ANALISA PERANCANGAN *SERVER* VOIP *(VOICE INTERNET PROTOCOL)* DENGAN *OPENSOURCE ASTERISK* DAN VPN *(VIRTUAL PRIVATE NETWORK)* SEBAGAI PENGAMAN JARINGAN ANTAR *CLIENT*

Domiko Fahdi Jaya Patih*. Helmy Fitriawan. Yetti Yuniati.
Jurusan Teknik Elektro. Fakultas Teknik.Universitas Lampung
Email: *domicofahdi@yahoo.com

Abstrak

Voice over Internet Protocol* (VoIP) merupakan teknologi yang memanfaatkan *Internet Protocol* untuk menyediakan komunikasi *voice* secara elektronis dan *real-time*. Unsur pembentuk VoIP adalah *User agent, Proxy, Protocol* dan *Coder-Decoder* (CODEC). *Asterisk* merupakan *softswicth* untuk mengoperasikan *proxy,* yang berbasis session *initiation protocol* (SIP). Sistem operasi Ubuntu 10.10 sebagai *server* VoIP cukup fleksibel untuk mendukung kinerja paket *Asterisk*. Tujuan dari penelitian ini adalah membangun *server* VoIP berbasis *Asterisk,* agar dapat dikembangkan pada penelitian selanjutnya sesuai dengan kebutuhan. Metodologi penelitian yang dilakukan, secara garis besar terdiri dari dua alur, yaitu studi literatur dan percobaan. Penelitian ini dilakukan pada instalasi yang sudah dibangun jaringan *internet* sebelumnya. Sehingga VoIP disini difungsikan sebagai pemaksimalan jaringan *internet* yang sudah ada tersebut untuk menekan biaya pengeluaran kebutuhan komunikasi. Layanan yang disediakan pada penelitian ini berbentuk *voice* dan *video* dengan layanan *call client to server, call client to client, video call conference, video conference.

Kata Kunci : ***Voice over Internet Protocol* , (VoIP),** ***Asterisk, Session Initiaton Protocol* (SIP), VPN.**

Abstrack

Voice over Internet Protocol (VoIP) is a technology that utilizes the Internet Protocol to provide real-time voice communication. VoIP technology is a today telecommunication technology, where the costs of the technology infrastructure is much cheaper than the telecommunications technology that is commonly used today. Forming elements are VoIP User Agent, Proxy, Protocol and Coder-Decoder (CODEC). Asterisk is a softswicth to operate a proxy, which is based on session initiation protocol (SIP). 10.10 Ubuntu operating system as a VoIP server is flexible to support a package of performance Asterisk. The goal of this research is to build Asterisk-based VoIP server, that can be developed in further research as needed. The methodology of research conducted, is devided by two, the study of literature and experimental. The research was conducted at the installation that has been built before the Internet network. VoIP so here functioned as maximizing existing internet network is to reduce expenses communication needs. Services provided in this study form with voice and video call services client to server, client to client call, video call conferencing, video conferencing

Key Word : Voice over Internet Protocol (VoIP), Asterisk, Session Initiaton Protocol (SIP), VPN

