port 5000
verb 3
remote 200.200.200.1
tls-client
ca ca.crt
cert client.crt
key client.key
cipher AES-128-CBC
tls-cipher DHE-RSA-AES256-SHA
auth SHA1
key-method 2
pull
comp-lzo
```

3.3.8 Menjalankan server Openvpn

Untuk menjalankan server Openvpn tinggal mengeklik icon openvpn yang berada pada system tray, dan memilih konfigurasi untuk server dan selanjutnya klik Connect.

Gambar 3.2 Icon Openvpn

Icon yang ditunjuk oleh tanda panah pada gambar 3.2 merupakan icon daripada openvpn.

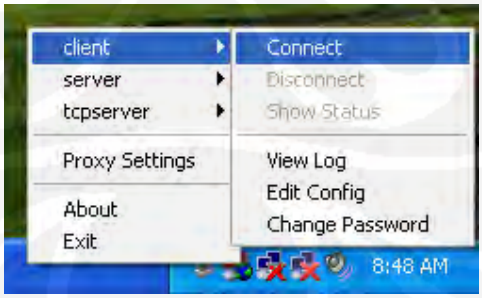


Gambar 3.3 Menjalankan Openvpn sebagai server

Pada gambar 3.3 di atas, untuk menjalankan openvpn sebagai server kita pilih konfigurasi server dan klik Connect, apabila telah terhubung dengan baik, maka server akan mendapatkan IP Address 10.10.10.1 sesuai dengan konfigurasi.

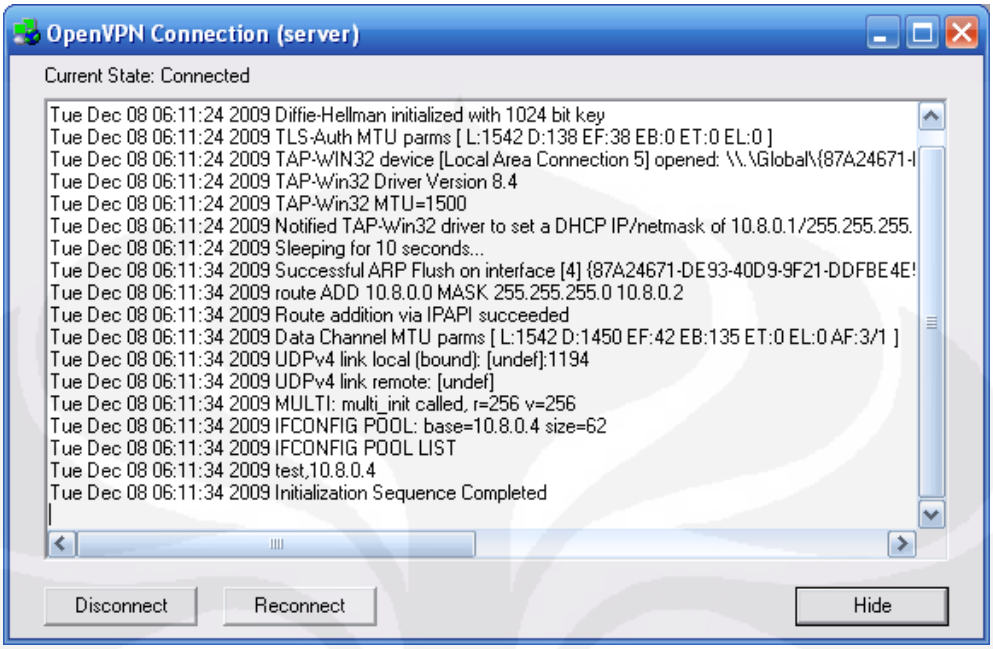
3.3.9 Menjalankan Openvpn pada sisi client

Untuk menjalankan openvpn sebagai caranya sama dengan menjalankan openvpn sebagai server, hanya saja pilih konfigurasi client dan click Connect.



Gambar 3.4 Menjalankan Openvpn sebagai client

Sesuai gambar 3.4 di atas Openvpn dijalankan pada mode client dan openvpn akan menjalankan konfigurasi openvpn client.



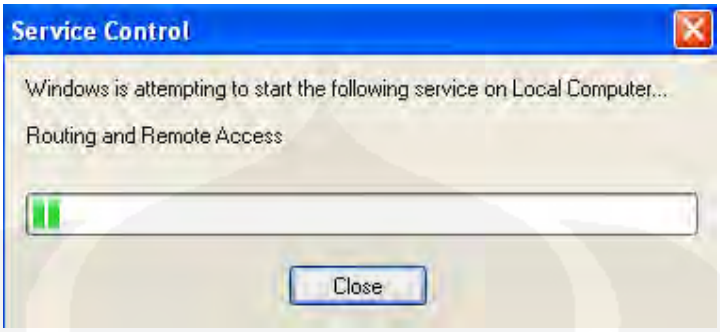
Gambar 3.5 Proses menjalankan Openvpn

Gambar 3.5 menunjukkan proses yang terjadi sebelum client terhubung pada server, client akan melakukan negosiasi dengan server mengenai *key* dan *certificate* apabila sesuai maka client akan mendapatkan IP Address sesuai dengan range IP client pada konfigurasi dari Openvpn server.

3.3.10 Mengaktifkan fungsi routing pada server

Fungsi routing harus diaktifkan pada sisi server agar server dapat meneruskan paket antar client VPN dengan langkah-langkah sebagai berikut :

- Klik start pilih My Computer klik kanan lalu manage
- Akan muncul Tab Computer Management, explore menu Service and Applications lalu pilih Services
- Cari pilihan routing and remote access, pada kolom startup type ganti dengan pilihan automatic lalu klik apply
- Jalankan routing dengan mengklik tombol start



Gambar 3.6 Proses starting routing and remote access

Pada gambar 3.6 menunjukkan proses windows mengaktifkan fungsi routing setelah kita mengeklik tombol start dan selanjutnya komputer server dapat meneruskan paket kepada client.

3.3.11 Melakukan Tes Koneksi

Tes komunikasi dapat dilakukan dengan menggunakan perintah ping dengan mengirimkan pesan ICMP pada komputer yang dituju, jika komunikasi telah terbentuk maka komputer yang dituju akan mengembalikan paket ICMP tersebut, pengujian dapat dilakukan pada sisi server ataupun client, tetapi pada contoh berikut dilakukan pada sisi server :

- Test ping dari server menuju client tanpa jaringan VPN dengan perintah :

  C:\> Ping 200.200.200.18

Apabila komunikasi dari server menuju client berhasil maka akan muncul reply ICMP dari client.

```
Pinging 200.200.200.18 with 1000 bytes of data:

Reply from 200.200.200.18: bytes=1000 time=27ms TTL=128
Reply from 200.200.200.18: bytes=1000 time=27ms TTL=128
Reply from 200.200.200.18: bytes=1000 time=27ms TTL=128

Ping statistics for 192.168.1.2 :
    Packets: Sent = 20, Received = 30, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 26ms, Maximum = 29ms, Average = 26ms
```

- Test ping dari server menuju client menggunakan IP Address VPN dengan menggunakan perintah :

  C:\> ping 10.10.10.6

  Jika komunikasi sukses maka akan muncul reply dari client

Pinging 10.10.10.6 with 1000 bytes of data:

Reply from 10.10.10.6: bytes=1000 time=27ms TTL=128
Reply from 10.10.10.6: bytes=1000 time=27ms TTL=128
Reply from 10.10.10.6: bytes=1000 time=27ms TTL=128

Ping statistics for 10.10.10.6 :
Packets: Sent = 20, Received = 30, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 26ms, Maximum = 29ms, Average = 26ms

3.3.12 Konfigurasi Cisco Router

Router adalah sebuah device yang berfungsi untuk meneruskan paket-paket dari sebuah network ke network yang lainnya (baik LAN ke LAN atau LAN ke WAN) sehingga host-host yang ada pada sebuah network dapat berkomunikasi dengan host-host yang ada pada network yang lain. Router menghubungkan network-network tersebut pada network layer dari model OSI, sehingga secara teknis Router adalah Layer 3 Gateway.

Pada skripsi ini router yang digunakan adalah router cisco seri 2600. Dalam mengkofigurasi router cisco ini dapat dilakukan dengan 2 cara yaitu :

- Melalui port console
- Melalui network

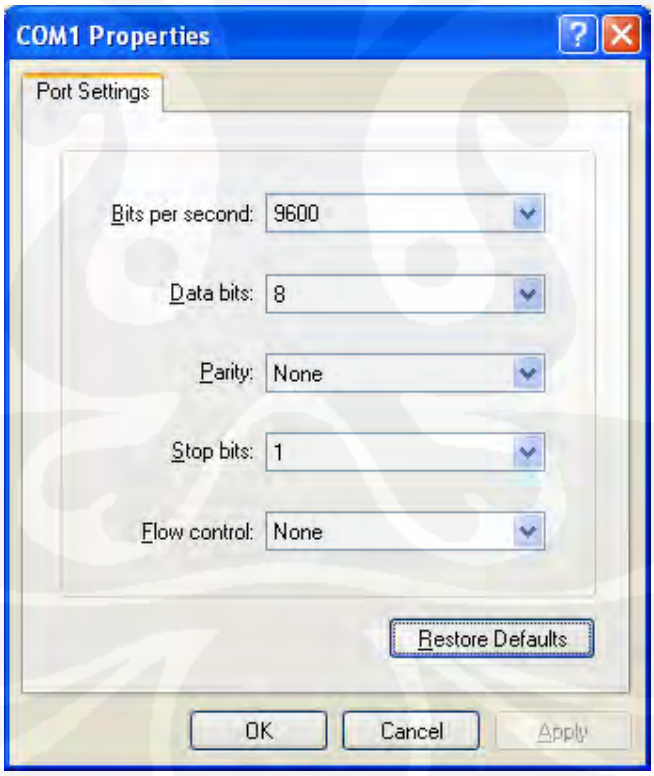
Namun dalam skripsi ini, router hanya akan dikonfigurasi dengan cara yang pertama yaitu melalui port console. Port console adalah sebuah port pada router yang disediakan untuk menghubungkan router tersebut pada "dunia luar". Sebuah kabel *rollover* dibutuhkan untuk menghubungkan serial interface pada PC dan port console pada router tersebut. Setelah Router terhubung dengan PC, Router dapat dikonfigurasi dengan menjalankan applikasi HyperTerminal dari PC.

