BAB 3

ANALISIS DAN PERANCANGAN SISTEM

3.1. Analisis system

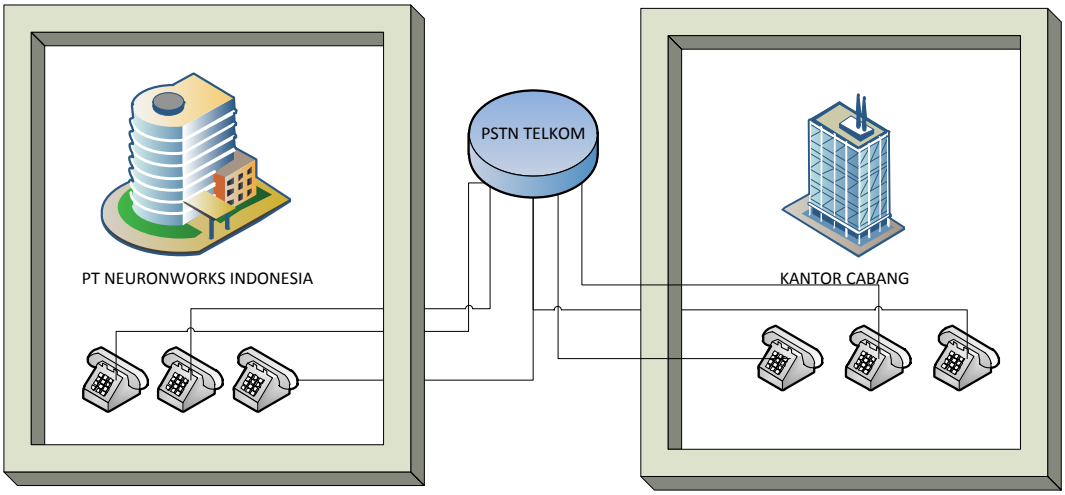
Banyak perusahaan-perusahaan besar seperti PT. Neuronworks Indonesia yang memiliki banyak cabang perusahaan dan mitra kerja yang tersebar di beberapa tempat yang berbeda yang menuntut perusahaan tersebut harus melakukan komunikasi jarak jauh dengan perusahaan lainnya maupun.

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

Perusahaan tersebut membutuhkan komunikasi yang dapat dilakukan setiap saat. Salah satu masalah yang dimiliki oleh Perusahaan PT. Neuronworks Indonesia adalah tidak memiliki jalur telekomunikasi yang aman untuk komunikasi. Banyak jalur komunikasi yang membutuhkan dana yang tidak cukup murah untuk melakukan *voice call*, akan tetapi komunikasi yang dimiliki tidak cukup aman untuk digunakan. Karena masih dapat di sadap oleh orang lain yang berdampak buruk terdahap perusahaan, bocornya rahasia perusahaan ini.

Penulis akan menganalisis performansi dari VOIP tersebut dari segi kualitas dari suara yang akan di hasilkan oleh VOIP tanpa mengggunakan VPN dan yang menggunakan keamanan VPN. Penulis akan menganalisa VOIP dari delay yang akan dihasilkan, paket loss, jitter dan keamanan yang ada pada saat implementasi VOIP tanpa menggunakan VPN dan VOIP yang menggunakan VPN.

3.2. Analisis Sistem yang sedang berjalan



Gambar 3.1 Komunikasi yang sedang berjalan

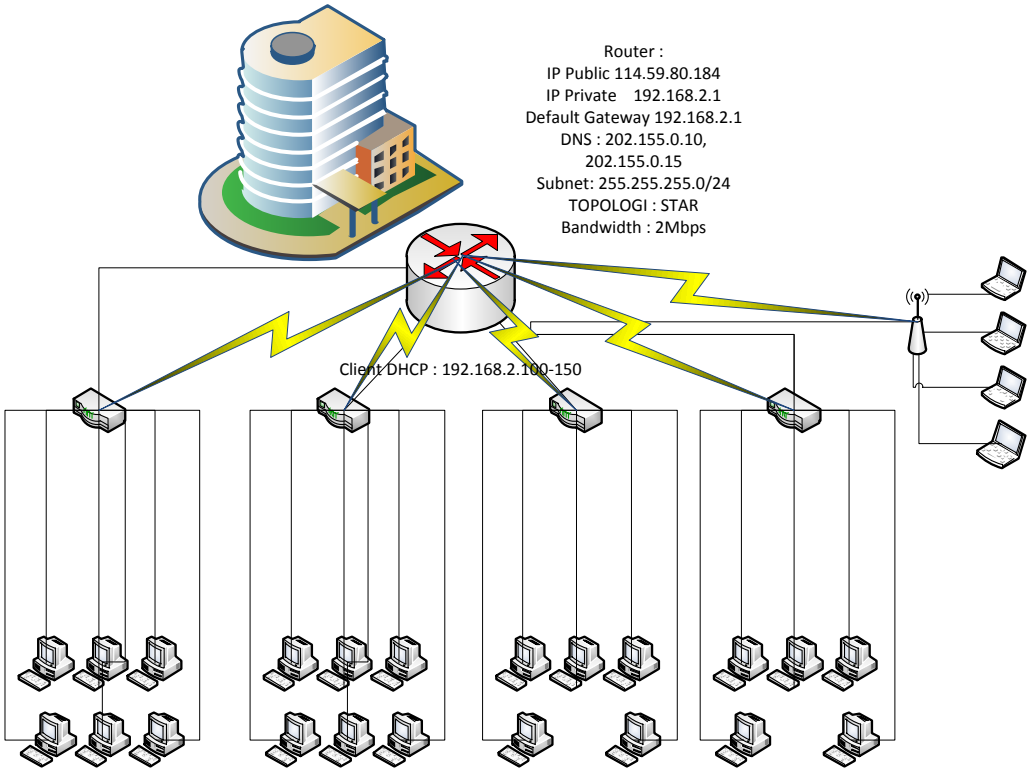
Gambar 3.1 diatas adalah sistem yang sedang berjalan di dalam perusahaan tersebut. Berdasarkan hasil penelitian, sistem yang sedang berjalan masih menggunakan PSTN Telkom sebagai jalur untuk berkomunikasi antara pusat dan cabang, antara lain :