I. Pendahuluan

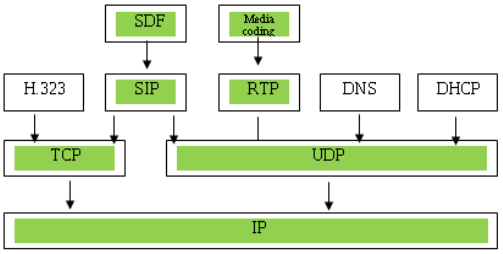
Perkembangan jaringan komputer yang semakin pesat memungkinkan untuk melewatkan trafik suara melalui jaringan komputer atau biasa yang disebut VoIP *(Voice over Internet Protocol*). *Voice over Internet Protocol* (juga disebut VoIP, IP *Telephony*, *Internet telephony* atau *Digital Phone*) adalah teknologi yang memungkinkan percakapan suara jarak jauh melalui media *internet*. Data suara diubah menjadi kode *digital* dan dialirkan melalui jaringan yang mengirimkan paket-paket data dan bukan lewat sirkuit *analog* telepon biasa. Definisi VoIP adalah suara yang dikirim melalui *Internet Protocol* (IP). Saat ini terdapat 2 teknologi utama *internet telephony*, yaitu teknologi H.323 dan *Session Initiation Protocol* (SIP), keduanya sering digunakan[1]. Penggunaan jaringan IP memungkinkan penghematan biaya, karena tidak perlu membangun sebuah infrastruktur baru untuk komunikasi suara dan penggunaan lebar data (*bandwidth*) yang lebih kecil dibandingkan telepon biasa. Penggunaan teknologi VoIP yang lebih efisien akan semakin dipermudah karena dapat digabungkan dengan jaringan telepon lokal yang sudah ada. Setiap individu dapat membangun dan mengembangkan infrastrukturnya secara mandiri, dikarenakan penggunaan sistem operasi berbasis *linux* / *open source Asterisk* yang memang dikhususkan untuk menangani VoIP. Penggunaan teknologi VoIP sangat menguntungkan bagi penggunanya. Namun, penggunaan komunikasi yang murah dari sisi keamanan kurang begitu diperhatikan. Oleh karena itu keamanan ketika melakukan komunikasi suara merupakan sesuatu yang sangat penting karena menyangkut privasi penggunanya. Penggunaan VPN (*Virtual Private Network*) merupakan salah satu alternatif untuk mengirimkan *voice*, yang bersifat *private* atau aman, karena penggunaan koneksi yang telah terenkripsi serta penggunaan *private keys*, *certificate*, *username* atau *password* untuk melakukan *authentikasi* dalam membangun koneksi.

II. Tinjauan Pustaka

2.1 VoIP (*Voice over Internet Protocol*)

VoIP (*Voice over Internet Protocol)* adalah teknologi yang mampu mengirimkan trafik suara, *video* dan data yang berbentuk paket secara *real-time* dengan jaringan *Internet Protocol*. VoIP memanfaatkan infrastruktur *internet* yang sudah ada untuk berkomunikasi seperti layaknya menggunakan telepon biasa dan tidak dikenakan biaya telepon biasa untuk berkomunikasi dengan pengguna VoIP lainnya dimana saja dan kapan saja. Teknik dasar *Voice over Internet Protocol* atau yang biasa dikenal dengan sebutan VoIP adalah teknologi yang memungkinkan kemampuan melakukan percakapan telepon dengan menggunakan jalur komunikasi data pada suatu jaringan (*networking*), sehingga teknologi ini memungkinkan komunikasi suara menggunakan jaringan berbasis IP (*internet protocol*) untuk dijalankan diatas infrastruktur jaringan *packet network*. Jaringan yang digunakan bisa berupa *internet* atau *intranet*. Teknologi ini bekerja dengan jalan mengubah suara menjadi *format digital* tertentu yang dapat dikirimkan melalui jaringan IP. Teknologi ini pada dasarnya mengkonversi sinyal analog (suara) ke format digital dan kemudian dikompres atau ditranslasikan ke dalam paket-paket IP yang kemudian ditransmisikan melalui jaringan *internet*. Standarisasi *protocol* komunikasi pada teknologi VoIP adalah SIP (*Session Initiation Protocol*) dan H.323. Gambar 1 memperlihatkan susunan *stack* pada *internet* media *protocol*.

Gambar 1. Cara kerja VoIP[2]



Gambar 2. *Internet Multimedia Protocol stack*[3]

Pada Gambar 2, *protocol* yang berwarna hijau merupakan *protocol* yang digunakan pada VoIP berbasis SIP. Dari gambar tersebut dapat dilihat bahwa VoIP menggunakan TCP dan UDP sebagai *transport layer*-nya.

