RANCANG BANGUN SERVER INTERACTIVE VOICE RESPONS (IVR) PADA EMERGENCY CALL MENGGUNAKAN VIRTUAL PRIVATE NETWORK (VPN) BERBASIS WIRELESS

SKRIPSI

Disusun Oleh

FINO DWI JAYANTO

NIM : 08.12.508

PROGRAM STUDI TEKNIK ELEKTRO S-1

KONSENTRASI TEKNIK KOMPUTER

FAKULTAS TEKNOLOGI INDUSTRI

INSTITUT TEKNOLOGI NASIONAL MALANG

2012

LEMBAR PERSETUJUAN

RANCANG BANGUN SERVER INTERACTIVE VOICE RESPONS (IVR) PADA EMERGENCY CALL MENGGUNAKAN VIRTUAL PRIVATE NETWORK (VPN) BERBASIS WIRELESS

SKRIPSI

Disusun dan diajukan untuk melengkapi dan memenuhi persyaratan guna mencapai gelar Sarjana Teknik Strata satu (S-1)

Disusun oleh :

FINO DWI JAYANTO
0812508

Mengetahui,

Ketua Program Studi Teknik Elektro S-1

M. Ibrahim Ashari.ST ,MT
NIP.Y.1030100358

Diperiksa dan disetujui,

Dosen Pembimbing I	Dosen Pembimbing II
Dr. Eng. Aryuanto Soetedjo, ST.MT	**Bima Aulia Firmandani, ST**
NIP.P.1030800417	**1121**

JURUSAN TEKNIK ELEKTRO S-1
KONSENTRASI TEKNIK KOMPUTER
FAKULTAS TEKNOLOGI INDUSTRI
INSTITUT TEKNOLOGI NASIONAL MALANG
2013

SURAT PERNYATAAN ORISINALITAS

Yang bertanda tangan di bawah ini :

Nama	: **Fino Dwi Jayanto**
NIM	: **08.12.508**
Program Studi	: **Teknik Elektro S-1**
Konsentrasi	: **Teknik Komputer**

Dengan ini menyatakan bahwa Skripsi yang saya buat adalah hasil karya sendiri, tidak merupakan plagiasi dari karya orang lain. Dalam Skripsi ini tidak memuat karya orang lain, kecuali dicantumkan sumbernya sesuai dengan ketentuan yang berlaku.

Demikian surat pernyataan ini saya buat, dan apabila di kemudian hari ada pelanggaran atas surat pernyataan ini, saya bersedia menerima sangsinya.

Malang, 7 Mei 2014

Yang membuat Pernyataan,

Fino Dwi Jayanto
0812508

RANCANG BANGUN SERVER INTERACTIVE VOICE RESPONS (IVR) PADA EMERGENCY CALL MENGGUNAKAN VIRTUAL PRIVATE NETWORK (VPN) BERBASIS WIRELESS

Fino Dwi Jayanto
(08.12.508)

Dr. Eng. Aryuanto Soetedjo, ST, MT dan Bima Aulia Firmandani, ST

Konsentrasi Komputer, JurusanTeknik Elektro
Fakultas Teknologi Industri
Institut Teknologi Nasional Malang
Jln. Raya Karanglo Km 2 Malang
Email: Onif_18@yahoo.com

Abstark

Saat ini system IVR banyak digunakan untuk layanan informasi tagihan rekening listrik, informasi paket penginapan di hotel, cek tagihan telepon. Dalam skripsi ini penulis akan mencoba untuk lebih memaksimalkan fitur-fitur sistem IVR yang sudah ada agar sistem IVR tidak hanya dikenal sebagai system informasi saja. Sistem IVR juga dapat digunakan sebagai pe-routing panggilan telepon. Nomor-nomor panggilan instansi tersebut akan dikemas menjadi satu paket layanan. User cukup mengakses nomor panggilan layanan darurat yang telah disediakan, dan langsung berhadapan dengan sistem IVR sebagai pemandu user untuk memilih instansi layanan sesuai yang dibutuhkan.

Pada penelitian ini telah dirancang server interactive voice response (IVR) pada Emergency Call Menggunakan Virtual Private Network (Vpn) Berbasis Wireless. Karena menggunakan Wireless, maka transmisi data akan dilindungi dengan menggunakan VPN (virtual private network). VoIP dengan VPN yang menggunakan Open VPN, merupakan VPN dengan teknologi tunneling dan enskripsi berfungsi melindungi jalur komunikasi VoIP. Implementasi VoIP tanpa menggunakan VPN terbukti rentan dari ancaman penyadapan yang.

Dalam sistem ini, komunikasi VoIP melalui VPN menggunakan wireless terbukti aman dari bentuk penyadapan suara, ini dibuktikan dari hasil pengujian dan analisa jalur komunikasi VoIP dengan VPN menggunakan wireless secara lokal menunjukan bahwa komunikasi suara yang terjadi pada VoIP tidak bisa dilakukan penyadapan oleh yang tidak berkepentingan.

Kata Kunci: *Interactive Voice Response (IVR), VoIP, Virtual Private Network (VPN), OpenVPN, Wireless*

KATA PENGANTAR

Puji syukur kehadirat Allah SWT atas segala limpahan berkat dan rahmat-Nya sehingga penelitian yang berjudul "RANCANG BANGUN SERVER INTERACTIVE VOICE RESPONS (IVR) PADA EMERGENCY CALL MENGGUNAKAN VIRTUAL PRIVATE NETWORK (VPN) BERBASIS WIRELESS" dapat terselesaikan.

Penelitian ini dibuat untuk memenuhi salah satu syarat dalam memperoleh gelar sarjana teknik. Ucapan terima kasih yang sebesar–besarnya kami ucapkan kepada :

1. Bapak Ir. SoeparnoJiwo, MT selaku Rektor ITN Malang.
2. Bapak Ir. Anang Subardi, MT selaku Dekan Fakultas Teknologi Industri ITN Malang.
3. Bapak M. Ibrahim Ashari, ST.MT selaku Ketua Program Studi Teknik Elektro S-1 ITN Malang.
4. Bapak Dr. Eng. Aryuanto Soetedjo, ST.MT selaku Dosen Pembimbing I.
5. Bapak Bima Aulia Firmandani, ST selaku Dosen Pembimbing II.
6. Kedua orangtua dan saudara-saudara yang telah memberi motivasi dalam penyusunan penelitian ini.
7. Mahasiswa Elektro S-1 angkatan 2008 dan asisten Lab. P K&M.
8. Semua pihak yang telah membantu dalam penulisan dan penyusunan penelitian ini.

Penulis menyadari bahwa penelitian ini masih jauh dari sempurna, untuk itu kritik dan saran dari pembaca sangat penulis harapkan untuk perbaikan penelitian ini.

Malang, Agustus 2013

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1 Latar Belakang

IVR merupakan suatu sistem yang dapat digunakan untuk menerima dan menjawab setiap panggilan telepon secara otomatis dengan cara penekanan digit tombol telepon. Aplikasinyapun beragam mulai dari layanan informasi tagihan rekening listrik, informasi paket-paket penginapan di hotel, informasi cek tagihan telepon. Dengan kata lain fitur dari sistem IVR selama ini banyak digunakan sebagai layanan system informasi saja.

Dari latar belakang tersebut penulis akan mencoba untuk lebih memaksimalkan lagi dari fitur layanan sistem IVR yang sudah ada agar sistem IVR tidak hanya dikenal dan digunakan sebagai system informasi saja melainkan sistem IVR juga dapat digunakan sebagai pe-routing panggilan telepon. Disini penulis akan merancang suatu server IVR untuk layanan panggilan darurat (*Emergency Call*), dimana di dalam server IVR ini terdapat beberapa nomor – nomor panggilan instansi layanan darurat, seperti layanan rumah sakit, kantor kepolisian, dan dinas pemadam kebakaran. Nomor – nomor panggilan instansi tersebut akan dikemas menjadi satupaket layanan (*Emergency call*). *User* hanya cukup mengakses / men-*dial* nomor panggilan layanan darurat yang telah disediakan, kemudian *user* akan langsung berhadapan dengan sistem IVR yang akan memandu *user* untuk memilih instansi layanan sesuai yang dibutuhkan oleh *user*. Dan perancangan server IVR ini membutuhkan transmisi data melalui jaringan computer .

Pada penelitian tentang *IVR (Interactive Voice Response)* sebelumnya, *IVR (Interactive Voice Response)* yang telah dibuat mempunyai kelemahan dengan system keamanan dalam transmisi data dan system koneksinya yang masih menggunakan kabel sebagai perantara jaringannya. Sehingga dalam penulisan skripsi ini penulis menambahkan *VPN (Virtual Private Network)* sebagai pengaman komunikasi atau transmisi data.Sehingga pada saat IVR melakukan transmisi data melalui *Wireless*, maka data yang akan ditransmisikan oleh IVR akan terjaga keamanannya.

VPN adalah jaringan privat yang secara fisik tidak ada, tapi mengapa disebut secara fisik tidak ada karena jaringan ini dibentuk dengan memanfaatkan infrastruktur

internet yang telah ada kemudian dilakukan tunneling sehingga disebut privat karena tidak semua bias mengakses *tunnel* tersebut. Untuk mengimplementasikan *VPN* dibutuhkan *server VPN* yang akan digunakan untuk menyediakan *tunnel* dan enkripsi jalur transmisi data.

Denganadanya server IVRpada (*Emergency call*) dan*VPN (Virtual Private Network)* yang dirancangolehpenulisini, diharapakan*user*bisalebih optimal dalammenggunakanlayanankomunikasiberbasis IVR terutamadalamhalpanggilandarurat (*Emergency call*).

1.2 Rumusan Masalah

Permasalahan yang diangkat pada skripsi ini dapat dirumuskan sebagai berikut :

1. Bagaimana merancang dan membangun server *Interactive Voice Response* (IVR) sebagai pe-routing nomor ekstensi panggilan darurat dengan menggunakan *Virtual Private Network* (VPN) sebagai pengaman komunikasi atau transmisi data menggunakan wireless connection.
2. Bagaimana memaksimalkan kinerja dari fungsi server IVR tersebut yang bertujuan untuk menyediakan suatu layanan yang praktis dan mudah untuk pengguna, guna berkomunikasi dengan layanan instansi darurat.

1.3 Tujuan

Adapun tujuan dari skripsi ini, antara lain :

1. Dapat merancangs ebuah *Server Interactive Voice Response* (IVR) sebagai pe-routing panggilan darurat dan *Virtual Private Network* (VPN) sebagai pengaman komunikasi atau transmisi data melalui wireless connection.
2. Menyediakan suatu layanan yang praktis dan mudah untuk pengguna / pengakses guna berkomunikasi dengan pihak instansi layanan darurat pada saat pengguna / pengakses membutuhkan layanan dari instansi terkait.

1.4 Batasan Masalah

Pada penulisan skripsi ini permasalahan hanya di batasi pada :

1. Menggunakan jalur komunikasi *internet protocol*(IP).
2. IP-PBX menggunakan Asterisk.
3. Untuk pengujian *request* layanan *emergency cal l*menggunakan *softphone* pada PC / laptop.
4. Hanya menyediakan satu nomor ekstensi untuk pengaksesan server IVR (1000 untuk server IVR) dan tiga nomor untuk terhubung / dial ke setiap instansi (1001 untuk rumah sakit, 1002 untuk kepolisian, 1003 untuk pemadam kebakaran).
5. Tidak membahas kecepatan panggilan.

1.5 Metodologi Penelitian.

Adapun metode penelitian yang digunakan adalah sebagai berikut:

1. Studi literatur

Pengumpulan data yang dilakukan dengan mencari bahan-bahan kepustakaan dan referensi dari berbagai sumber sebagai landasan teori yang ada hubunganya dengan permasalahan yang dijadikan objek penelitian.

2. Perancangan dan Implementasi

Berdasarkan data dan informasi yang telah diperoleh serta analisa kebutuhan untuk membangun sistem ini, akan dibuat rancangan kerangka global yang menggambarkan mekanisme dari sistem yang akan dibuat dan diimplementasikan kedalam sistem.

3. Eksperimen dan Evaluasi

Pada tahap ini, sistem yang telah selesai dibuat akan diuji coba, yaitu pengujian berdasarkan fungsionalitas, dan akan dilakukan koreksi dan penyempurnaan jika diperlukan.

1.6 Sistematika Penulisan

Pada penulisan skripsi ini terdiri atas lima pembahasan yaitu :

BAB I : PENDAHULUAN

Bab ini merupakan bagian pendahuluan dimana akan tercakup secara umum mengenai latar belakang penulisan laporan, ruang lingkup karya tulis skripsi ini, tujuan dan manfaat yang mau dicapai, metodologi yang dipakai dalam penyusunan laporan dan sistematika penulisan yang digunakan.

BAB II : TINJAUAN PUSTAKA

Bab ini berisi tentang teori – teori yang mendukung dan berhubungan dengan judul penulisan skripsi.

BAB III : ANALISA DAN PERANCANGAN SISTEM

Bab ini berisi mengenai analisa kebutuhan sistem baik sofware maupun hardware yang di perlukan untuk membuat kerangka global yang menggambarkan mekanisme dari sistem yang akan di buat.

BAB IV : IMPLEMENTASI DAN PENGUJIAN SISTEM

Bab ini berisi penjelasan pembahasan program sesuai dengan permasalahan yang diambil dalam penulisan skripsi.

BAB V : PENUTUP

Bab ini berisi kesimpulan dan saran dari penulisan skripsi.

BAB II

LANDASAN TEORI

2.1 Interactive Voice Response (IVR).

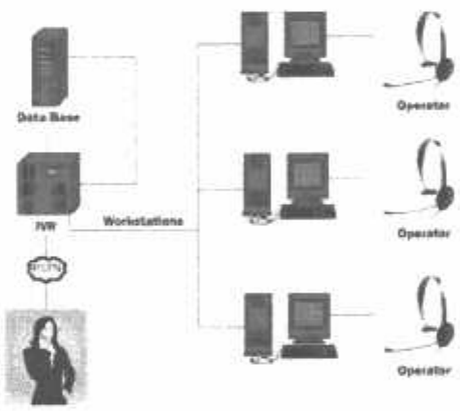
Interactive Voice Response (IVR) adalah teknologi telepon dimana sebuah komputer bisa mendeteksi suara (*voice*) dan penekanan tombol pesawat telepon dengan menggunakan panggilan telepon normal. *Interactive Voice Response* (IVR) merupakan suatu sistem yang dapat digunakan untuk menerima dan menjawab setiap panggilan telepon secara otomatis. Sistem IVR dapat merespon panggilan menggunakan suara yang telah direkam terlebih dahulu, kepada pemanggil untuk pemrosesan berikutnya. Pada sistem IVR komputer berinteraksi dengan pemanggil, dimana pemanggil memberikan input terhadap sistem dengan cara menekan keypad pada telepon *dual tone multy frequency* (DTMF) atau dengan mengatakan sesuatu (bahasa yang natural untuk dikenali). Kebanyakan sistem IVR menyediakan seleksi menu untuk *routing* panggilan tanpa membutuhkan campur tangan operator. Petugas operator hanya berperan bila perlu interaksi percakapan secara langsung, sehingga dapat lebih berkonsentrasi terhadap keluhan atau pembicaraan telepon yang *urgent* sifatnya. Prinsip dasar dari semua sistem IVR adalah bagaimana pemanggil membaca menu dan memilih pilihan dan menu untuk melakukan tindakan atau sebagai alternatif memasukkan informasi (pada format nomor melalui penekanan keypad).

Sistem merubah kompleksitas IVR banyak kemajuan untuk me*generate text on the fly* dengan menggunakan sistem *text-to-speech* (TTS) dan menyutujui input suara *user speech recognation*. Ketika TTS dan *speech recognition* dapat diimplementasikan, maka hal ini dapat menyediakan level yang tinggi dalam penggunaannya, tetapi implementasinya tidak sekompleks seperti yang sering digunakan.Sebelum perekaman pesan dimainkan untuk pemanggil maka pemanggil akan merespon dengan input dari keypad DTMF,dimana asterisk dapat dengan mudah mengenali pada saat pengistalan.

Perbedaan IVR dengan *audiotext* adalah *audiotext* merupakan suatu pemrosesan suara yang mempresentasikan pesan yang direkam lebih dahulu (*pre-recorded massages*), sedangkan IVR mempresentasikan respon suara berdasarkan data yang disimpan dalam database. *Audiotext* merupakan fitur standart untuk semua sistem *voice mail.*

Saat ini sistem IVR dapat digunakan untuk menjawab pertanyaan telepon dari pelanggan, Contoh layanan yang sering digunakan, antara lain untuk mengetahui jumlah tagihan rekening telepon untuk bulan sekarang , saldo rekening bank, suku bunga hari ini,

jumlah stock barang di gudang, dan sebagainya. Secara otomatis sistem IVR akan menjawab dan menterjemahkan data dari database dalam bentuk suara sehingga dapat didengar dan dimengerti oleh *customer* atau *client*. Sistem IVR harus mempunyai *recording* suara untuk menterjemahkan data – data tersebut dan mengkonversikan dalam bentuk suara. IVR akan sangat berguna untuk mendukung layanan *call center* yang beroprasi selama 24 jam. Sistem IVR sangat membantu proses pelayanan pelanggan, karena didukung oleh sistem komputerisasi yang dapat beroprasi 24 jam sehari. Sistem IVR adalah sistem komputer yang membantu pelanggan untuk mendapatkan informasi yang dibutuhkan atau untuk menyampaikan informasi yang hendak disampaikan korporasi melalui telepon.



Gambar 2.1 Sistem Interactive Voice Response (IVR)

2.1.1 Fitur – Fitur IVR

2.1.1.1 Otomasi Layanan.

Penerapan sistem IVR yang salah untuk beberapa jenis pelayanan, pelanggan yang ingin mendapatkan informasi *rate* atau informasi klaim dari perusahaan asuransi, akan tepat bila dilayani dengan sistem IVR. Namun jika pelanggan ingin melaporkan kehilangan kartu kredit dan membatalkan transaksi maka akan lebih tepat dan meyakinkan jika dilayani oleh pegawai. Oleh karena itu, sebelum memutuskan untuk mengotomasikan sebuah pelayanan perlu diklihat terlebih dahulu mengenai sudut pandang pelanggan. Bagaimana kompleksitas transaksi antara korporasi dengan pelanggan. Seberapa penting hasil yang akan diperoleh oleh pelanggan. Apakah pelanggan menyukai privasi atau interaksi manusia langsung.