1. Dalam satu gedung perusahaan tersebut masih menggunakan telepon melalui jaringan telkom untuk dapat saling berkomunikasi antara Direksi dan Karyawan, sehingga perusahaan tersebut mengeluarkan biaya lebih untuk komunikasi tersebut.

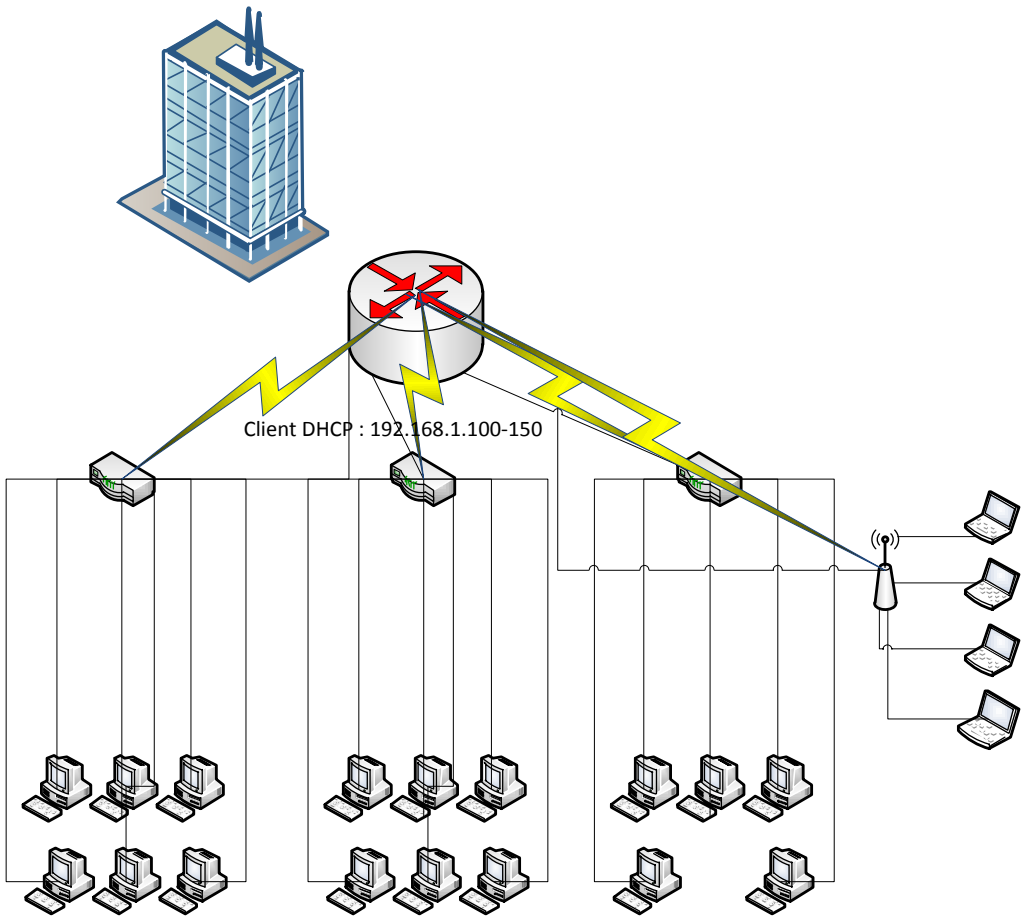
2. Antara kantor cabang dan kantor pusat saat berkomunikasi masih menggunakan jalur telkom dalam kesehariannya untuk melalukan komunikasi dengan karyawan kantor cabang.

Dari gambaran prosedur tersebut terdapat kelemahan-kelemahan adalah setiap kali melakukan komunikasi, maka perusahaan tersebut harus mengeluarkan biaya yang cukup mahal untuk dapat berkomunikasi dangan lawan bicara nya didalam satu gedung ataupun dalam beda gedung dalam satu rekan kerja.

3.3. Analisis topologi jaringan di perusahaan



Gambar 3.2 Topologi Jaringan di Perusahaan



Gambar 3.3 Topologi di Kantor Cabang

Topologi jaringan merupakan tata letak serta struktur hubungan antara komponen-komponen (*node*) dalam suatu jaringan. Topologi jaringan berkaitan dengan mekanisme yang digunakan untuk mengelola cara *station* (komputer) dalam mengakses jaringan, sehingga tidak terjadi konflik.

Topologi Jaringan komputer yang digunakan dalam VPN ini adalah topologi *star* karena jaringan yang sudah ada di PT. Neuronworks Indonesia menggunakan topologi *star*.