Buka aplikasi HyperTerminal dengan cara :

Klik start → klik All Program → klik Accessories → klik Communication → klik HyperTerminal

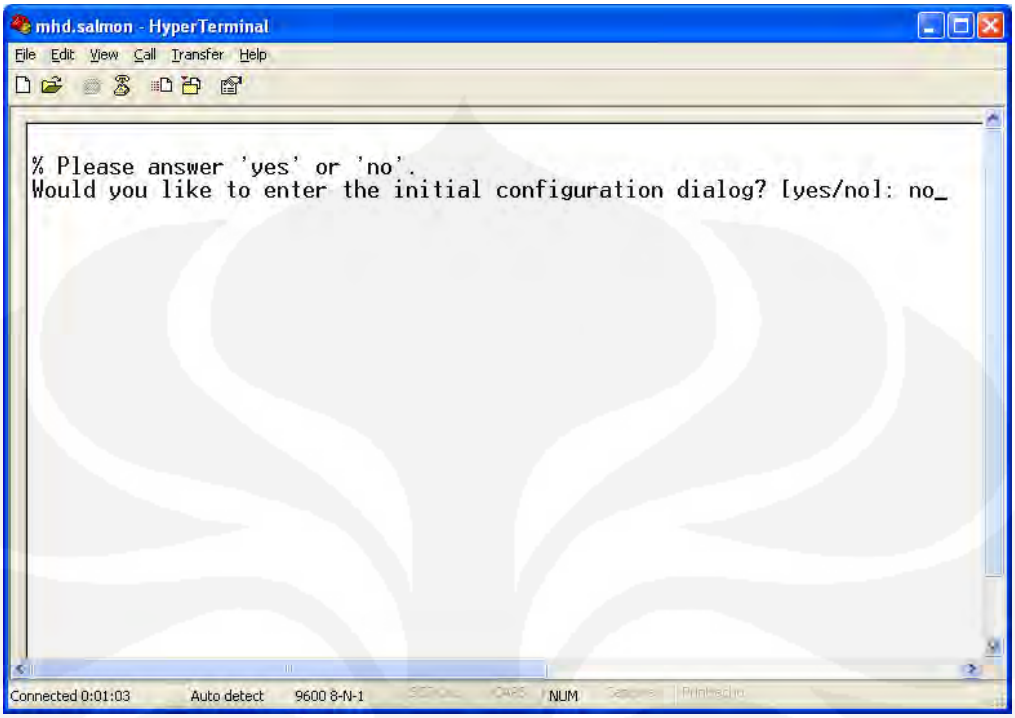
Gambar 3.7 Aplikasi HyperTerminal saat pertama kali dijalankan

Setelah itu pilih port serial yang akan digunakan dan selanjutnya klik restore default.



Gambar 3.8 Port serial yang digunakan pada aplikasi HyperTerminal

Selanjutnya ketik "no" saat aplikasi *HyperTerminal* telah terbuka.



Gambar 3.9 Inisiasi konfigurasi HyperTerminal

Selanjutnya router 1 dan router 2 masing-masing dikonfigurasi.

1. Konfigurasi router 1

```
Router>enable
Router#configure terminal
Router(config)#enable secret class
Router(config)#hostname Router1
Router1(config)#username Router2 password cisco
Router1(config)#int fa0/1
Router1(config-if)#ip address 200.200.200.1 255.255.255.240
Router1(config-if)#no shut
Router1(config-if)#int s0
Router1(config-if)# ip address 200.200.200.33 255.255.255.252
Router1(config-if)#clock rate 64000
Router1(config-if)#encapsulation ppp
Router1(config-if)#ppp authentication chap
Router1(config-if)#ppp chap sent-username Router1 password cisco
Router1(config-if)#no shut
Router1(config-if)#router rip
Router1(config-router)#ver 2
Router1(config-router)#network 200.200.200.0
Router1(config-router)#exit
Router1(config)#
```

2. Konfigurasi router 2

```
Router>enable
Router#configure terminal
Router(config)#enable secret class
Router(config)#hostname Router2
Router2(config)#username Router1 password cisco
Router2(config)#int fa0/1
Router2(config-if)#ip address 200.200.200.17 255.255.255.240
Router2(config-if)#no shut
Router2(config-if)#int s0
Router2(config-if)# ip address 200.200.200.34 255.255.255.252
Router2(config-if)#encapsulation ppp
Router2(config-if)# ppp authentication chap
Router1(config-if)#ppp chap sent-username Router2 password cisco
Router2(config-if)#no shut
Router2(config-if)#router rip
Router2(config-router)#ver 2
Router2(config-router)#network 200.200.200.0
Router2(config-router)#exit
Router2(config)#
```

3.3.13 Melakukan setting dan menjalankan netmeeting pada client

Netmeeting merupakan software yang berjalan di atas sistem operasi windows dan dapat melakukan *video streaming* maupun voip antar host dalam jaringan komputer.

Gambar 3.10 Halaman awal konfigurasi netmeeting

Selanjutnya klik tombol next untuk melakukan konfigurasi berikutnya

Gambar 3.11 Kolom isian client video streaming

Isikan kolom sesuai dengan identitas user client, setelah selesai klik tombol next

Gambar 3.12 Memilih jenis koneksi yang digunakan

Pilih jenis komunikasi yang digunakan untuk *video streaming*, dalam skripsi ini digunakan *Local Area Network*, setelah memilih klik tombol next, dan atur volume headphone dan volume record dari mic, apabila konfigurasi telah selesai maka netmeeting siap untuk digunakan.

Gambar 3.13 Aplikasi Netmeeting siap digunakan

Untuk melakukan *video streaming*, isikan IP Address dari client pada kolom call netmeeting dan klik icon telepon.