2.1.1.2 Teknologi Terbaru.

Apakah pelanggan merespon sistem IVR secara negatif atau positif seringkali tergantung kepada bagaimana *state-of-the-art* atau keterbaruan teknologi dari sistem IVR tersebut Bentuk paling dasar dari sistem IVR adalah suara yang terekam untuk memandu pelanggan melalui telepon, kemudian mempersilahkan pelanggan untuk memilih informasi yang dikehendaki dengan cara menekan tombol-tombol pesawat telepon. Teknologi dasar ini tepat digunakan untuk pelayanan transaksi antara korporasi dan pelanggan yang sederhana. Jika diterapkan untuk pelayanan yang kompleks tentu saja berarti korporasi telah mengabaikan pelanggan.

2.1.1.3 Konfigurasi Berbasis Web

Dalam pemanfaatannya, sebuah sistem IVR harus dapat beradaptasi dengan kebutuhan konten informasi yang ingin disajikan kepada pelanggan. Sistem IVR yang ssat ini ada di pasaran biasanya membutuhkan pemrograman ulang untuk membuat perubahan aliran menu pada sistem IVR. Cara konvensional tersebut tidak mudah dilakukan oleh administrator atau operator sistem Hal ini karena sumber daya manusia yang dimiliki oleh korporasi belum tentu mampu melakukan pemrograman ulang karena fungsi tersebut tidak termasuk ke dalam *core bussines* dari korporasi yang bersangkutan. Sistem IVR yang mudah dikonfigurasi dengan antarmuka berbasis web akan memudahkan operator sistem IVR dengan kemampuan komuter dasar dapat melakukan konfigurasi dan perubahan pada aliran menu, isi suara, dan data-data yang ingin disajikan.

Operator dapat merekam suara yang ingin disajikan dalam aliran menu IVR di PC biasa dengan menggunakan software perekam yang menu umum (misalnya adalah *windows sound recorder* yang sudah tersedia di sistem operasi windows). Selanjutnya operator tersebut dapat mengupload file-file sound yang telah direkam ke sistem IVR. Disini operator dapat menentukan urutan dan aliran menu, yaitu disesuaikan dengan tombol telepon dalam melakukan pilihan menu setelah konfigurasi tersebut dilakukan. Sistem IVR dapat menyesuaikan diri dengan konfigurasi yang baru dan semuanya itu dapat dilakukan tenpa melakukan pemrograman ulang.

2.1.1.4 IVR *Engine*

Perangkat lunak IVR bertugas membaca file konfigurasi yang berisi aliran menu dan isi menu, mebterjemahkannya, dan kemudian mengeksekusinya. Jika pelanggan telah melakukan dial ke sistem IVR maka IVR *engine*akan segera mengeksekusi setiap baris

konfigurasi. Masing-masing baris konfigurasi berisi perintah-perintah yang umum pada sistem IVR. Contoh perintah tersebut adalah perintah untuk mem-*playback file sound* yang telah direkam. File sound tersebut misalnya ada *greeting* dan menu pilihan awal yang dilanjutkan perintah untuk menunggu penelepon untuk menekan tombol sesuai dengan pilihan yang disajikan.

Salah satu perintah yang dapat dieksekusi adalah perintah untuk membaca data di database berdasarkan informasi tertentu untuk melakukan pencarian data di database. IVR *engine*akan memerintahkan *Dbridge* untuk menghubungi sistem database. Sistem database tersebut dapat local atau *remote*, yaitu jika tersedia koneksi ke internet melalui ISP. Hasil *query* dari database yang dapat berupa angka, waktu, dan tanggal dapat langsung dibacakan oleh sistem IVR *engine* yaitu dengan menggunakan file-file *sound default* yang sudah ada di sistem IVR. .

2.2Linux Ubuntu.

Ubuntu merupakan salah satu distribusi Linux yang berbasiskan Debian dan didistribusikan sebagai software bebas. Nama Ubuntu berasal dari filosofi dari Afrika Selatan yang berarti "Kemanusiaan kepada sesama". Ubuntu didesain untuk kepentingan penggunaan personal, namun versi server Ubuntu juga tersedia, dan telah dipakai secara luas.Proyek Ubuntu resmi disponspori oleh *Canonical Ltd.*yang merupakan sebuah perusahaan yang dimiliki oleh pengusaha Afrika Selatan Mark Shuttleworth. Tujuan dari distribusi Linux Ubuntu adalah membawa semangat yang terkandung di dalam Filosofi Ubuntu ke dalam dunia perangkat lunak. Ubuntu adalah sistem operasi lengkap berbasis Linux, tersedia secara bebas dan mempunyai dukungan baik yang berasal dari komunitas maupun tenaga ahli profesional.Ubuntu terdiri dari banyak paket, kebanyakan berasal dari distribusi di bawah lisensi lisensi software bebas. Namun, beberapa software khususnya driver menggunakan *Proprietary software*. Lisensi yang pada umumnya adalah *GNU General Public License* (GNU GPL) dan *GNU Lesser General Public License* (GNU LGPL), dengan tegas menyatakan bahwa pengguna dengan bebas dapat menjalankan, menggandakan, mempelajari, memodifikasi, dan mendistribusikan tanpa pembatasan apapun. Namun tetap ada software proprietary yang dapat berjalan di Ubuntu. Ubuntu berfokus pada ketersediaan kegunaan pada orang disfungsi, keamanan dan stabilitas. Ubuntu juga berfokus pada internasionalosasi dan aksesibilitas untuk dapat menjangkau sebanyak-banyaknya orang. Dalam hal keamanan, perangkat sudo dapat meningkatkan privilage secara sementara untuk melakukan tugas

administratif, sehingga akun *root* dapat terus terkunci, dan mencegah orang tidak terauthorisasi melakukan perubahan sistem atau membuka kelemahan keamanan.Desktop Ubuntu memakai *desktopenvironment* graphis, di antaranya yang paling terkenal adalah GNOME, KDE, Xfce, dan LXDE.Sebelum Ubuntu 11.04 interaksi grafis pengguna adalah GNOME Panel, namun setelah versi 11.04, berubah menjadi Unity. Unity adalah *interface* yang dikembangkan oleh *Canonical* yang awalnya dirancang untuk edisi Netbook.

Gambar 2.2 Logo Linux Ubuntu

Tabel 2.1 Kode Dan Versi Rilis Linux Ubuntu

Versi	Kode Nama	Tanggal Perilisan	Didukung Sampai	
			Desktop	Server
4.10	Warty Warthog	20-10-2004	2006-04-30	
5.04	Hoary Hedgehog	08-04-2005	2006-10-31	
5.10	Breezy Badger	13-10-2005	2007-04-13	
6.06 LTS	Dapper Drake	01-06-2006	2009-07-14	2011-06-01
6.10	Edgy Eft	26-10-2006	2008-04-25	
7.04	Feisty Fawn	19-04-2007	2008-10-19	
7.10	Gutsy Gibbon	08-10-2007	2009-04-18	
8.04 LTS	Hardy Heron	24-04-2008	2011-05-12	2013-04
8.10	Intrepid Ibex	30-10-2008	2010-04-30	
9.04	Jaunty Jackalope	23-04-2009	2010-10-23	
9.10	Karmic Koala	23-04-2009	2011-04-30	
10.04 LTS	Lucid Lynx	29-04-2010	2013-04	2015-04
10.10	Maverick Meerkat	10-10-2010	2012-04	

11.04	Natty Narwhal	28-04-2011	2012-10
11.10	Oneiric Ocelot	13-10-2011	2013-04
12.04 LTS	Precise Pangolin	26-04-2012	2017-04
12.10 LTS	Quantal Quetza	18-10-2012	2014-04

Warna	Arti
Merah	Sudah tidak didukung
Hijau	Masih di dukung
Biru	Rilis masa depan

2.3 Asterisk

Asterisk merupakan salah satu *software* Server VoIP yang di distribusikan melalui GPL (*GNU General Public License*) yang artinya Asterisk adalah seperti *softwareopen source* lainya yang bisa didownload secara gratis di internet. Asterisk sering disebut juga sebagai IPPBX, yaitu memiliki fungsi dan kemampuan layaknya PBX akan tetapi bebasis IP.Asterisk merupakan implementasi dari telepon *Private Branch Exchange* (PBX) yang dibuat oleh *Mark Spencer* dari digium.Inc pada tahun 1999. Asterisk mengizinkan sejumlah telepon untuk membuat panggilan dan menghubungkan servis telepon lain termasuk *Public Switched Telephony Network*(PSTN). Nama Asterisk berasal dari simbol "*", yang berarti *wildcard* di dalam lingkungan sistem operasi DOS, UNIX, dan UNIX-like misalnya Linux. Asterisk memiiki dukungan yang luas terhadap sistem operasi Linux, BSD, MacOSX dan Windows, namun kebanyakan digunakan dalam Linux karena lebih stabil dan lebih mudah. Asterisk dikembangkan untuk memenuhi semua tuntutan aplikasi telephony. Asterisk dapat dioperasikan sebagai SIP Server, IAX Server. Sama seperti Open H.323 Gatekeeper, Asterisk itu sendiri bukan software dengan sebuah sistem yang sederhana karena untuk membangun server ada proses *set up*, konfigurasi sistem termasuk *setup interface* yang digunakan agar dapat dikenali oleh asterisk. Didalam Asterisk terdapat *management tool* yang telah ter-*built in* dalam *engine* tersebut dan dapatdikonfiguarasi secara terpisah. Sehingga dapat disetting pada suatu *interface* tergantungkebutuhan penggunanya.

Asterisk dapat menyediakan layanan *voicemail* berikut direktorinya. Fitur lain yang ada adalah *Call Conference, Interactive Voice Response* (IVR), dan *Call Queuing*. Asterisk

adalah sebuah *Interactive Voice Response*(IVR) yangakan memberikan kemudahan kepada user. Pelayanan yang berbasis IVR memungkinkan komunikasi yang *interactive* antara sistem Asterisk dan *user*. Contohnya dari IVR adalah "silahkan tekan satu untuk... tekan dua untuk...". Asterisk mendukung terlaksananya fasilitas ini. Asterisk adalah *Voice Mail* sistem Layanan *voice mail* layaknya PBX yang umum. Asterisk juga menyediakan layanan pemberitahuan bahwa ada *voice mail* yang masuk dengan mengirimkan ke *email user*.. Asterisk adalah VoIP(*Voice Over Internet Protokol*). Sistem Asterisk menawarkan fitur yang lengkap untuk mendukung VoIP. Asterisk mendukung protokol VoIP yang dapat berinterkoneksi sebagai contoh H.323 dan SIP (*Session Initiation Prokol*).

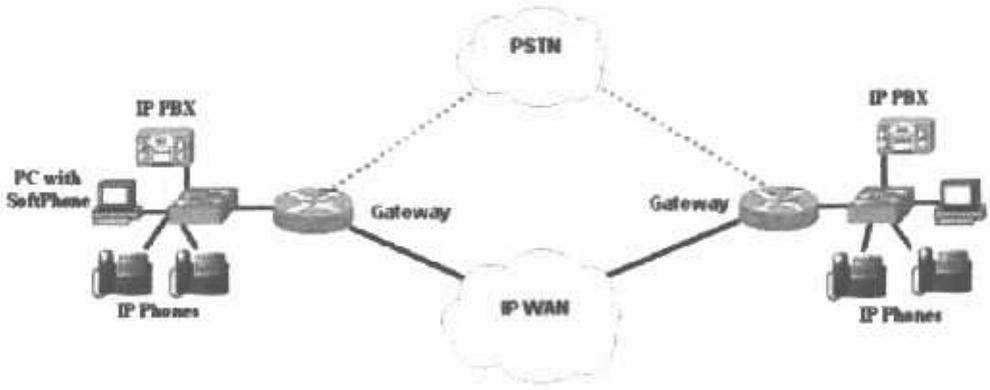
2.4 Voice Over Internet Protocol(VoIP)

VoIPadalah singkatan dari *Voice over Internet Protocol*. Sering kita kenal dengan istilah *Internet telephony*, *IP Telephony*, atau *Digital Phone*. Proses pengiriman suara pada VoIP adalah dengan cara pengiriman suara melalui protokol internet (IP). Sehingga dengan teknologi VoIP ini 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 telephone biasa.

2.4.1 Perbandingan VoIP dengan jaringan suara konvensional

Pada jaringan suara konvesional, pesawat telepon langsung terhubung dengan PABX(*Privat Automated Branch Exchange*). Sedangkan pada operator telepon, seperti PT Telkom, maka pesawat telepon terhubung langsung dengan STO (Sentral Telepon Otomatis) terdekat. Di dalam STO ini terdapat daftar nomor-nomor telepon yang disusun secara bertingkat sesuai dengan daerah cakupannya. Jika seseorang ingin menghubungi rekan yang lain maka ia menekan tuts pesawat telepon dan penekanan tuts tersebut akan menginformasikan lokasi yang dituju melalui nada-nada tertentu, kemudian jaringan akan secara otomatis menghubungkan kedua titik tersebut. Berbeda dengan jaringan suara konvensional, pada jaringan VoIP, setiap *user* yang ingin berkomunikasi haruslah memiliki koneksi ke internet, mempunyai kartu suara yang dihubungkan dengan *speaker* dan *mikrofon*, dan aplikasi *client user* yang berupa perangkat lunak tertentu, maka komputer dapat saling terhubung dalam koneksi VoIP antara satu dengan yang lainnya. Bentuk hubungan tersebut bisa dalam bentuk pertukaran file, suara, gambar. Namun penekanan utama dalam VoIP adalah hubungan keduanya dalam bentuk suara. Bayangkan apabila kedua lokasi yang terkoneksi memiliki jarak yang cukup jauh (antar kota, antar pulau ataupun antar Negara)

maka dapat dilihat keuntungan dari segi biaya. Karena kedua pihak hanya cukup membayar biaya koneksi internet saja, yang tentunya akan lebih murah daripada biaya pulsa telepon sambungan langsung jarak jauh (SLJJ) atau internasional (SLI).Pada perkembangannya, sistem koneksi VoIP mengalami beberapa kali perubahan. Bentuk peralatan pun berkembang, tidak hanya berbentuk komputer yang saling berhubungan, tetapi peralatan lain seperti pesawat telepon biasa dapat terhubung dengan jaringan VoIP. Jaringan data digital dengan *gateway* untuk VoIP memungkinkan berhubungan dengan PABX atau jaringan analog telepon biasa. Bentuk komunikasinya tidak hanya suara saja. Dapat berbentuk tulisan (*chating*) atau jika jaringan memiliki *bandwidth* cukup besar maka dapat dipakai untuk Video Conference. Dalam bentuk yang lebih lanjut dikenal dengan UC (*unified communication*) komunikasi dalam bentuk multimedia sebagai kelanjutan bentuk komunikasi suara (VoIP). Keluwesan dari VoIP dalam bentuk jaringan, peralatan dan media komunikasinya membuat VoIP menjadi cepat populer di masyarakat umum.



Gambar 2.3 Jaringan *Voice Over Internet Protokol*(VoIP)

Keuntungan VoIP :

1. Biaya yang rendah untuk sambungan langsung jarak jauh. Karena penekanan utama dari VoIP adalah biaya. Untuk dua lokasi yang terhubung dengan internet maka biaya percakapan menjadi sangat rendah.
2. Memanfaatkan infrastruktur jaringan data yang sudah ada untuk suara. Bagi perusahaan sudah mempunyai infrastruktur jaringan. Jika memungkinkan jaringan yang ada bisa dibangun jaringan VoIP dengan mudah. Karena tidak diperlukan tambahan biaya bulanan untuk penambahan komunikasi suara VoIP.

3. Penggunaan bandwidth yang lebih kecil daripada telepon biasa. Dengan majunya teknologi penggunaan *bandwidth* untuk *voice*, sekarang ini menjadi sangat kecil. Teknik pemampatan data memungkinkan suara hanya membutuhkan sekitar 8kbps *bandwidth.*
4. Dapat digabung dengan jaringan telepon lokal yang sudah ada. Dengan adanya *gateway* bentuk jaringan VoIP bisa disambungkan dengan PABX yang ada dikantor. Komunikasi antar kantor bisa menggunakan pesawat telepon biasa.
5. Berbagai bentuk jaringan VoIP bisa digabungkan menjadi jaringan yang besar. Contoh di Indonesia adalah *VoIP Rakyatwww.voiprakyat.or.id.*
6. Variasi penggunaan peralatan yang ada, misal dari PC sambung ke telepon biasa, *IP phone* handset.

Kelemahan VoIP :

1. Kualitas suara tidak sejernih Telkom. Hal ini sering terjadi karena efek dari kompresi suara dengan *bandwidth* kecil maka akan ada penurunan kualitas suara dibandingkan jaringan PSTN konvensional. Namun jika koneksi internet yang digunakan adalah koneksi internet pita lebar/*broadband* seperti Telkom *Speedy*, maka kualitas suara akan jernih - bahkan lebih jernih dari sambungan Telkom dan tidak terputus-putus.
2. Ada jeda dalam berkomunikasi. Proses perubahan data menjadi suara, jeda jaringan, membuat adanya jeda dalam komunikasi dengan menggunakan VoIP. Kecuali jika menggunakan koncksi *Broadband.*
3. Tidak pernah ada jaminan kualitas jika VoIP melewati internet.
4. Peralatan relatif mahal. Peralatan VoIP yang menghubungkan antara VoIP dengan PABX (*IP telephony gateway*) relatif berharga mahal. Diharapkan dengan makin populernya VoIP ini maka harga peralatan tersebut juga mulai turun harganya.

2.5 VPN (Virtual Private Network)

VPN adalah singkatan dari *Virtual Private Network*, yaitu Sebuah cara aman untuk mengakses jaringan lokal yang berada diluar jangkauan, dengan menggunakan media internet atau jaringan umum lainnya untuk melakukan transmisi data secara pribadi, Perlu penerapan teknologi tertentu,agar walaupun menggunakan media 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.*

VPN adalah suatu jaringan privat (biasanya untuk instansi atau kelompok tertentu) di dalam jaringan internet (publik), dimana jaringan privat ini seolah-olah sedang mengakses jaringan lokalnya tapi menggunakan jaringan publik.

VPN adalah sebuah koneksi Virtual yang bersifat privat mengapa disebut demikian karena pada dasarnya jaringan ini tidak ada secara fisik hanya berupa jaringan virtual dan mengapa disebut privat karena jaringan ini merupakan jaringan yang sifatnya privat yang tidak semua orang bisa mengaksesnya.*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 untuk keamanan data.