Jaringan PT. Neuronworks Indonesia

Ruang lingkup kerja PT. Neuronworks Indonesia dibagi menjadi beberapa bagian diantaranya :

1. Direksi
2. Center Manager
3. *Departement Finance*
4. *Departement Marketing*
5. *Departement Engineering*
6. *Departement* IT .

1. Direksi

   Direksi adalah bagian yang memegang penuh semua tindak keputusan dan tanggung jawab atas perusahaan PT. Neuronworks Indonesia.

2. *Department Finance*

   Bagian ini terdiri atas dua orang, *center manager* dan *skretaris center manager. Center Manager* membawahi kepala bagian dari tiap. Di ruangan *Center Manager* terdapat dua unit .

3. *Department Marketing*

   Departement finance mengurus semua urusan keuangan di PT. Neuronworks Indonesia dan di kepalai seorang kepala bagian. Di bagian *finance* terdapat lima unit.

4. Department Engineering

   Departement engineering bertugas sebagai maintenance gedung, operasional mulai buka sampai tutup gedung, dan perbaikan aset gedung. Di bagian engineering terdapat lima unit.

5. Department Marketing

   Departement marketing bertugas untuk pemasaran Software, area pameran danpemasangan iklan. Di bagian marketing terdapat lima unit.

6. Deparment IT

   Departement IT adalah yang menangani permasalahan yang berhubungan dengan perangkat, jaringan dan software. Di bagian IT terdapat empat unit .

1.4. Solusi yang diusulkan

Dari permasalahan sebelumnya dapat diambil simpulan bahwa salah satu solusi yang diusulkan untuk mengatasi hal-hal tersebut adalah dengan jaringan VoIP dengan keamanan VPN. VoIP adalah sebuahteknologi yang menjadikan media internet untuk melakukan komunikasi suara jarak jauh dengan menggunakan Internet Protokol(IP) sebagai jalur secara langsung. Sinyal suara analog, seperti yang anda dengar ketika berkomunikasi di telepon diubah menjadi data digital dan dikirimkan melalui jaringan berupa paket-paket data secara real time. Sedangkan VPN adalah sebuah teknologi komunikasi yang memungkinkan suatu jaringan dapat terkoneksi ke jaringan public dan dapat digabungkan dengan jaringan local yang memiliki keamanan enkripsi data yang sangat aman digunakan untuk dapat berkomunikasi dengan yang lain. Dengan cara tersebut akan didapatkan hak dan pengaturan yang sama seperti halnya berada di dalam kantor

atau jaringan LAN itu sendiri, walaupun sebenarnya menggunakan jaringan milik public.

1.5. Analisis VoIP

1.5.1. Teknologi *VoIP* yang digunakan

Teknologi *VoIP* yang digunakan dalam penelitian ini adalah teknologi SIP(*Session Initiation Protocol*). Teknologi ini lebih dapat diandalkan untuk dioperasikan di jaringan internet karena sifatnya yang *flexible* (bisa menembus *firewall* dan *proxy*). Dalam penelitian ini penulis meggunakan teknologi ini sebagai bahan analisa, karena kemudahan dalam implementasi sistem dan kompatibilitas sistem. Peralatan IP telephoni yang berbasis teknologi SIP sudah banyak beredar di pasaran dengan harga yang relatif terjangkau.

Dalam penelitian ini penulis menggunakan *codec* G.711 , karena *codec* ini mempunyai kualitas suara yang jernih dengan *delay* yang sangat rendah jika kita aplikasikan pada jaringan lokal.*codec* G.711 menghasilkan *bitrate* 64 kbps pada saat digunakan.

1.5.2. Pengkodean

Pengkodean suara merupakan pengalihan kode analog menjadi kode digital agar suara dapat dikirim dalam jaringan komputer . Hal ini dikenal dengan istilah codec, singkatan dari compressor-decompressor.Terdapat berbagai jenis codec yang dikembangkan untuk memampatkan/mengkompresi suara agar dapat menggunakan bandwidth secara lebih hemat tanpa mengorbankan kualitas suara (suara yang keluar masih dapat didengar dengan baik).

1.5.3. Bit Rate

Jenis *codec* dengan algoritma kompresi yang digunakan menentukan *bit rate* yang dibutuhkan untuk melakukan transmisi data suara. Sebagai contoh, setiap percakapan suara analog menggunakan PSTN membutuhkan *bandwidth* 64 Kbps. Nilai ini didapatkan dari *encoding* dan algoritma kompresi (PCM), yang dapat menyediakan data dan suara dengan kualitas tinggi. Salah satu keuntungan menggunakan telepon IP adalah kemampuan untuk memanfaatkan perkembangan teknologi *codec* yang terkini, sehingga *bandwidth* 64 Kbps yang hanya dapat digunakan untuk sebuah percakapan pada jaringan PSTN, dapat dimanfaatkan untuk sekitar 10 percakapan pada jaringan *packet-switched* menggunakan *codec* G.723.