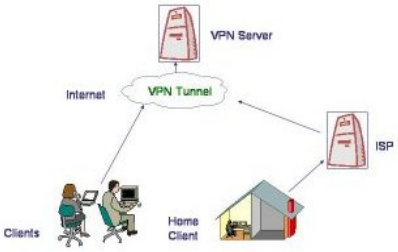
2.2 Parameter penentu kualitas layanan (QoS dan MOS) VoIP

QOS didefinisikan sebagai suatu pengukuran tentang seberapa baik jaringan dan merupakan suatu usaha untuk mendefinisikan karakteristik dan sifat dari suatu layanan. QoS mengacu pada kemampuan jaringan untuk Menyediakan layanan yang lebih baik pada trafik

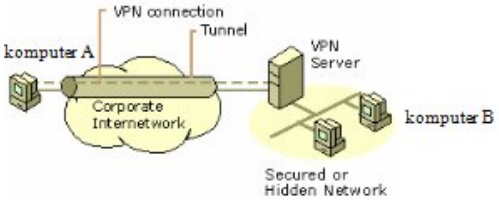
jaringan tertentu melalui teknologi yang berbeda-beda. Tujuan dari QoS adalah untuk memenuhi kebutuhan-kebutuhan layanan yang berbeda, yang menggunakan infrastruktur yang sama. Beberapa parameter Qos yaitu *delay, jitter, throughput,* dan *paket loss*. *Delay* adalah waktu yang dibutuhkan oleh satu paket dari tempat ke sumber tujuan. *Jitter* adalah variasi yang ditimbulkan oleh *delay*, terjadi karena adanya perubahan terhadap karakteristik dari suatu sinyal sehingga menyebabkan terjadinya masalah terhadap data yang dibawa oleh sinyal tersebut. *Throughput* adalah jumlah data persatuan waktu yang dikirim dari suatu titik jaringan ke titik jaringan yang lain *Packet loss* merupakan suatu parameter yang menggambarkan suatu kondisi yang menunjukkan jumlah total paket yang hilang. Kualitas sinyal yang diterima dapat diukur dengan subjektif dan objektif. Metode pengukuran subyektif yang umum dipergunakan dalam pengukuran kualitas *speech coder* adalah ACR (*Absolute Category Rating*) yang akan menghasilkan nilai MOS (*Mean Opinion Score*). Tes subyektif ACR meminta pengamat untuk menentukan kualitas suatu *speech coder* tanpa membandingkannya dengan sebuah referensi. Bila pengukuran dengan objektif maka pengukuran MOS menggunakan parameter QoS, yaitu *delay*, *jitter*, *packet loss* yang didapat pada saat pengukuran. Skala rating umumnya mempergunakan penilaian yaitu beruturut – turut: *Exellent, Good, Fair, Poor* dan *Bad* dengan nilai MOS (*Mean Opinion Score*) berturut – turut: 5, 4, 3, 2 dan 1.

2.3 VPN (*Virtual Private Network*)

Virtual Private Network atau biasa disingkat dan dikenal umum sebagai VPN atau VPN *tunnel* adalah sebuah mekanisme menyambungkan sebuah titik (atau biasa dengan *node*) pada sebuah jaringan komputer dengan titik yang lain melalui mediasi sebuah jaringan yang lain, sebuah titik dapat berupa sebuah jaringan komputer lokal (atau biasa disebut LAN) atau sebuah komputer. VPN adalah sebuah cara aman untuk mengakses *local area network* yang berada pada jangkauan dengan menggunakan *internet* atau jaringan umum lainnya untuk melakukan transmisi data paket secara pribadi dengan *enkripsi* perlu penerapan teknologi tertentu agar walaupun menggunakan medium yang umum, tetapi *traffic* (lalu lintas) antar *remote-site* tidak dapat disadap dengan mudah, juga tidak memungkinkan pihak lain untuk menyusupkan *traffic* yang tidak semestinya ke dalam *remote-site*. Teknologi VPN sesungguhnya adalah sebuah *software* yang dijalankan oleh kedua pihak yang hendak berkomunikasi melalui *internet*[2]. VPN adalah sebuah koneksi *virtual* yang bersifat privat, disebut demikian karena pada dasarnya jaringan ini tidak ada secara fisik hanya berupa jaringan *virtual* VPN Menghubungkan PC dengan jaringan publik atau *internet* namun sifatnya privat, karena bersifat privat maka tidak semua orang bisa terkoneksi ke jaringan ini dan mengaksesnya. Oleh karena itu diperlukan keamanan data dalam VPN. Dalam VPN tersebut terdapat *tunnel*, *tunnel* sendiri adalah istilah generik yang menjelaskan bahwa sebuah hubungan antar titik pada sebuah jaringan komputer dilakukan melalui semacam terowongan antar kedua titik.