2.6 Fungsi Utama Teknologi *VPN*

Teknologi *VPN* menyediakan tiga fungsi utama untuk penggunanya. Ketiga fungsi utama tersebut antara lain sebagai berikut:

2.6.1 *Confidentially* (Kerahasiaan)

Dengan digunakannnya jaringan publik yang rawan pencurian data, maka teknologi *VPN* menggunakan sistem kerja dengan cara mengenkripsi semua data yang lewat melauinya. Dengan adanya teknologi cnkripsi tersebut, maka kerahasiaan data dapat lebih terjaga. Walaupun ada pihak yang dapat menyadap data yang melewati internet bahkan jalur *VPN* itu sendiri, namun belum tentu dapat membaca data tersebut, karena data tersebut telah teracak. Dengan menerapkan sistem enkripsi ini, tidak ada satupun orang yang dapat mengakses dan membaca isi jaringan data dengan mudah.

2.6.2*Data Intergrity* (Keutuhan Data)

Ketika melewati jaringan internet, sebenarnya data telah berjalan sangat jauh melintasi berbagai negara. Pada saat perjalanan tersebut, berbagai gangguan dapat terjadi terhadap isinya, baik hilang, rusak, ataupun dimanipulasi oleh orang yang tidak seharusnya. Pada *VPN* terdapat teknologi yang dapat menjaga keutuhan data mulai dari data dikirim hingga data sampai di tempat tujuan.

2.6.3 *Origin Authentication* (Autentikasi Sumber)

Teknologi *VPN* memiliki kemampuan untuk melakukan autentikasi terhadap sumber-sumber pengirim data yang akan diterimanya. *VPN* akan melakukan pemeriksaan terhadap semua data yang masuk dan mengambil informasi dari sumber datanya.

Kemudian, alamat sumber data tersebut akan disetujui apabila proses autentikasinya berhasil. Dengan demikian, *VPN* menjamin semua data yang dikirim dan diterima berasal dari sumber yang seharusnya. Tidak ada data yang dipalsukan atau dikirim oleh pihak-pihak lain

2.7 OpenVPN

OpenVPN adalah sebuah implementasi *VPN open source* yang didasarkan pada *SSL (Secure Socket Layer)*. Implementasi klien *OpenVPN* tersedia untuk banyak sistem operasi, termasuk *Linux*, *Windows 2000/XP* atau yang lebih tinggi, *OpenBSD*, *FreeBSD*, *NetBSD*, *Mac OS X*, dan *Solaris*. Pada sebuah *VPN*, *OpenVPN* akan meng-enkapsulasi semua trafik (termasuk protokol DNS dan protokol-protokol lain) di *tunnel* yang terenkripsi, jadi bukan hanya satu *port TCP* saja.

Gambar 2.4. Logo *OpenVPN*

OpenVPN juga mempunyai beberapa kerugian, seperti latensi yang cukup tinggi.Beberapa latensi tak terelakan karena semua enkripsi/dekripsi dilakukan di aplikasi *user*, dengan memakai komputer yang relatif baru kedua ujung tunnel dapat mengurangi latensi ini. Biarpun bisa memakai *shared key* yang tradisional, *OpenVPN*akan lebih baik jika digunakan bersama sertifikat *SSL* dan *Certificate Authority*. *OpenVPN* mempunyai banyak keuntungan yang membuatkannya pilihan yang baik untuk menyediakan keamanan *end-to-end*.

OpenVPN perlu menyambung sebuah *port TCP* atau *UDP* di *remote site*. Setelah tersambungkan, *OpenVPN*akan mengenkapsulasi semua data ke *Networking Layer*, atau bahkan sampai ke lapisan *Data-Link*.

2.7.1 Perbandingan OpenVpn Dengan Perangkat Lunak VPN Yang Lain

2.7.1.1 *Remote Access* VPN

Remote access yang biasa juga disebut *virtual private dial-up network* (VPDN), menghubungkan antara pengguna yang *mobile* dengan *local area network* (LAN). Jenis

VPN ini digunakan oleh pegawai perusahaan yang ingin terhubung ke jaringan khusus perusahaannya dari berbagai lokasi yang jauh (*remote*) dari perusahaannya. Biasanya perusahaan yang ingin membuat jaringan VPN tipe ini akan bekerjasama dengan *enterprise service provider* (ESP). ESP akan memberikan suatu *network access server* (NAS) bagi perusahaan tersebut. ESP juga akan menyediakan *software* klien untuk komputer-komputer yang digunakan pegawai perusahaan tersebut.

Untuk mengakses jaringan lokal perusahaan, pegawai tersebut harus terhubung ke NAS dengan men-*dial* nomor telepon yang sudah ditentukan. Kemudian dengan menggunakan *sotware* klien, pegawai tersebut dapat terhubung ke jaringan lokal perusahaan.

Perusahaan yang memiliki pegawai yang ada di lapangan dalam jumlah besar dapat menggunakan *remote access* VPN untuk membangun WAN. VPN tipe ini akan memberikan keamanan, dengan mengenkripsi koneksi antara jaringan lokal perusahaan dengan pegawainya yang ada di lapangan. Pihak ketiga yang melakukan enkripsi ini adalah ISP.

2.7.1.2 *Point-to-Point* Tunneling Protocol (PPTP)

PPTP dikembangkan oleh Microsoft dan Cisco merupakan protokol jaringan yang memungkinkan pengamanan transfer data dari remote client ke server pribadi perusahaan dengan membuat sebuah VPN melalui TCP/IP (Snader, 2005). Teknologi jaringan PPTP merupakan pengembangan dari remote access Point-to-Point protocol yang dikeluarkan oleh Internet Engineering Task Force (IETF). PPTP merupakan protokol jaringan yang merubah paket PPP menjadi IP datagrams agar dapat ditransmisikan melalui intenet. PPTP juga dapat digunakan pada jaringan private LAN-to-LAN.

Fasilitas utama dari penggunaan PPTP adalah dapat digunakannya public-switched telephone network (PSTNs) untuk membangun VPN. Pembangunan PPTP yang mudah dan berbiaya murah untuk digunakan secara luas, menjadi solusi untuk remote users dan mobile users karena PPTP memberikan keamanan dan enkripsi komunikasi melalui PSTN ataupun internet.

2.7.1.3 IPsec

IPSec merupakan suatu pengembangan dari protokol IP yang bertujuan untuk menyediakan keamanan pada suatu IP dan*layer* yang berada diatasnya (Carmouche,

2006). IPSec (*Internet Protocol Security*) merupakan salah satu mekanisme yang diimplementasikan pada *Virtual Private Network*. Paket IP tidak memiliki aspek *security*, maka hal ini akan memudahkan untuk mengetahui isi dari paket dan alamat IP itu sendiri. Sehingga tidak ada garansi bahwa menerima paket IP merupakan dari pengirim yang benar, kebenaran data ketika ditransmisikan. IPSec merupakan metode yang memproteksi IP datagram ketika paket ditransmisikan pada *traffic*. IPSec berkerja pada*layer* tiga OSI yaitu *network layer* sehingga dapat mengamankan data dari *layer* yang berada atasnya.

2.7.1.4 Perbedaan Antara PPTP, L2TP, dan IPSec

Adanya perbedaan sistem dari masing-masing protocol menimbulkan pertanyaan bagaimana QoS (*Quality of Services*) dari masing-masing protocol pada jaringan VPN. Menurut Arora, 2001 menyebutkan IPsec adalah protocol yang memberikan keamanan paling kuat diantara protocol lainnnya, sementara L2TP protocol yang mempunyai basic keamanan seperti protocol PPTP, tetapi protocol L2TP ini dapat di gabungkan dengan IPsec apabila ingin mendapatkan interoperabilitas yang lengkap dan keamanan yang kuat. Penelitian yang dilakukan oleh Arora ini menggunakan beberapa *vendor* yang berbeda dengan menggunakan indikator seperti keamanan, performansi dengan meliputi *throughput* dan *latency*, skalabilitas, flesibelitas, interoperabilitas dan aplikasi.

Penelitian lain menyebutkan bahwa perbedaan kinerja protocol VPN ini berada pada sistem security dari masing-masing protocol. Menurut Berger, 2006 menyebutkan bahwa perbedaan terdapat pada komplesitas dari metode autentikasi dari masing-masing protocol. Semakin aman sebuah protocol mengirimkan sebuah data maka semakin rumit proses enkasulasi dan enkripsi pada data tersebut, sehingga menyebabkan penambahan ukuran *file* yang akan di transferkan. Penelelitian yang dilakukan Berger untuk membandingkan performansi dari *protocol tunneling vpn* ini menggunakan *vendor* yang berbeda. Perbandingan dilakukan dengan menggunakan indikator seperti fungsional dasar VPN *establishment time, link quality,* dan *tunnel re-initiation time*,Performansi menggunakan parameter *throughput,* dan keamanan.

Dari ke dua penelitian di atas dilakukan dengan membandingkan performansi dealam berbagai aspek seperti fusgionalitas, keamanan, sakalabilitas, dan aplikasi. Hasil dari kedua percobaan di atas menunjukan masing-pasing protokol memiliki kelebihan dan kelemahan dalam performansi di dalam jaringan VPN. Oleh karena itu penelitian terbaru harus dilakukan karena dengan perkembangan teknologi dan metode yang

berkembang pada tunneling VPN. Penellitian ini dimaksudkan untuk melihat perkembangan metode tunneling VPN, dalam hal ini yang akan di bandingkan adalah Tunneling VPN L2TP pada Layer 2 dan IPsec pada Layer 3. pada peneleitian ini PPTP tidak dikutsertakan karena Implementasinya saat ini sudah tidak banyak yang memamkai. QoS (Quality of Services) menjadi sorotoan utama dari penelitian ini, parameter yang akan digunakan adalah *delay, jitter,* dan *throughput* sebagai indikator performansi metode tunneling pada jaringan VPN.

2.8 Softphone

Selain berupa telepon utuh (hardware), perangkat telepon juga bisa berbentuk software. Di dunia VoIP, perangkat ini disebut *SoftPhone.Softphone* memiliki jenis yangberagam baik dari kemampuan dan lisensi. Saat ini banyak *Softphone* yang disebarkan dengan lisensi gratis. Bahkan ada yang menyediakan lisensi software gratis sekalligus layanan jaringan VoIP -nya. *SkyPe* salah satu penyedia *Softphone* Cuma-Cuma,sekaligus layanan PC-to-PC call yang prima. *SoftPhone Skype* ini hanya bisa bekerja di jaringan milik *Skype*. Jika ingin membuat jaringan sendiri harusmenggunakan *Softphone* jenis lain. *Softphone* lain diantaranya adalah X-Lite, IAX-Lite, *MyPhone*. X-Lite merupakan softphone untuk VoIP yang berjalan melalui protokol SIP. Selain suara, X-Lite juga bisa digunakan untuk saling berkirim text dan video. IAX-Lite merupakan softphone yang berjalan melalui protokol IAX. IAX merupakan protokol signaling yang dikembangkan oleh pembuat Asterisk (IP PBX). Untuk protokol H323 dapat menggunakan *MyPhone*.

Gambar 2.5 Softphone X-lite 3.0

2.9 Pengertian Wireless

Wireless adalah teknologi tanpa kabel, dalam hal ini adalah melakukan hubungan telekomunikasi dengan menggunakan gelombang elektromagnetik sebagai pengganti kabel. Saat ini teknologi wireless berkembang dengan pesat, secara kasatmata dapat dilihat dengan semakin banyaknya pemakaian telepon sellular, selain itu berkembang pula teknologi wireless yang digunakan untuk akses internet.

Wireless LAN menggunakan gelombang elektromagetik (radio dan inframerah) untuk melakukan komunikasi data menyalurkan data dari satu point ke point yang lain tanpa melalui fasilitas fisik. Koneksi ini menggunakan frekuensi tertentu untuk menyalurkan data tersebut, kebanyakan Wireless LAN menggunakan frekuensi 2,4GHz. Frekuensi inilah yang disebut dengan Industrial, *Scientificand Medical Band* atau sering disebut ISMBand.

Characteristic	802.11 Wireless LAN	802.3 Ethernet LANs
Physical Layer	Radio Frequency (RF)	Cable
Media Access	Collision Avoidance	Collision Detection
Availability	Anyone with a radio NIC in range of an access point	Cable connection required
Signal Interference	Yes	Inconsequential
Regulation	Additional regulation by local authorities	IEEE standard dictates

Gambar 2.6 Perbandingan Wireless LAN dengan LAN

WLAN menggunakan radio frequencies (RF) sebagai pengganti kabel pada lapisan fisik dan sub-layer MAC dari layer datalink. Dibandingkan dengan kabel, RF memiliki karakteristik sebagai berikut:

1. RF tidak memiliki batas-batas.
2. RF terlindungi dari sinyal luar, sedangkan kabel dalam selubung isolasi. Radio beroperasi secara independen di wilayah geografis yang sama tetapi menggunakan yang sama atau mirip RF dapat mengganggu satu sama lain.
3. Transmisi RF mempunyai tantangan yang sama dengan teknologi gelombang radio lainnya, seperti *Consumer Radio*.
4. Band RF diatur berbeda di berbagai negara. Penggunaan WLAN dikenakan peraturan tambahan dan menetapkan standar yang tidak diterapkan pada LAN kabel.

2.10 Standarisasi Wireless LAN

Beberapa Standar wireless LAN yang dibuat oleh IEEE (Instituteof Electrical Electronic Engineers) yaitu :

1. IEEE 802.11 (Legacy)

IEEE 802.11 adalah versi asli dari standar Wireless LAN yang dirilis pada 1997, namun kini sudah sama sekali tidak digunakan lagi. Beroperasi pada band 2.4 GHz, dan data rate yang ditawarkan hanya 1 Mbps dan 2 Mbps, itu sebabnya kini sudah tidak digunakan lagi karena untuk saat ini data rate 2 Mbps terlalu kecil untuk komunikasi jaringan.

2. IEEE 802.11a

Generasi Penerus dari sang Legacy ini dirilis pada tahun 1999, dengan menggunakan Band 5 GHz dan menawarkan data rate sebesar 6, 9, 12, 18, 24, 36, 48, dan 54 Mbps. Serta menggunakan skema modulasi OFDM.

3. IEEE 802.11b

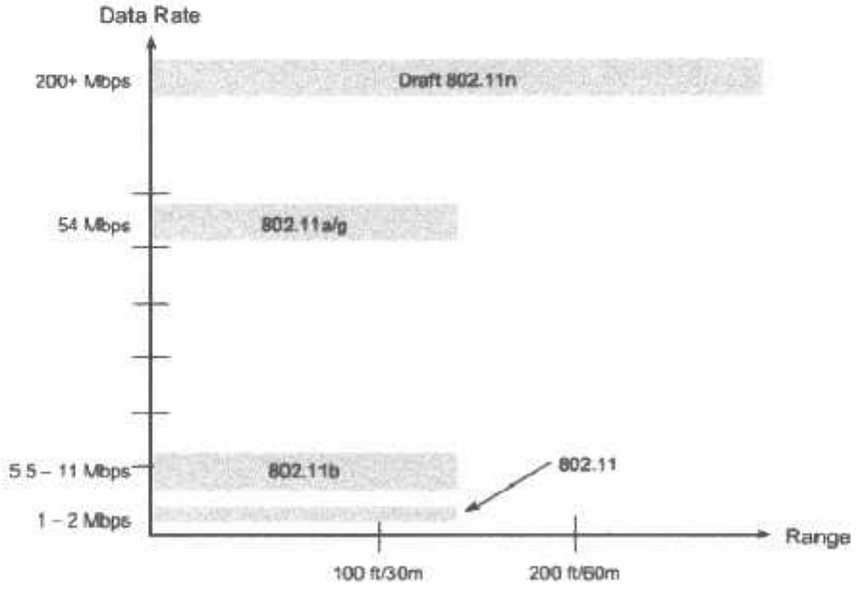
Standar ini dirilis bersamaan dengan IEEE 802.11a pada 1999, namun ia beroperasi pada Band 2.4 GHz, namun IEEE 802.11b ini justru menawarkan data rate yang lebih rendah yaitu 1, 2, 5.5 dan 11 Mbps. Rendahnya data rate ini dibandingkan dengan IEEE.802a dikarenakan menggunakan skema modulasi DSSS, karena skema modulasi yang digunakan IEEE 802a (OFDM) lebih memungkinkan untuk mentransfer data dengan data rate yang lebih tinggi.

4. IEEE 802.11g

Standar yang dirilis pada Juni 2003 ini merupakan soulusi dan juga gabungan dari IEE 802.11a dan IEEE 802.11b, karena menggunakan Band 2.4 GHz namun data rate yang ditawarkan dapat mencapai 54 Mbps, ini dikarenakan menggunakan skema modulasi yang dipakai IEEE 802.11a yaitu OFDM, selain itu keunggulan IEEE 802.11g juga kompatibel secara penuh dengan IEEE 802.11b karena menggunakan frekuensi yang sama 2.4 GHz. Dengan munculnya IEEE 802.11g, perlahan standar IEEE 802.11a mulai ditinggal karena ketidak kompatibelannya dengan standar b dan g.

5. IEEE 802.11n

IEEE 802.11g dapat beroperasi pada frekuensi band 2.4 GHz maupun 5 GHz, namun meski begitu standar yang dirilis pada tahun 2009 ini tidak sepenuhnya kompetibel dengan standar IEEE 802.11g, meski tidak kompatibel dengan IEEE 802.11, data rate yang ditwarkan masih cukup besar dalam mode mix (kompatibel dengan b/g/n) yaitu 150 Mbps, sedangkan dalam mode yang menggunakan standar IEEE 802.11n sepenuhnya (menggunakan band 5 GHz dan tidak standar dengan b/g) maka data rate dapat mencapai 600 Mbps, ini hanya dapat digunakan setelah semua perangkat berpindah ke standar IEEE 802.11n. Keunggulan lainnya menggunakan antena MIMO (Multiple Input Multiple Output) yaitu menggunakan antena penerima dan pengirim yang jumlahnya lebih dari satu. Dengan penggunaan antena MIMO ini, didapat banyak keuntungan, misalnya peningkatan throughput data dan link range tanpa tambahan bandwidth atau daya transmisi, Peningkatan spectral efisiensi, dan mengurangi fading (link reability)



Gambar 2.7 Perbandingan Standarisasi Wireless LAN

BAB III

ANALISA DAN PERANCANGAN SISTEM

3.1 Analisa.

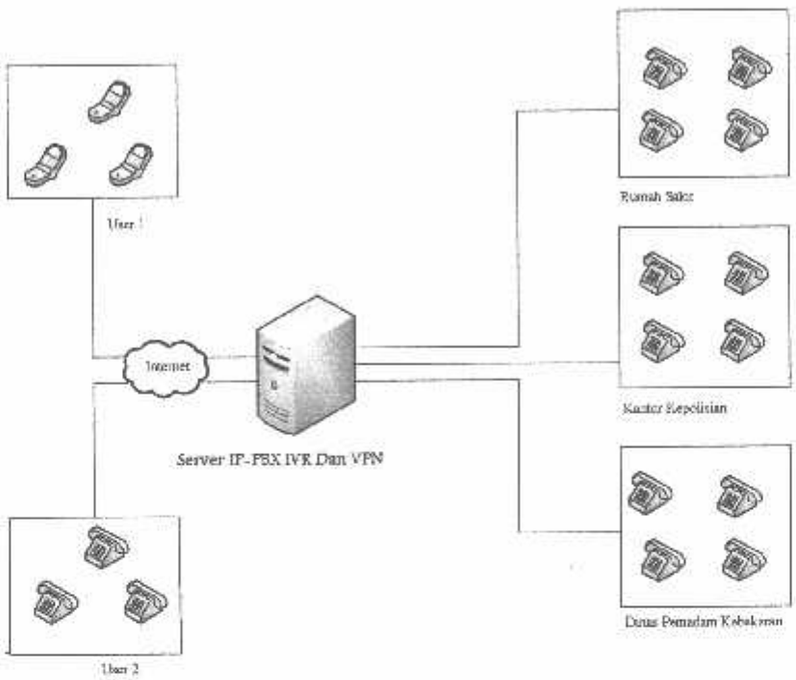
3.1.1 Gambaran Umum.