Gambar 3.14 Aplikasi Netmeeting setelah terjadi komunikasi

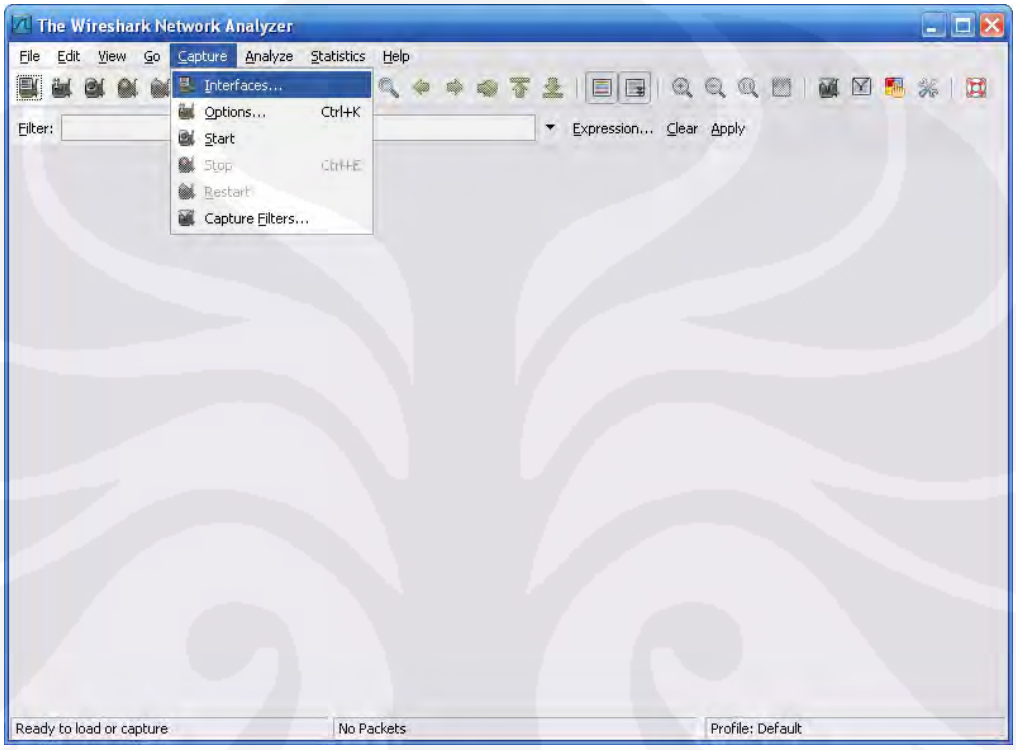
3.4 Uji coba dan Pengambilan data

Uji coba dilakukan dengan menjalankan aplikasi *video streaming* pada virtual private network pada kondisi jaringan tanpa beban maupun pada kondisi jaringan terbebani oleh paket UDP dan TCP, kemudian dari hasil uji coba tersebut di ambil data dengan bantuan software wireshark, adapun data-data yang diambil saat ujicoba meliputi :

1. Data ujicoba *video streaming* pada vpn tanpa beban
2. Data ujicoba *video streaming* pada vpn dengan beban TCP 50Kb
3. Data ujicoba *video streaming* pada vpn dengan beban TCP 500Kb
4. Data ujicoba *video streaming* pada vpn dengan beban TCP 1,5Mb

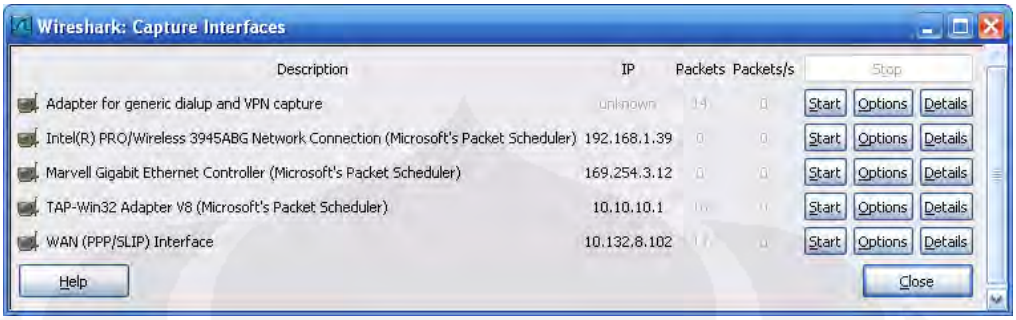
Langkah-langkah pengambilan data menggunakan wireshark adalah sebagai berikut :

- Menjalankan software wireshark dari server dan client pada menu start → All Program → wireshark
- Mengcapture protokol yang sedang berjalan pada *video streaming* dengan bantuan wireshark, dengan mengklik Capture → interfaces



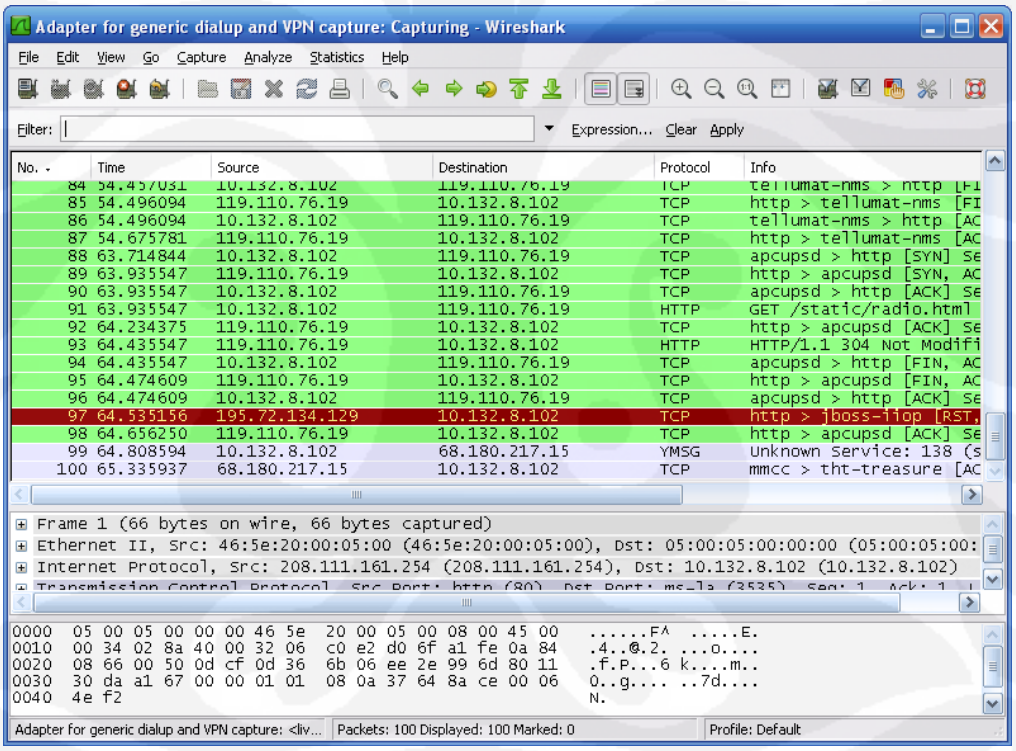
Gambar 3.15 Langkah mengcapture protokol pada wireshark

- Klik option pada interface dan pilih interface VPN (TAP-Win32 Adapter) untuk mengatur opsi wireshark
- Pada menu interface, pilih opsi TAP VPN
- Pada menu stop capture pilih after dan isi dengan 2 menit untuk menentukan lama proses capture



Gambar 3.16 Memulai mengcapture trafik paket data

- Proses capture data berjalan, pada skripsi ini pengambilan data pada masing-masing kondisi dilakukan selama 2 menit.
- Setelah proses capture selesai dengan mengklik stop maka akan muncul protokol-protokol yang muncul pada saat proses capture untuk di analisa.



Gambar 3.17 Protokol yang tercapture pada ujicoba

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

BAB IV
ANALISA DATA DAN PEMBAHASAN

Pada Bab IV ini akan dilakukan analisa terhadap performansi *video steraming* pada jaringan virtual private network, baik dalam kondisi tanpa beban maupun saat sistem terbebani paket TCP, ICMP maupun paket protokol lainnya, parameter yang diukur meliputi *packet loss*, *throughput* dan *delay*. Proses *streaming* pada skripsi ini dilakukan dengan menggunakan aplikasi netmeeting antara client dan server.

Pengamatan dilakukan pada saat client membentuk hubungan VPN dengan server dengan menggunakan aplikasi OpenVPN yang dipasang di kedua sisi. Paket yang dikirimkan berupa suara dan gambar antara client dan server, selanjutnya dilakukan capture menggunakan perangkat lunak wireshark untuk mengetahui parameter *packet loss*, pengukuran dilakukan di sisi server dan client pada saat kondisi jaringan terbebani maupun saat jaringan tidak terbebani paket UDP dan TCP.

4.1 Penentuan Parameter Pengukuran

Parameter pengukuran yang digunakan dalam penelitian ini meliputi *packet loss*, *throughput* dan *delay*.

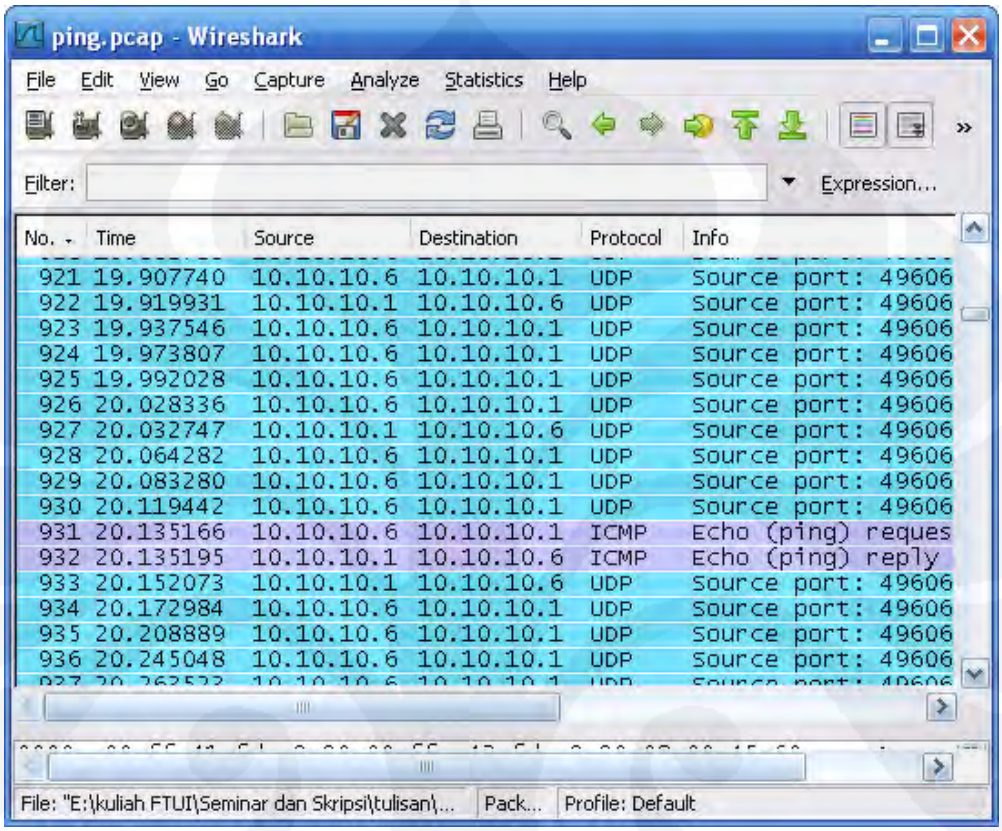
Packet loss adalah banyaknya paket yang gagal dikirimkan ke tujuan. Pada saat kondisi jaringan tanpa beban. Dengan membandingkan antara paket yang dikirim dengan paket yang diterima maka kita dapat mengetahui jumlah paket hilang. *Delay* merupakan waktu yang diperlukan untuk mengirimkan paket dari satu node asal ke node tujuan. Sedangkan *throughput* merupakan banyaknya bit yang diterima pada suatu node per satuan waktu.

