UNIVERSITAS INDONESIA

IMPLEMENTASI DAN ANALISA PERBANDINGAN QoS PADA PPTP DAN L2TP/IPSEC REMOTE ACCESS VPN UNTUK LAYANAN SECURED MOBILE IP BASED VIDEO TELEPHONY

SKRIPSI

ARDIANSYAH
0606078273

FAKULTAS TEKNIK
PROGRAM STUDI TEKNIK KOMPUTER
DEPARTEMEN TEKNIK ELEKTRO
DEPOK
JULI 2010

UNIVERSITAS INDONESIA

IMPLEMENTASI DAN ANALISA PERBANDINGAN QoS PADA PPTP DAN L2TP/IPSEC REMOTE ACCESS VPN UNTUK LAYANAN SECURED MOBILE IP BASED VIDEO TELEPHONY

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh gelar
Sarjana Teknik Komputer

ARDIANSYAH
0606078273

FAKULTAS TEKNIK
PROGRAM STUDI TEKNIK KOMPUTER
DEPARTEMEN TEKNIK ELEKTRO
DEPOK
JULI 2010

HALAMAN PERNYATAAN ORISINALITAS

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

Nama	**: Ardiansyah**
NPM	**: 0606078273**
Tanda Tangan	**:**
Tanggal	**: 1 Juli 2010**

HALAMAN PENGESAHAN

Skripsi ini diajukan oleh :
Nama : Ardiansyah
NPM : 0606078273
Program Studi : TeknikKomputer
Judul Skripsi : Implementasi dan Analisa Perbandingan QoS Pada PPTP dan L2TP/IPSec Remote Access VPN untuk Layanan Secured Mobile 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 Komputer, Departemen Teknik Elektro, Fakultas Teknik, Universitas Indonesia.

DEWAN PENGUJI

Pembimbing : Muhammad Salman, ST, M.IT ( )

Penguji : Prof.Dr.Ir.Riri Fitri Sari,M.Sc,MM ( )

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

Ditetapkan di : Depok

Tanggal : 1 Juli 2010

UCAPAN TERIMA KASIH

Puji syukur saya panjatkan kehadirat Allah SWT, karena atas segala rahmat dan hidayat-Nya saya dapat menyelesaikan skripsi ini. Saya menyadari bahwa skripsi ini tidak akan terselesaikan tanpa bantuan dari berbagai pihak. Oleh karena itu, saya mengucapkan terimakasih kepada :

1. Bapak Ir.Muhammad Salman, ST, M.IT. selaku pembimbing skripsi ini, yang telah meluangkan waktunya, serta masukan-masukan selama bimbingan;
2. Para peneliti sebelum ini yang juga memberikan sumber bacaan yang banyak bagi saya;
3. Ibu dan Bapak, saudara dan adik saya yang selalu memberi nasehat dan memotivasi saya untuk selalu berusaha keras dan semangat dalam setiap pekerjaan yang dilakukan;
4. Teman – teman satu bimbingan skripsi dengan saya dan rekan laboratorium jaringan komputer: Taufik, Dina, Alfa, Burhan, Yudi, Aneta, Ruki, dan Irvanda; terimakasih atas bantuan, dan motivasi yang diberikan pada saya.
5. Dan seluruh Sivitas Akademik Departemen Teknik Elektro yang tidak dapat saya sebutkan satu persatu.

Akhir kata, semoga Allah SWT berkenan membalas kebaikan semua pihak yang telah membantu. Semoga skripsi ini bermanfaat bagi perkembangan ilmu pengetahuan.

Depok, Juli 2010

Ardiansyah

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI
TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademika Universitas Indonesia, saya bertandatangan di bawah ini :

Nama : Ardiansyah
NPM : 0606078273
Program studi : TeknikKomputer
Departemen : TeknikElektro
Fakultas : Teknik
Jeniskarya : 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 :

Implementasi dan Analisa Perbandingan QoS Pada PPTP dan L2TP/IPSec Remote Access VPN untuk Layanan Secured Mobile IP Based Video Telephony

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non Eksklusif ini Universitas Indonesia berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta sebagai pemegang Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Depok
Pada tanggal: 2 Juli 2010
Yang menyatakan

Ardiansyah

Nama : Ardiansyah

Program Studi : Teknik Komputer, S1 Reguler

Judul : Implementasi dan Analisa Perbandingan QoS Pada PPTP dan L2TP/IPSec Remote Access VPN untuk Layanan Secured Mobile IP Based Video Telephony

ABSTRAK

Seiring dengan perkembangan teknologi, banyak layanan multimedia telah dikembangkan di internet Salah satu dari layanan itu adalah IP Video Telephony. Tetapi IP Video Telephony memiliki kelemahan yaitu keamanan yang tidak terjamin. Karena berbasis IP, maka siapapun bisa melakukan penyadapandan perekaman terhadap data IP Video Telephony. Dari sinilah muncul suatu pemikiran tentang bagaimana caranya untuk mengamankan data IP Video Telephony tanpa mengurangi kinerja dari jaringan IP Video Telephony itu sendiri. Salah satu cara adalah dengan menggunakan VPN (Virtual Private Network). VPN sendiri telah diketahui sebagai salah satu metode yang handal dalam menangani masalah keamanan jaringan, terutama untuk pengiriman data penting. Untuk mengimplementasikan pemikiran tersebut maka dibuatlah suatu sistem *IP Video Telephony over Remote Access VPN*. Kemudian dianalisa bagimana kinerja dan keamanan IP Video Telephony sebelum dan sesudah menggunakan VPN. Apakah *voice*dan *video* yang dihasilkan oleh IP Video Telephony over VPN masih memenuhi standar ITU-T berdasarkan delay, jitter dan packet loss dan bernilai baik menurut standar ITU-R 500. Dari pengujian dengan menggunakan codec video H.263 dan H.264 serta codec audio G.711, G.729 dan GSM didapatkan bahwa kinerja (delay, jitter dan packet loss) dengan menggunakan VPN berubah meskipun besarnya tidak signifikan dan masih memenuhi standar. VPN dapat mengamankan data dari ancaman keamanan. Sebelum menggunakan VPN data IP Video Telephony dapat direkam dan dimainkan ulang. Data payloadnya juga dapat ditangkap dan dilihat tetapi setelah menggunakan VPN IP Video Telephonytidak dapat direkam dan data payloadnya tidak terlihat. Bandwith yang diperlukan untuk implementasi IP Video Telephony berkisar 256 kbps untuk sepasang pengguna. Kombinasi IP Video Telephony yang paling baik ialah video codec H.263, audio codec G.729 dengan protokol VPN yang digunakan ialah PPTP VPN karena kinerja yang didapat masih memenuhi standar, data payloadnya aman, penggunaan bandwith efisien, dan nilai pengukuran kualitas subjektif videonya bernilai 4 yang artinya cukup baik.

Kata Kunci : IP Video Telephony, VPN, codec, PPTP

Name : Ardiansyah

Study Program : Computer Engineering, S1 Reguler

Title : Implementation and Comparative Analysis of QoS in PPTP and L2TP/IPSec VPN for Remote Access Service Secured Mobile IP-Based Video Telephony

ABSTRACT

Currently, IP based technologies are growing faster as well as many multimedia services in the internet. One of them is IP Video Telephony. It becomes more popular in term of the interactivity, scalability, cost efficiency and reachability, however IP Video Telephony has a weakness in the lack of security guarantee because it is based on IP so everyone can tap and record the data of IP Video telephony. One of the ways to protect the data without reducing the performance is by using VPN (Virtual Private Network). VPN is well-known as one of reliable methods in handling the problems of security network, especially to send important data securely. In this final thesis, the IP Video Telephony over Remote Access VPN is implemented. Then, the performance and the security of IP Video Telephony before and after using the VPN is analyzed to know whether the voice and the video transmitted over VPN still meet the standard of ITU-T in term of the delay, jitter, and packet loss and has an adequate value based on the standard of ITU-R 500. The result from the experiment carried out by using codec video H.263 and H.264, and also codec audio G.711, G.729 and GSM shows that the performance (delay, jitter, and packet loss) by using VPN is slightly changed and not quite significant. It shows that the standard performance is still acceptable. VPN can secure the data from any security threat. Before using the VPN, the data of IP Video Telephony can be recorded and replayed. The payload data can be captured and seen. Meanwhile, after using the VPN, the data of IP Video Telephony could not be recorded and the payload data is hidden. The required bandwidth capacity to implement the IP Video Telephony is around 256 kbps for a pair of users. The best audio and video codec combination to implement IP Video Telephony is H.263 video and G.729 audio codec with PPTP VPN Protocol because the performance measurement result still meets the standard, the data payload are secure, the use of bandwidth capacity is efficient, and the measurement value of subjective quality video reaches 4 , which means it is quite good and acceptable.

Keyword : IP Video Telephony, VPN, codec, PPTP

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR GRAFIK

DAFTAR ISTILAH

Delay : Waktu yang dibutuhkan paket dari dikirim sampai diterima di penerima.

Jitter : Variasi total delay (perbedaan waktu kedatangan antara paket satu dengan paket lainnya).

Packet Loss : Jumlah paket yang hilang dalam pengiriman

Bandwidth : Jumlah bit maksimum yang dapat ditransmisikan dalam satu satuan waktu

Capture : Proses penangkapan paket data yang lewat dalam jaringan

Bitrate : besarnya bit yang dapat ditransmisikan dalam satu detik

Payload : kumpulan bit – bit yang merupakan isi dari data yang ingin dikirim

Throughput : Banyaknya paket yang dikirim persatuan waktu

Protokol : aturan yang berlaku sesuai standar yang telah disepakati

BAB I

PENDAHULUAN

1.1 Latar Belakang

Teknologi komunikasi berbasis IP berkembang dengan begitu cepatnya seiring dengan kemajuan teknologi. Saat ini jaringan internet tidak hanya terfokus pada layanan paket data dan aplikasi standar seperti WWW (world wide web), http, smtp, ftp, atau layanan data lainnya yang bersifat non *real-time* dan tidak memiliki QoS. Saat ini kebutuhan akan layanan atau aplikasi berbasis multimedia dilewatkan melalui jaringan IP telah menjadi sesuatu yang mungkin. Pada dasarnya jaringan IP dibuat untuk tidak melewati data yang bersifat *real time*. Tetapi dengan ditemukannya teknologi penunjang QoS jaringan seperti RTP, *streaming via internet*, RSVP, dan MPLS membuat jaringan IP menjadi handal untuk mengirim data yang bersifat *real time*seperti *voice, video*.

Kemajuan – kemajuan inilah yang membuat berbagai layanan multimedia berbasis IP muncul di masyarakat. *IP Video Telephony* adalah salah satunya. Teknologi ini pengembangan dari VoIP yang dapat melewati suara (speech) dan video kedalam jaringan. Dengan teknologi *IP Video Telephony* biaya untuk melakukan telekomunikasi antara satu *user* ke *user* lainnya menjadi lebih efisien. Hal ini disebabkan karena *IP Video Telephony* tidak tergantung pada jarak.Sehingga membuat layanan bertelekomunikasi menggunakan PC menjadi lebih murah. Skype, Yahoo Messengger with Voice dan masih banyak lagi provider layanan VoIP menawarkan jasa pelayanan ini.

Berkembangnya layanan ini bukan berarti bahwa tidak akan ada masalah. Salah satu kelemahan jaringan internet adalah bahwa data yang terkirim tidak terjamin kerahasiaannya sehingga siapapun dapat menangkap dan memanipulasi data tersebut. Jika data yang ditangkap ternyata rahasia maka akan menjadi kerugian bagi kita jika data tersebut diketahui orang lain atau bahkan digunakan untuk hal yang dapat merugikan. Dalam skripsi ini dianalisis mengenai keamanan

aplikasi *IP Video Telephony* di jaringan. Seberapa amankah telekomunikasi menggunakan *IP Video Telephony* dan apakah perlu untukmengamankan jaringan *IP Video Telephony* serta bagaimana perubahan kinerja dari jaringan ini jika data tersebutdiamankan dengan suatu metode keamanan kemudian dibandingkan apakah perubahan tersebut masih sesuai dengan standar yang telah ditetapkan oleh ITU-T. Dimana pada skripsi kali ini metode yang akan digunakan adalah *Remote Access Virtual Private Network (VPN).*

1.2 Maksud dan Tujuan

Penyusunan skripsi ini dimaksudkan untuk memenuhi salah satu syarat kelululusan pendidikan Strata 1 di Program Studi Teknik Komputer Departemen Teknik Elektro Universitas Indonesia. Sedangkan tujuan dari penyusunan skripsi ini adalah:

1. Mengetahui celah keamanan pada *IP Video Telephony* dan kinerja parameter jaringan seperti *delay, jitter, packet loss* dan *throughput.*
2. Mengetahui kualitas suara dan keamanan yang dihasilkan dari konfigurasi *IP Video Telephony over Remote Access VPN* dengan melakukan *recorded streaming.*
3. Mengetahui bagaimanakah perubahan kinerja dari *IP Video Telephony* sebelum dan sesudah diamankan dengan *Remote Access VPN* dengan menganalisa *delay, packet loss,* dan*jitter* dan dibandingkan dengan standar ITU-T.
4. Mengetahui Codec Optimum yang dapat direkomendasikan untuk Jaringan *IP Video Telephony over Remote Access VPN.*

1.3 Perumusan Masalah

Perumusan masalah yang diambil dalam tugas akhir ini adalah analisis mengenai keamanan aplikasi *IP Video Telephony* di jaringan. Seberapa amankah telekomunikasi menggunakan *IP Video Telephony* dan apakah perlu untuk mengamankan jaringan *IP Video Telephony* serta bagaimana perubahan kinerja dari jaringan *IP Video Telephony* jika data tersebut diamankan dengan suatu

metode keamanan kemudian dibandingkan apakah perubahan tersebut masih sesuai dengan standar yang telah ditetapkan oleh ITU-T.Dimana pada skripsi ini metode yang akan digunakan adalah *Remote Access Virtual Private Network (VPN)*dengan protokol *PPTP* dan *L2TP/IPsec VPN*.

1.4 Batasan Masalah

Dalam pembahasan ini ,ada beberapa batasan yaitu antara lain :

1. Paket yang dianalisa adalah paket RTP, paket lain yang tertangkap bersama paket RTP akan dibuang dan tidak masuk perhitungan analisa.
2. Codec yang digunakan untuk analisis *IP Video Telephony* ada 3 buah codec suara yakni GSM, G.711, dan G.729 dan 2 buah codec video yakni H.263 dan H.264
3. Analisis kinerja secara pengukuran objektif dilakukan terhadap codec suara sedang untuk codec video dilakukan pengukuran secara subjektif dengan metode yang disesuaikan dengan standar ITU-R 500. Untuk MOS digunakan referensidari ITU – T.
4. Jaringan yang akan diamankan adalah jaringan antara jaringan publik yang terdapat di Departemen Teknik Elektro Universitas Indonesia dengan jaringan privat di belakang VPN Server yang diimplementasikan NAT yang terdapat di Laboratorium Jaringan Komputer.
5. Bandwith yang digunakan berdasarkan best-effort bandwith sesuai dengan mekanisme yang ada dan diamati pada kondisi jaringan dengan asumsi trafik tinggi pada siang hari di Departemen Teknik Elektro Universitas Indonesia.
6. Percobaan menggunakan IPv4 sebagai pengalamatannya.
7. Protocol VPN yang digunakan ialah PPTP dan L2TP/IPsec VPN.

1.5 Metodologi Penelitian

1. Studi literatur

   Mengumpulkan dan mempelajari referensi tentang jaringan *Remote Access VPN, IP Video Telephony,* dan *Vyatta Router*.

2. Perancangan sistem

   Pada tugas akhir ini dirancang sistem *IP-BASED Video Telephony* pada *Remote Access VPN* untuk dilakukan implementasi PPTP dan L2TP/IPsec VPN.

3. Implementasi sistem

   Model topologi jaringan yang digunakan pada pengujian skripsi ini terdiri dari beberapa perangkat yang saling terhubung satu sama lain di Departemen Teknik Elektro Universitas Indonesia yang diasumsikan mewakili *Campus Network* dan dikombinasikan dengan jaringan privat yang di implementasikan di Laboratorium Jaringan. Berdasarkan sumber dari administrator jaringan di Departemen Teknik Elektro diketahui bahwa jaringan uji mempunyai besaran*bandwith* yang transparant sesuai dengan proxy 152.118.101.8. Besarnya *bandwith transparent* tersebut sebanyak 25 Mbps yang dibagi kelima departemen di Universitas Indonesia dan salahsatunya ialah Departemen Teknik Elektro. Prinsip yang digunakan dalam membagi bandwith tersebut ialah secara *best-effort*. Selain itu kondisi trafik di jaringan Elektrocukup padat pada siang hari.

   Mobile VoIP Client 1 dan 2 dibuat seakan-akan sedang dalam keadaan *mobile* dengan akses kejaringannya melalui wireless dan menggunakan ip publik yang didapat secara DHCP dengan terhubung di jaringan Departemen Teknik Elektro Universitas Indonesia. Agar dapa tmengakses VoIP Server, *User Agent* yang diwakili oleh *Mobile VoIP Client* harus mengaktifkan koneksi *Remote Access VPN* baik dengan protokol PPTP ataupun L2TP/IPsec VPN. Penerapan VPN ini dikombinasikan dengan penerapan NAT sehingga system jaringan yang diterapkan untuk internal network dimana VoIP server berada berupa jaringan privat. Hal ini dilakukan agar seolah-olah mewakili keadaan jaringan yang sesungguhnya karena saat ini sebagian besar computer

berada di jaringan privat dan memerlukan NAT untuk dapat berkomunikasi ke jaringan internet ataupun sebaliknya.

4. Pengambilan data dan analisa

   Setelah dilakukan implementasi, untuk codec suara akan dicatat data-data yang berhubungan dengan parameter QoS (Quality of Service) pada jaringan terbebani RTP, kemudian menggunakan bantuan software wireshark dari system tersebut meliputi *delay, jitter, throughput* dan hasilnya akan dianalisa. Sedangkan untuk codec video akan dilakukan analisa sesuai dengan hasil kuisioner yang dibuat.

5. Penarikan kesimpulan

   Selanjutnya dari hasil analisa tersebut akan ditarik kesimpulan mengenai seberapa besar pengaruh implementasi kedua buah jenis enkripsi tersebut pada *Remote Access VPN* serta dilakukan pemilihan kombinasi video dan codec yang paling efisien.

6. Penulisan buku laporan

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

1.6 SistematikaPenulisan

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 :LANDASAN TEORI

Bab ini berisi penjelasan mengenai konsep IP Video Telephony, VPN, Protocol PPTP dan L2TP/IPsec VPN .

Bab III : PERENCANAAN DAN IMPLEMENTASI

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

Bab IV : PENGUJIAN DAN ANALISA DATA

Pada bab ini akan membahas proses analisa data untuk mengetahui pengaruh penerapan PPTP dan L2TP/IPSec pada *Remote Access VPN* terhadap kinerja *IP Video Telephony* yang meliputi *delay, jitter, throughput*. Selain itu juga dibahas mengenai kebutuhan bandwith dan pengukuran subjektif kualitas *IP Video Telephony*.