Pada bab ini akan dibahas mengenai perancangan, proses instalasi dan konfigurasi perangkat lunak untuk server *interactive voice response* (IVR) dan *Virtual Private Network* (VPN) dari sistem yang akan dibuat. Konsep dasar dari skripsi ini adalah merancang sebuah server *interactive voice response* (IVR) dengan menggunakan *Virtual Private Network* (VPN) sebagai pengaman proses transmisi data pada *emergency call*. Dimana suatu jaringan VoIP yang dilindungi oleh *Virtual Private Network*(VPN) dan terdiri dari 1 Server (*interactive voice response*) yang kemudian di akses dengan metode telepon (dalam perancangan ini menggunakan aplikasi *softphone*) . Skripsi ini bertujuan untuk menyediakan suatu layanan yang praktis dan mudah untuk pengguna dalam mengakses instansi seperti :rumah sakit, kantor polisi, dinas pemadam kebakaran pada saat yang dibutuhkan.

Kebutuhan dalam akses data yang dilakukan kapanpun memerlukan sebuah teknologi yang dapat mendukung keamanan pengaksesan dalam jaringan secara jarak jauh. Salah satu teknologi yang menyediakan kebutuhan keamanan yang diperlukan *end user* adalah *VPN (Virtual Private Network)*, yaitu fasilitas yang memungkinkan *end-user* mengirimkan sebuah data dalam sebuah kanal jaringan dengan aman.

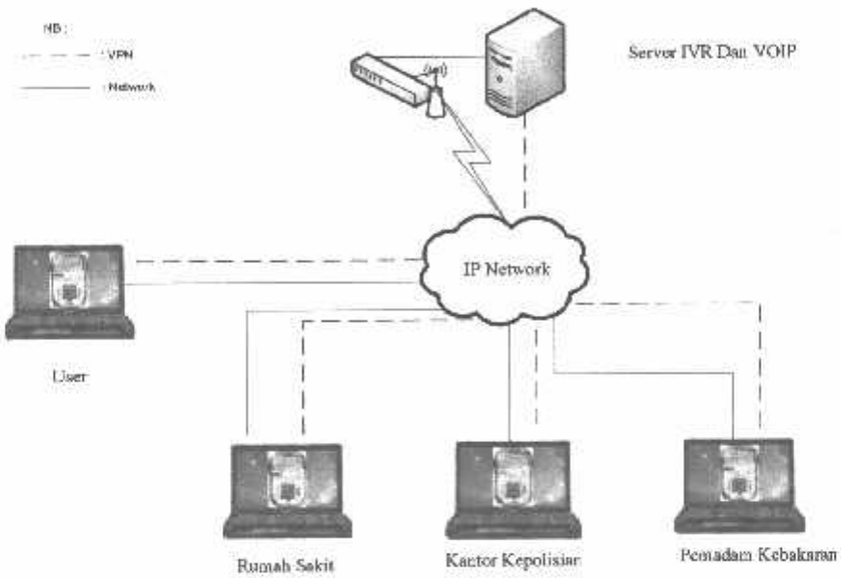
3.1.2 Diagram Blok Sistem VOIP IVR.

Gambar 3.1 Menunjukkan ilustrasi sistem server IVR pada *emergency call* dalam skala besar



Gambar 3.1 Ilustrasi system server IVR dalam skala besar / *public*

Ilustrasi pada gambar 3.1 adalah suatu system dari layanan aplikasi server interactive voice response pada emergency call yang terdiridari 1 *Server* yang kemudian dapat diakses dengan 2 metode yaitu via telepon IP dan via telepon celluler (dengan syarat telepon celluler harus terinstal softphone) serta Jalur komunikasi yang digunakan untuk mengakses sistem IVR pada gambar 3.1 menggunakan jalur komunikasi internet (VoIP). Sedangkan pada gambar 3.2 adalah desain gambar perancangan sistem server IVR yang akan dirancang oleh penulis dimana 2 metode pengaksesan sebelumnya (telepon IP dan telpon celluler) digantikan dengan softphone yang terinstal pada laptop namun jalur komunikasi yang digunakan masih sama yaitu internet.



Gambar 3.2 Perancangan Sistem Server IVR

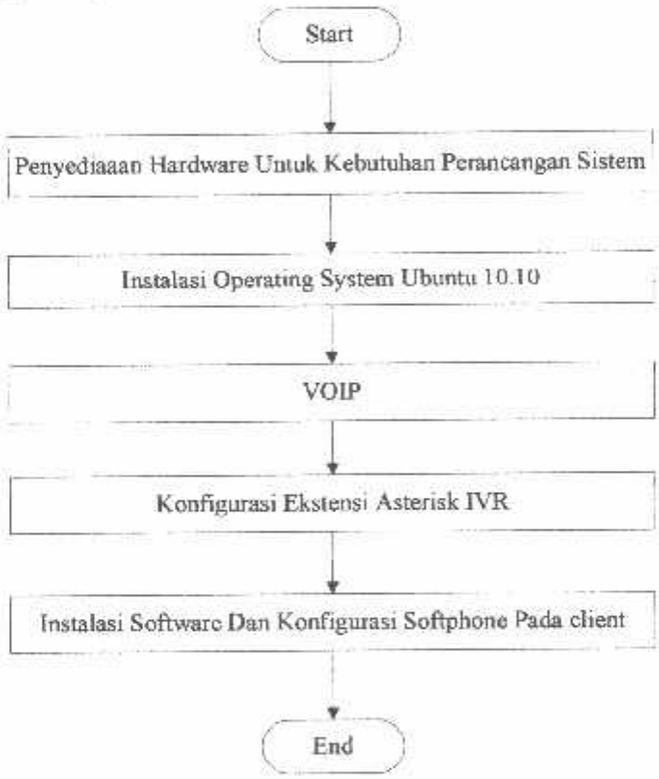
Prinsip Kerja Sistem :

Aplikasi layanan *call center* yang berbasis IVR dan VoIP merupakan pengaksesan server VoIP yang mana didalam server VoIP tersebut terdapat server IVR yang sudah di lindungi oleh VPN, untuk memperoleh layanan *emergency call*. *Local area network* digunakan sebagai penentuan penggunaan IP *Address*, VoIP Server, dan jaringan yang digunakan untuk menghubungkan antara X-Lite ke IVR Server. Software *Asterisk* merupakan inti dari IP yang digunakan sebagai *switching* panggilan telepon, pengatur file penyedia fitur, dan aplikasi IVR sebagai *call center*, misalnya pengguna ingin mengakses system layanan *emergency call* pada rumah sakit, maka *user* harus menekan nomor ekstensi yang telah di setting oleh server terlebih dahulu dan *user* akan mendengar suara rekaman operator apabila telah tersambung. Nomor server yang ditentukan adalah 1000, di dalam server tersebut terdapat nomor akses rumah sakit yaitu 1001, kantor kepolisian 1002, dinas pemadam kebakaran 1003. Sebelum *user* men-*dial* nomor ekstensi instansi layanan darurat, terlebih dahulu terdapat *voice record* pembuka IVR setelah itu akan dilanjutkan dengan *voice record* menu IVR penentuan lokasi. Disini user akan dipandu oleh *voice record* menu penentuan lokasi untuk menentukan layanan *emergency call* sesuai dengan lokasi yang diinginkan *user*. Setelah *user* menentukan lokasi layanan *emergency call* selanjutnya *user* akan dipandu untuk men-*dial* nomor ekstensi instansi darurat yang dibutuhkan oleh *user*.

3.2 Perancangan Sistem

3.2.1 Perancangan Server *Interactive Voice Response*(IVR)

Semua software yang dibutuhkan pada aplikasi ini sudah terinstall di dalam system linux server. Penggunaan linux menggunakan distributor (Distro) Ubuntu 10.10. Jenis distro dipilih karena kestabilan dan kehandalan yang cepat. Adapun proses pemrograman pada server terbagi beberapa tahap seperti yang ditunjukkan pada gambar 3.3



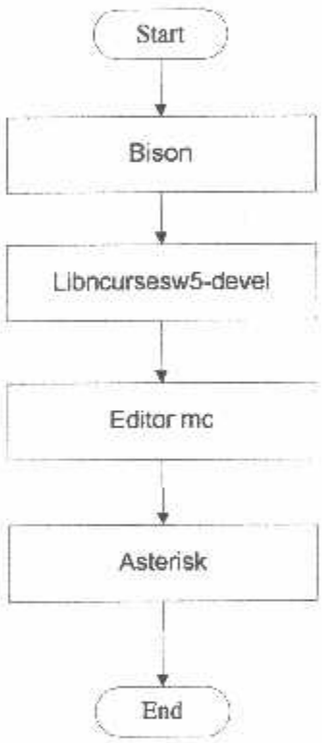
Gambar3.3 Flowchart Perancangan Server *Interactive Voice Response*(IVR)

Proses pertama adalah penyediaan kebutuhan hardware baik untuk server IVR maupun untuk *client*. Proses yang kedua adalah instalasi *operating system* Ubuntu 10.10 yang akan digunakan sebagai system operasi *server nteractive voice response* (IVR). Kemudian instalasi paket data. Proses yang ketiga adalah instalasi paket-paket data dari VOIP dan di lanjutkan dengan konfigurasi esktensi asterisk IVR. Konfigurasi ekstensi asterisk IVR merupakan pemrograman dari sistem IVR. Setelah pembuatan sistem IVR pada server maka untuk pengecekkan koneksi dan pengujian server IVR yang dirancang diperlukan instalasi

dan konfigurasi software pada *client*. Untuk itu diperlukan sebuah *softphone* yang disebut X-lite.

3.2.2 Instalasi Paket Data Session Initiation Protocol (SIP) / VOIP Asterisk

Flowchart instalasi paket data session initiation protocol (SIP)/VOIP Asterisk seperti terdapat pada gambar 3.4

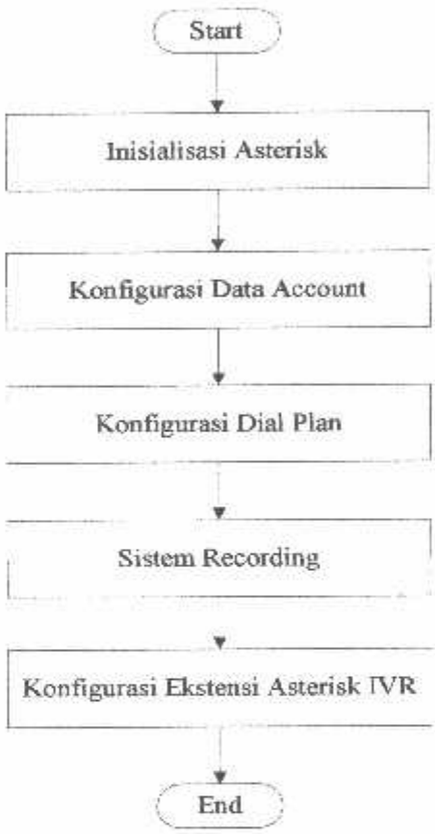


Gambar 3.4 Flowchart Instalasi Paket Data *Session Initiation Protocol*(SIP)

Paket-paket Session Initiation Protocol (SIP) sangat dibutuhkan untuk membangun jaringan VoIP. Sebuah jaringan VoIP sangat penting peranannya pada perancangan server IVR ini sebab jaringan VoIP merupakan media komunikasi antara pengakses sistem IVR dengan server IVR.

3.2.3 Flowchart Konfigurasi Pada Asterisk/ Server IVR

Flowchart konfigurasi asterisk terdapat pada gambar 3.5



Gambar 3.5 Flowchart Konfigurasi Pada Asterisk

Tahap pertama pada gambar 3.5 adalah menginstal asterisk. Dimana didalam asterisk ini terdapat beberapa konfigurasi guna menopang kinerja dari server IVR. Konfigurasi tersebut diantaranya adalah konfigurasi data *account*, dial plan, system *recording* dan konfigurasi ekstensi asterisk IVR. Konfigurasi data account sangat penting karena berhubungan dengan *setting* jalur komunikasi *user* pengakses dan server IVR. Konfigurasi dial plan merupakan konfigurasi untuk routing panggilan antar ekstensi. Sistem recording pada perancangan server IVR ini digunakan sebagai perekaman suara melalui nomor ekstensi tertentu. Tahap yang terakhir adalah konfigurasi asterisk IVR dimana semua pemrograman sistem IVR digabungkan, pada tahap ini mulai dari *dial plan, sistem recording*, dan pemrograman asterisk IVR.

3.2.4 Perancangan Sistem *Virtual Private Network*(VPN)

Untuk menyediakan transmisi data yang aman maka diperlukan proses enkripsi pada data yang dikirimkan, oleh karena itu proses enkripsi menjadi *point* penting dalam mengimplementasi sistem yang dibuat. Selain proses enkripsi sistemautentikasi dari *VPN* yang dibuat adalah langkah awal dari berhasilnya dalam mengimplementasi sistem.

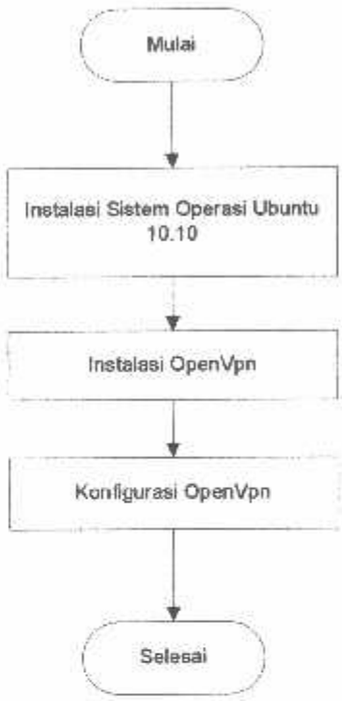
3.2.5 Analisa Kebutuhan Perangkat Lunak

Server VPN menggunakan system operasi berbasis *linux*. Penggunaan *linux* disini menggunakan *distroUbuntu 10.10. Distro* ini dipilih karena kestabilan dan kehandalannya untuk digunakan sebagai *server*. Selain itu dibutuhkan perangkat–perangkat lunak lain seperti yang terdapat padatabel 3.1.

Tabel 3.1.Spesifikasi perangkat lunak

No	Software	Keterangan
1	*Linux Ubuntu 10.10*	Sistem operasi
2	*OpenVPN*	*VPN*
3	*softphone*	*X-lite 3.0*
4	*VOIP*	*Asterisk*

Setelah ditentukan spesifikasi perangkat lunak kemudian dilakukan instalasi dengan tahap – tahap seperti pada gambar 3.6.



Gambar 3.6 Diagram alir tahap–tahap instalasi kebutuhan *server VPN*

Proses pertama adalah instalasi *Ubuntu 10.10* yang akan digunakan sebagai system operasi *server VPN*. Kemudian instalasi *OpenVPN* yang akan digunakan untuk penyedia layanan *VPN*, setelah *Open VPN* diinstal maka harus dikonfigurasi untuk membuat *CA (Certificate Authority)* dan *key* yang nantinya digunakan untuk membuka koneksi antara *client* dan *server VPN*.

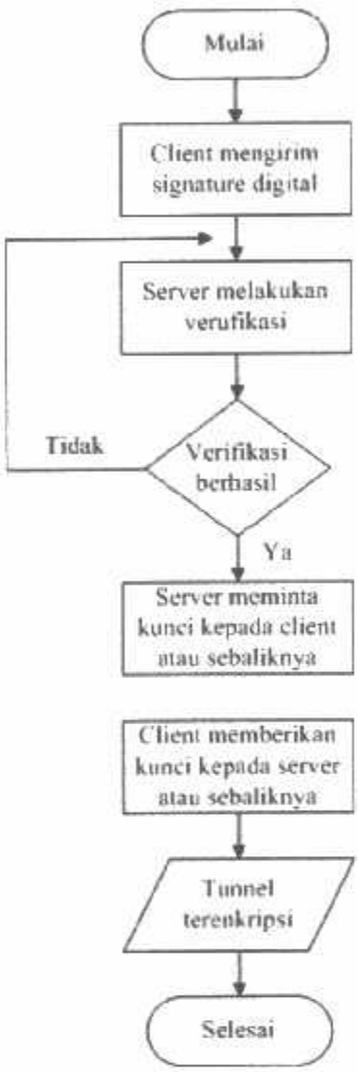
3.2.6 Metode Autentikasi

Metode autentikasi yang digunakan adalah menggunakan *PKI (Public Key Infrastructur)*, *PKI* adalah implementasi dari berbagai teknik kriptografi yang bertujuan untuk mengamankan data, memastikan keaslian data maupun pengirimnya dan mencegah penyangkalan.

Sebelum metode autentikasi *PKI (Public Key Infrastructure)* dapat di implementasikan perlu dilakukan pembuatan dengan tahap-tahap seperti pada gambar 3.7.