Seluruh parameter pengukuran diatas dapat kita amati dengan menggunakan perangkat lunak Wireshark.

4.1.1 Pengukuran Dengan Jaringan Tanpa Beban

Oleh karena koneksi yang digunakan untuk mengontrol pengiriman data adalah UDP maka *transport protocol* yang berperan selama proses *streaming* adalah UDP, disamping itu juga akan muncul *protocol* ICMP karena selama

proses *streaming* secara bersamaan juga dilakukan tes ping dengan beban yang kecil 32 *bytes* secara kontinyu, seperti ditunjukkan pada Gambar 4.1 berikut ini.



Gambar 4.1 Tampilan Wireshark saat melakukan tes ping

Pengukuran jaringan tanpa beban adalah kondisi dimana *video streaming* dilakukan tanpa ada gangguan pengiriman data antar node. Parameter protokoldapat diambil dengan melihat besarnya paket yang hilang ketika proses *streaming* berlangsung. Pada Wireshark dapat ditunjukkan dengan cara memfilter protokol *ICMP*, TCP, H.263 atau G.723.1 lalu pada *Menu Toolbar Wireshark* "*Summary*" kemudian dilihat pada data "*Packets*". Lalu dihitung selisih antara jumlah paket yang ditangkap disisi server dan client.

Pada pengukuran jaringan tanpa beban yang pertama ini protokol yang diamati yaitu protokol ICMP saat melakukan test ping antara client dengan server. Parameter *packet loss*, *delay* dan *troughput* berturut-turut dari atas ke bawah ditunjukkan pada nilai paket yang diberi tanda lingkaran merah pada gambar berikut 4.2 :

Client **Server**

Gambar 4.2 Data paket ICMP saat jaringan tanpa beban

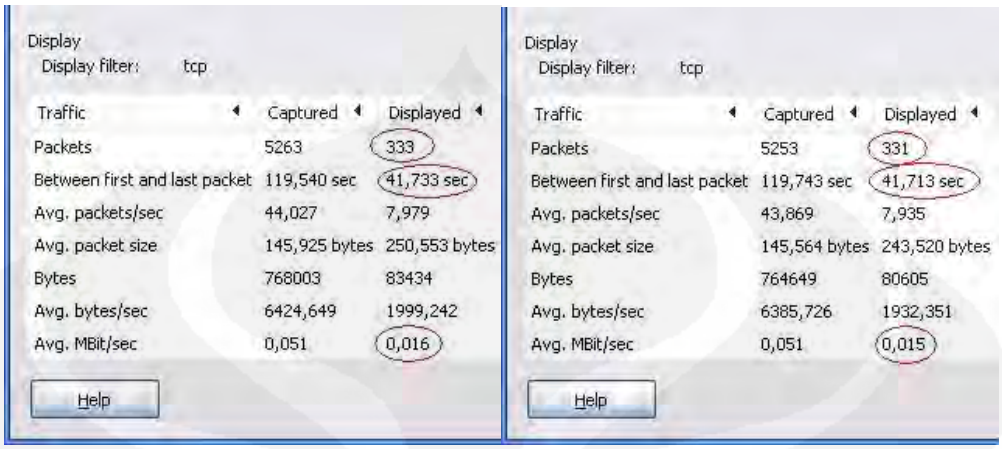
Dari data diatas terlihat bahwa paket data yang mengalir baik dari sisi client maupun dari sisi server adalah sejumlah 32 paket. Maka disini terlihat bahwa data telah tekirim seluruhnya atau dengan kata lain *packet loss* sama dengan 0%.

Parameter *delay* yang terukur terlihat bahwa selisih antara sisi pengirim dan penerima yaitu sebesar 0,004 detik atau = 4ms, sehingga dapat dikatakan hampir tidak ada *delay*. Sedangkan parameter kecepatan aliran data yang mengalir pada jaringan (*throughput*) yang terukur pada gambar diatas yaitu sebesar 41,345 bytes/sec (bps).

4.1.2 Pengukuran Dengan Beban 50Kb

Selanjutnya saat *video streaming* berlangsung, dikirimkan sebuah file gambar sebesar 50Kb dari sisi client ke sisi server. Dari data Wireshark pada percobaan pertama dengan durasi sekitar 2 menit diperlihatkan bahwa paket TCP yang dikirimkan sebanyak 333 paket. Sedangkan banyak paket TCP yang diterima disisi server adalah sebanyak 331. Dengan kata lain disini telah terjadi *packet loss* sebanyak 2 paket atau sama dengan 0,6% (*packet loss* sama dengan jumlah paket loss dibagi jumlah paket yang dikirim dikali 100%).

Client **Server**



Gambar 4.3 Data paket TCP saat jaringan diberi beban 50Kb

Dari gambar diatas terlihat bahwa *delay* antara client dan server adalah sekitar 0,020 detik (20 ms). Disini terlihat ada kenaikan pengaruh dari dari beban dimana ada kenaikan *delay* saat beban 50Kb dikirim saat *video streaming* berlangsung.

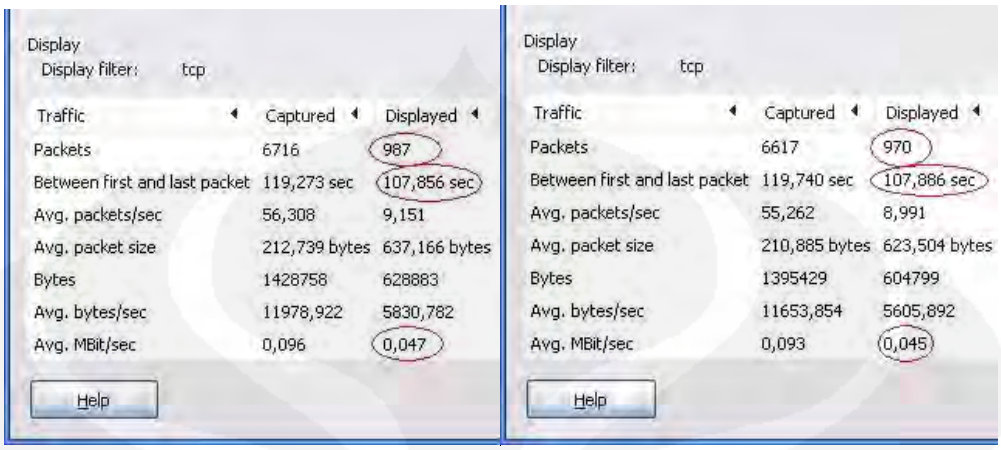
Sedangkan untuk data *throughput* berkisar 0,015 Mbps atau sama dengan 1,6 Kbps. Disini terjadi peningkatan nilai *throughput* saat beban bertambah. Karena beban yang dikirimkan tersebut menempati jalur jaringan sebanding dengan besar file yang dikirim dan berbanding terbalik dengan waktu.

4.1.3 Pengukuran Dengan Beban 500Kb

Langkah selanjutnya saat *video streaming* masih berlangsung, dikirimkan sebuah file gambar sebesar 500Kb dari sisi client ke sisi server. Dari data Wireshark dengan durasi sekitar 2 menit diperlihatkan bahwa paket TCP yang dikirimkan sebanyak 987 paket. Sedangkan banyak paket TCP yang diterima disisi server adalah sebanyak 970. Dengan kata lain disini telah terjadi *packet loss* sebanyak 17 paket atau sama dengan 1,17% (*packet loss* dibagi jumlah paket yang dikirim).

Dari gambar 4.4 terlihat bahwa *delay* antara client dan server adalah sekitar 0,030 detik (30 ms). Disini terlihat ada kenaikan pengaruh dari dari beban dimana ada *delay* hampir setengah detik saat beban 500Kb dikirim saat *video streaming* berlangsung.

Client **Server**



Gambar 4.4 Data paket TCP saat jaringan diberi beban 500Kb

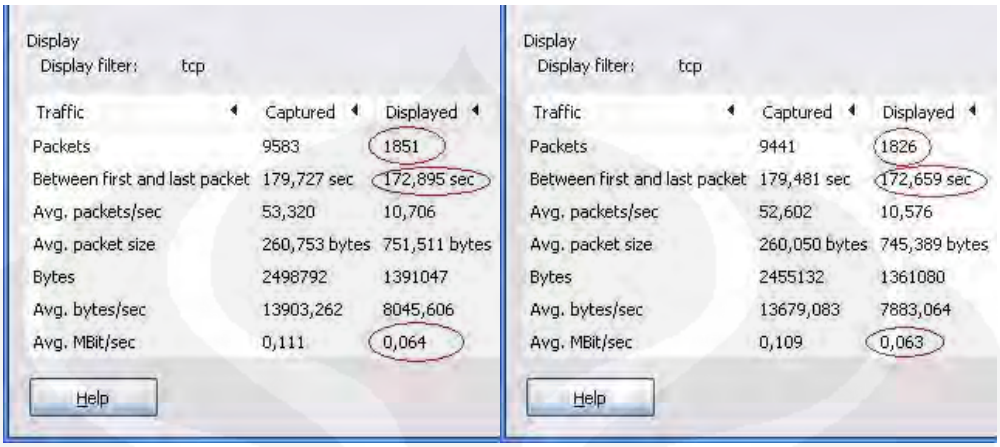
Sedangkan untuk data *throughput* berkisar diantara 0,045 – 047 Mbps. Terjadi peningkatan nilai *throughput* saat beban bertambah. Karena beban yang dikirimkan tersebut menempati jalur jaringan sebanding dengan besar file yang dikirim dan berbanding terbalik dengan waktu.