Bab V : PENUTUP

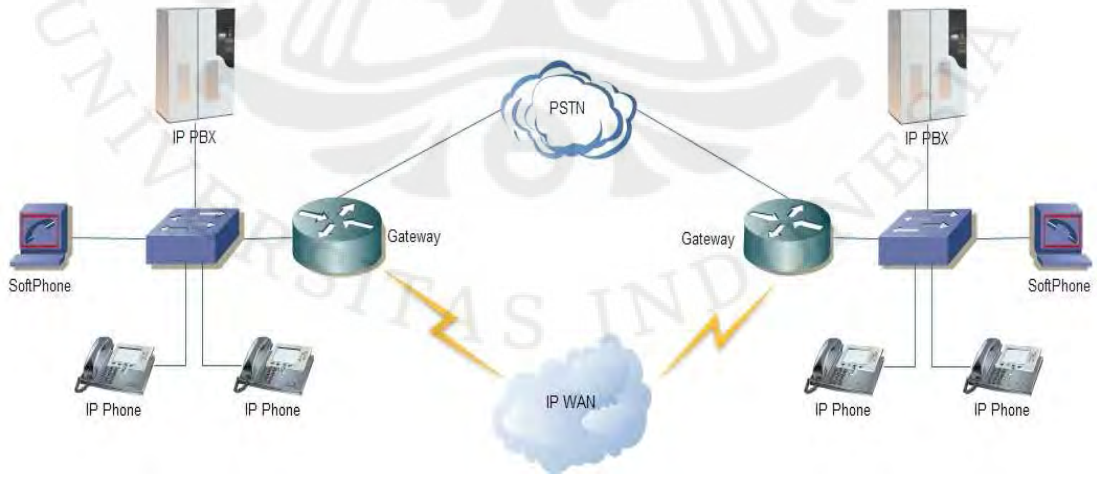
Bab ini berisi kesimpulan dan saran.

BAB II

IP VIDEO TELEPHONY DAN VPN

2.1 IP Video Telephony

Voice over Internet Protocol (VoIP) dikenal juga dengan sebutan IP Telephony di definisikan sebagai suatu system yang menggunakan jaringan internet untuk mengirimkan paket data suara dari suatu tempat ke tempat lainnya menggunakan perantara protokol IP (Tharom, 2002). Dengan kata lain teknologi ini mampu melewatkan trafik suara yang berbentuk paket melalui jaringan IP. Jaringan IP sendiri adalah merupakan jaringan komunikasi data yang berbasis *packet-switch.*Namun, pada saat ini semakin banyak orang yang tidak hanya menggunakan layanan VoIP tetapi lebih memilih menggunakan layanan video telephony.Layanan *IP Video Telephony* adalah suatu layanan teknologi yang memungkinan dua orang untuk berkomunikasi audio-visual secara *full-duplex* dan *real-time* tanpa harus bertatap muka secara langsung.Untuk aplikasi Video Telephony protocol yang adalah Realtime Transport Protocol (RTP) sesuai dengan standar ITU-T.Standar video codec yang dapat digunakan ialah H.263 dan H.264 sedangkan standar audio codecnya ialah G.711, G.723.1, G.729 dan GSM.



Gambar 2.1 Diagram IP Video Telephony[3]

IP Video Telephony merupakan teknologi yang membawa sinyal visual dan suara digital dalam bentuk paket data dengan protocol IP. Suara yang masuk diubah dalam bentuk format digital. Kita ketahui bahwa komputer merupakan suatu perangkat digital yang melakukan pengolahan data dalam bentuk bit (*binary digit*). Dengan perkembangan teknologi DSP (*Digital Signal Processing*) telah menghasilkan perangkat yang mampu mengolah sinyal analog (misalnya sinyal audio) sebagai sinyal input dan diolah menjadi sinyal digital lalu kemudian menghasilkan sinyal keluaran dalam bentuk sinyal analog kembali. Proses ini dilakukan oleh *soundcard* atau *DSP Board*. Data dalam format digital akan dikirimkan dalam jaringan internet, kemudian dibagi dalam paket – paket kecil. Hal ini dapat memudahkan dan mempercepat transportasi.Jadi kalau ada data yang hilang, data tidak perlu dikirim ulang cukup paket – paket yang hilang saja.

Pada awalnya perkembanganIP Video Telephony hanya dapat dipakai antar PC multimedia dengan kualitas rendah. Sesuai dengan perkembangan teknologi, kini IP Video Telephony memungkinan komunikasi antar PC ke telepon dan komunikasi antar telepon dengan kualitas layak sehingga layanan IP Video Telephony mulai banyak dijual oleh operator – operator telekomunikasi di dunia. Oleh karena itu jaringan IP harus didesain agar memenuhi persyaratan *delay* dan *packet loss*. *Packet loss* (kehilangan paket data pada proses transmisi) dan *delay* bukan hanya merupakan masalah yang berhubungan dengan kebutuhan bandwidth, namun lebih dipengaruhi oleh stabilitas rute yang dilewati data pada jaringan, metode antrian yang efisien, pengaturan pada router, dan penggunaan control terhadap kongesti (kelebihan beban data) pada jaringan.

Packet loss terjadi ketika terdapat penumpukan data pada jalur yang dilewati.Hal ini mendorong agar arsitektur IP Video Telephony menyediakan infrastruktur yang memiliki kemampuan dan fitur seperti halnya SS7 (*Signaling System No 7*) di PSTN. Panggilan IP Video Telephony memiliki dua jenis komunikasi yang menempati jaringan IP antara pemanggil (*calling party*) dan pihak yang dipanggil (*called party*), yaitu aliran informasi pembicaraan dan *message – message signaling* yang mengontrol hubungan dan karateristik aliran media. Untuk

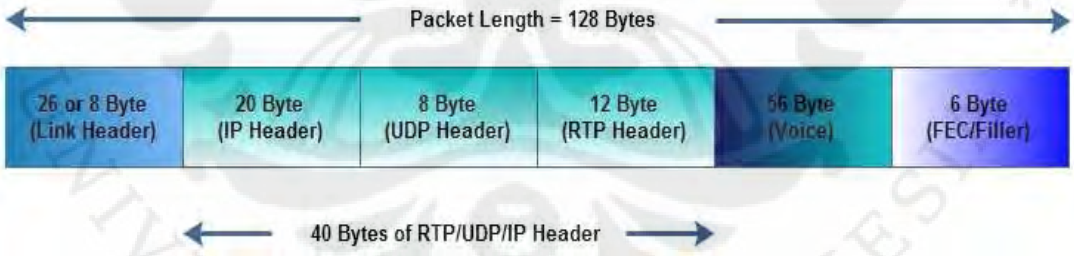
membawa informasi digunakan *Real-time Transport Protocol* (RTP). Sedangkan untuk pensinyalan terdapat dua standar yang dikeluarkan oleh dua badan dunia, yaitu H.323 yang dikembangkan oleh ITU-T dan *Session Intitation Protocol* (SIP) oleh IETF (*Internet Engineering Task Force*)

Ada berapa komponen yang dibutuhkan dalam membuat jaringan IP Video Telephony, yaitu:

- Codec
- TCP/IP dan VoIP protocols
- IP Telephony servers dan PBXs
- VoIP gateways dan routers
- IP Phones atau softphones

2.2 Format Paket IP Video Telephony

Tiap paket IP Video Telephony terdiri dari dua bagian, yakni *header* dan *payload* (beban).*Header* terdiri atas *IP Header*, *Real – time Transport Protocol* (RTP), *User Datagram Protocol* (UDP) *header*, dan *link header*. Format paket IP Video Telephony dapat dilihat pada gambar berikut (Tharom, 2002)



Gambar 2.2 Format Paket VoIP[3]

IP header bertugas menyimpan informasi routing untuk mengirimkan paket – paket ke tujuan. Pada tiap header IP disertakan tipe layanan atau *Type of Service* (ToS) yang memungkinkan paket tertentu seperti paket suara yang non real time.

UDP header memiliki ciri tertentu yaitu tidak menjamin paket akan mencapai tujuan sehingga UDP cocok digunakan pada aplikasi *voice real time* yang sangat peka terhadap *delay* dan *latency*.

RTP header adalah *header* yang dapat dimanfaatkan untuk melakukan *framing*, dan segmentasi data *real time*. Seperti UDP, RTP juga tidak mendukung realibitas paket untuk sampai ke tujuan. RTP menggunakan protokol kendali yang disebut RTCP (*Real-time Transport Control Protocol*) yang mengendalikan QoS dan sinkronisasi media stream yang berbeda. Untuk *link header*, besarnya sangat tergantung pada media yang digunakan. Tabel berikut menunjukkan perbedaan ukuran header untuk media yang berbeda dengan metode kompresi G.729

Tabel 2.1 Link Layer Header Size[3]

Media	Link Layer Header Size	Bit Rate
Ethernet	14 byte	29.6 kbps
PPP	6 byte	26.4 kbps
Frame Relay	4 byte	25.6 kbps
ATM	5 byte tiap cell	42.4 kbps

2.3 Protokol Signaling dalam Jaringan IP Video Telephony

Protokol signaling dalam IP Video Telephony diperlukan agar pemakai layanan IP Video Telephony dapat saling berkomunikasi dengan pesawat telepon. Beberapa protokol signaling yang ada saat ini adalah H.323, SIP, SCCP, MGCP, MEGACO dan SIGTRAN. Tetapi yang paling populer dan banyak digunakan adalahaH.323 dan SIP. H.323 merupakan teknologi yang dikembangkan oleh ITU-T (*International Telecommunication Union*) sedangkan SIP (*Session Initiation Protocol*) merupakan teknologi yang dikembangkan IETF (*Internet Engineering Task Force*).

2.4 Standar Kompresi Data Suara

Sebuah *codec* (yang merupakan kepanjangan dari *compressor/decompressor* atau *coder/decoder*) adalah suatu *hardware* atau *software* yang melakukan sampling terhadap sinyal suara analog, kemudian mengkonversi ke dalam bit – bit digital dan mengeluarkannya. Beberapa jenis codec melakukan kompresi agar dapat menghemat bandwidth.ITU –T (*International Telecommunication Union – Telecommunication Sector*) membuat beberapa standar untuk voice coding yang direkomendasikan untuk implementasi VoIP. Beberapa standar yang sering dikenal antara lain

2.4.1 G.711

Sebelum mengetahui lebih jauh apa itu G.711, sebelumnya diberikan sedikit gambaran singkat fungsi dari kompresi. Sebuah kanal video yang baik tanpa dikompresi akan mengambil bandwidth sekitar 9 Mbps. Sedangkan sebuah kanal suara (audio) yang baik tanpa dikompresi akan mengambil bandwidth sekitar 64 Kbps. Dengan adanya teknik kompresi, kita dapat menghemat sebuah kanal video menjadi sekitar 30 Kbps dan kanal suara menjadi 6 Kbps (*half-duplex*), artinya sebuah saluran internet yang tidak terlalu cepat sebetulnya dapat digunakan untuk menyalurkan video dan audio sekaligus. Tentunya untuk kebutuhan konferensi dua arah dibutuhkan double bandwidth, artinya minimal harus menggunakan kanal 64 Kbps ke internet. Dengan begitu suara/audio akan memakan bandwidth jauh lebih sedikit dibanding pengiriman gambar / video

G.711 adalah suatu standar Internasional untuk kompresi audio dengan menggunakan teknik *Pulse Code Modulation* (PCM) dalam pengiriman suara.Standar ini banyak digunakan oleh operator Telekomunikasi di seluruh dunia.

PCM mengkonversikan sinyal analog ke bentuk digital dengan melakukan sampling sinyal analog tersebut 8000 kali/detik dan dikodekan dalam kode angka.Jarak antar sampel adalah 125 μ detik.Sinyal analog pada suatu percakapan diasumsikan berfrekuensi 300 Hz – 3400 Hz. Sinyal tersampel lalu dikonversikan ke

bentuk diskrit.Sinyal diskrit ini direpresentasikan dengan kode yang disesuaikan dengan amplitude dari sinyal sampel.Format PCM menggunakan 8 bit untuk pengkodeannya. Laju transmisi diperoleh dengan mengkalikan 8000 sample/detik dengan 8 bit/sample, menghasilkan 64.000 bit/detik. Bit rate 64 Kbps ini merupakan standar transmisi untuk satu kanal telepon digital.

Percakapan berupa sinyal analog yang melalui jaringan PSTN mengalami kompresi dan pengkodean menjadi sinyal digital oleh PCM G.711 sebelum memasuki *VoIP gateway*. Pada *VoIP gateway*, di bagian terminal terdapat audio codec yang melakukan proses *framing* (pembentukan frame datagram IP yang dikompresi) dari sinyal suara terdigitasi (hasil PCM G.711) dan juga melakukan rekonstruksi pada sisi receiver. Frame – frame yang merupakan paket – paket informasi ini lalu ditransmisikan melalui jaringan IP dengan suatu standar komunikasi jaringan *packet – based*. Standar G.711 merupakan teknik kompresi yang tidak efisien, karena akan memakan bandwidth 64 Kbps untuk kanal pembicaraan. Agar bandwidth yang digunakan tidak besar dan tidak mengesampingkan kualitas suara, maka solusi yang digunakan untuk pengkompresi adalah menggunakan standar G.723.1

2.4.2 G.723.1

Pengkode sinyal suara G.723.1 adalah jenis pengkode suara yang direkomendasikan untuk terminal multimedia dengan bit rate rendah. G.723.1 memiliki *dual rate speech coder* yang dapat di switch pada batas 5.3 Kbit/s. Dengan memiliki *dual rate speech coder* ini maka G.723.1 memiliki fleksibilitas dalam beradaptasi terhadap informasi yang dikandung oleh sinyal suara. G.723.1 dilengkapi dengan fasilitas untuk meningkatkan kualitas sinyal suara hasil sintesis. Pada bagian *encoder* G.723.1 dilengkapi dengan *format perceptual weighting filter* dan *harmonic noise shaping filter* sementara di bagian decodernya G.723.1 memiliki *pitch postfilter* dan *format postfilter* sehingga sinyal suara hasil rekonstruksi menjadi sangat mirip dengan aslinya. Sinyal eksitasi untuk bit rate rendah dikodekan dengan *Algebraic Code Excited Linier Prediction* (ACELP) sedangkan untuk rate tinggi dikodekan

dengan menggunakan *Multipulse Maximum Likelihood Quantization* (MP-MLQ). Rate yang lebih tinggi menghasilkan kualitas yang lebih baik. Masukan bagi G.723.1 adalah sinyal suara digital yang di sampling dengan frekuensi sampling 8.000 Hz dan dikuantisasi dengan PCM 16 bit. *Delay* algoritmik dari G.723.1 adalah 37.5 msec (panjang frame ditambah *lookahead*), delay pemrosesannya sangat ditentukan oleh prossesor yang mengerjakan perhitungan – perhitungan pada algoritma G.723.1. Dengan menggunakan DSP prossesor maka delay pemrosessan dapat diperkecil.

2.4.3 Codec G.726

Merupakan teknik pengkodean suara ADPCM dengan hasil pengkodean pada 40, 32, 24 dan 16 Kbps. Biasanya juga digunakan pada pengiriman paket data pada telepon public maupun peralatan PBX yang mendukung ADPCM.

2.4.4 Codec G.728

Merupakan teknik pengkodean suara CELP dengan hasil pengkodean 16 Kbps. Codec ini memiliki kualitas suara yang bagus dan spesifik di desain untuk *low latency applications.*

2.4.5 Codec G.729

Codec ini adalah salah satu codec berkualitas lebih baik.G.729 merupakan pengkodean suara jenis CELP dengan hasil kompresi pada 8 Kbps. Terdapat 2 versi yaitu G.729 dan G.729a. G.729a memiliki algoritma yang lebih sederhana dan membutuhkan *processing power*lebih sedikit dibandingkan G.729

2.5 Standar Kompresi Data Video

Terdapat beberapa standar *video coding* yang dikembangkan oleh beberapa organisasiinternasional. *International Telecommunication Union* (ITU-T) yang berbasis di Geneva, Switzerland merupakan organisasi yang mengembangkan standar *video coding* untuk bidang telekomunikasi. Selain ITU-T, terdapat pula organisasi

lain yaitu *Motion Picture Experts Group* (MPEG), organisasi ini mengembangkan standar untuk *video* dan *audio coding*.

Berikut adalah beberapa standar *video coding* yang dikembangkan oleh *International Telecommunication Union* (ITU-T):

1. H.261

   Standar *video coding* ini diresmikan pada tahun 1990. Pada awalnya didesain untuk transmisi di atas ISDN. Algoritma *videocoding* ini didesain untuk dapat beroperasi pada *bitrate* antara 40 kbit/s sampai 2 Mbit/s. Standar ini mendukung dua ukuran video *frame*: CIF (352 x 288 *luma* dengan 176 x 144 *chroma*) dan QCIF (176 x 144 *luma* dengan 88 x 72 *chroma*).

2. H.262

   Standar *video coding* H.262 serupa dengan standard video ISO/IEC MPEG-2. Standar ini dikembangkan secara bersamaan oleh ITU-T dan ISO/IEC.

3. H.263

   H.263 merupakan standar yang didesain ITU-T pada tahun 1995/1996 sebagai format kompresi dengan *bitrate* rendah untuk *videoconference*. H.263 dikembangkan sebagai hasil perkembangan evolusi dari H.261, MPEG-1 dan MPEG-2. Versi pertama standar ini diselesaikan pada tahun 1995 dan merupakan pengganti yang cocok untuk H.261. Kemudian dikembangkan lagi pada proyek yang dikenal dengan nama H.263v2 (juga dikenal sebagai H.263+ atau H.263 1998) dan H.263v3 (juga dikenal sebagai H.263++ atau H.263 2000).

4. H.264

   Standar *video coding* berikutnya yang dikembangkan adalah H.264. H.264 menyediakan perkembangan yang signifikan melebihi H.263. Sebagian besar

produk *videoconferencing* sekarang mengikutsertakan standar video H.264, H.263 dan H.261. H.264 dikenal juga sebagai MPEG-4 *Part* 10 atau MPEG-4 AVC (*Advanced Video Coding*).

Sedangkan berikut ini adalah standar *video coding* yang dikembangkan oleh *Motion Picture Experts Group* (MPEG) [CHI94]:

1. MPEG-1

MPEG-1 merupakan standar untuk *audio* dan *video coding* dengan tipe kompresi *lossy*. Standar ini didesain untuk kompresi video dengan kualitas VHS dan CD *audio*. Saat ini MPEG-1 telah menjadi standar *lossy audio*/*video coding* paling kompatibel di dunia dan banyak digunakan dalam produk-produk dan teknologi yang ada.

2. MPEG-2

MPEG-2 digunakan secara luas sebagai format TV digital. Standar *video coding* ini juga digunakan sebagai format film atau program lain yang didistribusikan melalui DVD.