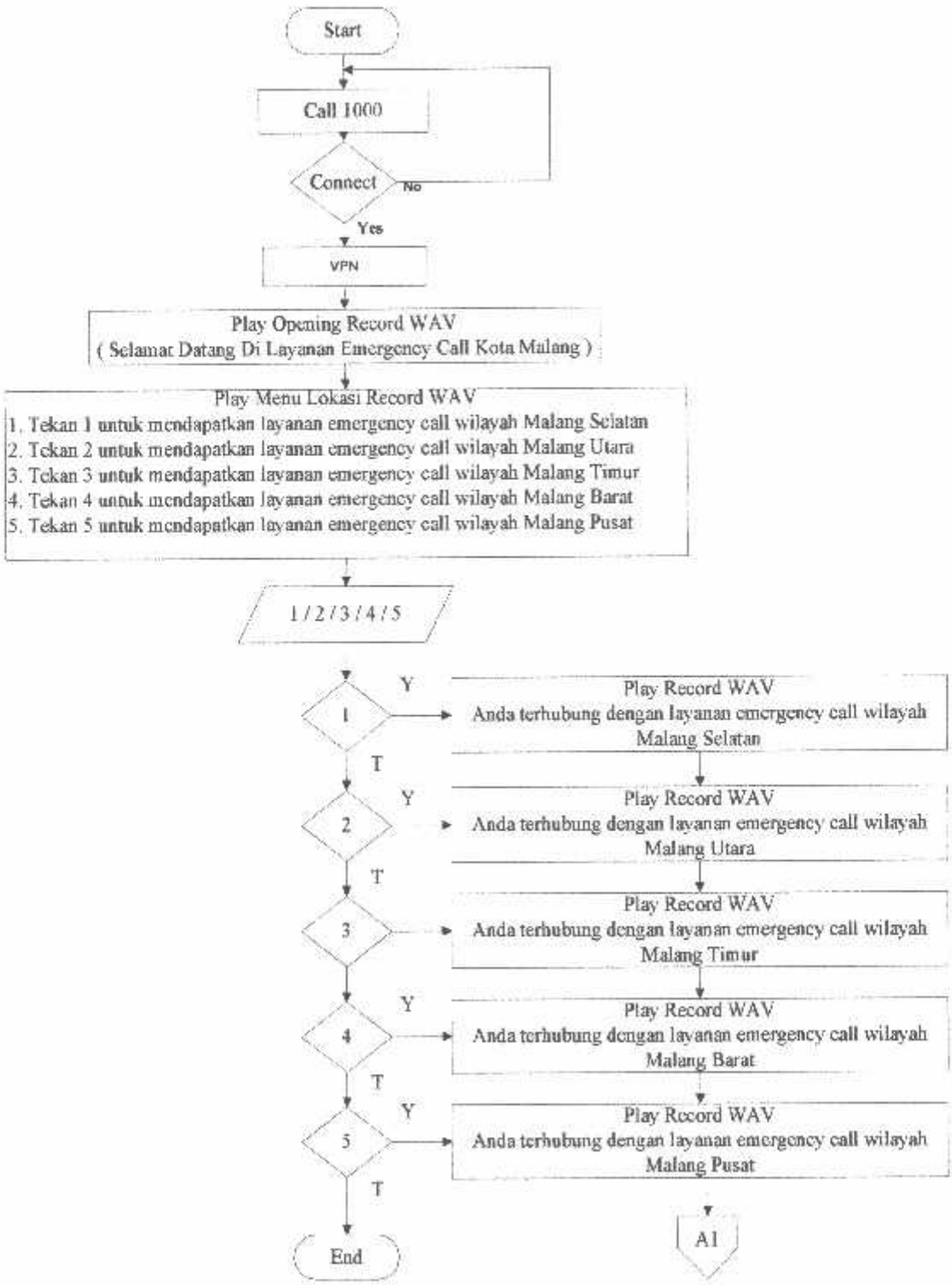
Gambar 3.7. Diagram alir pembuatan *PKI*

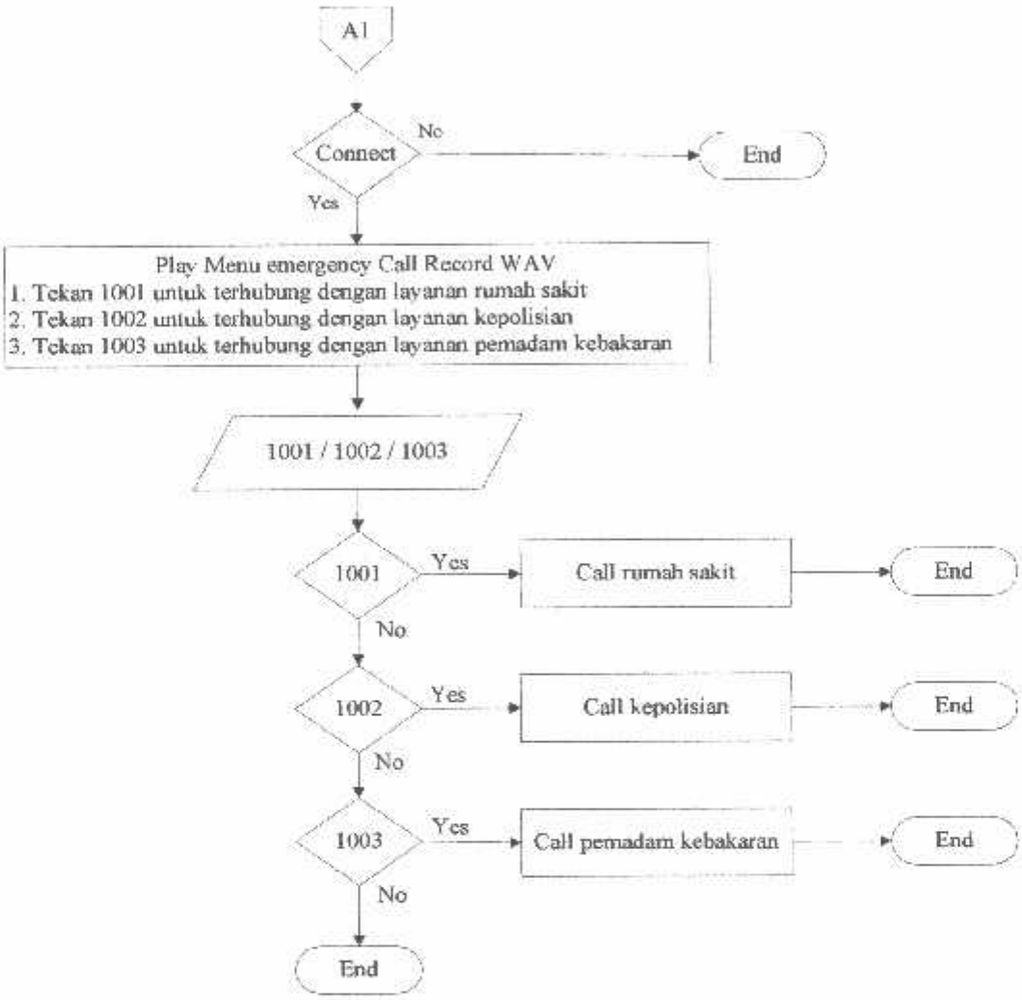
Setelah pembuatan *PKI* selesai, selanjutnya proses autentikasi menggunakan metode *PKI* dapat dilaksanakan. Berikut merupakan diagram alir proses autentikasi menggunakan *PKI* :



Gambar 3.8. Proses autentikasi

3.2.7 Flowchart Pengaksesan Server IVR





Gambar 3.12 Flowchart Pengaksesan Server IVR

BAB IV
IMPLEMENTASI DAN PENGUJIAN SISTEM

4.1 Implementasi Sistem

Dalam perancangan server *interactive voice response* (IVR) pada *emergency call* ini akan dilakukan pengujian yang mengacu pada desain sistem perancangan sistem pengamanan data pada server IVR. Parameter-parameter pengujian yang dapat menjadi indikator untuk pengambilan data dalam performansi sistem ini, diantaranya adalah *delay,packet loss, recording*. Dari beberapa parameter tersebutakan diambil datanya dalam beberapa kondisi untuk melihat kualitas dari pelayanan sistem jika di akses dari PC *client*. Data performansi - dari parameter-parameter tersebut akan dianalisa nilainya untuk menentukan berhasil atau tidaknya dari kinerja server IVR.

Pada Bab IV ini adapun proses yang harus dilakukan, yaitu :

1. Konfigurasi pada sisi server dan client, meliputi :
    1. Penyediaan hardware untuk kebutuhan perancangan sistem.
    2. Konfigurasi data *account*.
    3. Konfigurasi ekstensi asterisk IVR.
    4. Instalasi dan konfigurasi *OpenVPN*
    5. konfigurasi *softphone* pada *client*
2. Pengujian Sistem.

Implementasi sistem akan dilakukan sesuai dengan langkah – langkah diatas. Pada pengujian sistem akan dilakukan beberapa pengujian agar sistem dapat diketahui tingkat keberhasilannya.

4.2 Penyediaan hardware untuk kebutuhan perancangan sistem

4.2.1 Server.

Spesifikasi hardware server yang akan digunakan sebagai pusat dari semua instalasi VoIP server, IVR server adalah PC Pentium IV 3.00 GHz dan RAM 512 Mb. IP address yang digunakan adalah 192.168.0.222 (dipilih secara random). Subnetmask 255.255.255.0.

4.2.2 Client

Spesifikasi laptop client ini digunakan sebagai tempat penggunaan *softphone* X-lite. Operating system yang digunakan pada laptop client adalah windows XP dan *windows7*

4.2.3 Headphone.

Spesifikasi headphone sebagai media pendengar suara operator sistem IVR dan juga digunakan untuk merekam file yang akan dipasang pada layanan IVR.

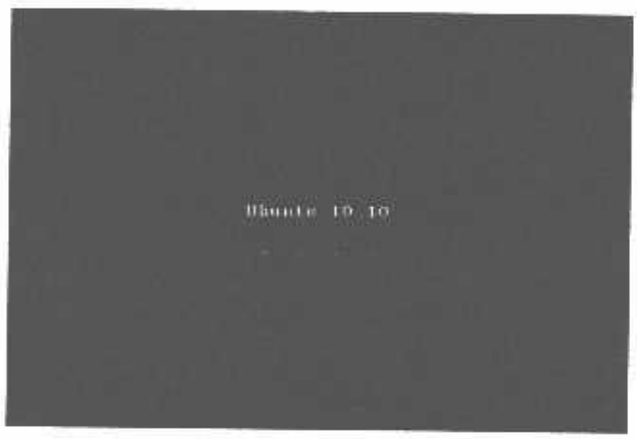
4.2 Instalasi Dan Konfigurasi Pada Server.

4.2.1 Instalasi Operating System Ubuntu 10.10

Beberapa tahapan yang dilakukan untuk membuat server IVR adalah menginstal sistem operasi terlebih dahulu. Disini penulis menggunakan sistem operasi Ubuntu 10.10.

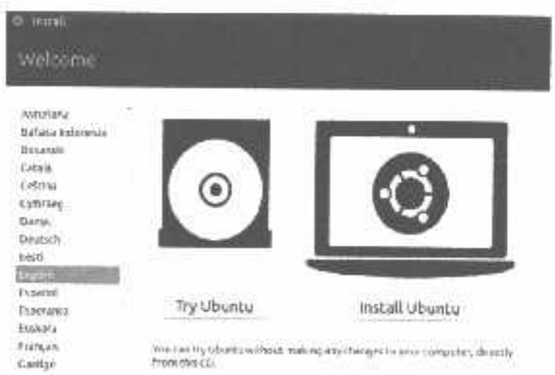
Langkah-langkah instalasi Ubuntu 10.10 sebagai berikut :

1. Siapkan seluruh peralatan yang diperlukan, seperangkat CPU/komputer, CD instalasi Ubuntu 10.10
2. Masukkan CD master instalasi Ubuntu 10.10 ke dalam CD ROM, ubah settingan bios agar load awal ke CD ROM.



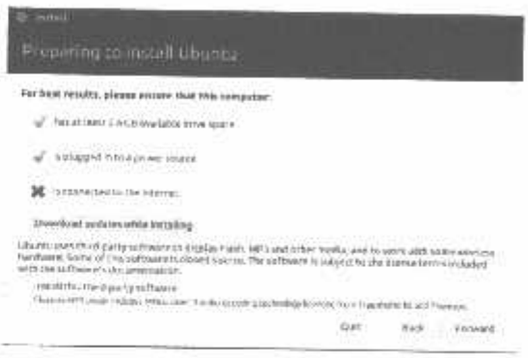
Gambar 4.1 Start Awal Instalasi Ubuntu 10.10

3. Muncul tampilan pertama sebelum instalasi, tampilan pemilihan bahasa untuk instalasi. Klik Menu Install Ubuntu.



Gambar 4.2 Tampilan Menu Bahasa Instalasi Yang Akan Digunakan

4. Jika Anda sudah memiliki modem atau berada di area Wifi klik *Download updates whiles installing*. Agar lebih cepat proses instalasinya sebaiknya pilihan tersebut dikosongkan. Klik *forward.*



Gambar 4.3 Tampilan Untuk Pemilihan Modem Jika Pada Saat Instalasi menggunakan modem.

5. Ini adalah langkah yang paling penting, jika di disk terdapat data penting dan OS lain misalnya Windows silakan pilih *Specify partitions manually*. Lalu klik *forward.*

Gambar 4.4 Tampilan Pemilihan Partisi.

6. Akan muncul form partisi hardisk, Langkah selanjutnya membuat partisi root dan partisi swap seperti pada gambar.

Gambar 4.5Tampilan Partisi Hardisk apabila memilih *Specify partitions manually*

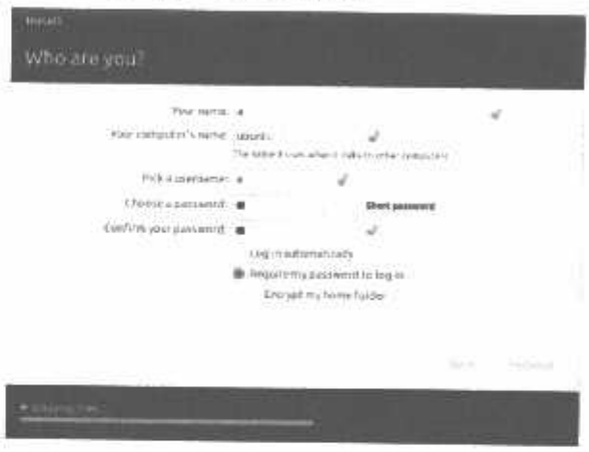
7. Akan muncul pemilihan regional setting untuk *date time*, pilih Jakarta. Kemudian klik *foward*

Gambar 4.6 Tampilan Setting Regional *Date Time*

8. Selanjutnya pemilihan keyboard layout, pilih standar (USA), kemudian klik *forward.*

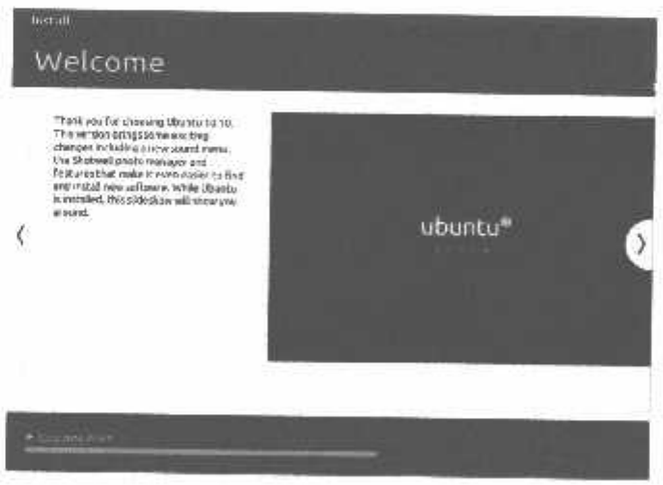
Gambar 4.7 Tampilan Menu Layout Keyboard

9. Muncul form tentang pengisian identitas pemilik komputer. Bisa diisi dengan identitas sebenarnya atau tidak. Gunakan juga kata sandi yang kuat untuk komputer umum atau kata sandi untuk yang mudah diingat.



Gambar 4.8 Tampilan Menu Pengisian Identitas Pemilik Komputer

10. Selanjutnya, proses instal dilakukan. Untuk tahap ini cukup ditunggu sampai selesai.

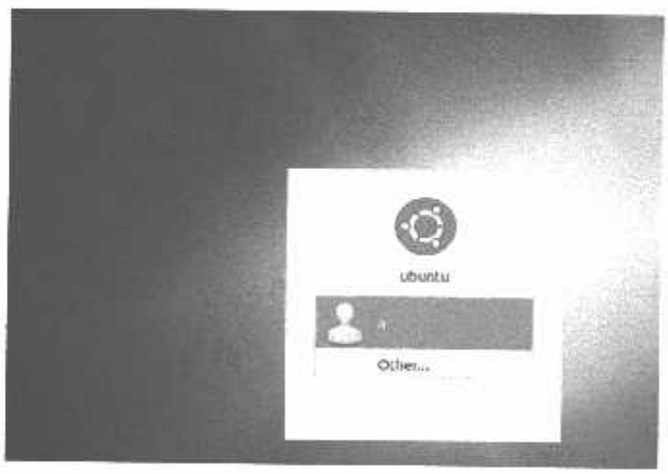


Gambar 4.9 Tampilan Proses Instalasi

11. Instalasi selesai dengan ditandai *message box* berikut ini. Klik *restart now* dan keluarkan CD instalasi dari CD Rom, komputer akan *restart* dan tunggu hingga menyala. Instalasi selesai

Gambar 4.10 Tampilan Setelah Selesai Instalasi.

12. Pada layar *login,* klik *username* lalu masukan *password.* Klik tombol "*Log In*" atau tekan *Enter* untuk *log in*



Gambar 4.11 Tampilan Untuk *login* Ke Sistem Operasi

14. Desktop Ubuntu 10.10 (Maverick Meerkat) telah siap digunakan

Ganbar 4.12 Sistem Operasi Ubuntu 10.10 Siap untuk Digunakan

4.2.2 Instalasi Paket Data *Session Initiation Protocol* (SIP)

Paket-paket *session initiation protocol* (SIP) sangat dibutuhkan untuk membangun VoIP. VoIP digunakan sebagai media komunikasi antara *client / user* dengan server IVR. Paket-paket SIP yang dibutuhkan antara lain sebagai berikut :

1. Bison.
2. Libncursesw5-devel.
3. Libncurses5-devel.
4. Editor mc.
5. Asterisk.

Proses instalasi yang digunakan langsung melalui situs yang dituju, dengan mengetikkan syntax berikut yang sesuai dengan urutannya.