4.1.4 Pengukuran Dengan Beban 1,5Mb

Selanjutnya dilakukan pengamatan terhadap jaringan saat diberi beban 1,5Mb yang mana dikirim dari sisi client ke server sebesar 1,5Mb selama selang waktu 3 menit. Dari data Wireshark diperlihatkan bahwa paket TCP yang dikirm sebanyak 1851 dan data yang diterima disisi server adalah sebesar 1826. Disini terlihat bahwa telah terjadi *packet loss* sebanyak 25 paket yang mana merupakan selisih antara paket yang dikirim dengan paket yang diterima. Dengan kata lain *packet loss* nya sebesar 1,35%.

Parameter *delay* yang terukur adalah sekitar 236 ms. Ini keliatan cukup signifikan karna beban yang dikirim cukup besar dan ini membuat *delay* yang besar dalam jaringan. Sedangkan parameter *throughput* yang terbaca adalah berkisar antara 0,063 - 0,064 Mbps.

Client **Server**



Gambar 4.5 Data paket TCP saat jaringan diberi beban 1,5Mb

4.2 Pengukuran Video Loss dan Voice Loss

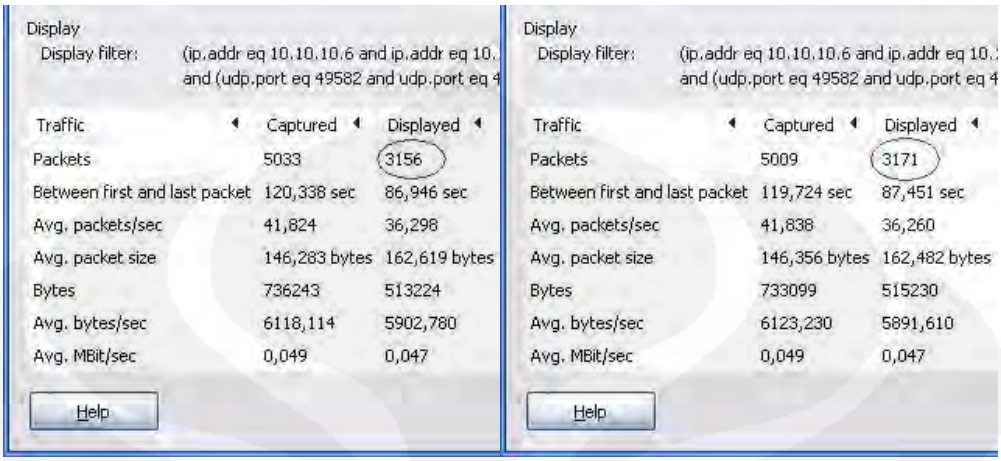
Pengukuran selanjutnya dapat menggunakan parameter *voice loss* dan *video loss*. Protokol video salah satu nya adalah protokol H.263 yang merupakan sebuah *video codec* yang telah di standarisasi oleh ITU dan dirancang untuk low-bitrate untuk format *video streaming* dan *videoconfrence*. Dan protokol voice yang diukur yaitu G.723.1 yang merupakan protokol *audio codec* untuk komunikasi multimedia.

4.2.1 Pengukuran Video Loss

Dalam *video streaming* yang mempengaruhi kualitas selain *throughput* jaringan juga dipengaruhi oleh nilai frame rate (frame per second). Frame rate adalah jumlah bingkai gambar atau frame yang ditunjukkan setiap detik dalam membuat gambar bergerak yang diberi nilai satuan fps. Jika nilai fps nya kecil maka semakin baiklah kualitas *video streaming* tersebut, namun jika nilai fps nya besar maka semakin buruklah kualitas dari *video streaming* tersebut.

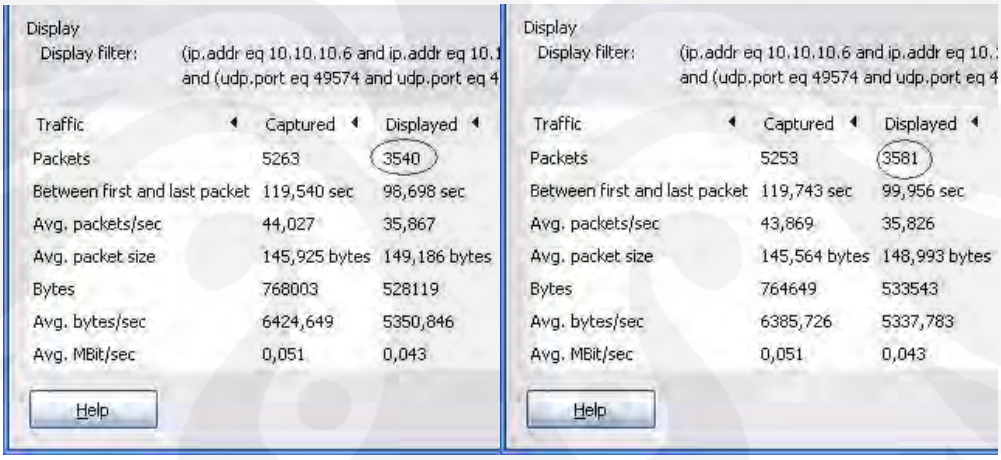
Nilai fps yang besar tersebut dapat dipengaruhi jika ada loss saat melakukan *video streaming*. Sama seperti sebelum nya dalam mengamati *packet loss*, untuk mengukur *video loss* dalam proses *video streaming* juga perlu dilakukan, hanya protokol yang diamati adalah protokol H.263. Dalam mengukur *video loss* dan audio loss ini digunakan metode seperti sebelum nya yaitu dengan kondisi tanpa beban, diberi beban 50Kb dan 500Kb.

Client **Server**



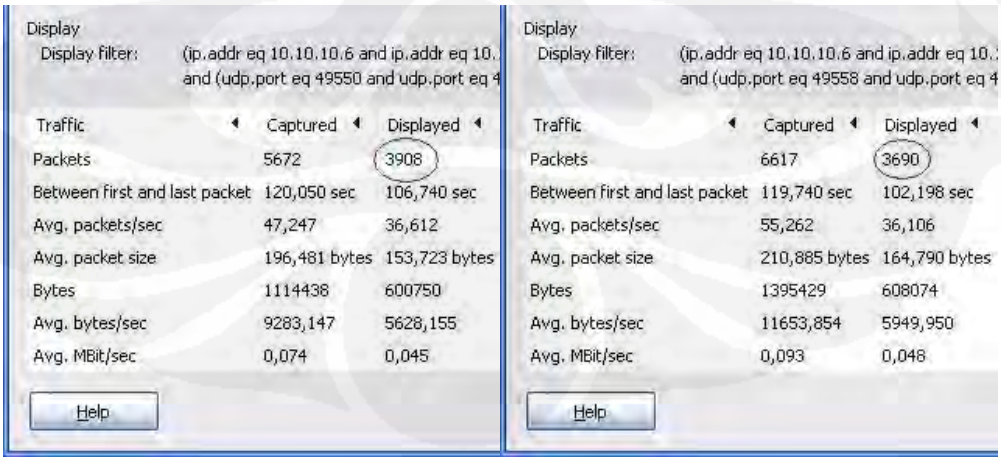
Gambar 4.6 Data paket protokol H.263 tanpa beban

Client **Server**



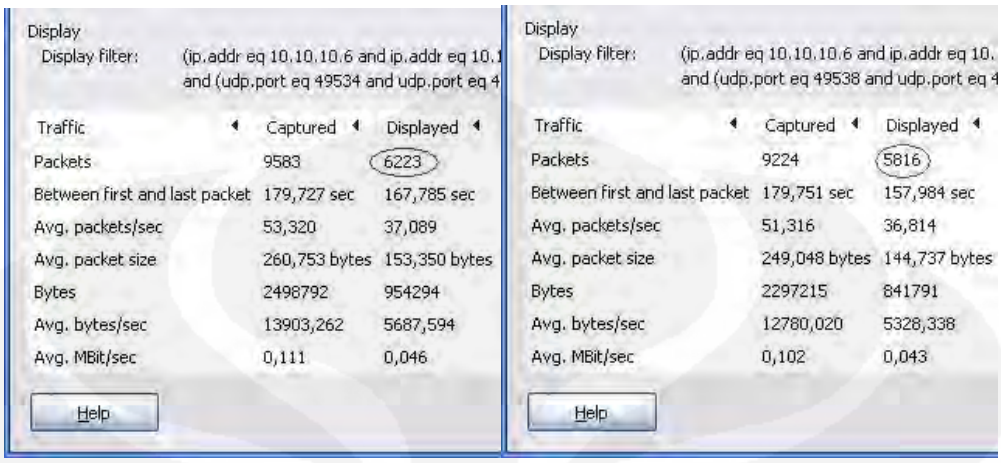
Gambar 4.7 Data paket protokol H.263 dengan beban 50Kb

Client **Server**



Gambar 4.8 Data paket protokol H.263 dengan beban 500Kb

Client **Server**



Gambar 4.9 Data paket protokol H.263 dengan beban 1,5Mb

Dari gambar 4.6 sampai 4.9 diatas terlihat bahwa telah terjadi loss saat pengiriman paket video. Parameter diatas diambil selama selang waktu 1 sampai 3 menit. Nilai *video loss* disini merupakan selisih antara *packet loss* di sisi server dan *packet loss* di sisi client.