1.5.4. Bandwidth

Dalam perancangan *VoIP*, *bandwidth* merupakan suatu yang harus diperhitungkan agar dapat memenuhi kebutuhan yang dapat digunakan menjadi parameter untuk menghitung jumlah peralatan yang di butuhkan dalam suatu jaringan. Perhitungan ini juga sangat diperlukan dalam efisiensi jaringan dan biaya serta sebagai acuan pemenuhan kebutuhan untuk pengembangan di masa mendatang. Kebutuhan *bandwidth* akan sangat tergantung pada pemilihan *codec* yang digunakan. Untuk menghitung *bandwidth* yang dibutuhkan tiap satu panggilan *VoIP* dapat dihitung dengan rumus berikut :

Voice payload = codec bit rate x frame rate

voice packet size = (Header layer 2 MLPPP atau FRF.12 header) +

(IP/UDP/RTP) + (voice payload)

voice packets per second (pps) = codec bit rate / voice payload size

bandwidth = voice packet size * pps

Pada kasus ini kita akan menghitung besar *bandwidth* yang dibutuhkan oleh *codec*

G.711 dengan *frame rate* sebesar 20 ms (0,02 detik) dan *bitratenya* 64 kbps maka,

Voice payload = 64000 bits x 0,02 = 1280 bits = 160 bytes

Voice packet size = 6 bytes + 4 bytes + 160 bytes =170 Bytes

= 170 bytes x 8 bits per byte= 1360 Bit

Voice packet per second = 64000 / 1280 = 50 pps

Bandwidth = 1360 x 50 = 68000 = 68 kbps

Maka *bandwidth* yang dibutuhkan oleh codec G..711 tiap satu saluran komunikasi

adalah sebesar 68 kbps.

1.5.5. Delay/Jitter

Router dan jaringan IP memiliki karakteristik khusus yang menyulitkan pengontrolan *delay* dan variasinya (*jitter*). Proses penanganan paket IP selama ini selalu dilakukan secara *best effort*. Paket IP yang datang diperlakukan sama dan diservice sesuai dengan urutan kedatangan. Ukuran paket IP sendiri bervariasi, sehingga *delay* dan variasi *delay* di jaringan menjadi besar dan tidak menentu.

Delay dan variasi *delay* ini dapat berakibat buruk bagi kualitas suara. Hal ini terjadi karena informasi suara memiliki karakteristik *timing*. Suku kata tertentu dari suatu kata harus diucapkan dalam selang waktu tertentu antara ia dan suku

kata berikutnya. Karakteristik waktu ini harus dipertahankan agar pembicaraannya tetap memiliki arti.

Agar jaringan IP ini dapat digunakan untuk menangani paket suara, maka baik *delay* maupun variasinya harus dapat dikontrol dan ditekan serendah mungkin. Besarnya *delay* maksimum yang direkomendasikan oleh ITU-T pada G.114 untuk aplikasi suara adalah 150 ms, sedangkan *delay* maksimum dengan kualitas suara dan gambar yang masih dapat diterima pengguna adalah 250 ms.

1.5.6. Throughput jaringan

Throughput adalah jumlah bit yang ditransmisikan perdetik melalui sebuah sistem atau media komunikasi. *Throughput* diukur setelah transmisi data (host/*client*) karena suatu sistem akan menambah *delay* yang disebabkan *rocessor limitations*, kongesti jaringan, *buffering inefficients*, error transmisi, *traffic loads* atau mungkin desain *hardware* yang tidak mencukupi. Aspek utama *throughput* yaitu berkisar pada ketersediaan *bandwidth* yang cukup untuk menjalankan aplikasi. Hal ini menentukan besarnya trafik yang dapat diperoleh suatu aplikasi saat melewati jaringan. Aspek penting lainnya adalah error (pada umumnya ber*hub*ungan dengan *link error rate*) dan *losses* (pada umumnya ber*hub*ungan dengan kapasitas *buffer*). *Throughput* tergantung pada faktor-faktor berikut ini:

Karakteristik link : *bandwidth, error rate*.

1. Karakteristik node : kapasitas *buffer*, daya pemrosesan.
2. Karakteristik node : kapasitas *buffer*, daya pemrosesan.

1.5.7. Derau(noise)

Derau (*noise*) adalah bentuk gangguan suara latar belakang yang berasal dari lingkungan sekitar pembicara (segmen ujung koneksi) yang masuk ke kanal komunikasi. Gangguan ini biasa muncul di dalam komunikasi berbasis sirkit, namun akan semakin lebih besar di sistem komunikasi berbasis paket.

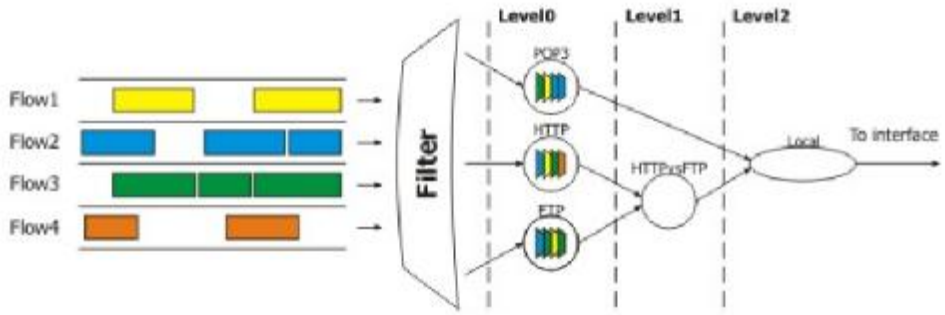
Di dalam sistem telepon baik analog maupun digital, bunyi gaung terjadi ketika pembicara mendengar kembali perulangan pembicaraannya dengan daya yang cenderung melemah. Salah satu faktor yang cukup berpengaruh terhadap kejadian suara gaung adalah waktu tunda *round-trip*, yaitu waktu yang diperlukan oleh sinyal suara sejak keluar dari mulut pembicara kemudian diteruskan ke jaringan telepon, mengalami kebocoran di suatu sumber suara gaung dan kembali lagi sampai terdengar oleh telinga pembicara. Hal ini dapat diatasi dengan menggunakan fitur *echo canceler* yang biasanya ada pada *SIP terminal*.