1. *sudo apt-get install bison.*
2. *sudo apt-get install libncursesw5-dev*
3. *sudo apt-get install libncurses5-devel*
4. *sudo apt-get install mc*

Seluruh file yang terinstall tersebut masuk didalam directori */etc/asterisk/.*

4.2.3 Instalasi Asterisk

Pertama untuk melakukan instalasi asterisk dengan mendownload paket asterisk serta paket-paket pendukung asterisk dari *www.asterisk.org*. Adapun paket yang harus didownload adalah asterisk.deb. Ketikkan di terminal sudo dpkg –I asterisk deb.

4.2.4 Konfigurasi Data Account

Supaya *softphone* X-lite dapat berhubungan langsung dengan IVR server, maka akses data account harus diinput terlebih dahulu didalam aplikasi asterisk yang telah terinstal dalam operating system ubuntu, adapun konfigurasi data accountnya adalah sebagai berikut. Ketikkan perintah sudo gedit /etc/asterisk/sip.conf pada fungsi terminal linux.

```
[general]
context = default
bindport = 5060
bindaddr = 0.0.0.0
tcpbindaddr = 0.0.0.0
tcpenable = yes
```

```
[1000]
type = friend
callerid = Pengelola <1000>
secret = 1000
host = dynamic
canreinvite = no
dtmfmode = rfc2833
mailbox = 1000
disallow = all
allow = ulaw
transport = udp
[1001]
type = friend
callerid = User One <1001>
secret = 1001
host = dynamic
canreinvite = no
dtmfmode = rfc2833
mailbox = 1001
disallow = all
allow = ulaw
transport = udp

[1002]
type = friend
callerid = User Two <1002>
secret = 1002
host = dynamic
canreinvite = no
dtmfmode = rfc2833
mailbox = 1002
disallow = all
allow = ulaw
transport = udp
```

```
[1003]
type = friend
callerid = User Three <1003>
secret = 1003
host = dynamic
canreinvite = no
dtmfmode = rfc2833
mailbox = 1003
disallow = all
allow = ulaw
transport = udp

[1004]
type = friend
callerid = Client 1 <1004>
secret = 1004
host = dynamic
canreinvite = no
dtmfmode = rfc2833
mailbox = 1004
disallow = all
allow = ulaw
transport = udp

[1005]
type = friend
callerid = Client 2 <1005>
secret = 1005
host = dynamic
canreinvite = no
dtmfmode = rfc2833
mailbox = 1005
disallow = all
allow = ulaw
```

transport – udp

4.2.5 Dial Plan

Dial plan berfungsi sebagai *routing* panggilan antar ekstensi, baik yang berada dalam satu IP-PBX (lokal) maupun antar IP-PBX atau biasa disebut dengan *dial trunk*.Di dalam asterisk dial plan di program dalam satu file yang bernama *extension.conf*. Secara umum ekstensi dalam asterisk menuju pada *user* tertentu yang ter-register ke asterisk tersebut sehingga biasanya nomor ekstensi sama dengan *id user*. Untuk mengkonfigurasi dial plan, edit file *extensions.conf* dengan mengetik *sudo gedit /etc/asterisk/extensions.conf*. Pastikan bahwa seluruh perintah pada file ini sudah di non aktifkan. Ketik perintah dibawah ini pada bagian paling akhir dari isi file *extensions.conf*.

```
exten => 1001,1,Answer()
exten => 1001,n,Dial(SIP/1001,20,tr)
exten => 1001,n,Hangup

exten => 1002,1,Answer()
exten => 1002,n,Dial(SIP/1002,20,tr)
exten => 1002,n,Hangup
exten => 1003,1,Answer()
exten => 1003,n,Dial(SIP/1003,20,tr)
exten => 1003,n,Hangup

exten => 1004,1,Answer()
exten => 1004,n,Dial(SIP/1004,20,tr)
exten => 1004,n,Hangup

exten => 1005,1,Answer()
exten => 1005,n,Dial(SIP/1005,20,tr)
exten => 1005,n,Hangup
```

4.2.6 Sistem Recording

Aplikasi *record*() digunakan untuk merekam suara melalui nomor ekstensi tertentu. Suara hasil rekaman dapat dikodekan dalam format .wav atau .gsm. Hasil rekaman disimpan dalam file .wav atau .gsm pada folder tertentu. *Record* dapat dilakukan dengan menggunakan

sebuah aplikasi yaitu aplikasi audacity dan dapat dilakukan berulang-ulang dengan mengganti nama file rekaman.

Tabel 4.1 Tabel Rekaman

Nama File	Rekaman
Pembukaan	Selamat datang di layanan emergency call kota Malang
Voice menu record	1. Tekan 1 untuk terhubung pada layanan emergency call wilayah Malang Selatan. 2. Tekan 2 untuk terhubung pada layanan emergency call wilayah Malang Utara. 3. Tekan 3 untuk terhubung pada layanan emergency call wilayah Malang Timur. 4. Tekan 4 untuk terhubung pada layanan emergency call wilayah Malang Barat. 5. Tekan 5 untuk terhubung pada layanan emergency call wilayah Malang Pusat.
Malang Selatan	Anda terhubung dengan layanan emergency call wilayah Malang Selatan
Malang Utara	Anda terhubung dengan layanan emergency call wilayah Malang Utara
Malang Timur	Anda terhubung dengan layanan emergency call wilayah Malang Timur
Malang Barat	Anda terhubung dengan layanan emergency call wilayah Malang Barat
Malang Pusat	Anda terhubung dengan layanan emergency call wilayah Malang Pusat
Voice call record	1. Tekan 1001 untuk terhubung dengan layanan rumah sakit. 2. Tekan 1002 untuk terhubung dengan layanan kepolisian. 3. Tekan 1003 untuk terhubung dengan layanan pemadam kebakaran.

4.2.7 Konfigurasi Ekstensi Asterisk IVR

Konfigurasi pemrograman pada asterisk, setting dengan cara *sudo gedit/etc/asterisk/extensions.conf* pada perintah terminal di server IVR

```
[general]
static=yes
writeprotect=no

[default]
exten => 1000,1,Answer()
```

```
exten => 1000,2,playback(pembukaan)
exten => 1000,3,background(record menu lokasi)
exten => 1,1,playback(malangselatan)
exten => 1,2,background(record voice call)
exten => 2,1,playback(malangutara)
exten => 2,2,background(record voice call)
exten => 3,1,playback(malangtimur)
exten => 3,2,background(record voice call)
exten => 4,1,playback(malangbarat)
exten => 4,2,background(record voice call)
exten => 5,1,playback(malangpusat)
exten => 5,2,background(record voice call)

exten => 1001,1,Answer()
exten => 1001,n,Dial(SIP/1001,20,tr)
exten => 1001,n,Hangup

exten => 1002,1,Answer()
exten => 1002,n,Dial(SIP/1002,20,tr)
exten => 1002,n,Hangup

exten => 1003,1,Answer()
exten => 1003,n,Dial(SIP/1003,20,tr)
exten => 1003,n,Hangup
```

4.2.8 Instalasi OpenVPN

Berikut ini adalah langkah – langkah instalasi *OpenVPN* untuk keamanan transmisi data :

1. Masuk ke terminal Ubuntu 10.10 kemudian mengganti hak akses menjadi *super user*.
2. setelah hak akses menjadi *super user* kemudian mengetikkan *yum install openvpn* pada terminal Seperti pada gambar 4.13.

Gambar 4.13. Proses instalasi *OpenVPN* di Ubuntu

4.2.9 Pembuatan CA (Certificate Authority) dan Key

Setelah proses instalasi *OpenVPN* selesai maka akan dilakukan pembuatan *CA* dan *key* untuk autentikasi dengan langkah – langkah sebagai berikut :

1. Menginisialisasi *PKI (Public Key Infrastructure)* dengan perintah sebagai berikut :

   . /vars

   ./clean-all

   ./build-ca

2. Kemudian membuat *CA* dan *key* untuk *server* dengan perintah ***./build-key-server server.***

```
[root@oi-PC 2.0]# ./build-key-server server
Generating a 2048 bit RSA private key
.....................................................+++
.....+++
writing new private key to 'server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [ID]:
State or Province Name (full name) [JT]:
Locality Name (eg, city) [Malang]:
Organization Name (eg, company) [Fort-Funston]:
Organizational Unit Name (eg, section) [changeme]:
Common Name (eg, your name or your server's hostname) [server]:server
Name [changeme]:
Email Address [mail@host.domain]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /etc/openvpn/easy-rsa/2.0/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName               :PRINTABLE:'ID'
stateOrProvinceName       :PRINTABLE:'JT'
localityName              :PRINTABLE:'Malang'
Country Name (2 letter code) [ID]:
State or Province Name (full name) [JT]:
Locality Name (eg, city) [Malang]:
Organization Name (eg, company) [Fort-Funston]:
Organizational Unit Name (eg, section) [changeme]:
Common Name (eg, your name or your server's hostname) [server]:server
Name [changeme]:
Email Address [mail@host.domain]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /etc/openvpn/easy-rsa/2.0/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName               :PRINTABLE:'ID'
stateOrProvinceName       :PRINTABLE:'JT'
localityName              :PRINTABLE:'Malang'
organizationName          :PRINTABLE:'Fort-Funston'
organizationalUnitName:PRINTABLE:'changeme'
commonName                :PRINTABLE:'server'
name                      :PRINTABLE:'changeme'
emailAddress              :IA5STRING:'mail@host.domain'
Certificate is to be certified until Jul 28 03:35:43 2022 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
[root@oi-PC 2.0]#
```

Gambar 4.14. Pembuatan *CA* dan *key*untuk *server*

3. Membuat *CA* dan *key* untuk client dengan perintah ***./build-key client1***.

```
File  Edit  View  Search  Terminal  Help
[root@oi-PC 2.0]# ./build-key client1
Generating a 2048 bit RSA private key
.....................................+++
.............+++
writing new private key to 'client1.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [ID]:
State or Province Name (full name) [JT]:
Locality Name (eg, city) [Malang]:
Organization Name (eg, company) [Fort-Funston]:
Organizational Unit Name (eg, section) [changeme]:
Common Name (eg, your name or your server's hostname) [client1]:client1
Name [changeme]:
Email Address [mail@host.domain]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /etc/openvpn/easy-rsa/2.0/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'ID'
stateOrProvinceName   :PRINTABLE:'JT'
localityName          :PRINTABLE:'Malang'
Country Name (2 letter code) [ID]:
State or Province Name (full name) [JT]:
Locality Name (eg, city) [Malang]:
Organization Name (eg, company) [Fort-Funston]:
Organizational Unit Name (eg, section) [changeme]:
Common Name (eg, your name or your server's hostname) [client1]:client1
Name [changeme]:
Email Address [mail@host.domain]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /etc/openvpn/easy-rsa/2.0/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'ID'
stateOrProvinceName   :PRINTABLE:'JT'
localityName          :PRINTABLE:'Malang'
organizationName      :PRINTABLE:'Fort-Funston'
organizationalUnitName:PRINTABLE:'changeme'
commonName            :PRINTABLE:'client1'
name                  :PRINTABLE:'changeme'
emailAddress          :IA5STRING:'mail@host.domain'
Certificate is to be certified until Jul 28 03:37:37 2022 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
[root@oi-PC 2.0]#
```

Gambar 4.15. Pembuatan *CA* dan *key* untuk *client*

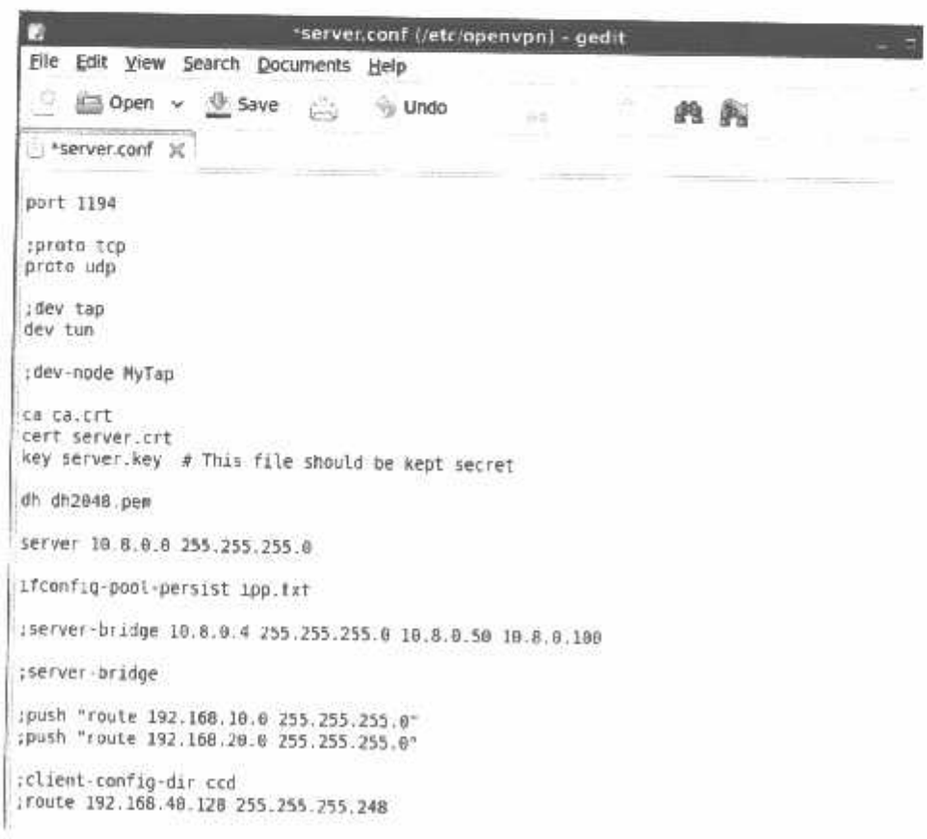
Berikut Hasil pembuatan *CA* dan *key* yang tersimpan pada direktori */etc/openvpn/easy-rsa/2.0/keys.*

Tabel 4.2. Hasil pembuatan *CA* dan *key* beserta penjelasannya

Nama	Dibutuhkan Oleh :	Fungsi	Rahasia
ca.crt	Server dan semua client	CA root	Tidak
ca.key	Server	Key CA root	Ya
server.crt	Server	Certificate server	Tidak
server.key	Server	Key server	Ya
client1.crt	Client	Certificate client	Tidak
client1.key	Client	Key client	Ya

4.2.10 Pembuatan Berkas Konfigurasi Server VPN

Berkas ini berjalan pada sisi *server VPN* dan berkas ini yang akan menjadi acuan untuk membuat konfigurasi disisi *client*. berikut merupakan isi dari berkas *server.conf* yang telah dibuat.

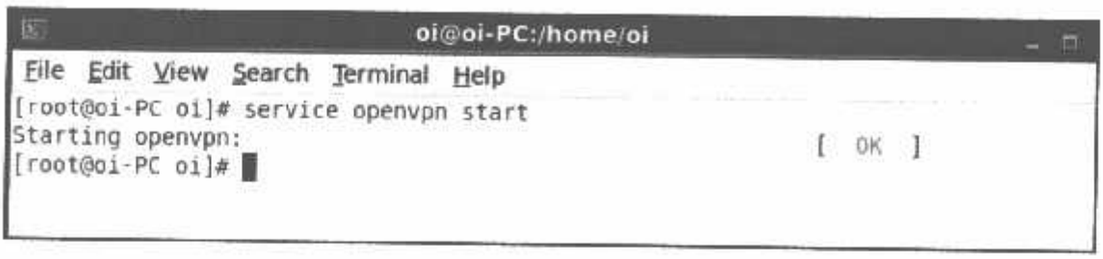


```
;client-config-dir ccd
;route 10.9.0.0 255.255.255.252

;learn-address ./script

;push "redirect-gateway def1 bypass-dhcp"

;push "dhcp-option DNS 208.67.222.222"
;push "dhcp-option DNS 208.67.220.220"

;client-to-client

;duplicate-cn

keepalive 10 120

;tls-auth ta.key 0 # This file is secret

;cipher BF-CBC        # Blowfish (default)
;cipher AES-128-CBC   # AES
;cipher DES-EDE3-CBC  # Triple-DES

comp-lzo

;max-clients 100

;user nobody
;group nobody

persist-key
persist-tun

status openvpn-status.log
;push "dhcp-option DNS 208.67.222.222"
;push "dhcp-option DNS 208.67.220.220"

;client-to-client

;duplicate-cn

keepalive 10 120

;tls-auth ta.key 0 # This file is secret

;cipher BF-CBC        # Blowfish (default)
;cipher AES-128-CBC   # AES
;cipher DES-EDE3-CBC  # Triple-DES

comp-lzo

;max-clients 100

;user nobody
;group nobody

persist-key
persist-tun

status openvpn-status.log

;log         openvpn.log
;log-append  openvpn.log

verb 3

;mute 20
```

Plain Text ▾ Tab Width: 8 ▾ Ln 1, Col 1 INS

Gambar 4.16. Berkas konfigurasi *server VPN*

Setelah konfigurasi selesai dapat dilakukan pengujian *serverVPN* apakah dapat berjalan seperti yang diharapkan atau tidak, berikut perintah untuk menjalankan layanan *serverVPN*.



Gambar 4.17. Perintah untuk menjalankan layanan *OpenVPN* pada sisi *server*

Pada gambar diatas tampak layanan *OpenVPN* dapat berjalan sesuai dengan yang diharapkan.

4.3 Konfigurasi Dan Instalasi Software Pada Client

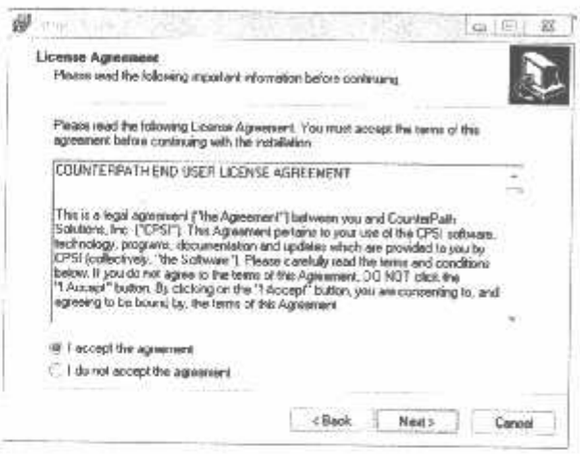
Setelah pembuatan sistem IVR dan VPN pada server maka untuk pengecekan koneksi dan pengujian aplikasi IVR yang dirancang, maka diperlukan instalasi dan konfigurasi software pada client, untuk itu diperlukan sebuah software softphone yang disebut X-lite dan OpenVPN yang dapat di download secara gratis di internet.