Gambar 3. Model Jaringan VPN[15]



Gambar 4. Model Tunnel VPN[16]

III. Metode Penelitain

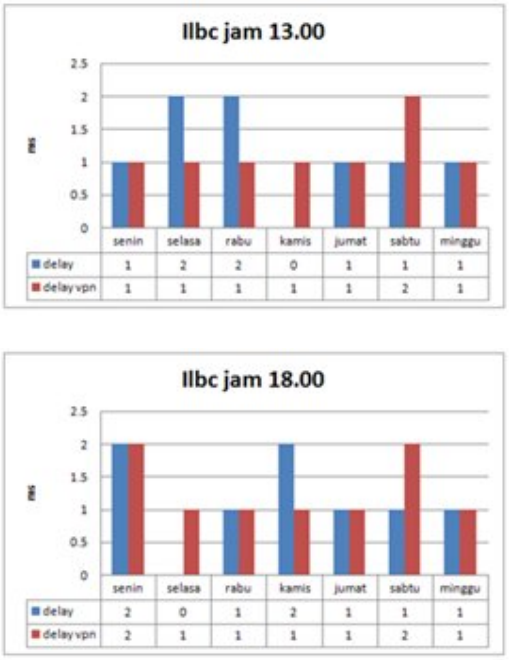
Metode yang digunakan pada penelitian ini adalah perancangan *server* VoIP, menggunakan OS Ubuntu, *software Asterisk*, *software* VPN, *software VQManager*, *software Wireshark* dan *software cain and abel*. Pada *server* VoIP ini menggunakan *software Asterisk* dikarenakan terbukti handal, kemudian menggunakan *software* VPN untuk pengaman jaringan untuk mencegah penyadapan, *software VQManager* dan *Wireshark* berfungsi untuk monitoring performa *server* VoIP dengan menganalisa QoS dan MOS, kemudian *software Wireshark* digunakan untuk mengukur *throughput*, dan *software cain and abel* untuk pengujian keamanan komunikasi. Pada penelitian ini dilakukan pengamatan terhadap parameter-

parameter yang mempengaruhi kualitas suara seperti *delay*, *jitter*, *packet loss* dan *throughput.* Pengukuran membandingkan QoS pada komunikasi VoIP dengan menggunakan VPN dan tidak menggunakan VPN, kemudian akan dilakukan perbandingan penggunaan *codec* yang digunakan pada saat komunikasi dilakukan, yaitu *codec alaw*, *gsm*, *ilbc*, dan *speex*. Semua pengukuran QoS dan MOS dilakukan bersamaan. Pengukuran dilakukan dalam waktu 5 menit agar dapat terlihat nilai maksimum dan nilai minimum nilai QoS dan nilai MOS pada *software* pengukur.

IV. Hasil dan Pembahasan

4.1 Hasil pengukuran rata-rata *Delay*

Pada penelitian ini salah satu parameter QoS adalah dengan pengukuran *delay*. Media yang digunakan untuk pengukuran QoS adalah dengan jaringan kabel RJ-45 dengan topologi *delay end-to-end. Delay end-to-end* mengacu pada waktu yang dibutuhkan untuk paket yang akan dikirim melintasi jaringan dari sumber ke tujuan pengukuran dilakukan pada 13.00 dan 18.00. Hasil pengukuran delay ilbc adalah sebagai berikut :