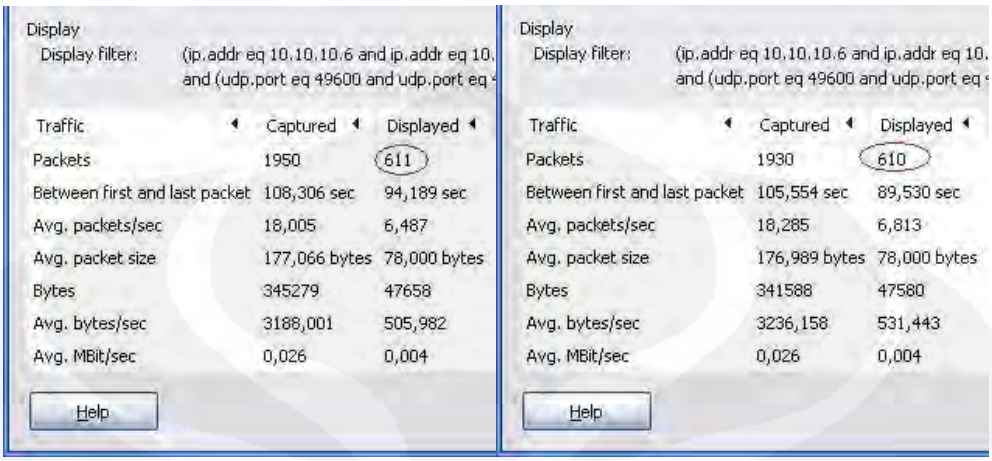
Pada saat kondisi jaringan tanpa beban nilai *video loss* yang diperoleh adalah 0,47%. Lalu saat kondisi jaringan diberi beban 50Kb diperoleh nilai *video loss* sebesar 1,14%. Selanjutnya beban diberikan sebesar 500Kb diperoleh nilai *video loss* 5,58%. Dan saat kondisi jaringan diberi beban 1,5Mb diperoleh nilai *video loss* sebesar 6,54%.

4.2.2 Pengukuran Voice Loss

Voice loss yang terjadi pada saat *video streaming* dilakukan dapat dipengaruhi oleh faktor kompresi audio. Sama seperti sebelum nya dalam mengamati *packet loss*, untuk mengukur *voice loss* dalam proses *video streaming* juga perlu dilakukan, hanya protokol yang diamati adalah protokol G723.1. Dalam mengukur *voice loss* ini digunakan metode seperti sebelum nya yaitu dengan kondisi tanpa beban, diberi beban 50Kb dan 500Kb.

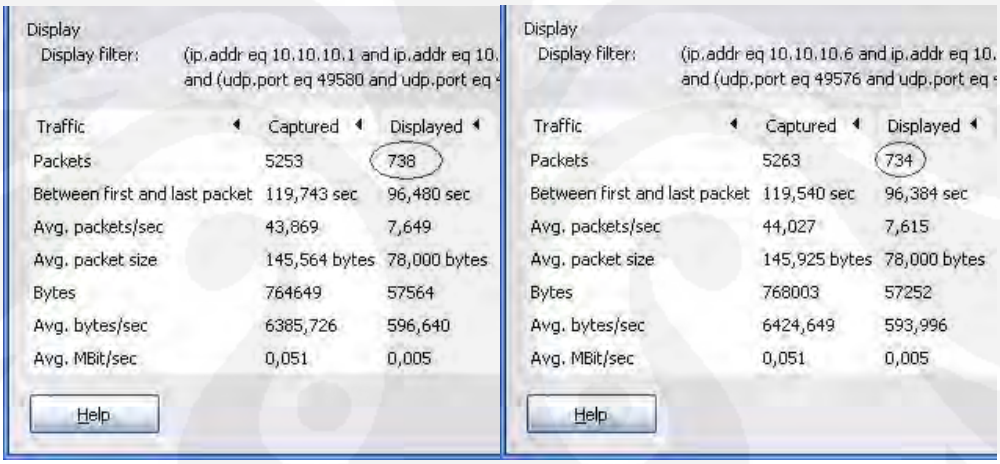
Pada pengukuran diperoleh data sebagai berikut:

Client **Server**



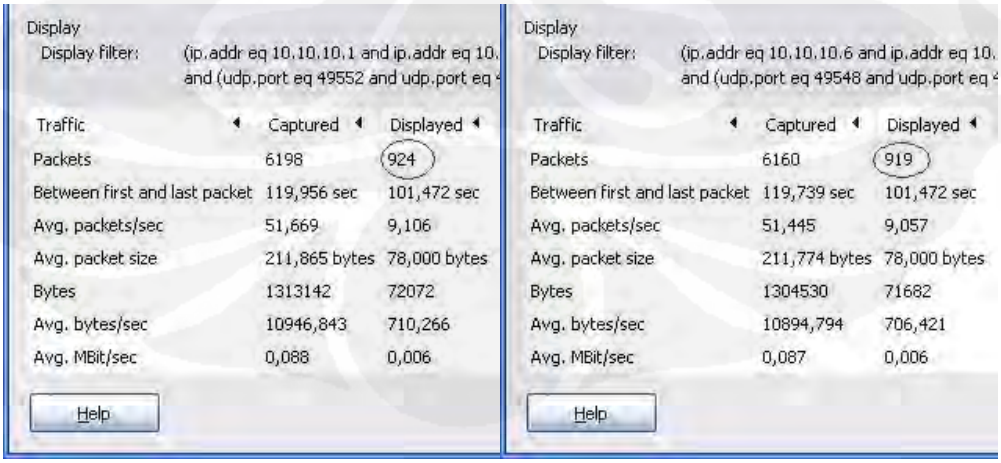
Gambar 4.10 Data paket protokol G.723.1 tanpa beban

Client **Server**



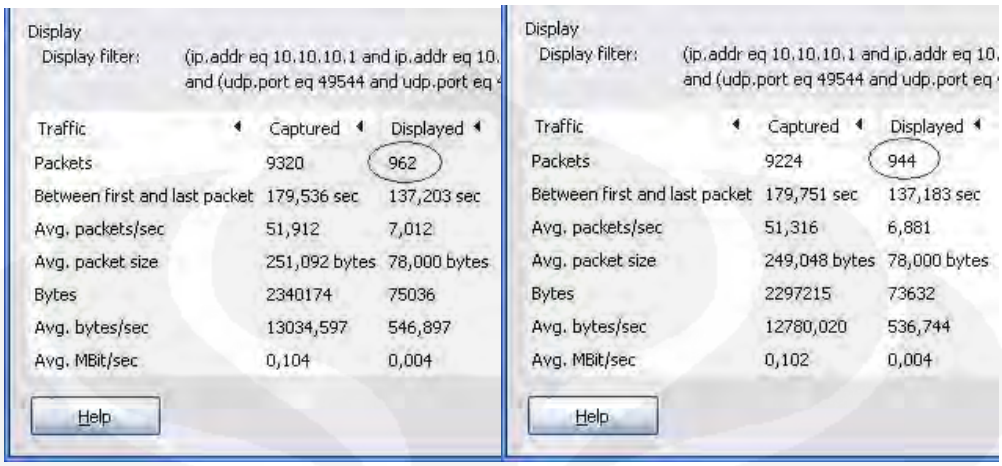
Gambar 4.11 Data paket protokol G.723.1 dengan beban 50Kb

Client **Server**



Gambar 4.12 Data paket protokol G.723.1 dengan beban 500Kb

Client **Server**



Gambar 4.13 Data paket protokol G.723.1 dengan beban 1,5Mb

Dari gambar 4.10 sampai 4.13 diatas dapat dilihat bahwa telah terjadi loss pada saat pengiriman peket voice. Parameter diatas diambil selama selang waktu 2 menit. Nilai *voice loss* disini merupakan selisih antara *packet loss* disisi server dan *packet loss* di sisi client yang nilainya bervariasi.

Pada saat kondisi jaringan tanpa beban nilai *voice loss* yang diperoleh adalah 0,16%. Lalu saat kondisi jaringan diberi beban 50Kb diperoleh nilai *voice loss* sebesar 0,54%. Selanjutnya beban diberikan sebesar 500Kb juga diperoleh nilai *voice loss* yang hamper sama yaitu 0,54%. Dan saat beban diberikan 1,5Mb maka data yang diperoleh adalah sebesar 1,87%

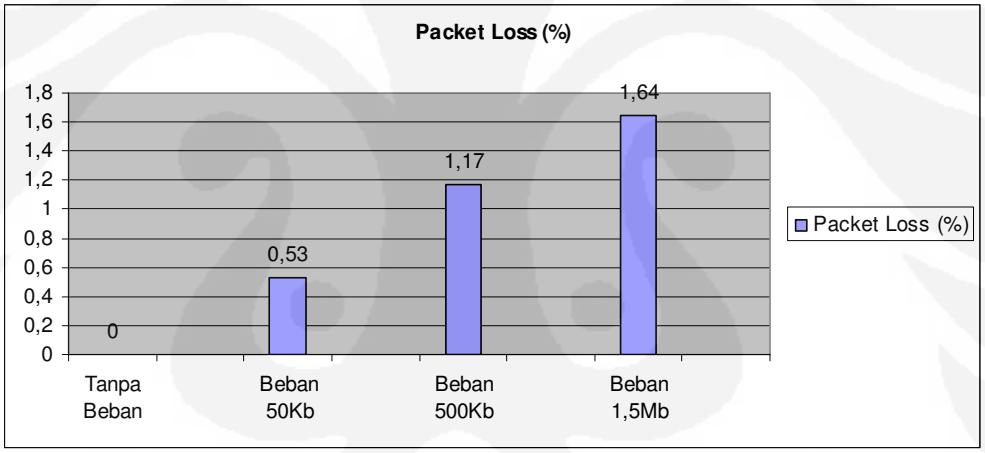
4.3 Analisa Data Hasil Pengukuran

Seperti telah dijelaskan pada proses pengambilan data sebelumnya, aplikasi *video streaming* yang dijalankan pada setiap konfigurasi jaringan yang digunakan dapat diukur protokol ICMP untuk ping saat kondisi jaringan tanpa beban, serta menggunakan protokol TCP saat kondisi jaringan diberikan beban. TCP merupakan protokol yang bersifat *connection oriented* dimana mendukung pengiriman kembali paket apabila ada yang hilang, sehingga bisa diketahui jumlah paket yang hilang. Sehingga dapat diukur *packet loss*, *delay* paket yang dikirimkan serta *throughput* atau yang lebih dikenal sebagai aktual bandwidth.