3. MPEG-4

MPEG-4 merupakan kumpulan metoda-metoda yang mendefinisikan kompresi data *audio* dan visual (AV) digital. Penggunaan standar MPEG-4 ini termasuk kompresi data AV untuk *web* dan distribusi CD, suara (*telephone*, *videophone*) dan aplikasi TV *broadcast*.

4. MPEG-7

MPEG-7 adalah standar deskripsi *content* multimedia. Deskripsi ini akan diasosiasikan dengan *content*-nya untuk membuat pencarian menjadi cepat dan efisien. MPEG-7 disebut juga *Multimedia Content Description Interface*. Standar

ini tidak berurusan dengan *encoding* dari gambar bergerak dan audio seperti MPEG-1, MPEG-2 dan MPEG-4.

2.6 Celah Keamanan IP Video Telephony

Sistem VoIP memiliki beberapa potongan informasi yang harus di proteksi.Percakapan itu sendiri, voice mail, rekaman aktivitas telepon, dan nomor telepon adalah beberapa contoh dari informasi yang harus dapat dirahasiakan. Tetapi bagaimanapun juga ada masalah lain yang jauh lebih besar yang ada di dalam keamanan layanan VoIP, yaitu informasi telepon yang seharusnya rahasia, privat dan penting berada dalam jaringan internet berupa paket – paket data VoIP.

Bagaimana paket – paket data VoIP dapat begitu terbuka untuk keamanan datanya? Dalam system VoIP, data suara dikirimkan dari pengirim ke penerima menggunakan protocol RTP. Header dari paket RTP memiliki standar format, semua orang tahu bagaimana payload dapat di encoding dengan hanya melihat isi dari RTP payload.VoIP payload menggunakan standar codec seperti G.711 dan G.729. Paket RTP dapat di tangkap,direkonstruksi dan dimainkan ulang. Bahkan di dalam internet terdapat tool yang bernama Voice Over Misconfigured Internet Telephone (VOMIT) yang dapat menangkap paket RTP dan membuat suatu file dengan ekstensi .wav yang dapat dijalankan dalam computer dengan system operasi windows[4]. Jadi dapat kita simpulkan bahwa mendistribusikan paket VoIP di internet sangat riskan karena dapat ditangkap dan didengarkan.

VoIP juga sangat riskan terhadap penggunaan rogue server dan spoofing. Jika seorang hacker memasang rogue VoIP server atau gateway, maka telepon dapat dengan mudah dialihkan dan di tangkap. Sebagai tambahan, seorang hacker dapat mengubah IP nya menjadi IP phone yang valid dan menangkap telepon yang ditujukan untuk penerima yang sesungguhnya.

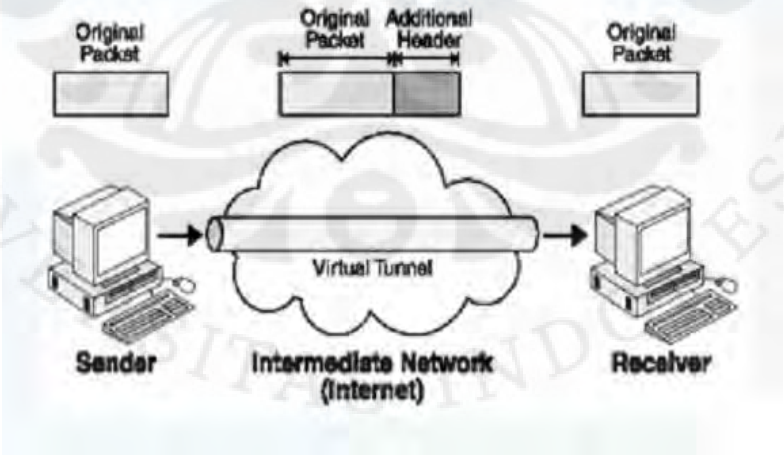
Mungkin area dari keamanan VoIP dan internet yang paling kurang diperhatikan adalah bahwa faktanya para penyerang melakukan berbagai cara untuk merusak system yang kita miliki dengan berbagai cara antara lain :

2.7 Virtual Private Network

2.7. 1 Pengertian VPN

2.7.1.1 Tunneling

Tunneling merupakan inti dari teknologi VPN.Tunneling merupakan suatu teknik untung melakukan enkapsulasi terhadap seluruh data pada suatu paket yang menggunakan suatu format protokol tertentu. Dengan kata lain, header dari suatu protokol tunneling ditambahkan pada header paket yang asli. Kemudian barulah paket tersebut dikirimkan ke dalam jaringan paket data.Ketika paket yang telah "ditunnel" dirutekan ke terminal tujuan. Maka paket – paket tersebut akan melewati suatu jalur logika yang dikenal dengan nama kanal. Ketika penerima menerima paket tersebut, maka akan dibuka dan dikembalikan lagi ke dalam format aslinya.

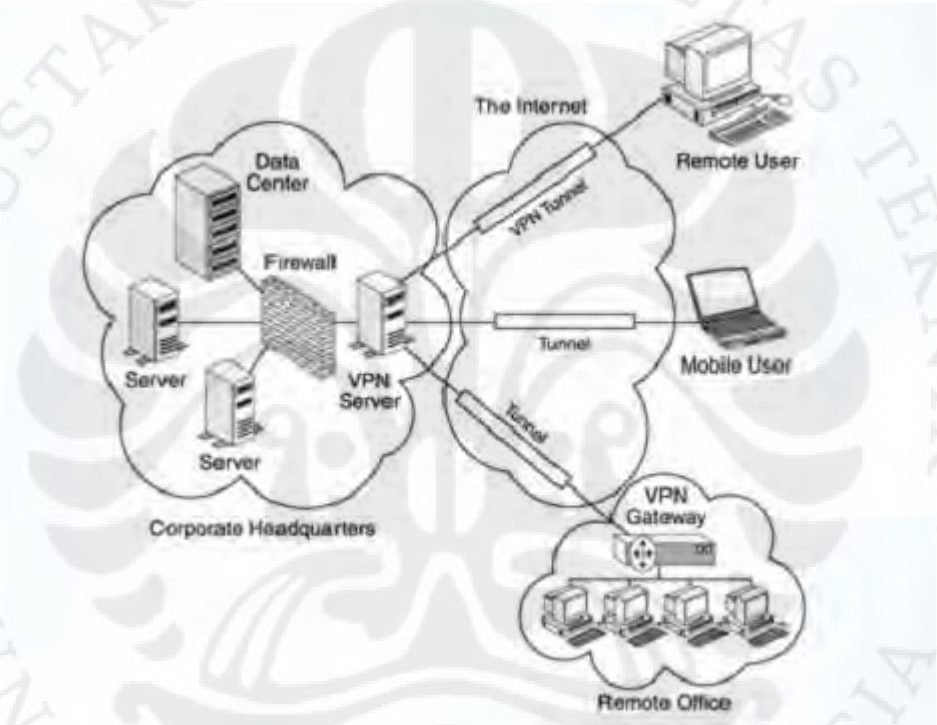


Gambar 2.3 Protocol stack untuk VPN tunneling[4]

2.7.1.2 Jenis Jaringan VPN

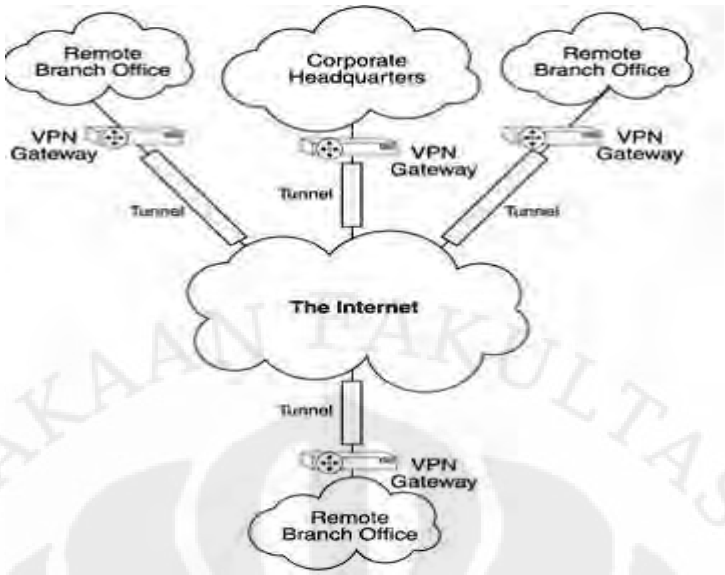
Ada 3 jenis jaringan VPN antara lain :

1. Access VPN – menyediakan remote access ke jaringan intranet atau extranet perusahaan yang memiliki kebijakan yang sama sebagai jaringan privat. Access VPN memungkinkan user untuk dapat mengakses data perusahaan kapanpun dimanapun dan bagaimanapun mereka mau.



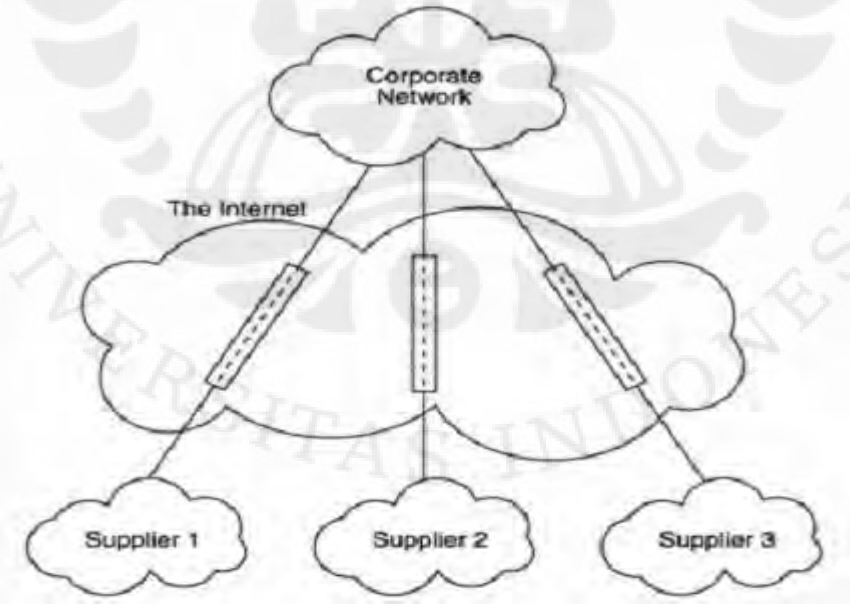
Gambar 2.4 Access VPN [4]

2. Intranet VPN - menghubungkan antara kantor pusat suatu perusahaan dengan kantor cabang, kantor pembantu melalui shared network menggunakan koneksi yang permanent (dedicated).



Gambar 2.5 Intranet VPN[4]

3. Extranet VPN – menghubungkan konsumen, suppliers, mitra bisnis atau berberapa komunitas dengan kepentingan yang sama ke jaringan intranet perusahaan melalui infrastruktur yang terbagi menggunakan koneksi permanent (dedicated).



Gambar 2.6 Extranet VPN[4]

2.7.2 Protokol Pada VPN

2.7.2.1 Point to Point Tunneling VPN

Point-to-Point Tunneling Protocol (PPTP) adalah suatu protokol jaringan yang memungkinkan pengiriman data secara aman dari remote client kepada server perusahaan swasta dengan membuat suatu virtual private network (VPN) melalui jaringan data berbasis TCP/IP.

Teknologi jaringan PPTP merupakan perluasan dari remote access Point-to-Point protocol yang telah dijelaskan dalam RFC 1171 yang berjudul "The Point-to-Point Protocol for the Transmission of Multi-Protocol Datagrams over Point-to-Point Links" . PPTP adalah suatu protokol jaringan yang membungkus paket PPP ke dalam IP datagram untuk transmisi yang dilakukan melalui internet atau jaringan publik berbasis TCP/IP.PPTP dapat juga digunakan pada jaringan LAN-to-LAN.

Protokol PPTP termasuk dalam sistem operasi server Windows NT versi 4.0 dan Windows NT Workstastion versi 4.0.Komputer menjalankan sistem operasi ini dapat dengan menggunakan protokol PPTP untuk koneksi ke jaringan private sebagai remote access client secara aman melalui jaringan publik data seperti internet. Dengan kata lain, PPTP digunakan sesuai dengan permintaan, misalnya dapat digunakan dengan VPN melalui internet atau jaringan publik data berbasis TCP/IP lainnya. PPTP juga dapat digunakan pada LAN untuk membuat VPN dalam LAN.

Fitur penting dalam penggunaan PPTP adalah PPTP mendukung VPN dengan menggunakan Public-Switched Telephone Networks (PSTNs). PPTP menyederhanakan dan mengurangi biaya dalam penggunaan pada perusahaan besar dan sebagai solusi untuk remote atau mobile users karena PPTP memberikan komunikasi yang aman dan terenkripsi melalui line public telephone dan internet.

Secara umum, terdapat tiga komponen di dalam komputer yang menggunakan PPTP yaitu

1. PPTP client
2. Network access server
3. PPTP server

Dimana PPTP juga adalah sebuah protokol yang mengizinkan hubungan Point-to Point Protocol (PPP) melewati jaringan IP, dengan membuat Virtual Private Network (VPN). Berikut adalah karakteristik dari PPTP VPN :

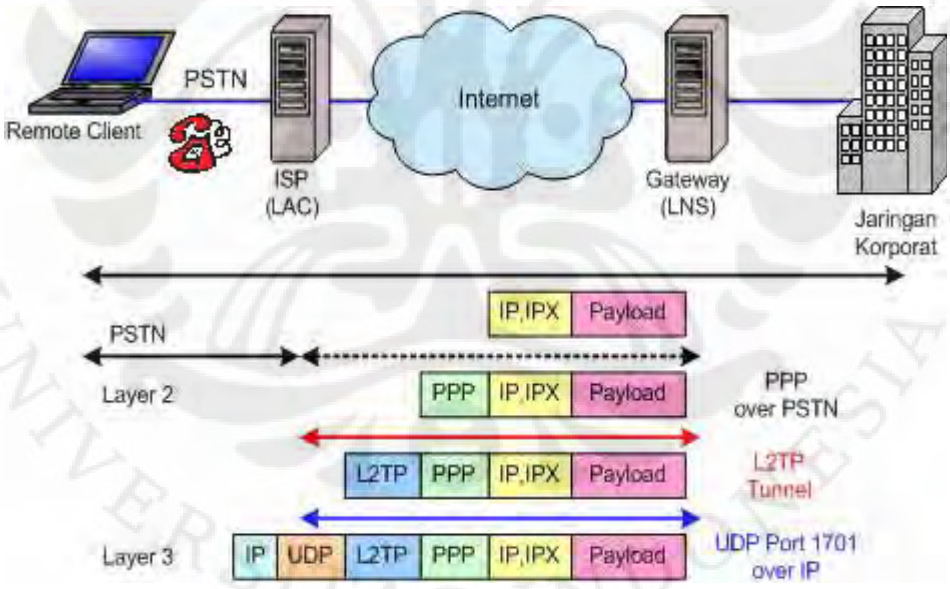
- algorima enkripsi (40bit - 128bit)
- cara kerja :
  1. Membuat enkapsulasi frame pada ip, ipx atau netbeui dalam sebuah Generic Routing Encapsulation (GRE)
  2. GRE dibungkus dalam sebuah paket IP untuk membuat tunnel data asli dienkripsi dengan MPPE (Microsoft Point to Point Encryption)
- kelemahan :
  session key (kunci akses yang digenerate server) diambil dari password user sehingga mudah dibobol.
- Keamanan melalui paket-2 enkripsi PPTP ini kurang aman dibanding dengan jenis protocol L2TP/IPSec.
- Tidak memerikan integritas data (yaitu semacam suatu bukti bahwa data tidak dimodifikasi selama dalam transit pengiriman)
- Tidak memberikan data authentikasi asli/asal (semacam bukti bahwa data dikirim oleh user yang authorized)
- Berdasarkan pada ektensi protocol Point-to-point (PPP)
- Mendukung enkripsi melalui enkripsi Microsoft Point-to-Point Encryption (MPPE)
- Menggunakan user-name dan password untuk authentication
- Pilihan yang bagus untuk kemampuan dasar VPN
- Protocol PPTP ini sudah ada beserta didalam semua client OS Windows modern
- Tidak memerlukan suatu public-key infrastructure (PKI)

2.7.2.2 Layer 2 Tunneling Protocol VPN

L2TP adalah tunneling protocol yang memadukan dua buah tunneling protokol yaitu L2F (Layer 2 Forwarding) milik cisco dan PPTP milik Microsoft. L2TP biasa digunakan dalam membuat Virtual Private Dial Network (VPDN) yang dapat bekerja membawa semua jenis protokol komunikasi didalamnya. Umunnya L2TP menggunakan port 1702 dengan protocol UDP untuk mengirimkan L2TP encapsulated PPP frames sebagai data yang di tunnel.

Terdapat dua model tunnel yang dikenal, yaitu compulsory dan voluntary. Perbedaan utama keduanya terletak pada endpoint tunnel-nya.Pada compulsory tunnel, ujung tunnel berada pada ISP, sedangkan pada voluntary ujung tunnel berada pada client remote.

Model Compulsory L2TP

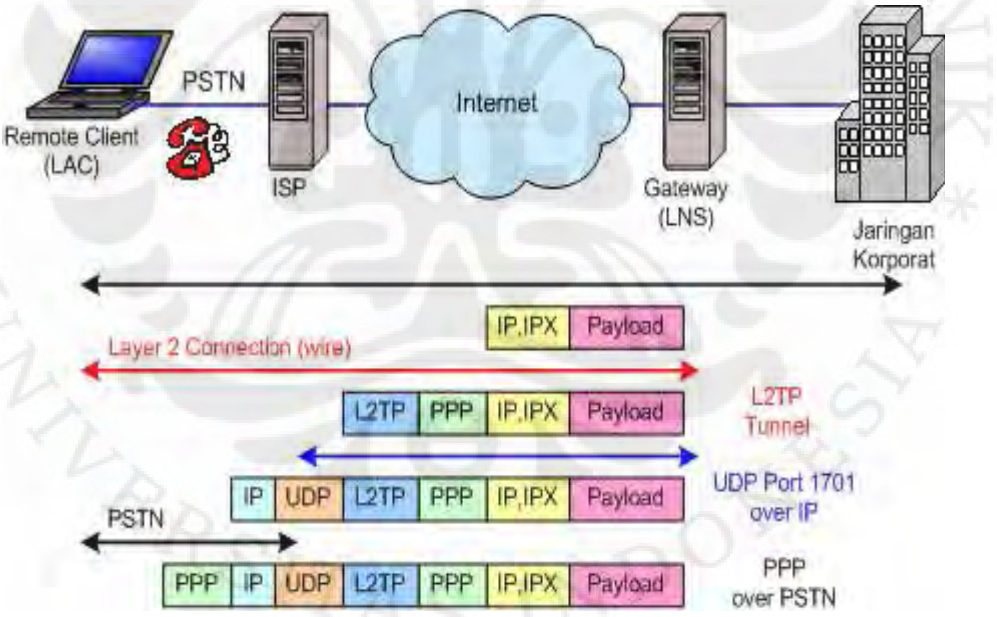


2.7 Model Compulsory L2TP [27]

1. *Remote client* memulai koneksi PPP ke LAC melalui PSTN. Pada gambar diatas LAC berada di ISP.
2. ISP menerima koneksi tersebut dan *link* PPP ditetapkan.