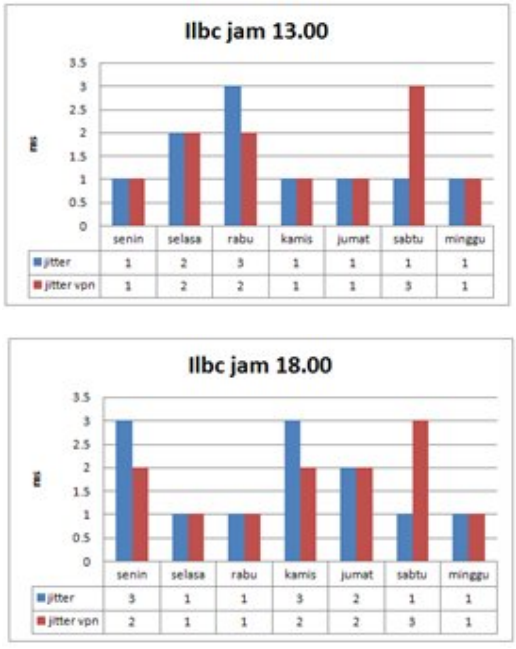


Gambar 5. Hasil pengukuran *delay* dengan *codec ilbc*

Pada pengukuran *delay* dengan keempat *codec*, *codec ilbc* yang stabil saat melakukan komunikasi.Suara yang dihasilkan terdengar jelas dengan sedikit *noise* dibandingkan dengan suara pada saat menggunakan *codec gsm*, *speex*, dan *alaw.*

4.2 Hasil pengukuran *jitter*

Parameter QoS selanjutnya adalah *jitter*. *Jitter* adalah variasi kedatangan paket yang diakibatkan oleh perubahan dalam karakteristik suatu sinyal. Variasi tersebut bisa berupa panjang antrian, waktu pengolahan data, dan juga waktu penghimpunan ulang paket-paket di akhir perjalanan *jitter*. Parameter *jitter* perlu 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*. Hasil pengukan *jitter* ilbc adalah sebagai berikut:



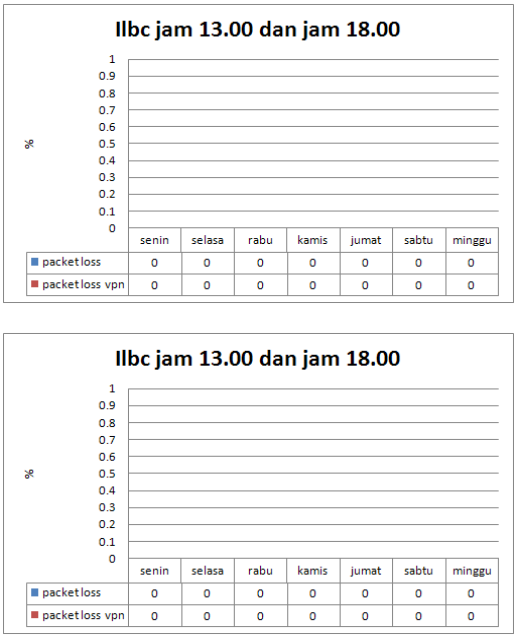
Gambar 6. Hasil pengukuran *jitter* dengan *codec ilbc*

Pada penelitian ini variasi *jitter* yang besar sangat dipengaruhi oleh *processing* data voice

dimana *processing* data *voice* dipengaruhi oleh penggunaan *codec*, sehingga sewaktu-waktu *jitter* bisa sangat besar. Nilai *jitter* berpengaruh ketika packet RTP yang datang akan di proses menjadi suara. Ketika nilai *jitter* lebih kecil dari waktu pemrosesan paket data maka sebelum paket selesai di proses paket selanjutnya telah datang untuk menunggu diproses.

4.3 Hasil pengukuran *packet loss*

Packet loss adalah jumlah paket hilang. Umumnya perangkat jaringan memiliki *buffer* untuk menampung data yang diterima. Jika terjadi kongesti yang cukup lama *buffer* akan penuh dan data baru tidak akan diterima. *Packet loss* (kehilangan paket data pada proses transmisi) dan *desequencing* 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 kontrol terhadap kongesti (kelebihan beban data) pada jaringan. Hasil pengukuran packet loss ilbc adalah sebagai berikut :