Tabel 4.1 Data parameter rata-rata pengukuran packet loss

Packet Loss (%)	Tanpa Beban	Beban 50Kb	Beban 500Kb	Beban 1,5Mb
Percobaan I	0	0,6	1,17	1,35
Percobaan II	0	0	1,14	1,46
Percobaan III	0	0,95	1,22	1,87
Percobaan IV	0	0,6	1,13	1,98
Percobaan V	0	0,2	1,21	1,53
Rata-rata (%)	0	0,53	1,17	1,64

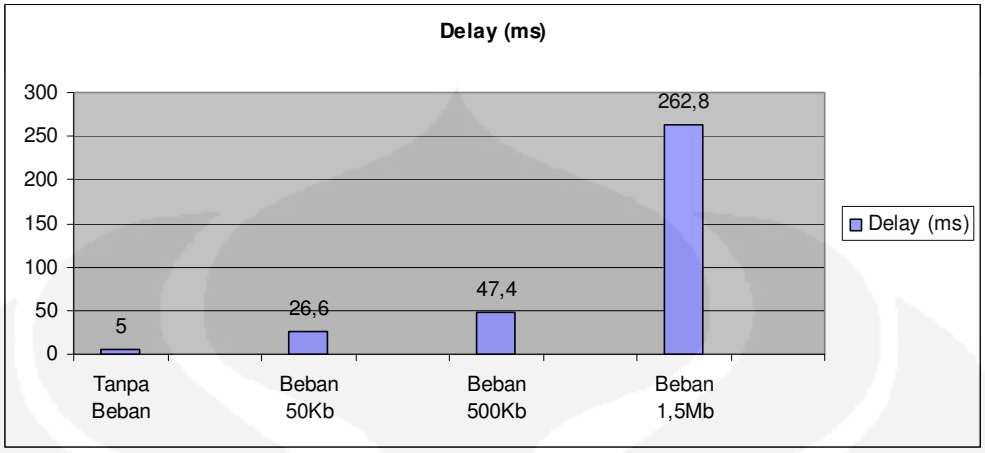
Dari tabel diatas terlihat bahwa semakin besar data yang dikirimkan maka nilai persentase *packet loss* dari protokol TCP juga semakin besar dari mulai 0% naik sampai 1,64%. Hal ini dapat dikarenakan ukuran file yang dikirim besar sehingga ada beberapa paket yang terbuang dalam proses pengiriman. Nilai *packet loss* yang diizinkan untuk *quality of service* adalah dibawah 1% [13]. Nilai ini hanya memenuhi syarat saat kondisi jaringan tanpa beban dan diberi beban 50Kb.



Gambar 4.14 Grafik rata-rata packet loss

Tabel 4.2 Data parameter rata-rata pengukuran delay

Delay (ms)	Tanpa Beban	Beban 50Kb	Beban 500Kb	Beban 1,5Mb
Percobaan I	4	20	30	236
Percobaan II	6	21	42	199
Percobaan III	4	33	65	288
Percobaan IV	7	28	51	348
Percobaan V	4	31	49	243
Rata-rata (ms)	5	26,6	47,4	262,8



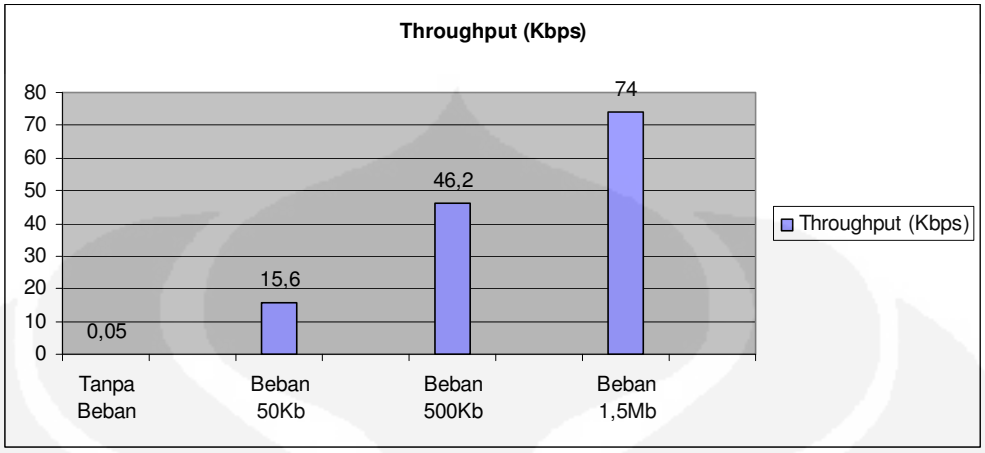
Gambar 4.15 Grafik rata-rata delay

Dalam proses *video streaming*, apabila data video menghabiskan terlalu banyak waktu pada saat berada di jaringan maka tidak dapat disebut sebagai *real-time.* Dari penelitian yang dilakukan, ditunjukkan bahwa dengan melakukan perubahan besar beban video dan audio pada proses *encoding* dan *decoding file* video yang akan digunakan dalam proses *streaming* maka akan berpengaruh terhadap *delay* yang terjadi selama proses *streaming*. Nilai *delay* rata-rata yang diperoleh disini bervariasi mulai dari 5 ms sampai 262,8 ms. Semakin besar file yang dikirimkan maka semakin besar *delay* yang dapat terjadi.

Untuk memenuhi syarat *quality of service* maka nilai *delay* maksimum yang diperbolehkan adalah 150ms [13]. Kondisi tersebut dapat terpenuhi saat kondisi jaringan dalam keadaan tanpa beban, diberi beban 50Kb dan diberi beban 500Kb. Namun saat jaringan dibebani file 1,5Mb maka kondisi *quality of service* menjadi tidak tercapai.

Tabel 4.3 Data parameter rata-rata pengukuran throughput

Throughput (Kbps)	Tanpa Beban	Beban 50Kb	Beban 500Kb	Beban 1,5Mb
Percobaan I	0,04	16	46	65
Percobaan II	0,05	14	50	77
Percobaan III	0,07	16	46	89
Percobaan IV	0,04	17	45	69
Percobaan V	0,05	15	44	70
Rata-rata (Kbps)	0,05	15,6	46,2	74



Gambar 4.16 Grafik rata-rata throughput

Pada grafik diatas terlihat bahwa besar *throughput* dapat menjadi semakin besar saat beban juga semakin besar. Hal ini karna *throughput* berpengaruh terhadap unjuk kerja jaringan VPN yang digunakan. Saat jaringan dipakai hanya untuk *video streaming* (tanpa beban yang berarti) maka nilai *throughput* pada saat melakukan tes ping adalah sangat kecil berkisar jauh dibawah 1Kbps.