3. ISP melakukan *partial authentication* (pengesahan parsial)untuk mempelajari *user name*. D*atabase map user* untuk layanan-layanan dan *endpoint tunnel* LNS, dipelihara oleh ISP.
4. LAC kemudian menginisiasi *tunnel* L2TP ke LNS.
5. Jika LNS menerima koneksi, LAC kemudian mengencapsulasi PPP dengan L2TP, dan meneruskannya melalui *tunnel* yang tepat.
6. LNS menerima *frame-frame* tersebut, kemudian melepaskan L2TP, dan memprosesnya sebagai *frame incoming* PPP biasa.
7. LNS kemudian menggunakan pengesahan PPP untuk memvalidasi *user* dan kemudian menetapkan alamat IP.

Model Voluntary L2TP



2.8 Model Voluntary L2TP [27]

1. *Remote client* mempunyai koneksi *pre- established* ke ISP. Remote Client befungsi juga sebagai LAC.Dalam hal ini, *host* berisi *software client* LAC mempunyai suatu koneksi ke jaringan publik (internet) melalui ISP.

2. *Client* L2TP (LAC) menginisiasi *tunnel* L2TP ke LNS.
3. Jika LNS menerima koneksi, LAC kemudian meng-encapsulasi PPP dengan L2TP, dan meneruskannya melalui *tunnel*.
4. LNS menerima *frame-frame* tersebut, kemudian melepaskan L2TP, dan memprosesnya sebagai *frame incoming* PPP biasa.
5. LNS kemudian menggunakan pengesahan PPP untuk memvalidasi *user* dan kemudian menetapkan alamat IP.

Yang perlu kita ketahui bahwa L2TP murini hanya membentuk jaringan tunnel, oleh karena itu L2TP sering dikombinasi dengan IPSec sebagai metode enkripsi.

2.7.2.3 IP Security (IPSec)

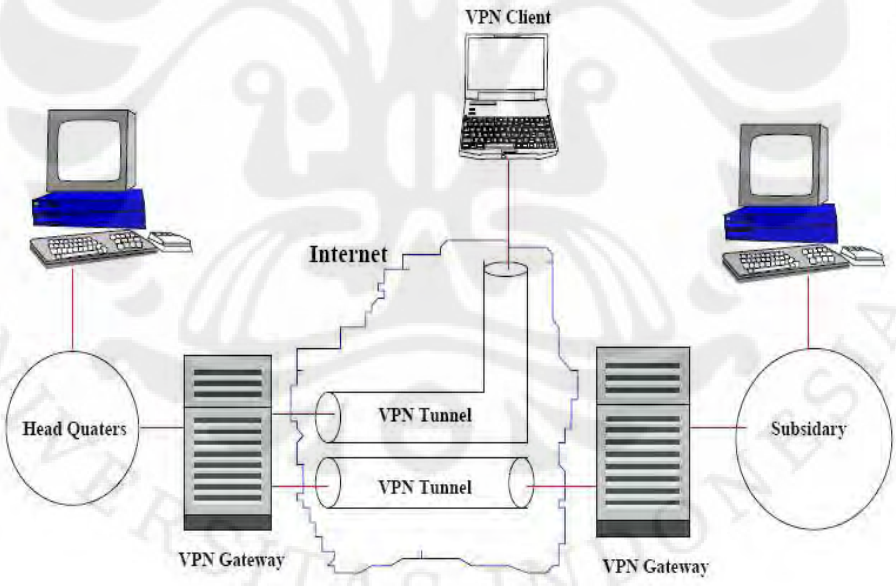
Ipsec merupakan tunneling protocol yang bekerja pada layer 3. IPSec menyediakan layanan sekuritas pada IPlayer dengan mengizinkan system untuk memilih protocol keamanan yang diperlukan, memperkirakan algoritma apa yang akan digunakan pada layanan, dan menempatkan kunci kriptografi yang diperlukan untuk menyediakan layanan yang diminta. IPSec menyediakan layanan-layanan keamanan tersebut dengan menggunakan sebuah metode pengamanan yang bernama Internet Key Exchange (IKE).IKE bertugas untuk menangani protokokl yang bernegosiasi dan algoritma pengamanan yang diciptakan berdasarkan dari policy yang diterapkan. Dan pada akhirnya IKE akan menghasilkan sebuah system enkripsi dan kunci pengamanannya yang akan digunakan untuk otentikasi yang digunakan pada system IPSec ini.

IPSec bekerja dengan tiga cara, yaitu:

1. Network-to-network
2. Host-to-network
3. Host-to-host

Contoh koneksi network-to-network, misalnya sebuah perusahaan yang memiliki banyak cabang dan ingin berbagi tau share data dengan aman, maka tiap cabang cukup menyediakan sebuah gateway dan kemudian data dikirim melalui infrastruktur jaringan internet yang telah ada. Lalu lintas data antara gateway disebut virtual tunnel.Kedua tunnel tersebut memverifikasi otentikasi pengirim dan penerima dan mengenkripsi sema lalu lintas.Namun lalu lintas di dalam sisi gateway tidak diamankan karena diasumsikan bahwa LAN merupakan segment jaringan yang dapat dipercaya.

Koneksi host-to-network, biasanya digunakan oleh seseorang yang menginginkan akses aman terhadap sumberdaya suatu perusahaan. Prinsipnya sama dengan kondisi network-to-network, hanya saja salah satu sisi gateway digantikan oleh client.



Gambar 2.9 Network-to-network dan Host-to-network[27]

Protokol yang berjalan dibelakang IPSec adalah:

1. AH (Authentication Header), menyediakan layanan authentication (menyatakan bahwa data yang dikirim berasal dari pengirim yang benar), intregrity (keaslian data), dan replay protection (transaksi hanya dilakukan sekali, kecuali yang berwenang telah mengizinkan), juga melakukan pengamanan terhadap IP header (header compression).
2. ESP (Encapsulated Security Payload), menyediakan layanan authentication, intregity, replay protection, dan confidentiality (keamanan terjaga) terhadap data. ESP melakukan pengamanan data terhadap segala sesuatu dalam paket data setelah header.

Kelebihan mengapa IPSec menjadi standar, yaitu:

1. Mengenkripsi trafik
2. Menvalidasi integritas data
3. Otentikasi
4. Anti-replay

BAB III

IP VIDEO TELEPHONY OVER REMOTE ACCESS VPN

3.1 Spesifikasi dan Perancangan Sistem

Telah dijelaskan dalam bab II tentang dasar teori yang mendukung pembuatan Tugas akhir ini. Pada bab III akan dijelaskan dengan lebih spesifik mengenai rancangan pemodelan sistem yang dibuat, *tools* yang digunakan, input yang dimasukkan serta output yang diinginkan. Topologi jaringan yang di buat disesuaikan agar dapat mendukung pengukuran terhadap aplikasi Video Telephony over Internet Protocol pada Jaringan Remote Access VPN.

3.1.1. Kebutuhan Hardware

Dalam pembuatan tugas akhir ini sistem yangingin dibangun berupa suatu jaringan komputer dengan menggunakan :

1. 2 buah Komputer PC yang berfungsi sebagai
   a. 1 buah komputer sebagai Vyatta VPN Router
   b. 1 buah komputer sebagai VoIP Server
2. 2 buah Notebook yang berfungsi sebagai
   a. 1 buah notebook sebagai User Agent Client
   b. 1 buah notebook sebagai User Agent Server
3. 2 buah Switch yang berfungsi sebagai
   a. 1 buah switch sebagai Private Network Switch
   b. 1 buah switch sebagai Public Network Switch
4. 1 buah Linksys Wireless Access Point
5. Kabel UTP tipe 5 dengan RJ-45
6. Kabel Console Serial to USB
7. Headset
8. Webcam

3.1.2 Kebutuhan Software

Software yang digunakan untuk merealisasikan sistem ini antara lain :

3.1.2.1 Vyatta OS Router

Vyatta adalah sistem operasi yang berfungsi sebagai router untuk mengatur jaringan di dalam sebuah gedung atau fasilitas yang berhubungan dengan jaringan, yaitu adanya aktivitas Server dan Client dalam melakukan transaksi data secara digital. Vyatta telah mengubah dunia networking dengan mendistribusikan router, firewall dan VPN sebagai komoditi dengan cara yang sama seperti Komoditi Linux memasarkan Sistem Operasinya.

Setiap bulannya lebih dari 10.000 user di seluruh dunia telah beralih ke Vyatta open-source, sebagai alternatif untuk menekan harga yang tidak fleksibel dari vendor.Vyatta ini bisa di download secara gratis di Vyatta.com.Versi Router Vyatta yang digunakan pada skripsi ini ialah versi 6.0 Community Edition.

3.1.2.2 Wireshark

Wireshark merupakan software yang digunakan untuk melakukan analisa jaringan computer. Wireshark dapat menganalisa beberapa parameter QoS seperti jitter, delay, throughput, dan packet loss serta dapat mengcapture protocol yang sedang berjalan dalam jaringan tersebut, versi wireshark yang digunakan untuk pengujian adalah wireshark 1.22 dan dapat diunduh secara gratis pada website www.wireshark.org.

3.1.2.3 Trixbox

Trixbox merupakan suatu PBX (Private Branch Exchange) virtual pengembangan dari Asterisk yang menghubungkan antara satu telepon lainnya.Sebagai PBX trixbox juga dapat berhubungan dengan PSTN (Publik Switch Telecomunication Network) analog seperti sentral POTS.Trixbox memiliki beberapa fitur yang sama seperti PBX analog yaitu call waiting, call return (*69), distinctive ring, transferring calls, call forwarding. Selain sebagai PBX, Trixboxjuga dapat bertindak sebagai VoIP server. Trixbox dapat

memproses panggilan VoIP dari IP phone/softphone dan meneruskannya ke IP phone/softphone tujuan. Trixbox mendukung protocol dalam VoIP diantaranya SIP,H 323 serta IAX yang dibuat dengan tujuan untuk menutupi kelemahan kedua protokol sebelumnya.

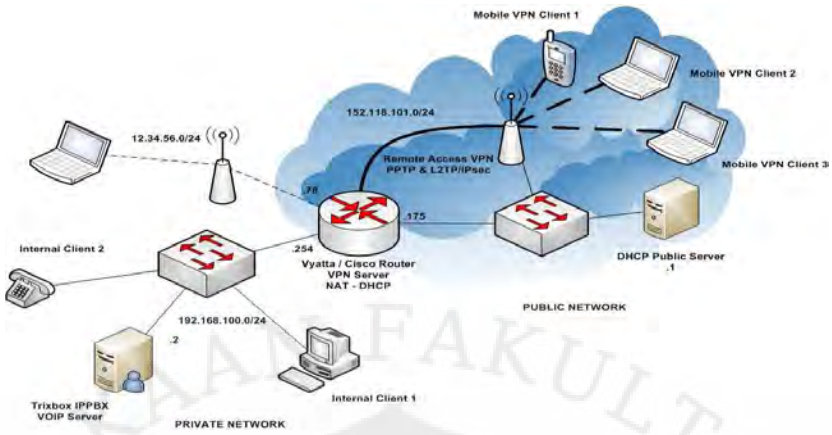
Sebagai VoIP server trixbox bertindak sebagai Registration server, Proxy server, dan redirect server dalam protokol SIP. Keuntungan dari Trixbox lainnya adalah dia dapat bertindak sebagai Gateway untuk interkoneksi antara jaringan VoIP yang berbasiskan packet switch dan Jaringan PSTN yang bersifat circuit switch.

3.1.2.4 EyeBeam Softphone

EyeBeam merupakan softphone yang berfungsi sebagai User Agen Client dan User Agent Server pada protokol SIP.EyeBeam digunakan karena memiliki beberapa kelebihan.Selain mendukung protokol SIP dan H323, EyeBeam juga mendukung berbagai jenis kompresi Codec, video conference, metode keamanan SRTP dan TLS.

3.2 Permodelan Sistem

Model topologi jaringan yang digunakan pada pengujian untuk skripsi ini terdiri dari beberapa perangkat yang saling terhubung satu sama lain di Departemen Teknik Elektro Universitas Indonesia yang diasumsikan mewakili *Campus Network*dan dikombinasikan dengan jaringan privat yang di implementasikan di Laboratorium Jaringan. Berdasarkan sumber dari administrator jaringan di Departemen Teknik Elektro diketahui bahwa jaringan uji mempunyai besaran bandwith yang transparant sesuai dengan proxy 152.118.101.8. Besarnya bandwith transparant tersebut sebanyak 25 Mbps yang dibagi ke lima departemen di Universitas Indonesia dan salah satunya ialah Departemen Teknik Elektro. Prinsip yang digunakan dalam membagi bandwith tersebut ialah secara best-effort.Selain itu kondisi trafik di jaringan Elektro cukup padat pada siang hari. Oleh karena itu percobaan ini dilakukan pada siang hari dengan skema jaringannya seperti pada gambar berikut :



Gambar 3.1 Topologi Pengujian

Tabel 3.1 Spesifikasi Jaringan Sistem Video Telephony

No	Nama Perangkat	Network Interface	Alamat IP / Netmask	Operating System
1	Mobile VoIP Client 1	Wireless	152.118.101.x /24	Windows XP
2	Mobile VoIP Client 2	Wireless	152.118.101.x /24	Windows XP
3	Vyatta Router	Eth1	192.168.100.254/24	Vyatta 6.0
		Eth2	152.118.101.175/24	
5	VoIP Server	Eth1	192.168.100.2/24	Trixbox 2.6

Mobile VoIP Client 1 dan 2 dibuat seakan-akan sedang dalam keadaan mobile dengan akses ke jaringannya melalui wireless dan menggunakan ip public yang didapat secara DHCP dengan terhubung di jaringan Departemen Teknik Elektro Universitas Indonesia. Agar dapat mengakses VoIP Server, User Agent yang diwakili oleh Mobile VoIP Client harus mengaktifkan koneksi Remote Access VPN baik dengan protokol PPTP ataupun L2TP/IPsec VPN. Penerapan VPN ini dikombinasikan dengan penerapan NAT sehingga sistem jaringan yang diterapkan untuk internal network dimana VoIP server berada berupa jaringan privat. Hal ini dilakukan agar seolah-olah mewakili keadaan jaringan yang sesungguhnya karena saat ini sebagian besar komputer berada di jaringan privat dan memerlukan NAT untuk dapat berkomunikasi ke jaringan internet ataupun

sebaliknya yakni mobile user agent berada dalam jaringan public yang memerlukan NAT untuk mengakses VoIP server di jaringan privat.

3.3 Implementasi Sistem

Rencana implementasi merupakan tahap awal dari penerapan sistem yang baru dirancang.Implementasi sistem Video Call over Remote Access VPN ini bertujuan agar sistem tersebut dapat beroperasi dan berjalan sesuai dengan yang diharapkan.

3.3.1 Pemilihan Komponen Video Telephony

Beberapa komponen yang diperlukan untuk membuat sistem ini agar dapat berfungsi atau dapat berjalan antara lain :

- User Agent
- Proxy Server
- Protocol

3.3.1.1 User Agent

Komponen ini berfungsi untuk memulai, menerima, dan menutup sesi komunikasi. User agent terdiri dari 2 komponen utama, yaitu :

1. User Agent Client (UAC). Komponen ini yang mempunyai tugas untuk memulai sesi komunikasi.
2. User Agent Server (UAS). Komponen ini yang mempunyai tugas untuk menanggapi atau menerima sesi komunikasi.

User agent yang dipakai dalam perancangan sistem ini berupa perangkat lunak telepon (softphone) bukan berupa handphone seperti IP Phone, USB Phone, maupun ATA.Beberapa softphone yang mendukung SIP antara lain EyeBeam, Kphone, Linphone, dan X-lite.EyeBeam softphone yang dipilih dalam perancangan sistem Video Call ini.

3.3.1.2 Proxy Server, Redirect Serverdan Registration Server

Proxy Server adalah media penghubung yang dirancang untuk melayani jaringan computer local untuk melakukan koneksi ke layanan jaringan yang lain atau ke internet. Proxy berfungsi untuk meningkatkan kinerja dari jaringan computer local, karena proxy server dapat menyimpan hasil dari semua permintaan user pada sejumlah waktu tertentu. Cara kerja komponen ini yaitu request message yang diterima dari user agent dapat dilayani sendiri ataupun disampaikan pada proxy atau server lain. Menerjemahkan atau menulis ulang request message sebelum menyampaikan pada user agent tujuan atau proxy lain. Proxy server menyimpan pernyataan sesi komunikasi antara UAC dan UAS.

Redirect Server merupakan komponen yang menerima request message dari user agent, memetakan alamat SIP user agent atau proxy tujuan kemudian menyampaikan hasil pemetaan kepada user agent pengirim (UAC). Redirect Server tidak menyimpan pernyataan sesi komunikasi antara UAC dan UAS setelah pemetaan disampaikan pada UAC dan juga tidak dapat memulai inisiasi request message. Redirect Server berbeda dengan UAS, dimana komponen ini tidak dapat menerima dan menutup sesi komunikasi.

Registrat Server dapat menambahkan fungsi otentikasi user untuk validasi.Registrat menyimpan database user untuk otentikasi dan lokasi sebenarnya berupa IP dan port agar user yang terdaftar dapat dihubungi oleh komponen SIP lainnya.Para perancangan sistem Video Telephony pada jaringan Remote Access VPN ini Trixbox IPPBX berperan sebagai Proxy Server, Redirect Server, dan Registrat Server sekaligus.

3.3.2 Pemilihan Codec

Saat ini terdapat cukup banyak video yang voice codec yang berkembang.Diantaranya standar G.711, GSM, G.722, G.729, dan Speex untuk audio codec, sedangkan untuk video codec telah ada standar H.263 dan H.264.Masing-masing dari voice maupun video codec tersebut mempunyai nilai bitrate dan MOS (tingkat kualitas) yang berbeda-beda.Untuk itu perlu dilakukan

suatu mekanisme pemilihan codec yang tepat dan sesuai untuk diterapkan dalam sistem jaringan yang dibangun.

Dalam implementasi sistem ini, kombinasi video dan voice ini akan digunakan dua buah video codec yakni H.263 dan H.264 yang mewakili medium dan high quality video, sedangkan untuk voice codecnya akan digunakan standar G.711, G.729 dan GSM yang mewakili beberapa variasi bitrate dan tingkat kepercayaan. Kombinasi video dan voice codec tersebut dapat dilihat pada tabel berikut :

Tabel 3.2 Video dan Voice Codec IP Video Telephony

Video Codec	Voice Codec
H.263	G.711
	G.729
	GSM
H.264	G.711
	G.729
	GSM

Pada tahap ini akan dikombinasikan video dan voice codec pada implementasi video telephony yang disesuaikan dengan teori dengan pengujian QoS parameter seperti troughput, delay, jitter, dan packet loss.Pengujian terhadap kombinasi video dan voice pada jaringan Remote Access VPN menggunakan protocol PPTP dan L2TP/IPsec VPN.