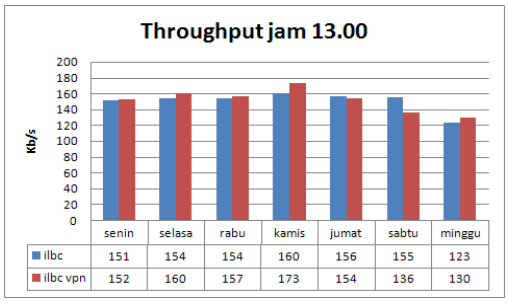


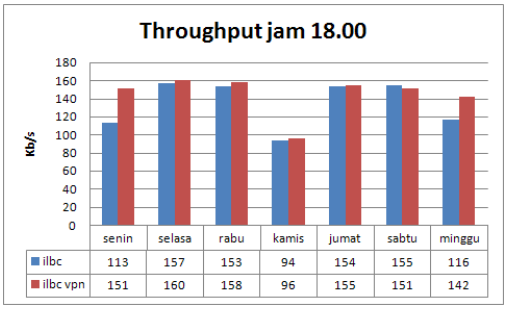
Gambar 7. Hasil pengukuran *packet loss* dengan *codec ilbc*

Pada penelitian ini *packet loss* data *Voice* dapat disebabkan pemrosesan data *voice* pada *codec*, karena pada saat *codec* memproses data *voice*, paket data *voice* dapat saja hilang, pada saat menggunakan *codec ilbc*, nilai *packet loss* adalah 0 % sedangkan *codec alaw*, *gsm*, dan *speex* nilai *packet loss* nya sangat fluktuatif.

4.4 Hasil pengukutan rata-rata *throughput*

Throughput yaitu kecepatan (rate) transfer data efektif yang diukur dalam bps. Pada penelitian ini *throughput* ilbc yang terukur adalah sebagai berikut :





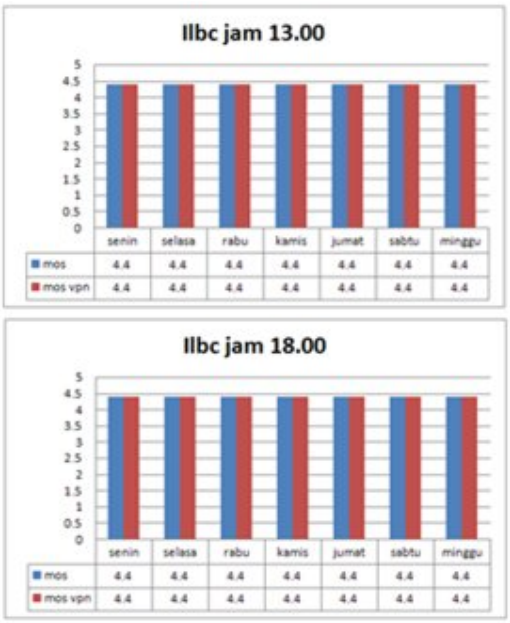
Gambar 8. Hasil pengukuran *throughput* dengan *codec ilbc*

Pada penelituan ini pengukuran *throughput* yang paling kecil adalah dengan menggunakan *codec ilbc*. Secara teori penggunaan VoIP saat menggunakan VPN membutuhkan *throughput* yang lebih besar namun pada saat pengukuran terkadang saat menggunakan VPN, *throughput* yang dihasilkan lebih kecil, hal ini dapat disebabkan pada jaringan *internet* dan terjadi ketidakstabilan saat pengkompresan data *voice* serta terjadinya *packet loss* data *voice.*

4.5 Hasil Pengukuran MOS

Pada penelitian ini pengukuran MOS menggunakan *Software VQManager*. Pada

pengukuran MOS dilakukan bersamaan dengan pengukuran QoS. Pengukuran MOS pada *VQManager* mengacu pada nilai *delay, jitter* dan *packet loss* yang terukur pada *software VQManager*, nilai MOS didapat ketika nilai QoS sudah terukur pada software *VQManager* sehingga secara otomatis saat nilai QoS sudah terukur maka nilia MOS akan tampil bersamaan pada nilai QoS pada *software VQManager* tersebut. Rumus pengukuran MOS pada *Software VQManager* secara default pada *software VQManager* adalah pada *delay* > 300 ms maka nilai MOS adalah < 3,1 dan jika *delay* < 300 ms nilai MOS adalah > 3,6. Kemudian saat *jitter* > 150 ms nilai MOS adalah < 3,1 dan jika nilai *jitter* < 150 ms nilai MOS > 3,6. Kemudian jika nilai *packet loss* > 30 % maka nilai MOS adalah < 3,1 dan jika *packet loss* < 30 % nilai MOS adalaha > 3,6. Nilai kualitas suara pada penelitian ini adalah sebagai berikut: 1 = *Bad (Very annoying)*, 2 = *Poor (Annoying)*, 3 = *Fair (Slightly annoying)*, 4 = *Good (Perceptible but not annoying)*, 5 = *Exellent (Imperceptible)*. Hasil pengkuran MOS ilbc adalah sebagai berikut :