1.5.8. Quality Of Service (QoS)

Pada saat sekarang pengiriman paket-paket dalam sebuah jaringan biasanya dilakukan secara *best effort*, dimana paket akan dikirimkan secara *FIFO* paket yang pertama samapi node akan diteruskan ke node berikutnya secara berururan berdasarkan kedatangannya. Hal ini tidak ada salahnya, tetapi aplikasi-aplikasi yang berada di jaringan semakin lama semakin meminta bandwith yang besar sedangakan harga bandwith ini masih realtif mahal untuk saat sekarang ini. Sehingga dibutuhkan langkah-langkah yang efektif yang harus dilakukan oleh

seorang *network administrator* untuk menrapkan kebijakan-kebijakan tertentu agar performansi jaringan mencapai kinerja yang optimal.

Salah satu cara untuk meningkatkan performansi jaringan yaitu dengan cara menerapkan metode *priority queing*. Pada saat ini penanganan pengiriman paket-paket data dilakukan secara best effort, router akan meneruskan paket sesuai dengan urutan kedatangan paket tersebut sehingga paket-paket tersebut akan berebut bandwith yang ada . Pada penelitian ini penulis menggunakan metode priority queing yang terdapat pada mikrotik routerOS, dimana nantinya trafik yang berupa paket-paket yang mempunyai prioritas lebih tinggi akan dialokasikan bandwith sebesar yang dibutuhkannya yang diset pada router. *VoIP* yang menggunakan protokol RTP akan mendapat prioritas utama untuk dilewatkan pada media transmisi yang digunakan. Pada penelitian ini penullis akan menerapkan *policy* pada *router* mikrotik yang akan diset urutan prioritas sebagai RTP untuk port 8000-20000 akan mendapatkan prioritas utama dengan alokasi badwith untuk tiap satu kanal komunikasi sebesar 84 kbps.



Gambar 3.4 Priority queing

Pada penelitian ini paket-paket RTP akan diset pada port 8000 sampai 20000 yang digunakan untuk media transimisi data. Dapat dilihat pada gambar 3.3

di atas urutan pengklasifikasian trafik yang diproses oleh filter paket data. Filter tersebut akan memilah-milah paket berdasarkan protokolnya. Paket yang mendapatkan prioritas pertama akan diproses terlebih dahulu. Setelah dipilah pilah paket akan diurutkan pengirimannya berdasarkan urutan prioritas yang sudah ditetapkan sebelumnya untuk selanjutnya dikirimkan ke node tujuan.

1.5.9. *Mean Opinion Score (MOS)*

MOS digunakan sebagai bahan pengukuran kualitas system *VOIP* secara subjektif. Penghitungan MOS ini didasarkan pada hasil pengujian komunikasi *VoIP* dari beberapa sampel yang lalu diambil rata-ratanya. Tetapi pada penelitian ini penulis menggunakan *software Commview* yang dapat menghasilkan nilai MOS secara otomatis pada hasil analisa jaringannya.

1 **Tabel 3.1 Ringkasan Codec**

Number	Standart by	Description	Description	Samping rate (kHz)	Frame Size (ms)	Remarks	MOS (Mean Opinion Score)
G.711*	ITU –T	Pulsecodemodulation (PCM)	64	8	Sampling	U-law (US, Japan) and A-law (Europe) companding	4.1
G.721	ITU –T	Adaptive differential pulse code modulation (ADPCM)	32	8	Sampling	Now described in G.726; obsolete.	
G.722	ITU –T	7 kHz audio-coding within 64 kbit/s	64	16	Sampling	Subband-codec that divides 16 kHz band into two subbands, each coded using ADPCM	
G.722.1	ITU –T	Coding at 24 and 32 kbit/s for hands-free operation in systems with low frame loss	24/32	16	20		
G.723	ITU –T	Extensions of Recommendation G.721 adaptive differential pulse code modulation to 24 and 40 kbit/s for digital circuit multiplication equipment application	24/40	8	Sampling	Superceded by G.726; obsolete. This is a completely different codec than G.723.1	
G.723.1	ITU –T	Dual rate speech coder for multimedia communications transmitting at 5.3 and 6.3 kbit/s	5.6/6.3	8	30	Part of H.324 video conferencing. It encodes speech or other audio signals in frames using linear predictive analysis-by-synthesis coding. The excitation signal for the high rate coder is Multipulse Maximum Likelihood Quantization (MP-MLQ) and for the low rate coder is Algebraic-Code-Excited Linear-Prediction (ACELP).	
G.726	ITU –T	40, 32, 24, 16 kbit/s adaptive differential	16/24/32/40	8	Sampling	ADPCM; replaces G.721 and G.723.	3.8-3.9

		pulse code modulation (ADPCM)					
G.727	ITU –T	5-, 4-, 3- and 2-bit/sample embedded adaptive differential pulse code modulation (ADPCM)	Var		Sampling	ADPCM. Related to G.726	3.85
G.728	ITU –T	Coding of speech at 16 kbit/s using low-delay code excited linear prediction	16	8	2.5	CELP.	
G.729	ITU –T	Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear-prediction (CS-ACELP)	8	8	10	Low delay (15 ms)	3.61
GSM 06.10	ETSI	RegularPulse Excitation LongTerm Predictor (RPE-LTP)	13	8	22.5	Used for GSM cellular telephony.	3.92
LPC10	USA						

1.6. Kelemahan VoIP dan Solusinya

1. Sulit mengirimkan fax
2. Perlu jalur internet yang cepat, biasanya backbone diharuskan menggunakan Fiber optic
3. Susah untuk menentukan emergency call.