3.3.3 Implementasi VPN Server

VPN Server yang akan digunakan pada implementasi ini ialah Vyatta Router. Pada tahap ini router tersebut akan dikonfigurasi sebagai Remote Access VPN Server dengan penambahan beberapa konfigurasi lainnya agar jaringan yang diimplemntasikan mewakili keadaan yang sesungguhnya. Adapun rincian konfigurasinya ialah sebagai berikut :

a. Konfigurasi 2 Protocol Remote Access VPN yang digunakan yakni PPTP dan L2TP/IPsec VPN dengan skema virtual addressnya 192.168.1.0/24 untuk PPTP, sedangkan virtual address untuk L2TP/IPSec VPN adalah 192.168.2.0/24. Interface yang digunakan adalah interface Ethernet yang terhubung dengan jaringan di Departemen Teknik Elektro Universitas Indonesia dengan alamat IP nya 152.118.101.175/24.
b. Konfigurasi interface Ethernet LAN sebagai gateway jaringan privat dengan alamat 192.168.100.254/24.
c. Konfigurasi NAT yang berupa Port Address Translation (PAT) pada interface Ethernet WAN Router dengan alamat IP 152.118.101.175/24 yang menghubungkan jaringan public yang beralamatkan 152.118.101.0/24 dengan jaringan privat yang beralamatkan 192.168.100.0/24.

3.3.4 Implementasi Video Telephony Server

Seperti yang telah dijelaskan pada bagian 3.3.1, pada implementasi ini akan digunakan Trixbox sebagai Video Telephony Server. Dengan spesifikasi dan konfigurasi perangkat sebagai berikut :

Sistem Operasi : Trixbox IPPBX Server 2.6.8

Processor : Intel Pentium 4 1,8GHz

Memory : 512 MB

Ethernet : D-Link System Inc RTL8139

IP Address : 192.168.100.2

Pada implementasi ini telah dibuat 7 SIP dengan kemampuan menggunakan Video Codec H.263 dan H.264 serta Voice Codec G.711, G.729, dan GSM. Hal ini dapat diatur pada PBX config file editor dibagian sip_addition.conf dengan konfigurasi sebagai berikut :

[00x]

deny=0.0.0.0/0.0.0.0

type=friend

secret=netlab

qualify=yes

port=5060

pickupgroup=

permit=0.0.0.0/0.0.0.0

nat=yes

mailbox=001@device

host=dynamic

dtmfmode=rfc2833

dial=SIP/001

context=from-internal

canreinvite=no

callgroup=

callerid=device <001>

accountcode=

call-limit=50

videosupport=yes

disallow=all

allow=gsm

allow=ilbc

allow=ulaw

allow=h261

allow=h263

allow=h263p

allow=h264

allow=h264p

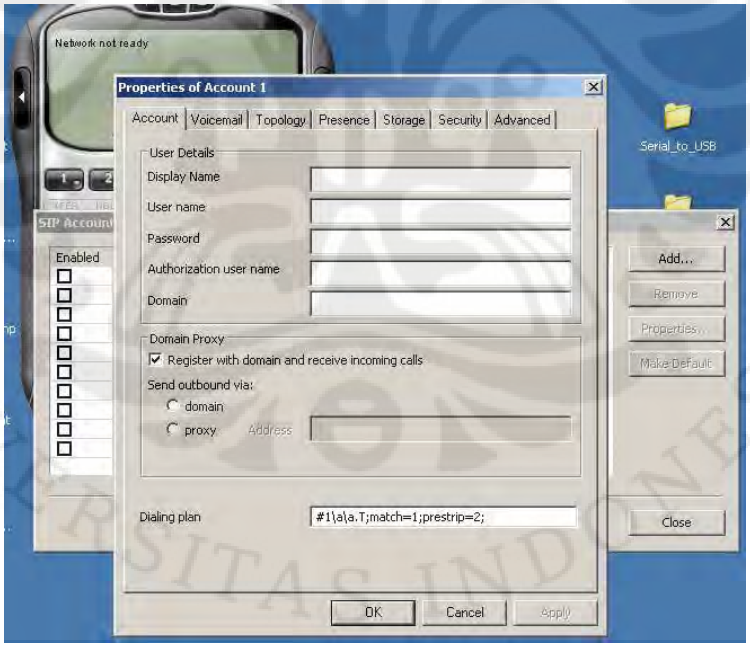
allow=g729

3.3.5 Implementasi Remote Access VPN Client

Pada simulasi ini akan diaktifkan dua Remote Access VPN yaitu PPTP dan L2TP/IPsec VPN dengan menggunakan sistem operasi Windows XP. Sebelum dapat terkoneksi secara VPN, Remote Acess VPN Client harus terlebih dahulu terkoneksi ke jaringan wireless di Departemen Teknik Elektro Universitas Indonesia yang dalam hal ini diumpamakan sebagai jaringan publik.

3.3.6 Implementasi EyeBeam Pada User Agent

Ketika pertama kali dijalankan maka tampilan X-lite sedikit tidaknya akantampak seperti di bawah ini. Karena belum ada accont yang aktif maka kita dapat menambah dengan menekan tombol add.



Gambar 3.2 Create VoIP Account Profile on EyeBeam

Akan ada beberapa kotak yang harus diisi diantaranya Display name, username,password, authentication user dan domain. Untuk username serta password harus sesuai dengan data pada SIP server yakni trixbox, sedangkan

untuk domain adalah ip address dari Server VoIP. Setelah selesai maka layer tersebut dapat ditutup dan X-lite akan meregistrasikan user name tersebut ke SIP Server. Setelah user terdaftar maka dapat melakukan panggilan ke pc lain.

Konfigurasi EyeBeam

VoIP client 1	VoIP client 2
Display name : ardisragen	Display name : alfa
User name : 001	User name : 002
Password : netlab	Password : netlab
Authorization user name : 001	Authorization user name : 002
Domanin : 192.168.100.2	Domain :192.168.100.2

3.4 Perancangan Skenario

Setelah semua yang diperlukan untuk membangun sistem Video Telephony selesai, maka ada beberapa skenario yang akan dilakukan untuk melakukan pengujian terhadap kinerja dari jaringan Video Telephony over Remote Access VPN. Adapun skenario pengujian ini dilakukan pada siang hari yang diasumsikan sebagai kondisi *high traffic*di Departemen Teknik Elektro Universitas Indonesia.

1. Skenario Pertama

   Pada skenario ujicoba petama dilakukan komunikasi video telephony oleh dua pengguna yang terhubung pada jaringan publik dengan menggunakan koneksi nirkabel.Dua orang pengguna tersebut berperan sebagai *user agent,* salah satunya sebagai *user agent client* dan lainnya berperan sebagai *user agent server.User agent* meminta layanan video telephony dengan menggunakan perangkat lunak EyeBeam yang telah terlebih dikonfigurasi terlebih dahulu.

Video dan voice codec yang dijalankan bervariasi mulai dari pasangan video codec H.263 dengan voice codec G.711, G.729, dan GSM Masing-masing pasangan codec tersebut diambil data parameter QoS seperti delay, troughput, jitter, dan packet loss sebanyak 5 kali percobaan. Pada percobaan ini juga diambil sampel bahwa komunikasi video telephony tanpa enkripsi akan dapat direkam dan diputar ulang percakapannya.

2. Skenario Kedua

Pada skenario ujicoba kedua sama halnya dengan ujicoba pertama, yang menjadi perbedaanya ialah pasangan video diganti dengan kombinasi Video Codec H.264 dengan Voice Codec G.711, G.729, dan GSM.

3. Skenario Ketiga

Pada skenario ujicoba ketigasama halnya dengan ujicoba pertama dan kedua, yang menjadi perbedaan ialah sebelum pengguna dapat terhubung dengan video telephony server, pengguna diharuskan terlebih dahulu terhubung melalui Remote Access VPN dengan protocol PPTP ataupun L2TP/IPsec pada Vyatta VPN Router. Percobaan pada skenario kedua ini diambil datanya sebagai 5 kali untuk masing-masing protocol VPN yang digunakan.Dari percobaan skenario pertama dan kedua kemudian disimpulkan kombinasi pasangan video codec terbaik yang dapat diterapkan dan data sementara mengenai pengaruh implementasi Remote Access VPN pada Video Telephony.

4. Skenario Ke Empat

Setelah diketahui kinerja IP Video Telephony baik tanpa VPN maupun dengan implementasi PPTP dan L2TP/IPsec VPN serta diketahui kebutuhan bandwithnya berdasarkan perhitungan, kemudian akan dilakukan pengukuran subjektif ujicoba IP Video Telephony menggunakan video dan voice codec serta protocol VPN yang paling efisien dengan melakukan kuisioner.

Secara lebih singkat, alur skenario pengujian secara berurut seperti pada tabel berikut :

Tabel 3.3 Skenario Pengujian

No	Nama Skenario	Video Codec	Voice Codec	VPN Protocol
1	NonH263G711	H.263	G.711	-
2	NonH263G729	H.263	G.729	-
3	NonH263GSM	H.263	GSM	-
4	NonH264G711	H.264	G.711	-
5	NonH264G729	H.264	G.729	-
6	NonH264GSM	H.264	GSM	-
7	PPTPH263G711	H.263	G.711	PPTP
8	PPTPH263G729	H.263	G.729	PPTP
9	PPTPH263GSM	H.263	GSM	PPTP
10	PPTPH264G711	H.264	G.711	PPTP
11	PPTPH264G729	H.264	G.729	PPTP
12	PPTPH264GSM	H.264	GSM	PPTP
13	L2TPH263G711	H.263	G.711	L2TP
14	L2TPH263G729	H.263	G.729	L2TP
15	L2TPH263GSM	H.263	GSM	L2TP
16	L2TPH264G711	H.264	G.711	L2TP
17	L2TPH264G729	H.264	G.729	L2TP
18	L2TPH264GSM	H.264	GSM	L2TP
19*	H263G729PPTP	H.263	G.729	PPTP

** ujicoba kualitas video*

4.5 Hipotesa

Berdasarkan beberapa daftar acuan, dinyatakan bahwa diperlukan suatu keamanan pada komunikasi *Video Telephony over Internet Protocol*, terutama untuk sambungan komunikasi yang berasal dari jaringan publik yang ingin terhubungan ke jaringan internal. Implementasi *Remote Access VPN* dapat dilakukan untuk memberikan keamanan sambungan komunikasi ini, namun tentunya implementasi VPN akan berpengaruh terhadap QoS dari layanan *Video Telephony over Internet Protocol*. Pengaruh implementasi VPN tersebut tentunya

bermacam-macam sesuai dengan karakteristik protokol VPN yang diterapkan. Ahmed A. Joha di dalam *paper*nya yang melakukan ujicoba pengiriman paket TCP menyimpulkan perbandingan PPTP dan L2TP/IPSec terhadap beberapa parameter QoS seperti terlihat pada tabel berikut :

Tabel 3.4 Hipotesa Parameter QoS

No	Parameter	PPTP	L2TP/IPSec
1	TCP Throughput	1st	2nd
2	Round Trip Time	1st	2nd
3	UDP Throughput	1st	2nd
4	Jitter	Low	High
5	Packet Loss	Low	Low

Dari tabel diatas terlihat kinerja beberapa parameter QoS seperti *troughput* dan*jitter*pada PPTP VPN lebih baik dibandingkan dengan L2TP/IPsec VPN sedangkan untuk *packet loss* pada PPTP dan L2TP/IPsec VPN sama-sama rendah.Kemudian yang menjadi pertanyaan apakah PPTP dan L2TP/IPSec VPN akan menghasilkan pengaruh yang sama terhadap kinerja dari protokol RTP pada IP Video Telephony. Percobaan ini akan menguji pengaruh implementasi PPTP dan L2TP/IPsec VPN terhadap packet QoS dari paket RTP dengan aplikasi Video Telephony.

BAB IV

PENGUJIAN DAN ANALISA SISTEM

4.1 Pengujian Sistem

Seperti yang telah dijelaskan pada bab sebelumnya bahwa terdapat beberapaskenario yang akan dijalankan. Dari skenario tersebut akan dianalisis performansi, keamanan serta perubahan sebelum dan sesudah ditambahkan aplikasi Remote Access VPN. Untuk membantu analisis performansi dan keamanan, maka akan digunakan alat bantu Wireshark. Software ini akan menangkap semua paket yang lewat dan melakukan analisis keamanan terhadap data VoIP, data VoIP yang lewat dapat direkam dan dimainkan ulang. Selain itu Wiresharkjuga digunakan untuk merekam data yang lewat untuk kemudian dianalisis kinerjanya dengan menghitung delay, jitter, packet loss. Data yang akan dianalisis adalah data dengan paket RTP.

Pada call setup VoIP client 1 akan malakukan panggilan ke VoIP client 2. Wireshak akan digunakan untuk menangkap paket yang lewat di jaringan dan akan digunakan untuk merekam paket VoIP yang lewat dan mereplay hasil rekaman tersebut. Codec yang akan digunakan sebagai percobaan ada 2 jenis yakni video codec H.263 dan H.264 serta 3 voice codec yakni G.711, G.729, dan GSM. Pada bab sebelumnya telah disebutkan bahwa ada 3 skenario yang akan dijalankan. Untuk skenario pertama akan di lakukan call setup dari client 1 ke client 2 dengan menggunakan masing – masing codec tanpa adanya VPN, kemudian dilanjutkan dengan skenario kedua dan ketiga yang dilakukan penerapan PPTP dan L2TP/IPsec VPN. Analisis kinerjaakan dilakukan untuk kinerja untuk masing – masing codec baik sebelum diterapkan maupun setelah diterapkan VPN.

4.2 Pengukuran dan Analisis Kinerja Codec

Pengukuran dan Pengujian terhadap performansi codec meliputi delay, jitter dan packet loss. Untuk skenario telah dijelaskan pada bab III.

4.2.1 Skenario Pengukuran dan Analisis Delay

4.2.1.1 Skenario Pengukuran Delay

Delay merupakan waktu yang diperlukan oleh paket dari terminal pengirim hingga sampai ke terminal penerima. Delay merupakan parameter penting untuk menentukan kualitas jaringan VoIP. Berdasarkan standar dari ITU-T G.104 untukkualitas VoIP yang baik, delay harus < 150 ms agar tidak terjadi overlap pada komunikasi.

Pada percobaan pertama (tanpa vpn) call setup dilakukan dari client 1 ke client 2. kemudian paket yang lewat akan ditangkap pada client. Digunakan Wireshark untuk menangkap paket yang masuk ke client.Dari hasil pengolahan data didapatkan data delay video telephony tanpa vpn seperti pada tabel berikut :

Tabel 4.1 Delay Jaringan IP Video Telephony tanpa VPN

No	Video Codec	Voice Codec	Video Delay Jaringan (ms)	Voice Delay Jaringan (ms)
1	H.263	G.711	50.84	20.20
2		G.729	54.55	19.99
3		GSM	50.86	20.11
4	H.264	G.711	71.21	20.13
5		G.729	71.34	20.11
6		GSM	72.05	20.24

Dari tabel diatas diketahui bahwa delay yang paling besar dimiliki oleh codec audio G.711 dengan kombinasi codec video apapun. Hal ini disebabkan karena G.711 memiliki payload yang paling besar yaitu 214 bytes. Perlu diperhatikan bahwa semakin besar payload, maka delay paketisasi, routing,

,transmisi dan switching akan semakin besar[7]. Sedangkan untuk codec video delay jaringan yang paling besar terjadi pada H.264 karena payload nya sangat besar yakni 1.25 Mbytes, jauh lebih besar dari H.263 yang hanya sebesar 561 bytes

Proses yang sama juga dilakukan pada jaringan yang diimplementasikan remote access VPN baik dengan protokol PPTP VPN maupun L2TP/IPsec VPN. Hasil pengolahan datanya terlihat pada tabel berikut ini :

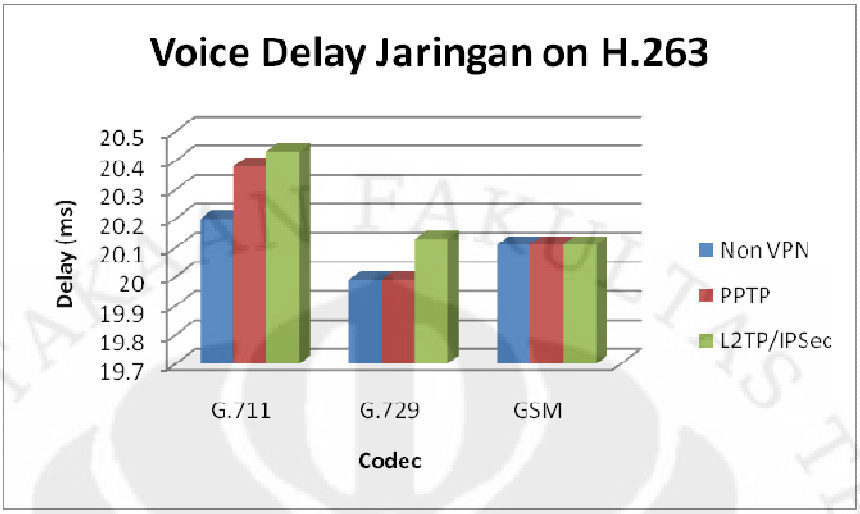
Tabel 4.2 Delay Jaringan IP Video Telephony dengan PPTP VPN

No	Video Codec	Voice Codec	Video Delay Jaringan (ms)	Voice Delay Jaringan (ms)
1	H.263	G.711	49.07	20.38
2		G.729	51.16	19.99
3		GSM	45.80	20.11
4	H.264	G.711	69.67	20.13
5		G.729	69.70	20.11
6		GSM	70.68	20.17

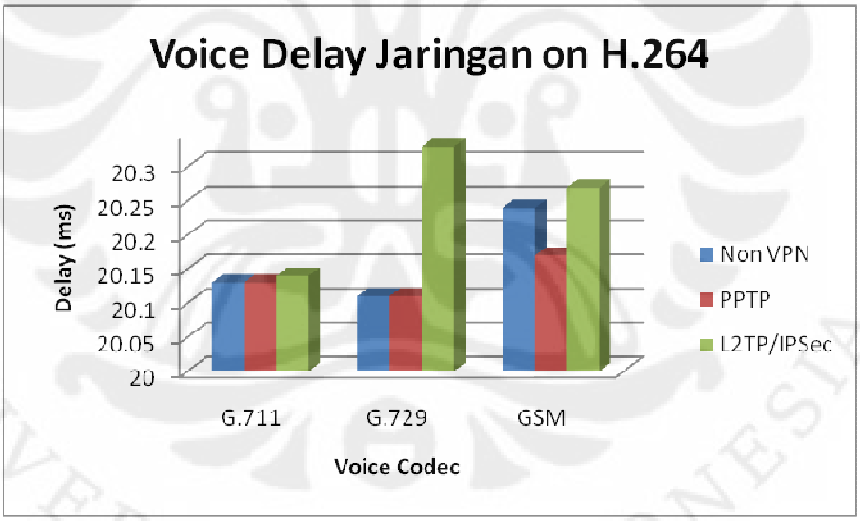
Tabel 4.3 Delay Jaringan IP Video Telephony dengan L2TP/IPsec VPN

No	Video Codec	Voice Codec	Video Delay Jaringan (ms)	Voice Delay Jaringan (ms)
1	H.263	G.711	58.64	20.43
2		G.729	56.22	20.13
3		GSM	53.98	20.11
4	H.264	G.711	72.04	20.14
5		G.729	72.67	20.33
6		GSM	72.65	20.27

Secara ringkas hasil percobaan mengenai delay jaringan terlihat seperti pada grafik berikut



Grafik 4.1 Voice Delay Jaringan on H.263



Grafik 4.2 Voice Delay Jaringan on H.264

Dari grafik didapat suatu gambar bawah ketika diimplementasikan PPTP VPN delay jaringan dari paket suaranya lebih kecil dibandingkan dengan L2TP/IPSec VPN meskipun pada video codec H.263 codec suara GSM menunjukkan hasil yang sama. Hal demikian itu terjadi karena pada implementasi L2TP/IPsec VPN diterapkan enkripsi berupa Pre-Shared Key untuk authentikasi IPsec.