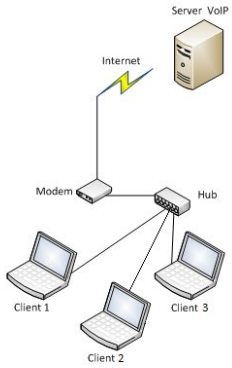


Gambar 9. Hasil pengukuran MOS pada *codec ilbc*

Dari hasil pengkuran, nilai MOS yang terbaik adalah dengan menggunakan *codec ilbc* yaitu sebesar 4,4. Pada saat dilakukan komunikasi hanya *codec ilbc* yang memiliki kualitas suara yang baik dibandingkan dengan *codec* yang lain.

4.6. Pengujian dan Analisis Keamanan VoIP

Pada penelitian ini setelah perancangan VoIP dibuat maka selanjutnya adalah pengujian keamanan. Pengujian keamanan pada VoIP ini dilakukan dengan cara penyadapan melalui *software cain and abel*, hasilnya terbukti dengan menggunakan *software cain and abel* saat *client* sedang berkomunikasi, *client* 3 dapat mencapture *protocol* SIP. Kelemahan dari komunikasi menggunakan VoIP adalah data *payload* tidak diproteksi sehingga ketika dikirimkan dan ditangkap maka akan dengan mudah data tersebut disadap pihak lain, ini terbukti setelah data *payload* VoIP ditangkap data *payload* dapat diputar kembali, sehingga komunikasi antara *client* 1 dan *client* 2 dapat didengar kembali. hal ini membuktikan bahwa komunikasi VoIP belum aman. Kemudian pada saat penyadapan dilakukan kembali, namun ditambahkan *software* VPN antara kedua *client* tersebut, ternyata *payload* tidak terdeteksi sehingga data *payload* tidak dapat dimainkan ulang. Hasil penelitian menunjukan bahwa komunikasi VoIP sangat mudah untuk disadap namun dengan penambahan *software* VPN komunikasi VoIP terbukti aman karena terdapat tunnel dan data dienkripsi sehingga pihak lain tidak dapat menyadapnya.



Gambar 10. Topologi penyadapan VoIP

V. Kesimpulan

Dari penelitian dan analisa data yang telah dilakukan maka dapat diambil beberapa kesimpulan sebagai berikut :

1. Dari keempat *codec* tersebut *codec ilbc* yang stabil untuk digunakan komunikasi
2. Pemilihan jenis *codec* yang tepat perlu untuk meminimalisasi nilai *QoS* yang terjadi pada jaringan VoIP karena pemilihan *codec* sangat menentukan kualitas suara.

3. Penggunaan VPN dapat mencegah penyadapan pada VoIP
4. Terbukti bahwa dengan menggunakan VoIP biaya telekomunikasi menjadi hemat
5. Nilai *throughput* menggunakan VPN lebih besar dibandingkan tanpa VPN

Daftar Pustaka

1. Purbo,W.Onno & Raharja, Anton. 2010. *VoiP Cookbook Building your own Telecommunication Infrastructure.* hlm 5.
2. Taufiq, Mochammad. 2008. Membuat SIP *Extensions* padan Linux Trixbox untuk *Server* VoIP (Skripsi). hlm 11.
3. Final,Muhamad Zuhdan. 2009. Rancang Bangun dan Analisis VoIP (Skripsi) Universitas Indonesia. hlm 10
4. Http://araihan.wordpress.com/2009/10/06/*configure-l2tp-ipsec-vpn-using-windows-server*-2008/
5. Http://computing.fnal.gov/vpn/