Kelemahan jaringan yang menjadi musuh VoIP :

1. Delay

Jaringan yang berbasis atau dengan backbone Satellite tidak cocok untuk VoIP. Karena delay satellite yang sangat besar. Sehingga menyebabkan suara kita lama didengar oleh lawan bicara.

Solusi : Backbone fiber optic.

2. Jitter

Jitter pada intinya adalah variasi dalam delay, terjadi karena adanya perubahan terhadap karakteristik dari suatu sinyal sehingga menyebabkan terjadinya masalah terhadap data yang dibawa oleh sinyal tersebut.

Solusinya : Mengaplikasikan suatu sistem buffer pada pesawat penerima untuk menstabilkan data suara sebelum ditampilkan. Efek sampingnya akan ada sedikit delay.

3. Packet Loss

Paket loss artinya hilangnya paket data yang sedang dikirimkan. Hilangnya data ini bisa disebabkan karena Jitter atau karena adanya permasalahan di perangkat-

perangakat jaringan seperti router yang terlalu sibuk, jalur komunikasi yang terlalu padat penggunanya.

Solusi : Peralatan yang lebih bagus dibandingkan peralatan jaringan untuk internet biasa, kualitas koneksi yang lebih baik dan perhitungan terhadap penggunaan bandwidth yang lebih baik.

4. Keamanan

Karena suara berjalan pada jaringan internet maka tetap akan ada kemungkinan data suara tersebut disadap oleh pihak-pihak yang tidak bertanggung jawab.

Solusi : Membangun sistem keamanan yang lebih baik, enkripsi data.

5. Echo

Echo atau gema disebabkan oleh kesalahan perangkat pengirim dan penerima suara dalam mengconversikan atau mengubah data dari suara menjadi digital atau sebaliknya biasanya karena adanya kesalahan faktor impedansi dalam rangkaian analog peralatan.

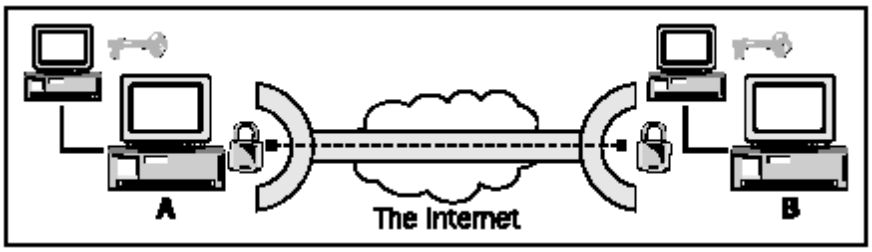
Solusi : Melengkapi peralatan dengan rangkaian analog coupling yang bisa meredam kesalahan faktor impedansi.

1.7. Analisis VPN

VPN memberikan keamanan serta *reliabilitas* yang sama seperti jaringan *private.* Oleh karena itu, pengguna VPN dapat mengakses *Local Area Network* suatu perusahaan atau organisasi dengan mengunakan jaringan *internet*.

1. Tunneling dan Overhead

VPN yang sering disebut terowongan (tunneling), sebab data dalam koneksi VPN dilindungi dari Internet sebagai dinding dari suatu jalur atau tunnel rel melindungi lalu lintas di dalam tunnel dari orang banyak batu gunung di atas.



Gambar 3.5 Tunneling lindungi *access* Internet

VPN perangkat lunak dalam lokasi A dan B encrypts(kunci) dan decrypts (membuka kunci) data dan mengirimkannya melalui tunnel itu. Seperti mobil atau kereta dalam suatu terowongan, data tidak bisa meninggalkan tetapi terowongan yang lain endpoint. Berikut yang dipasang dan dibungkus ke dalam satu paket baru:

a. Informasi tunnel.

b. Encryption data dan metoda

c. IP paket Yang asli

Paket yang baru kemudian mengirim kepada tunnel endpoint yang lain. Muatan penghasil untung dari paket ini sekarang menjaga IP paket yang lengkap (atau membungkus jaringan), tetapi di dalam format encrypted dan begitu menarik untuk seseorang yang tidak memiliki kunci. Header baru dari paket yang sederhana berisi alamat pengirim dan penerima dan metadata lain yang penting dan yang disajikan oleh VPN perangkat lunak.

2. 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.