Dari seluruh data delay jaringan yang ada, kemudian akan dihitung delay keseluruhan sesuai dengan standar ITU-T, begitu pula dengan data jitter, packet loss, dan throughput , namun dalam skripsi ini pengukuran dan perhitungan kualitas objektif dibatasi hanya suaranya saja karena untuk pengukuran kualitas video akan dilakukan secara pengukuran subjektif disesuaikan dengan standar ITU-R 500.

4.2.1.2 Pengukuran Delay Total

Dalam teknologi VoIP, parameter delay disebabkan oleh beberapa komponen delay yang secara garis besar yaitu delay coder (processing), delay packetization,dandelay network.

- Code (Processing Delay)

  Code (Processing) = (Waktu Kompresi) + (Waktu Dekompresi) + (Algoritma Delay) [1]

  - Untuk G.711 :

    Waktu kompresi = 0 x frame size + look ahead
    = 0 x 0,125 ms + 0 ms
    = 0,375 ms

    Waktu dekompresi = 10 % x waktu kompresi[26]
    = 0,1 x 0,375 = 0,0375 ms

    Algorithmic delay (G.711) = 0 ms

    Jadi, Coder (Processing) Delay = 0.4125 ms

  - Untuk GSM:

    Waktu kompresi = 20 ms

    Waktu dekompresi = 10 % x waktu kompresi
    = 2 ms

    Algorithmic delay (GSM) = 7,5 ms

    Jadi, Coder (Processing) Delay = 29,5 ms

- Untuk G.729 :

  Waktu kompresi = 10 ms

  Waktu dekompresi = 10 % x waktu kompresi

  = 1 ms

  Algorithmic delay (G.729) = 5 ms

  Jadi, Coder (Processing) Delay = 16 ms

- Packetization Delay

  Mengacu pada hasil pengukuran network analyzer diketahui panjang paket VoIP, besar data informasi paket VoIP dapat diperoleh dengan cara sebagai berikut :

  Voice payload size = Panjang paket IP – (Ethernet header + IP header + UDP header + RTP header)

  - Untuk G711 :

    Payload = 214 byte – (14+ 20+8 + 12) byte

    = 160 byte

  Untuk teknik kompresi G.711 dengan besar payload 160 byte maka delay paketisasi adalah 1 ms.

  - Untuk GSM :

    Payload = 87 byte – (14+20 + 8 + 12) byte

    = 33 byte

  Untuk teknik kompresi GSM dengan besar payload 33 byte maka delay paketisasi adalah 20 ms.

- Untuk G729 :

Payload = 74 byte – (14+12 + 8 + 20) byte

= 20 byte

Untuk teknik kompresi G.729 dengan besar payload 20 byte maka delay paketisasi adalah 25 ms.

Berdasarkan data yang didapat dari hasil pengukuran tersebut maka one way delay dapat dihitung dengan menjumlahkan coder processing delay, packetization delay, dan network delay

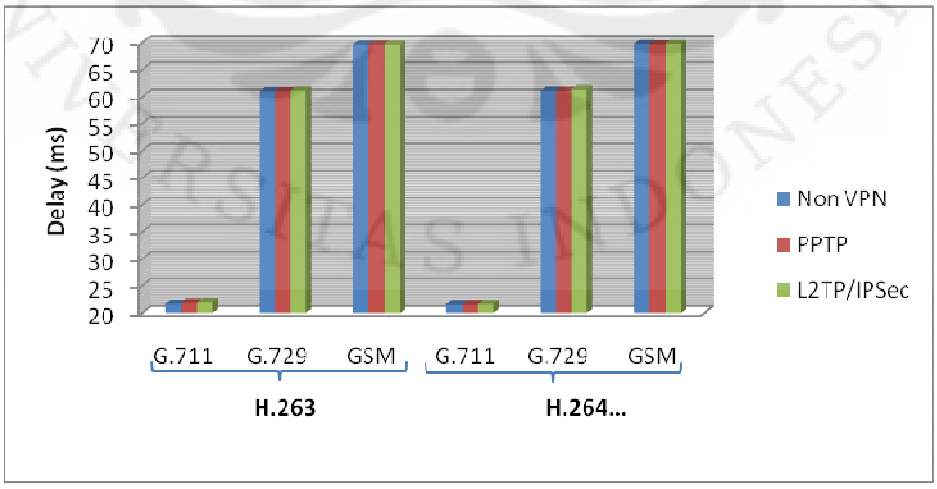
Tabel 4.4 Delay paketisasi,processing,jaringan dan delay total pada VoIP

No	Codec	Type	Delay Jaringan	Delay Processing	Delay Paketisasi	Delay Total
1	H263G711	NonVPN	20.20	0.4125 ms	1 ms	21.6125
		PPTP	20.38	0.4125 ms	1 ms	21.7925
		L2TP/IPSec	20.43	0.4125 ms	1 ms	21.8425
2	H263G729	NonVPN	19.99	16 ms	25 ms	60.99
		PPTP	19.99	16 ms	25 ms	60.99
		L2TP/IPSec	20.13	16 ms	25 ms	61.13
3	H263GSM	NonVPN	20.11	29.5 ms	20 ms	69.61
		PPTP	20.11	29.5 ms	20 ms	69.61
		L2TP/IPSec	20.11	29.5 ms	20 ms	69.61
4	H264G711	NonVPN	20.13	0.4125 ms	1 ms	21.5425
		PPTP	20.13	0.4125 ms	1 ms	21.5425
		L2TP/IPSec	20.14	0.4125 ms	1 ms	21.5525
5	H264G729	NonVPN	20.11	16 ms	25 ms	61.11
		PPTP	20.11	16 ms	25 ms	61.11
		L2TP/IPSec	20.33	16 ms	25 ms	61.33
6	H264GSM	NonVPN	20.24	29.5 ms	20 ms	69.74
		PPTP	20.17	29.5 ms	20 ms	69.67
		L2TP/IPSec	20.27	29.5 ms	20 ms	69.77

Setelah ditambahkan dengan delay lainnya, ternyata delay total masih bisa diterima oleh layanan VoIP berdasarkan standar G.114 ITU-T sebesar <150 ms baik tanpa VPN maupun yang diterapkan dengan VPN dengan delay yang besar terjadi pada penerapan L2TP/IPsec VPN. Delay total terbesar terjadi pada codec suara GSM baik dikombinasikan dengan video codec H.263 maupun H.264 yakni sebesar 69.61 dan 69.77 ms, sedangkan delay total terkecil terjadi pada codec suara G.711 baik dikombinasikan dengan video codec H.263 maupun H.264. Secara sederhana dapat terlihat pada tabel dan grafikberikut :

Tabel 4.5 Tabel Urutan Hasil Perhitungan Delay dari yang terbaik

Tabel UrutanHasil Perhitungan Delay dari yang terbaik					
Video Codec H.263					
1st	2st	3st	4st	5st	6st
PPTP on G.711	PPTP on G.729	PPTP on GSM	L2TP/IPsec on G.711	L2TP/IPsec on G.729	L2TP/IPsec on GSM
Video Codec H.264					
1st	2st	3st	4st	5st	6st
PPTP on G.711	PPTP on G.729	PPTP on GSM	L2TP/IPsec on G.711	L2TP/IPsec on G.729	L2TP/IPsec on GSM



Grafik 4.3 Delay Total Codec Suara

4.2.2 Pengukuran dan Analisa Jitter

Jitter merupakan variasi delay yang terjadi karena waktu kedatangan paket yang berbeda – beda. Secara sederhana bisa dikatakan bahwa jitter adalah perbedaan waktu kedatangan antara 1 paket dengan paket setelahnya. Parameter jitter perlu untuk dianalisis untuk mengetahui delay kedatangan antar satu paket dengan paket lainnya. Semakin besar jitter maka semakin perbedaan waktu antara suara asli dengan suara yang terdengar akan semakin besar. Hal itu dapat menyebabkan besarnya *collision*antara paket bahkan dapat menyebabkan *echo cancelation.*

4.2.2.1 Skenario Pengukuran Jitter

Pengukuran jitter dilakukan bersamaan dengan pengukuran delay dan packet loss. Paket Video Telephony yang lewat ditangkap dan dianalisa.Adapun hasil pengukuran jitter pada jaringan non vpn tampak pada tabel di bawah

Tabel 4.6 Jitter pada Jaringan Video Telephony non VPN

No	Video Codec	Voice Codec	Video Jitter Jaringan (ms)	Voice Jitter Jaringan (ms)
1	H.263	G.711	14.47	4.98
2		G.729	13.82	17.57
3		GSM	11.39	16.09
4	H.264	G.711	10.54	5.70
5		G.729	11.31	18.02
6		GSM	9.16	16.46

Dari tabel diatas diketahui bahwa jitter yang paling besar dimiliki oleh codec audio G.729 dengan kombinasi codec video apapun. Hal ini disebabkan karena G.729 memiliki bitrate yang paling kecil yaitu 24 kbps, jauh lebih kecil dari bitrate G.711 sebesar 80 kbps dan GSM sebesar 30 kbps.

Proses yang sama juga dilakukan pada jaringan yang diimplementasikan remote access VPN baik dengan protokol PPTP VPN maupun L2TP/IPsec VPN. Hasil pengolahan datanya terlihat pada tabel berikut ini :

Tabel 4.7 Jitter pada Jaringan Video Telephony PPTP VPN

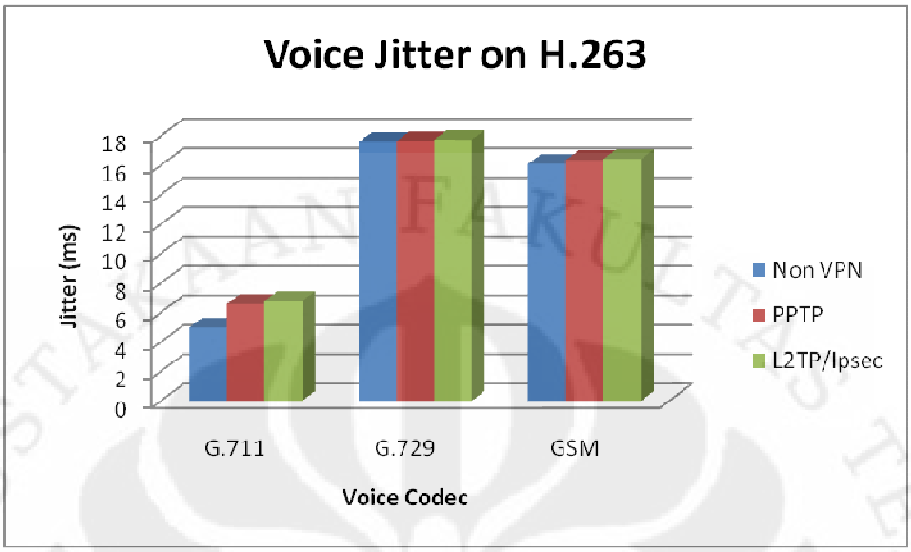
No	Video Codec	Voice Codec	Video Jitter Jaringan (ms)	Voice Jitter Jaringan (ms)
1	H.263	G.711	15.88	6.58
2		G.729	15.68	17.64
3		GSM	15.54	16.35
4	H.264	G.711	10.60	7.37
5		G.729	11.40	17.93
6		GSM	11.13	16.59

Tabel 4.8 Jitter pada Jaringan Video Telephony L2TP/IPsec VPN

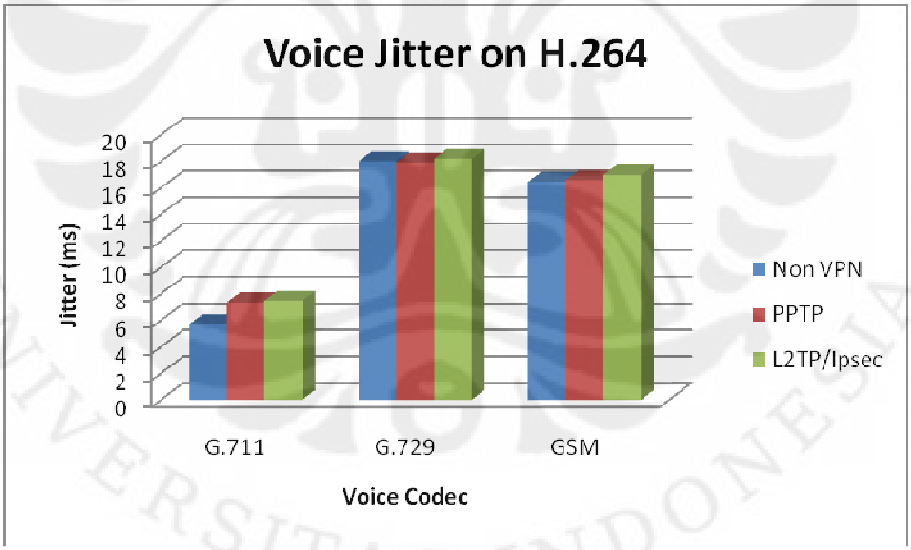
No	Video Codec	Voice Codec	Video Jitter Jaringan (ms)	Voice Jitter Jaringan (ms)
1	H.263	G.711	16.62	6.78
2		G.729	16.06	17.74
3		GSM	15.81	16.42
4	H.264	G.711	10.83	7.48
5		G.729	11.80	18.20
6		GSM	11.21	16.98

Dari dua tabel diatas didapat dua fenomena yang sama, ketika diimplementasikan PPTP maupun L2TP VPN jitter jaringan dari paket video dan suara mengalami peningkatan, namun peningkatan terbesar terjadi pada L2TP/IPsec VPN. Hal ini terjadi karena bertambahnya panjang paket akibat enkripsi penerapan L2TP/IPSec VPN padahal bitrate yang ada tetap sama.

Secara ringkas hasil percobaan mengenai delay jaringan terlihat seperti pada grafik berikut



Grafik 4.4 Voice Jitter Jaringan on H.263



Grafik 4.5 Voice Jitter Jaringan on H.264

Dari seluruh data jitter jaringan yang ada, kemudian akan dihitung jitter keseluruhan dan dibandingkan dengan standar ITU-T.

4.2.2.2 Analisis Pengujian Jitter

Jitter sangat mempengaruhi kualitas suara. Semakin besar jitter maka suara yang dihasilkan akan semakin tidak jelas (terputus - putus). Nilai jitterberpengaruh ketika packet RTP yang datang akan di proses menjadi suara. ITU-T merekomendasikan jitter yang baik untuk suara adalah < 30 ms. Pada hasil yang didapat dari pengujian diketahui bahwa jitter untuk semua codec suara baik G.711, G.729 dan GSM setelah diterapkan protokol PPTP VPN dan L2TP/IPsec VPN masih memenuhi rekomendasi. Hal demikian terjadi karena bitrate jaringan lebih besar dari bitrate codec sehingga jitter tidak akan terlalu jauh berubah.Jitter terbesar terjadi pada codec suara G.729 baik dikombinasikan dengan video codec H.263 maupun H.264 akibat dari L2TP/IPsec VPN yakni sebesar 17.74 dan 18.20 ms, sedangkan jitter terkecil terjadi pada codec suara G.711 baik dikombinasikan dengan video codec H.263 maupun H.264.Secara sederhana dapat terlihat pada tabel berikut :

Tabel 4.9 Tabel Urutan Hasil Perhitungan Jitter dari yang terendah

Tabel Urutan Hasil Perhitungan Jitter dari yang terendah					
Video Codec H.263					
1st	2st	3st	4st	5st	6st
PPTP on G.711	PPTP on GSM	PPTP on G.729	L2TP/IPsec on G.711	L2TP/IPsec on GSM	L2TP/IPsec on G.729
Video Codec H.264					
1st	2st	3st	4st	5st	6st
PPTP on G.711	PPTP on GSM	PPTP on G.729	L2TP/IPsec on G.711	L2TP/IPsec on GSM	L2TP/IPsec on G.729

4.2.3 Pengujian dan Analisa Troughput

4.2.3.1 Skenario Pengujian Troughput

RTP throughput diukur berdasarkan kecepatan transmisipaket. Percobaan yang sama diulang beberapa kaliuntuk mencari rata-rata throughput RTP. Tabel dibawah ini menunjukkan troughput dari percobaan video telephony tanpa VPN yang dilakukan

Tabel 4.10 Troughput pada Video Telephony non VPN

No	Video Codec	Voice Codec	Video Troughput (packet/s)	Voice Troughput (packet/s)
1	H.263	G.711	18.81	49.95
2		G.729	18.49	50.02
3		GSM	18.88	49.96
4	H.264	G.711	14.05	49.66
5		G.729	14.11	49.69
6		GSM	13.99	49.67

Dari tabel diketahui bahwa troughput yang paling besar dimiliki oleh codec audio G.729 dengan kombinasi codec video apapun. Hal ini disebabkan karena pengaruh dari delay jaringan yang lebih kecil pada G.729 dibandingkan dengan codec suara lainnya. Terdapat hubungan berbanding terbalik antara throughput dengan delay jaringan. Semakin kecil nilai delay jaringan maka semakin besar nilai throughput yang didapatkan.