4.3.1 Instalasi Softphone X-Lite 3.0

1. Double klik setup X-Lite, akan muncul seperti gambar dibawah ini. Kemudian klik **next** untuk melanjutkan instalasi.

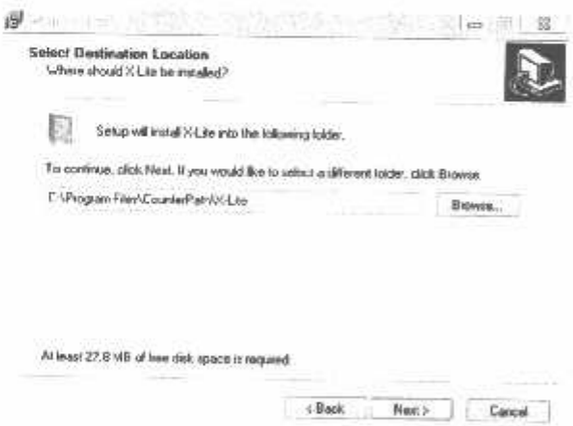
Gambar 4.18 Tampilan Awal X-Lite 3.0

2. Kemudian akan muncul license agreement pilih **I accept the agreement** yang merupakan pernyataan persetujuan, kemudian klik **next.**



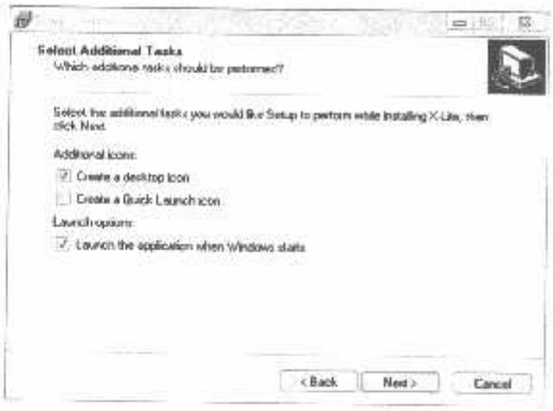
Gambar 4.19 Tampilan License Agreement X-Lite 3.0

3. Pilih letak folder untuk installasi X-Lite dengan klik *Browse*, klik *next*untuk melanjutkan instalasi, klik *next*dan instalasi selesai klik *finish*



Gambar 4.20 Tampilan Select Destination Location

4. Klik *next* untuk melanjutkan instalasi

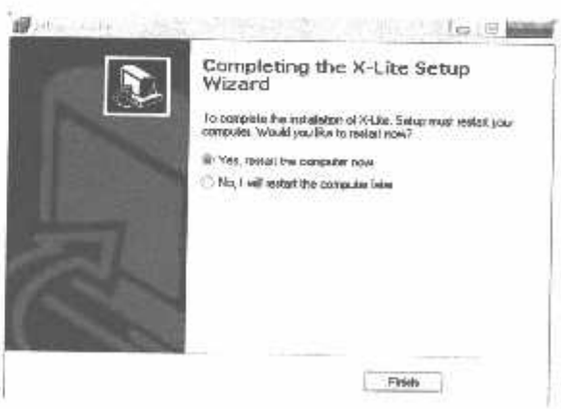


Gambar 4.21 Tampilan Sebelum Proses Instalasi

5. Proses instalasi

Gambar 4.22 Tampilan Proses Instalasi

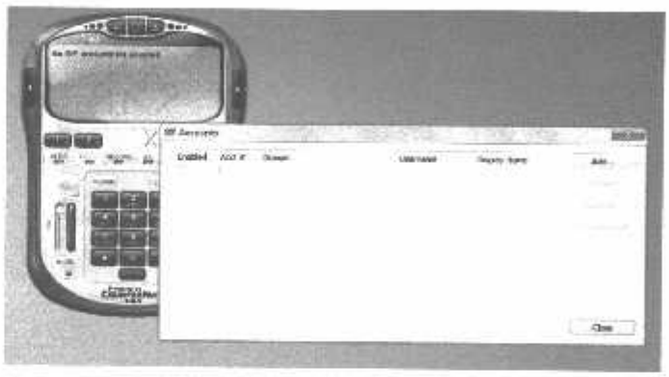
6. Tunggu proses instalasi sampai selesai dan akan muncul tombol finish bila instalasi telah selesai.



Gambar 4.23 Proses Instalasi Telah Selesai

4.3.2 Konfigurasi SIP Account Pada Softphone X-Lite 3.0

1. Klik tanda segitiga ke bawah pada head X-Lite 3.0, kemudian pilih SIP **Account Setting.**. Muncul tampilan **SIP Account Setting** pada gambar 4.6 dibawah ini. Klik Add untuk menambahkan user account dan password.



Gambar 4.24 Tampilan Langkah Pertama Konfigurasi SIP Account

2. Isikan account seperti pada gambar 4.24 dibawah ini. Lalu klik ok.

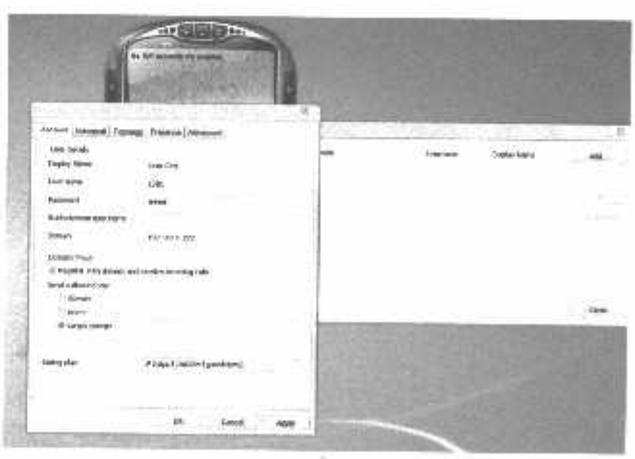
Display Name : User One

User Name : 1001

Password : 1001

Authorization :

Domain : 192.168.0.222



Gambar 4.25 Tampilan Konfigurasi SIP Account

3. Tampilan *softphone* setelah SIP accountdikonfigurasi

Gambar 4.26 Tampilan SIP Account Setelah Dikonfigurasi.

4.3.3 Konfigurasi OpenVPN Client

Sebelum dapat melakukan koneksi antara *client* dan *server*, *client* terlebih dahulu harus dilakukan instalasi dan konfigurasi *OpenVPNclient*.Berikut merupakan tahapan instalasi dan konfigurasi *OpenVPNclient*.

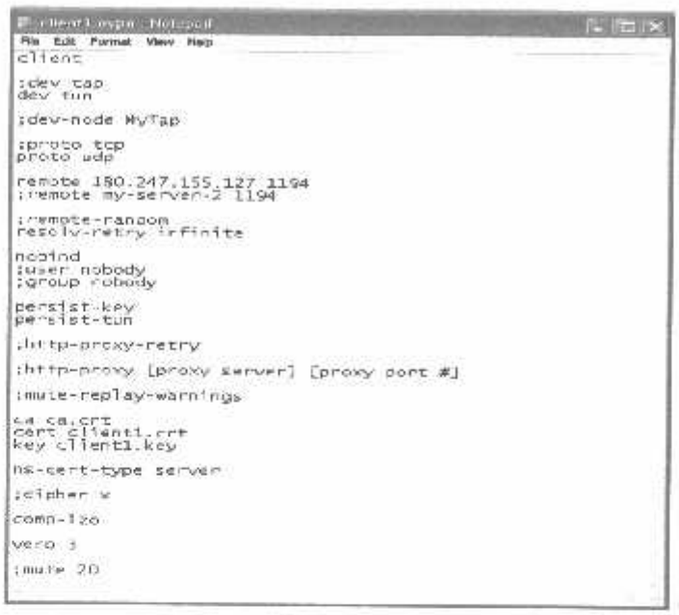
1. *Double* klik *berkas* instalasi *OpenVPNclient*, setelah selesai proses instalasi, *copy* CA-nya.
2. Meng-*copy CA* dan *key* hasil *generate OpenVPN server* ke direktori *C:\Program Files\OpenVPN\config*. Berikut *CA* dan *key* yang diperlukan untuk konfigurasi *OpenVPNclient* :

   Ca.crt

   Client1.key

   Client1.crt

Setelah instalasi *OpenVPN* selesai kemudian dilakukan pembuatan *berkas* konfigurasi untuk *clientOpenVPN*. Berikut merupakan *berkas* konfigurasi untuk *OpenVPNclient* :

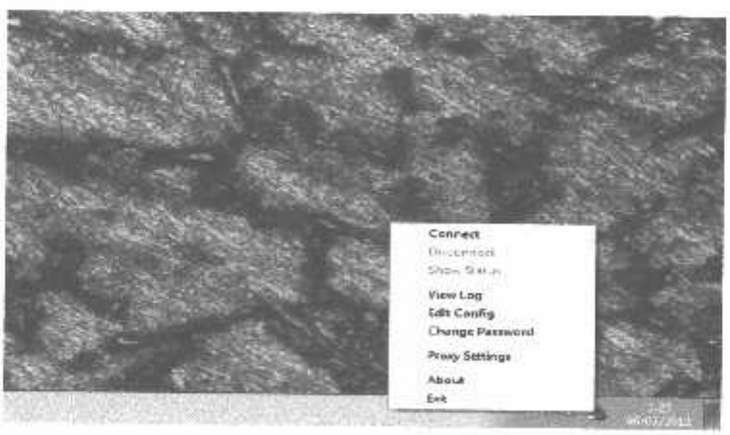


Gambar 4.27.*Berkas* konfigurasi *OpenVPNclient*

4.3.4 Membuat Koneksi Dan Melakukan Autentikasi CA dan Key

Berikut tahap –tahap pembuatan koneksi dan autentikasi *CA* dan *key* :

1. Masuk *Start menu -> All Programs -> openvpn -> openVPN GUI* kemudian klik.
2. Selanjutnya klik kanan *tray icon OpenVPN* seperti berikut :



Gambar 4.28. Melakukan koneksi ke *serverVPN*

3. Kemudian klik *connect*. Maka akan muncul jendela autentikasi seperti pada gambar 4.28.

Gambar 4.29. Proses autentikasi *CA* dan *key*

4. Jika proses autentikasi *CA* dan *key* berhasil, maka pada *tray icon OpenVPN* akan muncul notifikasi seperti pada gambar 4.29.

Gambar 4.30. Notifikasi bahwa *client* telah terhubung ke *serverVPN*

4.4 Pengujian Sistem

Pada tahap ini akan dilakukan pengujian dari dua buah implementasi yang telah dilakukan pada percobaan diatas. Pengujian Proyek Akhir ini menggunakan *tool Sniffing* yaitu WireShark untuk menyadap pada paket – paket data komunikasi VoIP. Berikut adalah pengujian yang akan dilakukan, yaitu :

4.4.1 Pengujian Penyadapan pada VoIP tanpa VPN

Pada tahap ini akan dilakukan pengujian dengan beberapa skenario, yaitu :

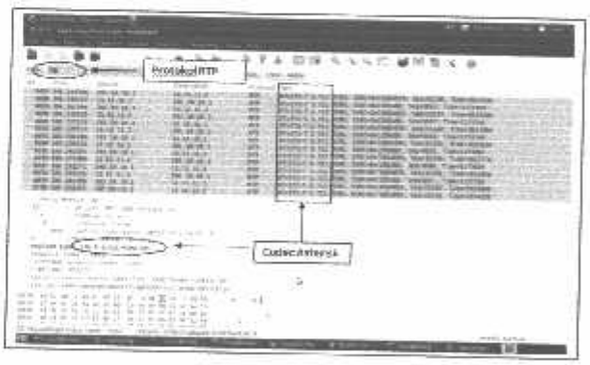
1. Koneksikan masing – masing *user* agar terhubung ke PC serverr VPN dan PC *user*.
2. Lakukan pengetesan koneksi dengan menggunakan ping ke IP *public internal*.

3. Konfigurasi X-Lite dengan menggunakan IP *public* sebagai domain-nya.
4. Nyalakan applikasi wireshark.
5. Amati protokol Asterisk yaitu protokol SIP dan lihat komunikasi yang terjadi.
6. Apabila protokol SIP terlihat, kemudian pilih menu "Telephony" pada WireShark dan pilih "VoIP Calls"
7. Lakukan penyadapan pada komunikasi yang terjadi antara server dan *user* eksternal

Berikut adalah gambar-gambar hasil penyadapan yang terjadi pada VoIP tanpa menggunakan VPN, yaitu :

1. Melakukan pengecekkan codec yang digunakan pada asterisk

Pada uji coba tahap ini dapat dilihat *capturing* data VoIP tanpa VPN dengan menggunakan filter protokol RTP, didapatkan data penting dalam sistem VoIP yaitu termonitornya codec yang digunakan (G.711).



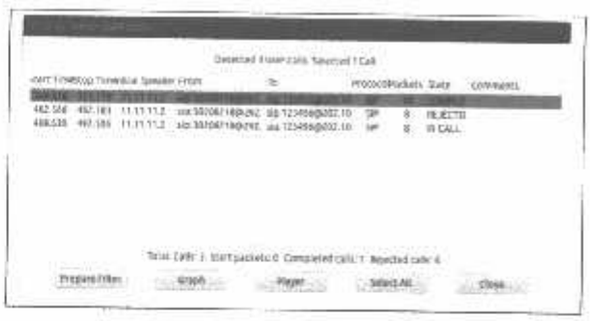
Gambar 4.31 Melihat codec asterisk

2. Melakukan pengecekkan pada jalur protokol SIP

Pada tahap ini dapat dilihat terjadinya panggilan yang menggunakan protokol SIP.

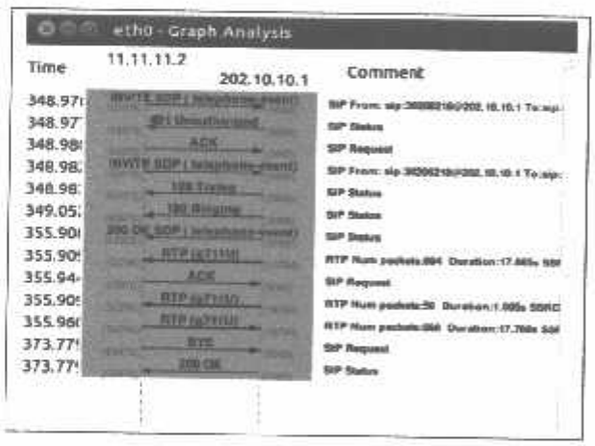
Gambar 4.32 Melihat protokol SIP

3.Melihat data komunikasi VoIP yang terjadi.



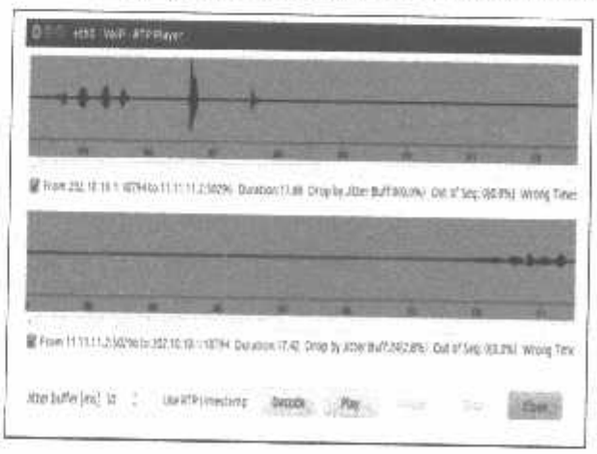
Gambar 4.33 Melihat data panggilan VoIP

4.Melihat flow panggilan VoIP.



Gambar 4.34 Melihat flow panggilan VoIP

5.Melihat isi data dan melakukan penyadapan pada komunikasi VoIP.



Gambar 4.35 Melakukan penyadapan

4.4.2 Pengujian Penyadapan pada VoIP melalui VPN

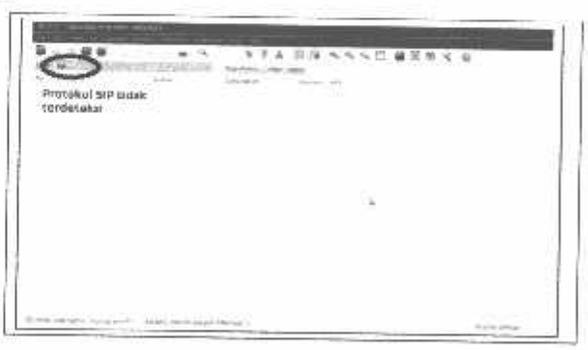
Pada tahap pengujian selanjutnya akan diuji VoIP dengan melalui VPN, dan melihat

terhadap terjadinya penyadapan pada jalur VoIP dengan melalui VPN. Pada tahap ini juga dilakukan dengan beberapa cara, yaitu :

1. Pertama koneksikan masing – masing *user* agar terhubung ke PC server VPN dan PC *user* eksternal.
2. Lakukan pengetesan terhadap koneksi dengan menggunakan ping ke IP public internal.
3. Kemudian lakukan login VPN bagi *user* eksternal dengan menggunakan GUI klien open VPN.
4. Melakukan uji koneksi kembali dengan mengetes ping antara server dan *user* eksternal.
5. Konfigurasi domain x-lite dengan mengganti menjadi IP VPN *server*.
6. Nyalakan applikasi wireshark.
7. Amati protokol Asterisk yaitu protokol SIP dan lihat komunikasi yang terjadi.
8. Lakukan penyadapan pada komunikasi yang terjadi antara *user* internal dan *user* eksternal

Berikut adalah gambar-gambar hasil penyadapan yang terjadi pada VoIP menggunakan VPN, yaitu :

1. Mengamati jalur protokol SIP.



Gambar 4.36 Jalur Protokol SIP setelah VoIP *over* VPN

2. Mengamati data komunikasi VoIP.

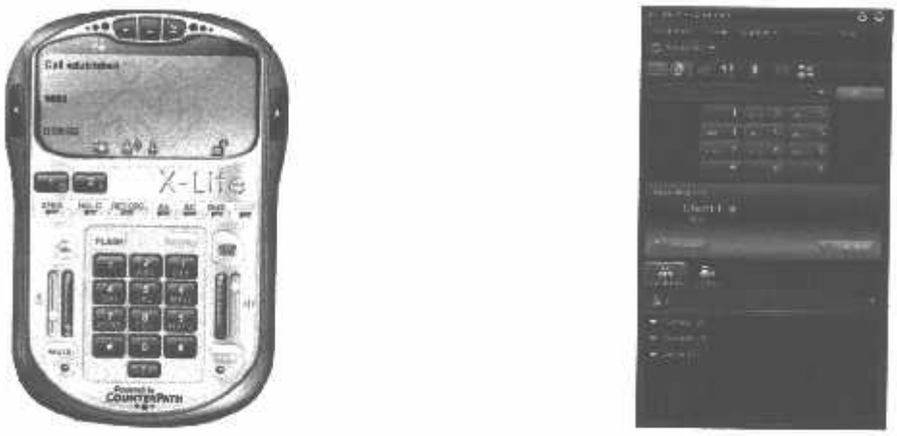
Gambar 4.37 Komunikasi data panggilan VoIP *over* VPN

Pada kedua tahap pengujian ternyata pada pengujian pertama yang berupa VoIP yang tidak melewati jalur VPN dapat dengan mudah dilakukan penyadapan mulai dari protokol VoIP yaitu SIP, data komunikasi yang sedang melakukan panggilan baik itu berupa asal *user* yang melakukan panggilan dan tujuan panggilan tersebut, grafik panggilan yang terjadi, sampai pada bagian terjadinya penyadapan yang memungkinkan seorang penyadap dapat mendengar komunikasi yang terjadi dari *user* internal dan *user* eksternal. Dari semua hasil yang didapat apabila *server* VoIP dibuat tanpa melalui jalur yang aman tentu saja akan membuat kenyamanan dalam penggunaan VoIP sebagai pengganti telpon tradisional menjadi sangat tidak nyaman karena adanya situasi di saat terjadinya penyadapan dan tujuan panggilan.