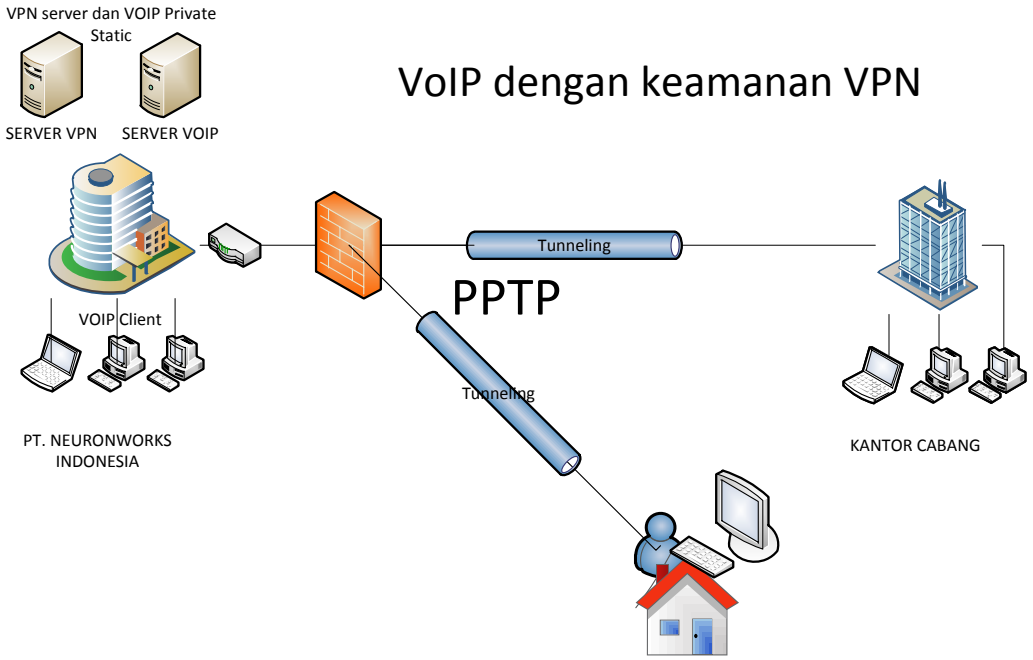
Perusahaan yang memiliki pegawai yang ada di lapangan dalam jumlah besar dapat menggunakan *remote access* VPN untuk membangun WAN. VPN tipe ini akan memberikan keamanan, dengan mengenkripsi koneksi antara jaringan lokal perusahaan dengan pegawainya yang ada di lapangan. Pihak ketiga yang melakukan enkripsi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

2. **Site-to-site VPN**

Jenis implementasi VPN yang kedua adalah *site-to-site* VPN. Implementasi jenis ini menghubungkan antara 2 kantor atau lebih yang letaknya berjauhan, baik kantor yang

dimiliki perusahaan itu sendiri maupun kantor perusahaan mitra kerjanya. VPN yang digunakan untuk menghubungkan suatu perusahaan dengan perusahaan lain (misalnya mitra kerja, *supplier* atau pelanggan) disebut ekstranet. Sedangkan bila VPN digunakan untuk menghubungkan kantor pusat dengan kantor cabang, implementasi ini termasuk jenis intranet *site-to-site* VPN.

Protokol *Tunneling* Utama VPN



Gambar 3.6 Tunneling PPTP

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.

PPTP terdapat sejak dalam sistem operasi Windows NT server dan Windows NT Workstation versi 4.0. Komputer yang berjalan dengan sistem operasi tersebut dapat menggunakan protokol PPTP dengan aman untuk terhubung dengan private network sebagai klien dengan remote access melalui internet. PPTP juga dapat digunakan oleh komputer yang terhubung dengan LAN untuk membuat VPN melalui 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.

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

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

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

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

1. PPTP client
2. Network Access Server
3. PPTP server

1.8. Algoritma Kriptografi RSA

RSA adalah salah satu contoh kriptografi yang menerapkan konsep *public key*. Algoritma ini pertama kali dipublikasikan di tahun 1977 oleh Ron Rivest, Adi Shamir, dan Leonard Adleman dari Massachusetts Institute of Technology (MIT). Nama RSA sendiri adalah singkatan dari nama belakang mereka bertiga. Clifford Cocks, seorang matematikawan Inggris sebenarnya juga telah mengembangkan

algoritma yang hampir sama dengan RSA ini pada tahun 1973. Namun algoritma buatannya tidak begitu dikenal oleh publik, dan baru dipublikasi pada tahun 1997 karena merupakan proyek rahasia. Walau begitu algoritma yang dikembangkan Rivest, Shamir, dan Adleman tidak berhubungan dengan pekerjaan Cocks. Pada algoritma RSA terdapat 3 langkah utama yaitu *key generation* (pembangkitan kunci), enkripsi, dan dekripsi. Kunci pada RSA mencakup dua buah kunci, yaitu *public key* dan *private key. Public key* digunakan untuk melakukan enkripsi, dan dapat diketahui oleh orang lain. Sedangkan *private key* tetap dirahasiakan dan digunakan untuk melakukan dekripsi. Pembangkitan kunci atau *key generation* dari RSA adalah sebagai berikut :

a. Pilih dua buah bilangan prima sembarang *a* dan *b*. Jaga kerahasiaan *a* dan *b* ini.
b. Hitung $n = a * b$. Besaran *n* ini tidak perlu dirahasiakan.
c. Hitung $m = (a-1) * (b-1)$. Sekali *m* telah dihitung, *a* dan *b* dapat dihapus untuk mencegah diketahuinya oleh pihak lain.
d. Pilih sebuah bilangan bulat untuk kunci publik, sebut namanya *e*, yang relatif prima terhadap *m* (relatif prima berarti GCD(e, m) = 1) dengan syarat $e \neq (p-1)$, $e \neq (q-1)$, dan $e < n$
e. Hitung kunci dekripsi, *d*, dengan kekongruenan $ed \equiv 1 \pmod{m}$.

Pada *public key* terdiri atas:

1. *N*, modulus yang digunakan.
2. *e*, eksponen publik (sering juga disebut eksponen enkripsi).