Proses yang sama juga dilakukan pada jaringan yang diimplementasikan remote access VPN baik dengan protokol PPTP VPN maupun L2TP/IPsec VPN. Hasil pengolahan datanya terlihat pada tabel berikut ini :

Tabel 4.11 Throughput pada Jaringan Video Telephony PPTP VPN

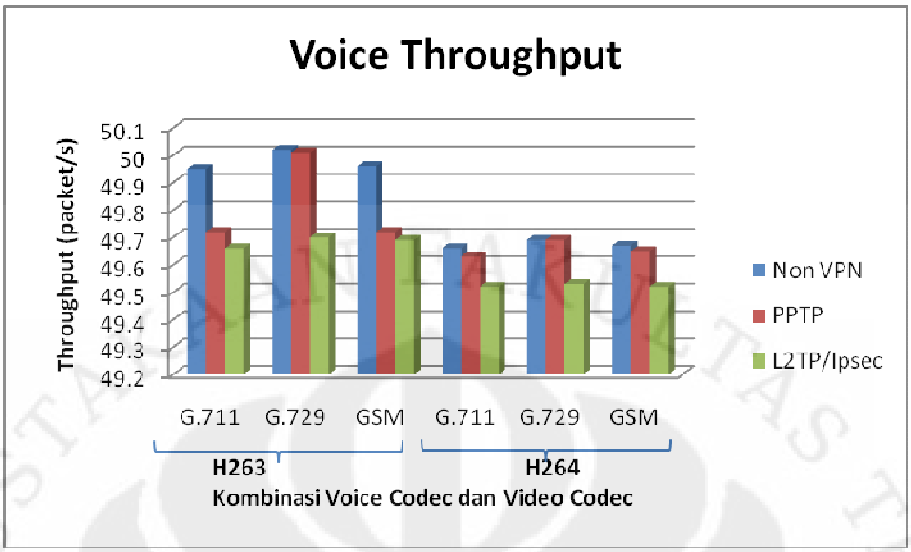
No	Video Codec	Voice Codec	Video Troughput (packet/s))	Voice Troughput (packet/s)
1	H.263	G.711	19.39	49.72
2		G.729	20.33	50.01
3		GSM	21.96	49.72
4	H.264	G.711	14.35	49.63
5		G.729	14.34	49.69
6		GSM	14.16	49.65

Tabel 4.12 Throughput pada Jaringan Video Telephony L2TP/IPsec VPN

No	Video Codec	Voice Codec	Video Troughput (packet/s)	Voice Troughput (packet/s)
1	H.263	G.711	14.38	49.66
2		G.729	17.73	49.70
3		GSM	18.68	49.69
4	H.264	G.711	13.90	49.52
5		G.729	13.74	49.53
6		GSM	13.78	49.52

Dari tabel diatas didapat dua fenomena yang sama, ketika diimplementasikan PPTP maupun L2TP VPN throughput jaringan dari video dan suara mengalami penurunan, namun penurunan terbesar terjadi pada L2TP/IPsec VPN. Hal ini terjadi karena delay jaringan pada L2TP/IPsec VPN lebih besar dibandingkan pada PPTP VPN.

Secara ringkas hasil pengujian throughput terlihat pada grafik berikut ini



Grafik 4.6 Hasil Pengujian Throughput

4.2.3.1 Analisis Pengujian Throughput

Pada hasil yang didapat dari pengujian diketahui bahwa throughput terkecil terjadi pada codec suara G.711 baik dikombinasikan dengan video codec H.263 maupun H.264 akibat delay jaringan terbesar yang disebabkan L2TP/IPsec VPN yakni sebesar 49.66 dan 49.52 packet/s, sedangkan throughput terbesar terjadi pada codec suara G.729 baik dikombinasikan dengan video codec H.263 maupun H.264. Secara sederhana dapat terlihat pada tabel berikut :

Tabel 4.13 Tabel Urutan Hasil Pengukuran dari Throughput yang terbesar

Tabel Urutan Hasil Pengukuran Throughput dari yang terbesar					
Video Codec H.263					
1st	2st	3st	4st	5st	6st
PPTP on G.729	PPTP on GSM	PPTP on G.711	L2TP/IPsec on G.729	L2TP/IPsec on G711	L2TP/IPsec on GSM

Video Codec H.264					
1st	2st	3st	4st	5st	6st
PPTP on G.729	PPTP on GSM	PPTP on G.711	L2TP/IPsec on G.729	L2TP/IPsec on G711	L2TP/IPsec on GSM

4.2.4 Pengujian dan Analisa Packet Loss

4.2.4.1 Skenario Pengujian Packet Loss

Packet loss menentukan besarnya paket yang hilang di dalam perjalanannya dari *source address* ke *destination address*. Semakin besar packet loss menyebabkan video semakin tidak jelas dan suara yang dikirim tidak akanbisa didengarkan (hilang).Adapun hasil pengukuran packet loss pada jaringan non vpn tampak pada tabel berikut

Tabel 4.14 Packet Loss pada Video Telephony non VPN

No	Video Codec	Voice Codec	Video Packet Loss (%)	Voice Packet Loss (%)
1	H.263	G.711	0.79	0.88
2		G.729	0.00	0.00
3		GSM	0.00	0.00
4	H.264	G.711	0.02	0.01
5		G.729	0.62	0.60
6		GSM	0.72	0.50

Packet loss diketahui dengan menggunakan wireshark yang menangkap paket VoIP yang lewat di jaringan. Ketika client 1 dan client 2 berkomunikasi, paket yang lewat akan ditangkap dan di analisis packet lossnya. Untuk mengetahui pengaruh dari implementasi VPN maka proses yang sama juga dilakukan pada jaringan yang diimplementasikan remote access VPN baik dengan

protokol PPTP VPN maupun L2TP/IPsec VPN. Hasil pengolahan datanya terlihat pada tabel berikut ini :

Tabel 4.15 Packet Loss pada Video Telephony PPTP VPN

No	Video Codec	Voice Codec	Video Packet Loss (%)	Voice Packet Loss (%)
1	H.263	G.711	0.41	0.63
2		G.729	0.04	0.00
3		GSM	0.02	0.00
4	H.264	G.711	0.00	0.03
5		G.729	0.05	0.06
6		GSM	0.09	0.09

Tabel 4.16 Packet Loss pada Video Telephony L2TP/IPsec VPN

No	Video Codec	Voice Codec	Video Packet Loss (%)	Voice Packet Loss (%)
1	H.263	G.711	0.98	1.04
2		G.729	0.00	0.02
3		GSM	0.15	0.03
4	H.264	G.711	0.05	0.01
5		G.729	0.00	0.02
6		GSM	0.14	0.07

4.2.4.2 Analisis Pengujian Packet Loss

Analisis packet loss diperlukan untuk mengetahui seberapa besar packet yang hilang dalam pengiriman. Semakin besar packet loss, maka kualitas IP Video Telephony over VPN akan semakin buruk.Menurut standar dari ITU-T packet loss yang masih dapat diterima berada pada 10% sampai 30%.Pada data pengujian didapatkan bahwa packet loss yang terjadi masih memenuhi standar baik tanpa maupun dengan implementasi VPN.Sama halnya dengan throughput,

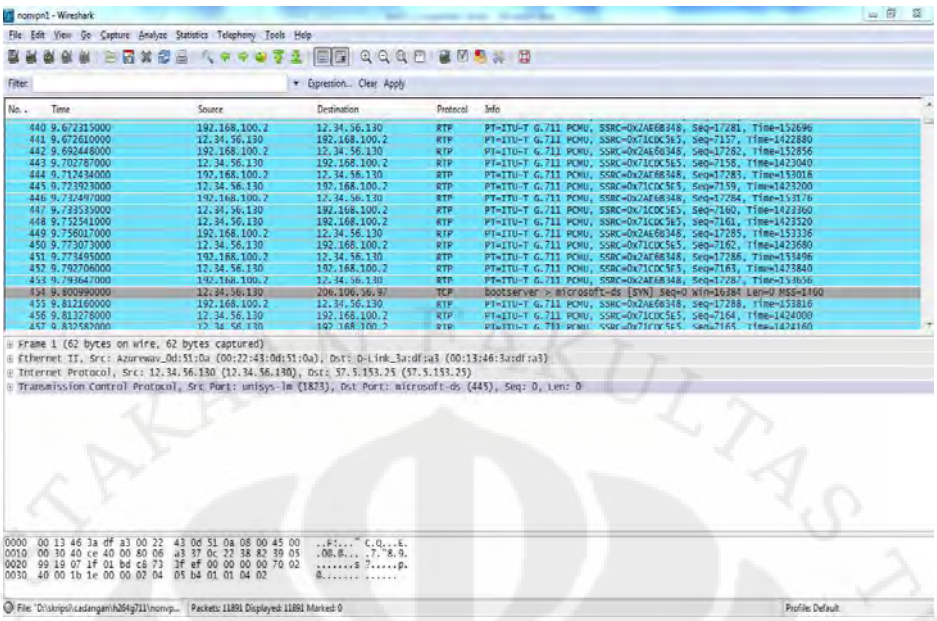
besarnya packet loss dipengaruhi oleh bitrate jaringan yang ada.Diketahui bahwa besarnya bitrate jaringan di Departemen Teknik Elektro Universitas Indonesia melebihi bitrate codec sehingga kemungkinan tabrakan antar packet sangat kecil. Secara ringkas peringkat packet loss dari yang paling kecil hingga terbesar terlihat pada tabel berikut

Tabel 4.17 Tabel Urutan Hasil Pengukuran Packet Loss dari yang terkecil

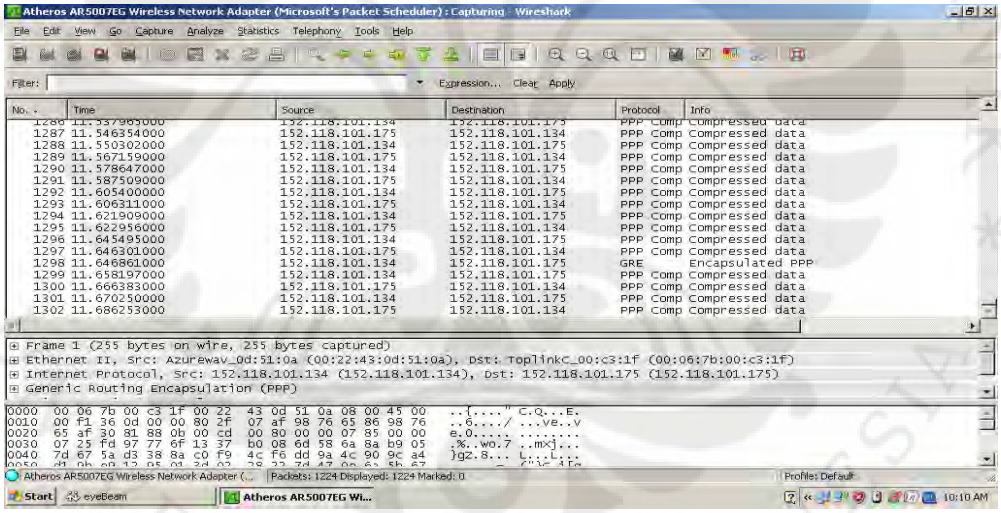
Tabel Urutan Hasil Pengukuran Packet Loss dari yang terkecil					
Video Codec H.263					
1st	2st	3st	4st	5st	6st
PPTP on GSM	PPTP on G.729	L2TP/IPsec on G.729	L2TP/IPsec on GSM	PPTP on G.711	L2TP/IPsec on G.711
Video Codec H.264					
1st	2st	3st	4st	5st	6st
L2TP/IPsec on G.711	L2TP/IPsec on G.729	PPTP on G.711	PPTP on G.729	L2TP/IPsec on GSM	PPTP on GSM

4.3 Analisis Keamanan IP Video Telephony over VPN

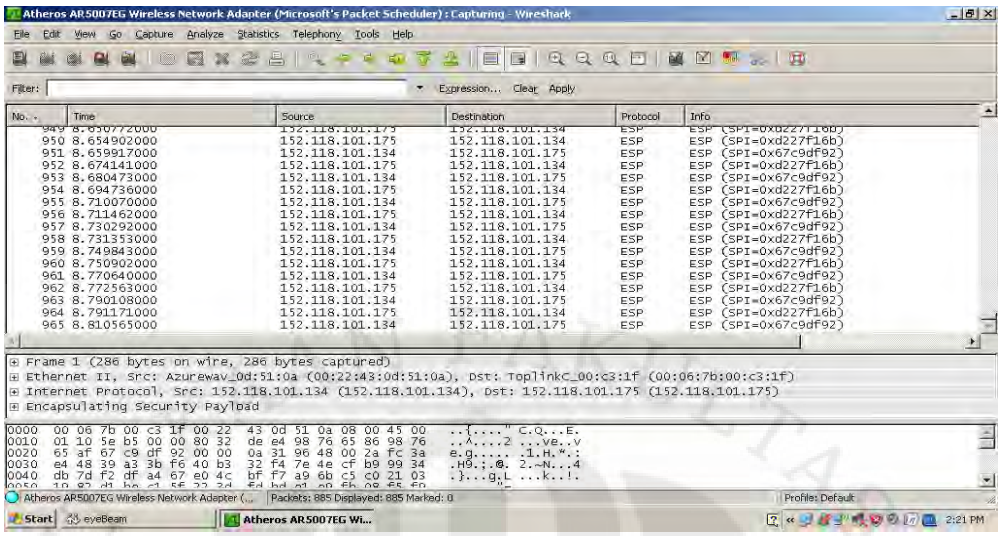
Analisis keamanan VoIP over VPN dilakukan melalui 2 cara yaitu merekam pembicaraandan menangkap paket IP Video Telephony untuk dilakukan analisa. Komunikasi IP Video Telephony dari Client 1 dan 2 dilakukan dengan melewati jaringan VPN melalui Vyatta Router. Dari hasil pengujian, data yang melewati VPN Vyatta Router tidak dapat direkam oleh software wireshark. Hal ini karena pada jaringan VoIP over VPN terdapat metode tunneling. Dimana data yang dikirim terenkripsi dan ditambahkan header baru sehingga baik data pengirim maupun penerima tidak dapat terlihat. Selain itu data yang dikirim dengan protokol PPP/GRE untuk PPTP dan ESP untuk L2TP/IPsec dan data payload dari IP Video Telephony tidak terlihat di jaringan.



Gambar 4.1 Capture IP Video Telephony tanpa VPN



Gambar 4.2 Capture IP Video Telephony over PPTP VPN



Gambar 4.3 Capture IP Video Telephony over L2TP/IPsec VPN

Isi dari payload hanya berisikan alamat IP dari kedua VPN server. Sedangkan alamat IP dari voip client dan VoIP server tidak terdeteksi, sehingga kecil kemungkinan bagi hacker untuk dapat melacak keberadaan client dan server VoIP. Sedangkan ketika data VoIP dicoba direkam oleh wireshark, ternyata stream RTP tidak dapat direkam.Hal ini karena paket telah berganti protocol dari RTP menjadi PPP dan ESP. Sedangkan software tidak dirancang untuk merekam paket dengan protokol PPP dan ESP.

4.4 Analisa Kebutuhan Bandwith

4.4.1 Kebutuhan Bandwith Tanpa Kompresi

Dalam mengimplementasikan IP Video Telephony perlu dipertimbangkan juga mengenai kebutuhan bandwith per *user* baik kebutuhan bandwith audio maupun video.Hal ini diperlukan untuk mengetahui berapa banyak user yang dapat melangsungkan komunikasi dalam waktu yang bersamaan dan mengelola penggunaan bandwith yang ada.Untuk itu diperlukan adanya pemilihan video dan audio codec yang tepat agar penggunaan bandwith dapat efisien.

Misalnya suatu video telephony dengan ukuran gambar QCIF (176 x 144) ditransmisikan tanpa kompresi maka kebutuhan bandwithnya sebagai berikut :

- ukuran gambar QCIF (176x144) = 25.344 pixel
- jika masing-masing pixel 3 warna dengan masing-masing level warna 8 bit, maka ukuran QCIF = 25.344x 3 x 8 bit/frame

  = 608.256 bit/frame
- misal standar bit frame perdetik = 30 fps

  maka kebutuhan bandwith = 608.256 x 30

  = 18.247.680 bps

  = 17.40 Mbps

Tentunya hal diatas menunjukkan kondisi yang sangat mahal untuk menyediakan kebutuhan bandwith yang sangat besar untuk aplikasi IP Video Telephony tanpa kompresi.

4.4.2 Kebutuhan Bandwith Dengan Kompresi

Berdasarkan sumber, dengan suatu teknik kompresi kebutuhan bandwith IP Video Telephony dapat menggunakan rumus berikut :

Rumus Bandwidh IP Video Telephony = ((H+V)/V) codec*[22]

Keterangan :

H = Total Header (UDP/RTP Header + IP Header + Layer 2 Header) (dalam bytes)

V = Video / Voice Payload (dalam bytes)

Codec = codec yang digunakan (dalam kbps)

VoIP adalah paket stream bit-bit suara yang dibungkus kedalam paket IP. Sebagaimana disebutkan bahwa stream bit-bit suara ini di paket menjadi voice payload.Paket Voice Payload ini kemudian harus ditambahkan header (semacam informasi alamat yang dituju dan informasi pengirim pada sebuah surat). Setelah proses paketitasi terjadi maka total voice payload (V) ini akan dibungkus dengan RTP header (8 byte), UDP header (12 byte), dan IP header (20 byte). Dalam hal paket VoIP berjalan diatas LAN maka akan

terjadi penambahan header untuk layer 2 (ethernet) sebesar 14 byte. Sehingga total header (H) menjadi 8 + 12 + 20 +14 = 54 byte (H = 54). Detail perhitungan bandwith pada masing-masing seperti berikut

1. Voice

a. G.711

H = RTP Header + UDP Header + IP Header + Ethernet Header

= 8 + 12 + 20 + 14

= 54 byte

V = 214 bytes

Codec G.711 di EyeBeam = 80 kbps

Jadi BW = ((H+V)/V)* codec

= ((54+214)/214)*80 kbps = 100.2 kbps

b. G.729

H = RTP Header + UDP Header + IP Header + Ethernet Header

= 8 + 12 + 20 + 14

= 54 byte

V = 74 bytes

Codec G.729 di EyeBeam = 24 kbps

Jadi BW = ((H+V)/V)* codec

= ((54+74)/74)*24 kbps = 41.5 kbps

c. GSM

H = RTP Header + UDP Header + IP Header + Ethernet Header

= 8 + 12 + 20 + 14

= 54 byte

V = 62 bytes

Codec GSM di EyeBeam = 30 kbps

Jadi BW = ((H+V)/V)* codec

= ((54+62)/62)*30 kbps = 56.1 kbps

2. Video

a. H.263

H = RTP Header + UDP Header + IP Header + Ethernet Header

= 8 + 12 + 20 + 14

= 54 byte

V = 561 bytes

Codec H.263 QCIF (176 x 144) = 64 kbps

Jadi BW = ((H+V)/V)* codec

= ((54+561)/561)* 64 kbps = 70.2 kbps

b. H.264

H = RTP Header + UDP Header + IP Header + Ethernet Header

= 8 + 12 + 20 + 14

= 54 byte

V = 1250 bytes

Codec H.264 = 64 kbps

Jadi BW = ((H+V)/V)* codec

= ((54+1250)/1250)* 64 kbps = 66.8 kbps

Kombinasi total kebutuhan bandwith video dan voice codec terangkum dalam tabel berikut ini

Tabel 4.18 Kebutuhan Bandwith IP Video Telephony setelah di kompresi

No	Video Codec	Voice Codec	Bandwith Video (kbps)	Bandwith Audio (kbps)	Total (kbps)
1	H.263	G.711	70.2	100.2	170.4
2		G.729	70.2	41.5	111.7
3		GSM	70.0	56.1	126.1
4	H.264	G.711	66.8	100.2	167
5		G.729	66.8	41.5	108.3
6		GSM	66.8	56.1	122.9