Akan tetapi pada percobaan kedua dengan membuat VoIP melewati jalur VPN (VoIP *over* VPN) dapat dilihat bahwa protokol VoIP yaitu SIP tidak dapat dilihat traffic yang sedang melakukan panggilan, dan juga data panggilan komunikasi antar *user* tidak akan bisa dilakukan penyadapan. Maka dari itu dengan membuat VoIP melalui jalur VPN bisa memberikan kenyamanan bagi pengguna layanan VoIP, karena dalam pembuatannya, VPN terdapat SSL yang dibuat pada saat awal pembuatan VPN berupa certificate Authority (CA), dan pembuatan certificate dan key bagi *user* maupun *server*. Pada VPN juga terdapat metoda Diffle-Hellman sebagai key exchanger dalam pembuatannya.

4.4.3 Dial Plan

Dial plan berfungsi sebagai *routing* panggilan antar ekstensi, baik yang berada dalam satu IP-PBX (lokal) maupun antar IP-PBX [2] maka dari itu harus dilakukan pengujian pada setiap *client* ketika *client* men-*dial* ke nomor ekstensi agar tepat sasaran sesuai dengan tujuannya.



Gambar 4.38*Client* 1 *Dial* Ke Ekstensi 1001

Gambar 4.39*Client* 1 *Dial* Ke Ekstensi 1002

Gambar 4.40*Client* 1 *Dial* Ke Ekstensi 1003

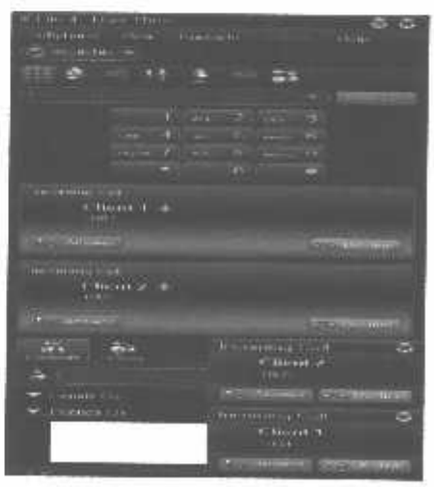
Gambar 4.41*Client* 2 *Dial* Ke Ekstensi 1001

Gambar 4.42*Client* 2 *Dial* Ke Ekstensi 1002

Gambar 4.43*Client* 2 *Dial* Ke Ekstensi 1003

Gambar 4.44*Client* 1 dan *Client* 2 *Dial* Ke Ekstensi 1001

Gambar 4.45*Client* 1 dan *Client* 2 *dial* ke ekstensi 1002



Gambar 4.46*Client* 1 dan *Client* 2 *Dial* Ke Ekstensi 1003

4.5 Hasil Pengujian Sistem.

Dari hasil perancangan server *interactive voice response* (IVR) pada *emergency call* tersebut maka diperoleh juga hasil pengujian sistem secara umum yang ditunjukkan pada tabel 4.3.

Tabel 4.3 Hasil Pengujian Perancangan Server IVR Pada *Emergency Call*

Pengujian	Hasil yang diharapkan	Keterangan	
		Berhasil	Gagal
Nomor ekstensi server IVR	Dapat diakses oleh *account / client*	✓	
Voice pembukaan	Menampilkan *voice* pembukaan dari layanan *emergency call*	✓	
Voice record menu lokasi	Menampilkan *voice* menu lokasi layanan *emergency call* dan dapat mengarahkan ke lokasi *emergency call* yang dibutuhkan *client*.	✓	
Voice lokasi	Dapat menampilkan *voice* lokasi sesuai dengan pilihan *client* pada saat *client* mendial nomor pilihan pada *voice record* menu lokasi.	✓	
Voice call	Menampilkan panduan kepada *client* untuk men-*dial* nomor-nomor ekstensi yang dibutuhkan oleh *client*.	✓	
Dial plan	Dapat menyediakan layanan agar *client* dapat tersambung dengan nomor ekstensi dan dapat berbicara dengan kualitas suara yang jernih.	✓	

BAB V
PENUTUP

5.1 Kesimpulan.

Setelah melakukan implementasi dan pengujian tentang server IVR pada *emergency call* menggunakan virtual private network (vpn) maka diperoleh kesimpulan sebagai berikut :

1. Server *interactive voice respons* (IVR) pada emergency call menggunakan *virtual private network* (VPN) berbasis *wireless* ini bersifat praktis dikarenakan menyimpan berbagai nomor ekstensi panggilan darurat, dimana didalam server IVR ini terdapat 3 nomor panggilan darurat antara lain rumah sakit, kepolisian, pemadam kebakaran.
2. Komunikasi VoIP melalui VPN (VoIP *over* VPN) terbukti aman dari bentuk penyadapan suara (sniffing), hal ini dibuktikan dari hasil pengujian dan analisa jalur komunikasi VoIP dengan VPN secara lokal yang menunjukan bahwa komunikasi suara yang terjadi pada VoIP tidak bisa dilakukan penyadapan atau didengarkan pembicaraan yang terjadi oleh orang yang tidak berkepentingan. VoIP dengan VPN yang menggunakan Open VPN, yang merupakan VPN dengan teknologi tunneling dan enskripsi yang melindungi jalur komunikasi VoIP.
3. Implementasi VoIP tanpa menggunakan VPN terbukti rentan dari ancaman penyadapan yang dapat merugikan *user* yang melakukan panggilan.
4. *Acces point* yang saya gunakan disini menggunakan antena 5dBi Fixed Omni-Directional, dengan frequensi 2.4-2.4835GHz sehingga dapat di jangkau dengan jarak dan kemampuan akses 54M: -68dBm@10% PER, 11M: -85dBm@8% PER, 6M:-88dBm@10% PER, 1M: -90dBm@8% PER.
5. Sesuai standar IEEE 802.11g dengan tingkat transmisi sampai dengan 54Mbps, dirancang untuk membangun koneksi nirkabel yang lebih baik dari sebelumnya, berbagi akses internet, file-download dan sebagainya. Bahkan di antara 1-2 dinding kamar, juga dapat menjaga sinyal yang bisa digunakan dan tingkat link yang baik setelah melewati dinding.

5.2 Saran.

Dalam pembuatan skripsi ini penulis menyadari masih terdapat kekurangan, Adapun saran-saran sebagai pengembangan pada masa mendatang agar fungsi dari sistem IVR ini lebih maksimal lagi.

1. IVR juga dapat berfungsi analog dengan menambahkan sebuah card pada PC server, instalasi dan konfigurasi card tersebut maka kita dapat berkomunikasi dari analog dan digital.
2. VoIP *over* VPN berharap dapat dijadikan media komunikasi yang aman oleh *user* untuk saling berkomunikasi.
3. Diharapkan untuk VoIP *over* VPN dapat dianalisis kualitas suara yang dihasilkan dan perbedaan saat melalui jalur VPN.

Daftar Pustaka

[1] Gozali F, Alex. "Virtual Server". Urnal Teknik Elektro Universitas Trisakti, Jakarta, Agustus 2002.

[2] Raharja, A. (2006). *Membangun layanan VoIP dengan murah.* http://voiprakyat.or.id/data/files/open_voip.pdf. Diakses Tanggal November 24, 2012

[3] Madcoms. (2010). *Sistem Jaringan.* Yogyakarta: Andi.

[4] "Red Hat Enterprise Linux 4 Virtual Server Administration Linux Virtual Server (LVS) for red Hat Enterprise Linux Edition 1.0". Red Hat Inc,Raleigh,2009.

[5] Sofana I. "Teori dan Modul Jaringan Komputer".Modula. Bandung. 2011.

[6] Wendi, A., & Ramadhana, A. S. (2005). *Membangun VPN Linux secara cepat.* Yogyakarta: Andi.

[7] Roddis, S. (2010). *OpenVPN: Easy and Secure Setup Guide.*, http://www.stevenroddis.com/documents/OpenVPN_Easy_and_Secure_Setup_Guide.pdf. Diakses Tanggal November 27, 2012

[8] Nico. (2013). IEE 802.11n, http://id.wikipedia.org/wiki/IEEE 802.11n. diakses tanggal 30 juni 2013.

[9] Fauziah, U. (2013). IEEE 802.11 Standar *Wireless* LAN, http://http://ulfa-fauziah.blogspot.com/IEEE 802.11 STANDAR WIRELESS LAN/. diakses tanggal 30 juni 2013.

[10] Wardana Erik R, Agustus 2012 "*Rancang Bangun Server Interactive Voice Response (IVR) Pada Emergency Call*", e-Jurnal Teknik Elektro ITN Malang.

LAMPIRAN

PROGRAM STUDI TEKNIK ELEKTRO S-1
FAKULTAS TEKNOLOGI INDUSTRI
INSTITUT TEKNOLOGI NASIONAL MALANG
Kampus II : Jl. Raya Karanglo Km. 2 Telp. (0341) 417636 Malang

Lampiran : 1 (satu) berkas
Pembimbing Skripsi

Kepada : Yth. Bapak/Ibu **Bima Aulia Firmandani, ST**
Dosen Teknik Elektro S-1
ITN Malang

Yang bertanda tangan dibawah

Nama	: **FINO DWI JAYANTO**
Nim	: **0812508**
Jurusan	: **Teknik Elektro S-1**
Konsentrasi	: **Teknik Komputer**

Dengan ini mengajukan permohonan, kiranya Bapak/Ibu bersedia menjadi Dosen Pembimbing untuk penyusunan Skripsi dengan judul ;

"RANCANG BANGUN SERVER INTERACTIVE VOICE RESPONS (IVR) PADA EMERGENCY CALL MENGGUNAKAN VIRTUAL PRIVATE NETWORK (VPN) BERBASIS WIRELESS"

Demikian permohonan kami buat dan atas kesediaan Bapak kami ucapkan terima kasih.

Mengetahui
Ketua Program Studi Teknik Elektro S-1

Ir. Yusuf Ismail Nakhoda, MT
NIP.Y. 1018800189

Hormat Kami

FINO DWI JAYANTO
NIM. 0812508

PROGRAM STUDI TEKNIK ELEKTRO S-1
FAKULTAS TEKNOLOGI INDUSTRI
INSTITUT TEKNOLOGI NASIONAL MALANG
Kampus II : Jl. Raya Karanglo Km. 2 Telp. (0341) 417636 Malang

PERNYATAAN KESEDIAAN DALAM PEMBIMBINGAN SKRIPSI

Sesuai permohonan dari mahasiswa/i :

Nama	: **FINO DWI JAYANTO**
Nim	: **0812508**
Semester	: **IX (Sembilan)**
Jurusan	: **Teknik Elektro S-1**
Konsentrasi	: **Teknik Komputer**

Dengan ini menyatakan bersedia/tidak bersedia*) Membimbing skripsi dari mahasiswa tersebut, dengan judul :

" RANCANG BANGUN SERVER INTERACTIVE VOICE RESPONS (IVR) PADA EMERGENCY CALL MENGGUNAKAN VIRTUAL PRIVATE NETWORK (VPN) BERBASIS WIRELESS"

Demikian surat pernyataan ini kami buat agar dapat dipergunakan seperlunya.

Hormat Kami

Bima Aulia Firmandani, ST
1121

Catatan :

Setelah disetujui agar formulir ini Diserahkan mahasiswa/I yang bersangkutan kepada jurusan untuk diproses lebih lanjut

*) Coret yang tidak perlu

PROGRAM STUDI TEKNIK ELEKTRO S-1
FAKULTAS TEKNOLOGI INDUSTRI
INSTITUT TEKNOLOGI NASIONAL MALANG
Kampus II : Jl. Raya Karanglo Km. 2 Telp. (0341) 417636 Malang

BERITA ACARA SEMINAR PROPOSAL SKRIPSI
PROGRAM STUDI TEKNIK ELEKTRO S-1
Konsentrasi : Teknik Komputer

1.	Nim	: 0812508	
2.	Nama	: FINO DWI JAYANTO	
3.	Konsentrasi Jurusan	: Teknik Komputer	
4.	Jadwal Pelaksanaan:	Waktu	Tempat
	24 Oktober 2012	09:00	III.1.3
5.	Judul proposal yang diseminarkan Mahasiswa	RANCANG BANGUN SERVER INTERACTIVE VOICE RESPONS (IVR) PADA EMERGENCY CALL MENGGUNAKAN VIRTUAL PRIVATE NETWORK (VPN) BERBASIS WIRELESS	
6.	Perubahan judul yang diusulkan oleh Kelompok Dosen Keahlian		
7.	Catatan : tabulasi perbandingan Metode yg benar untuk pengamanannya.		
8.	Catatan :		

Persetujuan judul Skripsi

Disetujui, Dosen Keahlian I	Disetujui, Dosen Keahlian II	Disetujui, Dosen Keahlian III
(M. Ibrahim, ST, MT)	(Yuli Wahyuni, ST, MT)	(.....)

Mengetahui, Ketua Program Studi Teknik Elektro S-1	Disetujui, Calon Dosen Pembimbing ybs	
	Pembimbing I	Pembimbing II
Ir. Yusuf Ismail Nakhoda, MT NIP. Y. 1018800189	(.....)	(.....)

PROGRAM STUDI TEKNIK ELEKTRO S-1
FAKULTAS TEKNOLOGI INDUSTRI
INSTITUT TEKNOLOGI NASIONAL MALANG
Kampus II : Jl. Raya Karanglo Km. 2 Telp. (0341) 417636 Malang

LEMBAR PENGAJUAN JUDUL SKRIPSI
PROGRAM STUDI TEKNIK ELEKTRO S-1
Konsentrasi : Teknik Komputer

1.	Nim	: **0812508**
2.	Nama	: **FINO DWI JAYANTO**
3.	Tanggal Pengajuan	: **2 Oktober 2012**
4.	Konsentrasi Jurusan	: **Teknik Komputer**
5.	Konsultasikan judul sesuai materi bidang ilmu kepada Dosen **Dr. Eng. Aryuanto S, ST, MT** NIP.P. 1030800417	Ketua Program Studi **Ir. Yusuf Ismail Nakhoda,MT** NIP. Y. 1018800189
6.	Judul yang diajukan mahasiswa:	RANCANG BANGUN SERVER INTERACTIVE VOICE RESPONS (IVR) PADA EMERGENCY CALL MENGGUNAKAN VIRTUAL PRIVATE NETWORK (VPN) BERBASIS WIRELESS
7.	Perubahan judul yang disetujui Dosen sesuai materi bidang ilmu	
8.	Catatan Persetujuan Judul skripsi yang Dikonsultasikan kepada Dosen materi Bidang ilmu	Disetujui, 11 Oktober 2012 **Dr. Eng. Aryuanto S, ST, MT** NIP.P. 1030800417

PROGRAM STUDI TEKNIK ELEKTRO S-1
FAKULTAS TEKNOLOGI INDUSTRI
INSTITUT TEKNOLOGI NASIONAL MALANG
Kampus II : Jl. Raya Karanglo Km. 2 Telp. (0341) 417636 Malang

Lampiran : 1 (satu) berkas
Pembimbing Skripsi

Kepada : Yth. Bapak/Ibu **Dr. Eng. Aryuanto Soetedjo, ST, MT**
Dosen Teknik Elektro S-1
ITN Malang

Yang bertanda tangan dibawah

Nama	: **FINO DWI JAYANTO**
Nim	: **0812508**
Jurusan	: **Teknik Elektro S-1**
Konsentrasi	: **Teknik Komputer**

Dengan ini mengajukan permohonan, kiranya Bapak/Ibu bersedia menjadi Dosen Pembimbing untuk penyusunan Skripsi dengan judul :

"RANCANG BANGUN SERVER INTERACTIVE VOICE RESPONS (IVR) PADA EMERGENCY CALL MENGGUNAKAN VIRTUAL PRIVATE NETWORK (VPN) BERBASIS WIRELESS"

Demikian permohonan kami buat dan atas kesediaan Bapak kami ucapkan terima kasih.

Mengetahui
Ketua Program Studi Teknik Elektro S-1

Ir. Yusuf Ismail Nakhoda, MT
NIP.Y. 1018800189

Hormat Kami

FINO DWI JAYANTO
NIM. 0812508

PROGRAM STUDI TEKNIK ELEKTRO S-1
FAKULTAS TEKNOLOGI INDUSTRI
INSTITUT TEKNOLOGI NASIONAL MALANG
Kampus II : Jl. Raya Karanglo Km. 2 Telp. (0341) 417636 Malang

PERNYATAAN KESEDIAAN DALAM PEMBIMBINGAN SKRIPSI

Sesuai permohonan dari mahasiswa/i :

Nama	: **FINO DWI JAYANTO**
Nim	: **0812508**
Semester	: **IX (Sembilan)**
Jurusan	: **Teknik Elektro S-1**
Konsentrasi	: **Teknik Komputer**

Dengan ini menyatakan bersedia/tidak bersedia*) Membimbing skripsi dari mahasiswa tersebut, dengan judul :

" RANCANG BANGUN SERVER INTERACTIVE VOICE RESPONS (IVR) PADA EMERGENCY CALL MENGGUNAKAN VIRTUAL PRIVATE NETWORK (VPN) BERBASIS WIRELESS"

Demikian surat pernyataan ini kami buat agar dapat dipergunakan seperlunya.

Hormat Kami

Dr. Eng. Aryuanto Soetedjo, ST, MT
NIP.P. 1030800417

*) Coret yang tidak perlu