Selanjutnya saat beban dinaikkan maka *throughput* dari beban tersebut juga semakin besar maka hal ini akan mempengaruhi dari kualitas dari *video streaming* tersebut. Karena jalur yang digunakan juga dipakai dalam mengirimkan beban. Pada pengukuran *voice loss* dan *video loss* diperoleh tabel berikut :

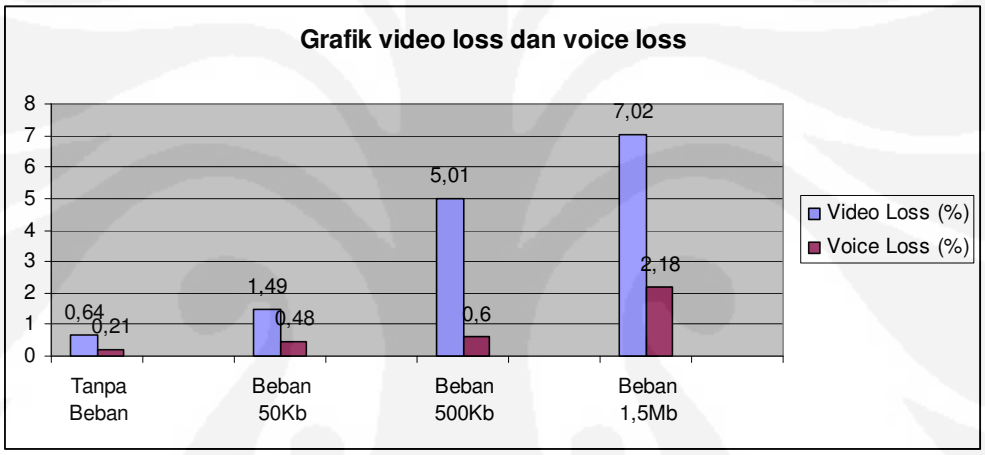
Tabel 4.4 Data parameter video loss

Video Loss (%)	Tanpa Beban	Beban 50Kb	Beban 500Kb	Beban 1,5Mb
Percobaan I	0,47	1,14	5,58	6,54
Percobaan II	0,38	0,98	4,79	7,18
Percobaan III	0,77	2,14	4,64	7,27
Percobaan IV	0,89	1,87	5,66	7,81
Percobaan V	0,69	1,34	4,81	6,31
Rata-rata (%)	0,64	1,49	5,01	7,02

Tabel 4.5 Data parameter voice loss

Voice Loss (%)	Tanpa Beban	Beban 50Kb	Beban 500Kb	Beban 1,5Mb
Percobaan I	0,16	0,54	0,54	1,87
Percobaan II	0,22	0,49	0,53	2,2
Percobaan III	0,18	0,52	0,61	2,31
Percobaan IV	0,27	0,42	0,63	1.98
Percobaan V	0,22	0,42	0,7	2,54
Rata-rata (%)	0,21	0,48	0,6	2,18

Berdasarkan tabel 4.4 dan table 4.5 di atas, terlihat bahwa kompresi video yang digunakan adalah H.263 dan G.723.1 untuk audio, dari data tersebut didapatkan rata-rata nilai *video loss* dan voice loss terlihat dari grafik berikut ini :



Gambar 4.17 Grafik Video Loss dan Voice Loss

Dari grafik diatas terlihat bahwa nilai *video loss* lebih besar dari nilai *voice loss*. Hal ini dapat terjadi dikarenakan ukuran data video lebih besar dari ukuran data voice sehingga menyebabkan nilai dari *video loss* lebih besar dari *video loss*.

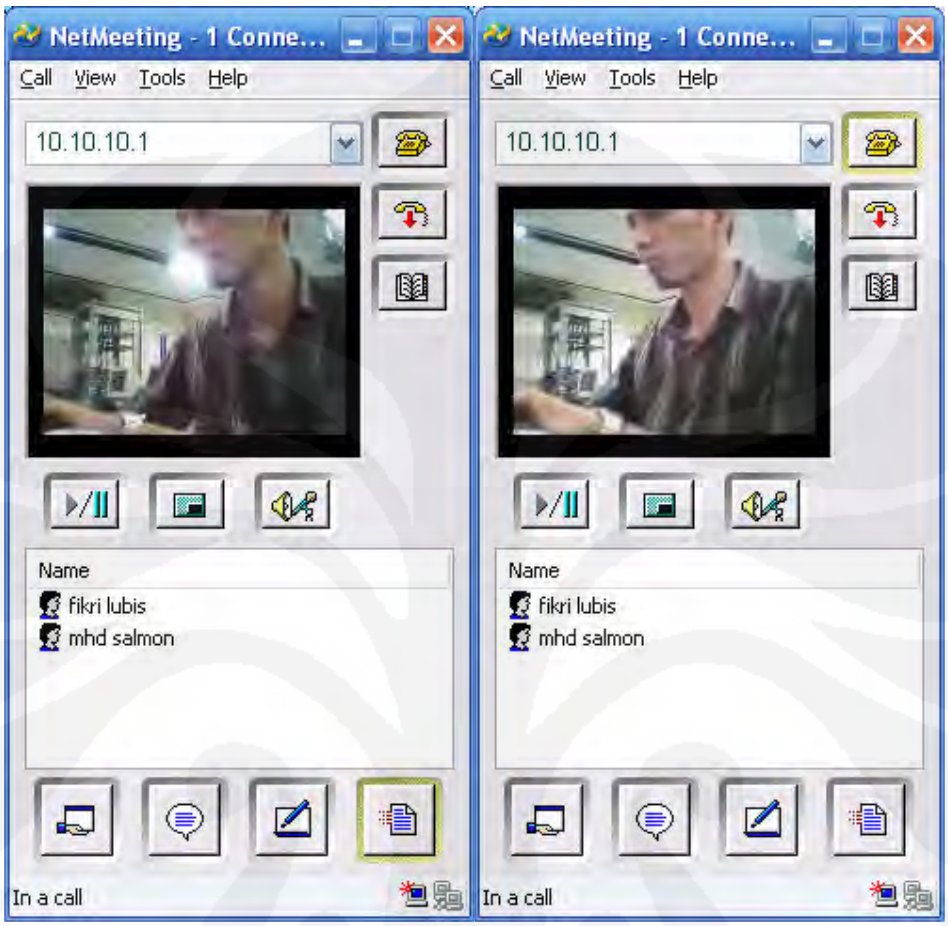
Dalam percobaan juga terlihat perbedaan dari gambar yang diperoleh saat *video streaming* berlangsung. Perbedaan ini terlihat saat beban yang dikirimkan berbeda-beda. Hal ini sesuai dengan grafik yang diperoleh dimana nilai *video loss* akan semakin besar saat beban yang dikirimkan semakin besar.

Berikut ini adalah gambar yang diambil saat *video streaming* berlangsung dimulai saat jaringan tanpa beban, diberi beban 50 Kb, 500Kb dan 1,5Mb.

Tanpa beban **Beban 50k**

Gambar 4.18 Tampilan Netmeeting saat tanpa beban dan diberi beban 50Kb

Beban 500K **Beban 1,5M**



Gambar 4.19 Tampilan Netmeeting saat diberi beban 500Kb dan 1,5Mb

BAB V
KESIMPULAN

Dari hasil penelitian mengenai analisa unjuk kerja dan *quality of service* dari aplikasi secure *video streaming* pada jaringan berbasis virtual private network (VPN) ini dapat diambil kesimpulan :

1. Besar nilai *packet loss* rata-rata dari hasil pengujian jaringan VPN dengan tanpa beban, diberi beban 50Kb, 500Kb dan 1,5Mb maka diperoleh nilai *packet loss* nya berturut-turut adalah 0%, 0,53%, 1,17% dan 1,35%. Sedangkan nilai *packet loss* yang diperbolehkan maksimal adalah 1%.
2. *Delay* rata-rata yang didapat dari hasil pengujian jaringan VPN dengan tanpa beban, diberi beban 50Kb, 500Kb dan 1,5Mb maka diperoleh nilai *delay* berturut-turut adalah 5 ms, 26,6 ms, 47,4 ms dan 262,8 ms. Sedangkan nilai *delay* maksimal yang diperbolehkan adalah 150 ms.
3. Nilai *throughput* rata-rata yang diukur dari hasil pengujian jaringan VPN dengan tanpa beban, diberi beban 50Kb, 500Kb dan 1,5Mb maka diperoleh nilai *throughput* berturut-turut adalah 0,05 Kbps, 15,6 Kbps, 46,2 Kbps dan 74 Kbps.
4. Nilai rata-rata *video loss* yang diperoleh dari pengujian melalui jaringan VPN dengan tanpa beban, diberi beban 50Kb, 500Kb dan 1,5 MB berturut-turut adalah 0,64%, 1,49%, 5,01% dan 7,02%.
5. Nilai rata-rata *voice loss* yang diperoleh dari pengujian melalui jaringan VPN dengan tanpa beban, diberi beban 50Kb, 500Kb dan 1,5 MB berturut-turut adalah 0,21%, 0,48%, 0,6% dan 2,18%.

DAFTAR ACUAN

[1]. Setiawan, Deris. ” Solusi Virtual Private Network sebagai alternative Jaringan Skala Luas (WAN)”, 2004.

[2]. Cisco Networking Academy, CCNA Exploration 4.0 (Cisco System, Inc., 2007).

[3]. Onno W. Purbo, “*Virtual Private Network* (VPN) sebagai alternatif Komunikasi Data Pada Jaringan Skala Luas (WAN)”. http://mirror.unej.ac.id/onnowpurbo/library/library-ref-ind/ref-ind-3/network/VPN_jurnal.pdf

[4]. Cisco Networking Academy Program, CCNA v3.1 (Cisco System, Inc., 2004).

[5]. William Stallings ”Komunikasi Data dan Komputer : Jaringan Komputer”, Salemba Teknika, 2002.

[6]. Wikipedia,”SYN flood”, Diakses 10 Desember 2009 dari Wikipedia. http://en.wikipedia.org/wiki/SYN_flood

[7]. SSL (*Secure Socket Layer*), diakses tanggal 4 Desember 2009. http://sdn.vlsm.org/share/ServerLinux/node171.html

[8]. Nurkholis Madjid, “Perbandingan SSL dan IPsec pada VPN”, 2007.

[9]. Eko Arianto, Kristian. ” Analisa Performansi Metode USOT Untuk Video Streaming”, Institut Teknologi Telkom, November, 2008

[10]. www.openvpn.se, diakses tanggal 6 Desember 2009.

[11]. www.wireshark.org, diakses tanggal 7 Desember 2009.

[12]. OpenVPN Windows HowTo, diakses tanggal 11 Desember 2009. http://www.runpcrun.com/howtoopenvpn

[13]. J. Arturo Pérez, Víctor Zárate, Ángel Montes, Carlos García, “*Quality of Service Analysis of IPSec VPNs for Voice and Video Traffic*”, Proceedings of the IEEE. 2006