Data pada tabel menunjukkan bahwa kebutuhan bandwith codec audio G.729 paling kecil dikombinasikan dengan codec video apapun. Sedangkan codec video yang ada menunjukkan konsumsi bandwith yang terlalu jauh berbeda. Jika codec audio G.729 dipilih sebagai codec degan efisien bandwith paling baik dan merujuk pada kondisi jaringan di Departemen Teknik Elektro Universitas Indonesia yang telah dijelaskan di bab perancangan, maka dapat diasumsikan banyaknya pasangan pengguna yang dapat berkomunikasi secara bersamaan ialah sebagai berikut :

- Kondisi bandwith = 25 mbps / 5 Departemen

  = 5 mbps

  = 5120 kbps

- Asumsi bandwith tersedia untuk IP Video Telephony

  = 50 % x Kondisi Bandwith

  = 50 % x 5120 kbps

  = 2560 kbps

- Diasumsikan kebutuhan bandwith IP Video Telephony

  = Total Kebutuhan Bandwith + 10 % Total Kebutuhan Bandwith

  = 111.70 + 11.17 kbps

  = 122.87 kbps

  Berarti untuk sepasang pengguna IP Video Telephony bandwith yang dibutuhkan ialah

  = 122.87 kbps x 2

  = 245.74 kbps atau ~ 256 kbps

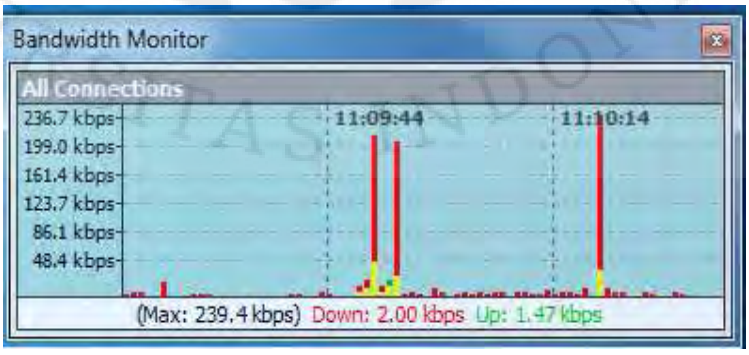
- Maka banyaknya pasangan pengguna

  = Kondisi Bandwith / (2 x Total Bandwith)

  = 2560 kbps / 256 kbps)

  = 10 pasangan pengguna

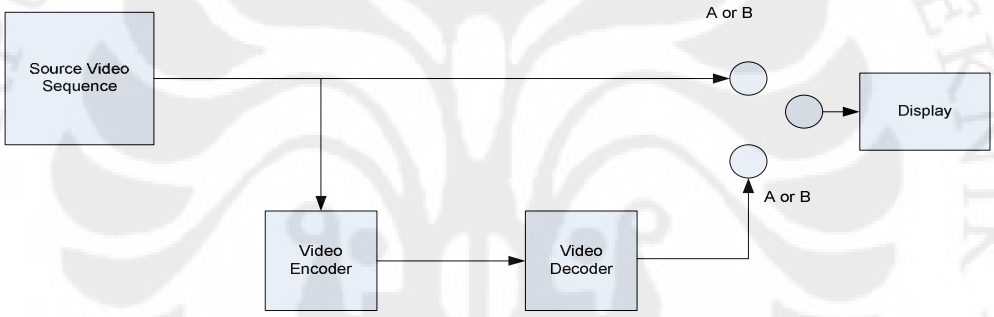
Kondisi diatas dibuktikan dengan hasil penangkapan / monitor bandwith seperti pada gambar berikut ini :



Gambar 4.4 Gambar Monitor Bandwith IP Video Telephony

4.2 Pengukuran dan Analisa Kualitas IP Video Telephony

Pengukuran kualitas video dapat dilakukan dengan dua (2) cara yakni secara subjektif dan objektif. Pengukuran kualitas video secara subjektif terkait dengan interaksi antara komponen *Human Visual System (HVS),* mata, dan otak. Faktor yang mempengaruhi kualitas penglihatan ialah *spatial fidelity*(tingkat kejernihan), *temporal quality* (naturalitas) ,*visual attention* (kelancaran) dan *recency effect* (pergerakan), (Richardson, 2003) . Pengukuran secara subjektif ini sulit untuk dilakukan secara akurat dan kuantitatif, namun terdapat beberapa prosedur tes yang telah dibuat salah satunya ialah *ITU-R Recommendation BT. 500-11[4]*. Prosedur ini menggunakan metode *Double Stimulus Continuous Quality Scale (DSCQS)* yang prosesnya diperlihatkan sebagai berikut :



Gambar 4.5 DSCQS Testing System

Sedangkan pengukuran secara objektif dapat dilakukan menggunakan suatu algoritma pengukuran. Algoritma pengukuran kualitas video yang sering digunakan ialah Peak Signal to Noise Ration (PSNR).

Pada skripsi IP Video Telephony over Remote Access VPN ini, pengukuran dan analisa kinerja dilakukan secara kuisioner kepada pengguna dengan memperhatikan pengukuran kualitas subjektif sesuai standar ITU-R 500 dimana nilai 5 sebagai nilai terbaik dan nilai 1 nilai yang terburuk. Codec yang digunakan ialah video codec H.263 dan voice codec G.729 dengan protokol VPN yang digunakan ialah PPTP VPN. Hal ini dipilih setelah mempertimbangkan hasil analisa pada bagian sebelumnya. Adapun hasil yang didapat dari kuisioner ialah sebagai berikut :

Tabel 4.19 Hasil Kuisioner Uji Video Telephony

No	Spatial Fidelity	Temporal Fidelity	Visual Attention	Recency Effect
1	4	4	4	4
2	4	4	4	5
3	4	3	4	4
4	4	4	4	4
5	4	3	4	4
6	3	4	4	4
7	3	4	4	5
8	4	4	4	5
9	4	3	4	4
10	4	4	3	4
Rata2	3.8	3.7	3.9	4.3

Tabel 4.14 menunjukkan nilai pengukuran kualitas video secara subjektif berapa dalam kisaran nilai 4. Melalui hasil ini dapat dikatakan bahwa implementasi IP Video Telephony dengan menggunakan video codec H.263 dan voice codec G.729 serta diakses melalui PPTP VPN menunjukkan hasil yang cukup baik.

BAB V

PENUTUP

5.1 Kesimpulan

Dari hasil analisa dan pengujian yang telah dilakukan, dapat disimpulkan sebagai berikut :

1. Aplikasi komunikasi menggunakan IP Video Telephony relative tidak aman, kerena pembicaraan yang terjadi dapat dilakukan *recorded streaming* dan IP Video Telephony server dapat diketahui. Dengan implementasi *Remote Access VPN* , *recorded streaming* tidak dapat dilakukan karena protocol yang dibaca berubah menjadi PPP/GRE untuk PPP dan ESP untuk L2TP/IPSec VPN serta IP Video Telephony server tidak dapat diketahui.

2. Penerapan protokol VPN untuk aplikasi IP Video Telephony ternyata menurunkan kinerja dari aplikasi tersebut karena terjadinya peningkatan nilai delay dan jitter, namun nilai delay dan jitter yang terjadi masih memenuhi rekomendasi ITU-T yakni dibawah 150 ms untuk delay suaranya, dan dibawah 30 ms untuk nilai jitte rnya. Penurunan kinerja tertinggi terjadi pada implementasi protokol L2TP/IPSec VPN. Hal demikian itu terjadi karena pada implementasi L2TP/IPsec VPN diterapkan enkripsi berupa *Pre-Shared Key* untuk authentikasi IPsec. Oleh karena itu protokol *Remote Access VPN* yang direkomendasikan ialah PPTP VPN.

3. Kombinasi codec IP Video Telephony yang direkomendasikan menggunakan video codec H.263 dan voice codec G.729. codec ini memiliki nilai delay jaringan paling rendah yakni untuk *audio codecnya* sebesar 19.99 ms dan video codecnya sebesar 54.55 ms. Hal ini terjadi karena payload nya cukup kecil jika dibandingkan codec lainnya yakni sebesar 74 bytes untuk G.729 dan 561 bytes untuk H.263.

4. Throughput yang paling besar dimiliki oleh codec audio G.729 dengan kombinasi codec video apapun yakni sebesar 50.02 packet/s untuk kombinasi dengan H.263 dan 49.69 untuk kombinasi dengan H.264. Hal ini terjadi karena pengaruh delay yang lebih kecil pada G.729 dibandingkan dengan codec lainnya. Ketika diterapkan Protokol VPN terjadi penurunan throughput, namun penurunan terbesar terjadi pada L2TP/IPSec VPN. Untuk voice codec G.729 throughput turun menjadi 49.70 untuk kombinasi dengan H.263 dan 49.53 untuk kombinasi dengan H.264.

5. Packet loss yang terjadi pada IP Video Telephony baik tanpa maupun dengan penerapan VPN masih memenuhi rekomendasi ITU-T. Packet loss yang terjadi rata-rata bernilai kurang dari 1% ,jauh dibawah nilai paket loss yang direkomendasikan oleh ITU-T sebesar 10-30%. Sama halnya dengan throughput, besarnya packet loss dipengaruhi oleh bitrate jaringan yang ada. Diketahui bahwa besarnya bitrate jaringan di Departemen Teknik Elektro Universitas Indonesia melebihi bitrate codec sehingga kemungkinan tabrakan antar packet sangat kecil.

6. Bandwith yang diperlukan untuk mentransmisikan IP Video Telephony dengan ukuran gambar QCIF (176x144) tanpa kompresi diperkirakan sebesar 17.40 Mbps per *user*, sedangkan dengan adanya kompresi bandwith yang dibutuhkan sekitar 128 kbps per *user* atau dapat dikatakan sebesar 256 kbps untuk komunikasi sepasang *user*.

7. Berdasarkan uji kualitas IP Video Telephony secara subjektif dengan kombinasi codec dan VPN yang direkomendasikan dan dengan menerapkan metode DSCQS *testing* yang disesuaikan dengan rekomendasi ITU-R 500 didapatkan hasil uji rata-rata *spasial fidelity*bernilai 3.8, *temporal fidelity* bernilai 3.7 , *visual attention* 3.9 dan *recency effect* bernilai 4.3. Hasil pengujian ini menunjukkan kualitas

IP Video Telephony dengan video codec H.263 dan audio codec G.729 serta protokol PPTP VPN bernilai cukupbaik karena berada diatas nilai yang dapat ditoleransi yakni sebesar 3.

5.2 Saran

1. Ujicoba IP Video Telephony dilakukan lebih dari dua pengguna sehingga dapat lebih detail diukur kinerja jaringannya.
2. Skala jaringan uji diperluas hingga seluruh wilayah Universitas Indonesia.
3. Aplikasi yang diujicoba ditingkatkan menjadi IP Multimedia Subsystem (IMS) teknologi yang sedang berkembang menggantikan *softswitching*.
4. Protocol Remote Access VPN nya diperbanyak karena system operasi yang ada saat ini telah mendukung protokol baru seperti Secure Socket Tunneling Protocol (SSTP), IKEv2, danOpenVPN.

DAFTAR REFERENSI

[1] Cisco System " Understanding Delay in Packet Voice Networks". USA : Cisco Press. 2004

[2] Davidsonn, J. Peters, J. 2000. Voice Over IP Fundamentals. Indianapolis : Cisco Press

[3] Tharom, Tabratas. Onno W. Purbo. 2001. Teknologi VoIP (Voice Over Internet Protocol). Jakarta : PT. Elex Media Komputindo

[4] Gupta Meeta, "Building a Virtual Private Network", Premier Press 2645 Erie Avenue, Suite 41 Cincinnati , Ohio 45208 , 2003

[5] DiabBou, Wafaa. VPN Analyis and New Perspective for Securing Voice over VPN Networks.IEEE Computer Society Journal, 2008.

[6] Joha A, Ahmed. Performance Evaluation for Remote Access VPN on Windows Server 2003 and Fedora Core 6.IEEE Computer Society Journal, 2007.

[7] KashnabhisBhumip "Implementing Voice over IP", Willey-Interscience Hoboken New Jersey, 2003

[8] Richardson, Iain E.G. " H.264 and MPEG-4 Video Compression, Video Coding for Next-Generation Multimedia." John Wiley & Sons, England. 2003.

[9] ITU-T Recommendation P.800, "Methods for subjective determination of transmission quality", 1996

[10] ITU-R Recommendation BT.500-11[4], " Double Stimulus Continuonus Quality Scale Standard"

[11] ITU-T G.104, " VoIP Quality Standard".

[12] ITU-T G.114, "One-way transmission time", 2003

[13] ITU-T Recommendation G.711, " Pulse Code Modulation (PCM) of Voice Frequencies", 1998

[14] ITU-T Recommendation G.729, "Coding of speech at 8 kbits/s using conjugate-structure algebraic-code excited linear-predition (CS-ACELP)", 1996

[15] ITU-T, "Video codec for audiovisual services at px64 kbits/s," ITU-T Rec. H.261 v1: Nov 1990, v2: Mar. 1993.

[16] ISO/IEC JTC 1, "Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbit/s – Part 2: Video," ISO/IEC 11172 (MPEG-1), Nov. 1993.

[17] ITU-T and ISO/IEC JTC 1, "Generic coding of moving pictures and associated audio information – Part 2: Video," ITU-T Rec. H.262 and ISO/IEC 13818-2 (MPEG-2), Nov. 1994 (with several subsequent amendments and corrigenda)

[18] ITU-T, "Video coding for low bit rate communication," ITU-T Rec. H.263; v1: Nov. 1995, v2: Jan. 1998, v3: Nov. 2000.

[19] ISO/IEC JTC 1, “Coding of audio-visual objects – Part 2: Visual,” ISO/IEC 14496-2 (MPEG-4 Part 2), Jan. 1999 (with several subsequent amendments and corrigenda).

[20] RFC 1171, “The Point-to-Point Protocol for the Transmission of Multi-Protocol Datagrams Over Point-to-Point Links,“ July 1990.

[21} RFC 2661, “Layer Two Tunneling Protocol "L2TP",“Agustus 1999.

[22] Rafdian. MenghitungBandwithuntuk VoIP.

http://ilmukomputer.org/2006/08/25/menghitung-bandwidth-untuk-voip/

[23] Arif, Muhammad. Teknologi Video Conference.

http://fadhly.web.id/repo/downloads/Documents/Teknologi%20Video%20Confrence.pdf , diakses 12 Mei 2010.

[24] Sulistyohati, Aprilia. Telekonferensi, Video Broadcasting, dan Security.

http://efrylia.files.wordpress.com/2009/12/teknologi-telekonferensivideo-broadcasting.pdf , diakses 12 Mei 2010.

[25] Virtual Private Network Consortium “VPN Standards Protocol”

http://www.vpnc.org/vpn-standards.html , diakses 4 April 2010.

[26] *http://www.xten.com/index.php?menu=Products&smenu=eyeBeam*

[27] http://www.docstoc.com/docs/29432036/Perbandingan-Tunneling-pada-Komunikasi-VPN

LAMPIRAN 1
KONFIGURASI VPN ROUTER

```
interfaces {
ethernet eth0 {
address 12.34.56.78/24
hw-id 00:13:46:3a:df:a3
   }
ethernet eth1 {
address 192.168.100.254/24
hw-id 00:06:7b:00:be:7c
   }
ethernet eth2 {
address 200.200.200.2/24
hw-id 00:55:d0:8b:96:1b
   }
ethernet eth3 {
address 152.118.101.175/24
hw-id 00:06:7b:00:c3:1f
   }
loopback lo {
   }
tunnel tun0 {
address 2001:db8:2::2/64
encapsulation sit
local-ip 200.200.200.2
remote-ip 200.200.200.1
   }
}
protocols {
ospf {
   }
rip {
network 192.168.100.0/24
network 12.34.56.0/24
network 200.200.200.0/24
redistribute {
connected {
         }
static {
         }
      }
   }
ripng {
interface eth2
interface eth0
         redistribute {
connected {
         }
```

```
        }
    }
static {
route 0.0.0.0/0 {
next-hop 152.118.101.175 {
            }
        }
    }
}
service {
dhcp-server {
disabled false
shared-network-name ETH0_POOL {
authoritative disable
subnet 12.34.56.0/24 {
default-router 12.34.56.78
start 12.34.56.101 {
stop 12.34.56.200
                }
            }
        }
    }
nat {
rule 1 {
outbound-interface eth3
source {
address 192.168.100.0/24
            }
type masquerade
        }
rule 10 {
outbound-interface eth3
outside-address {
address 152.118.101.175
            }
source {
address 192.168.1.0/24
            }
type source
        }
 }
telnet {
port 23
    }
}
system {
flow-accounting {
interface eth3
```

```
    }
login {
uservyatta {
authentication {
encrypted-password **********
          }
       }
    }
name-server 152.118.101.8
name-server 152.118.24.2
ntp-server 0.vyatta.pool.ntp.org
package {
auto-sync 1
repository supported {
components main
distribution stable
url http://packages.vyatta.com/vyatta-supported
       }
    }
syslog {
global {
facility all {
level notice
          }
facility protocols {
level debug
          }
       }
    }
}
vpn {
ipsec {
ipsec-interfaces {
interface eth3
       }
 }
nat-networks {
allowed-network 192.168.100.0/24 {
          }
       }
nat-traversal enable
    }
    l2tp {
remote-access {
authentication {
local-users {
usernametestuser {
password **********
```

```
                }
            }
mode local
        }
client-ip-pool {
start 192.168.2.50
stop 192.168.2.200
        }
ipsec-settings {
authentication {
mode pre-shared-secret
pre-shared-secret **********
            }
        }
outside-address 152.118.101.175
outside-nexthop 152.110.101.1
    }
  }
pptp {
remote-access {
authentication {
local-users {
usernametestuser {
password **********
            }
        }
mode local
        }
client-ip-pool {
start 192.168.1.101
                stop 192.168.1.200
        }
outside-address 152.118.101.175
    }
  }
}
```

KUISIONER UJI IP VIDEO TELEPHONY

Isilah kuisioner ini berdasarkan kualitas subjektif yang anda rasakan, berilah nilai

1 = *buruk*
2 = *agak buruk*
3 = *netral*
4 = *baik*
5 = *baik sekali*

1. Tampilan video yang ada lihat jernih / jelas.

   1 2 3 4 5

2. Pergerakan video terlihat natural dan “smooth”.

   1 2 3 4 5

3. Tampilah video lancar dan tidak terputus-putus.

   1 2 3 4 5

4. Ketika anda bergerak video tidak patah-patah.

   1 2 3 4 5

HASIL KUISIONER UJI IP VIDEO TELEPHONY

No	Spatial Fidelity	Temporal Fidelity	Visual Attention	Recency Effect
1	4	4	4	4
2	4	4	4	5
3	4	3	4	4
4	4	4	4	4
5	4	3	4	4
6	3	4	4	4
7	3	4	4	5
8	4	4	4	5
9	4	3	4	4
10	4	4	3	4
Rata2	3.8	3.7	3.9	4.3