Pada *private key* terdiri atas:

1. *N*, modulus yang digunakan, digunakan pula pada *public key*.
2. *d*, eksponen pribadi (sering juga disebut eksponen dekripsi), yang harus dijaga kerahasiaannya.

Biasanya, berbeda dari bentuk *private key* (termasuk parameter CRT):

1. *p* dan *q*, bilangan prima dari pembangkitan kunci.
2. *d mod (p-1)* dan *d mod (q-1)* (dikenal sebagai *dmp1* dan *dmq1*).
3. *(1/q) mod p* (dikenal sebagai *iqmp*).

Bentuk ini membuat proses dekripsi lebih cepat dan *signing* menggunakan Chinese Remainder Theorem (CRT). Dalam bentuk ini, seluruh bagian dari *private key* harus dijaga kerahasiaannya.

Alice mengirimkan *public key* kepada Bob, dan tetap merahasiakan *private key* yang digunakan. *p* dan *q* sangat sensitif dikarenakan merupakan faktorial dari *N*, dan membuat perhitungan dari *d* menghasilkan *e*. Jika *p* dan *q* tidak disimpan dalam bentuk CRT dari *private key*, maka *p* dan *q* telah terhapus bersama nilai-nilai lain dari proses pembangkitan kunci.

Proses enkripsi dapat dilakukan dengan :

$$C_i = P_i^e \bmod n$$

Sedangkan proses dekripsi dilakukan dengan :

$$P_i = C_i^d \bmod n$$

Blok-blok plainteks dinyatakan dengan *p1, p2, p3,* ... (harus dipenuhi persyaratan bahwa nilai pi harus terletak dalam himpunan nilai 0, 1, 2, ..., n-1 untuk menjamin hasil perhitungan tidak berada di luar himpunan).

Pada langkah kelima pembangkitan kunci atau *key generation*, kekongruenan $ed \equiv 1 \pmod{m}$ sama dengan $ed \bmod m = 1$. Sehingga dapat pula dikatakan bahwa $ed \equiv 1 \pmod{m}$ ekivalen dengan $ed = 1 + km$.

Maka *d* dapat dihitung dengan cara yang sederhana dengan persamaan $d = \frac{1+}{e}\frac{km}{}$.

Dengan mencoba nilai k = 1, 2, 3, ..., diperoleh nilai *d* yang bulat. Nilai itu yang akan dipakai sebagai kunci pribadi untuk dekripsi pesan.

Dalam implementasi sebenarnya, nilai *a* dan *b* diharapkan sangat besar sekali (misalnya 100 digit) agar pekerjaan memfaktorkan *n* menjadi faktor primanya menjadi sangat sukar, sehingga lebih susah untuk ditembus.

Contoh penerapan algoritma RSA.

1. Menentukan bilangan acak *a* dan *b*

   a = 13

   b = 5

2. Hitung *n* dan *m*

   *n = 13 * 5 = 65*

   *m = 12 * 4 = 48*

3. Cari nilai *e*

   GCD(e, 48) = 1

Misalnya, (GCD = Greatest Common divisor atau dua bilangan adalah bilangan positif terbesar yang dapat membagi habis kedua bilangan itu).

e = 2 maka GCD(2, 48) = 2

e = 3 maka GCD(3, 48) = 3

e = 4 maka GCD(4, 48) = 4

e = 5 maka GCD(5, 48) = 1 , jadi digunakan e = 5

4. Lalu cari nilai *d*

$$d = \frac{1 + km}{e}.$$

Misalnya

k = 1 maka d = 9,8

k = 2 maka d = 19,4

k = 3 maka d = 29 , jadi digunakan d = 29

Coba mengenkripsi pesan menggunakan angka-angka yang telah didapatkan. Misalkan pesan yang dikirim adalah angka 48.

- E = 48 ^ 5 mod 65

  = 254803968 mod 65

  = 3

Setelah dilakukan enkripsi, didapat nilai sekarang adalah 3. Kemudian akan kita coba lakukan dekripsi pada nilai tersebut.

- D = 3 ^ 29 mod 65

  = 68630377364883 mod 65

= 48

Perhatikan bahwa nilai yang didapat sama dengan nilai awal, yaitu 48.

Kekuatan algoritma RSA terletak pada tingkat kesulitan dalam memfaktorkan bilangan menjadi faktor primanya, dalam hal ini memfaktorkan *n* menjadi *a* dan *b*. Karena sekali *n* berhasil difaktorkan, maka menghitung nilai *m* adalah perkara mudah. Selanjutnya, walau nilai *e* diumumkan, perhitungan kunci *d* tidaklah mudah pula karena nilai *m* yang tidak diketahui.

1.9. Keuntungan Menggunakan PPTP

Para pegawai yang bekerja di luar kota atau bekerja dari rumahnya atau berada di jalan dan memerlukan akses kepada jaringan komputer di perusahannya akan sangat merasakan manfaat PTP ini. administrator LAN juga memperoleh keuntungan dengan kemudahan implementasi dan keamanan yang ditawarkan oleh protocol PPTP. Selain itu administrator LAN juga memperoleh keuntungan dari implementasi yang murah, dimana aplikasi PPTP tidak membutuhkan peralatan yang baru, kemudahan dalam pengaturan media pembawa/media komunikasi dan perawatan yang mudah. PPTP juga memungkinkan ISP (Internet Service Provider) dengan PPTP, dapat menyediakan layanan dengan nilai tambahdan nilai jual yang tinggi yang sangat diminati oleh perusahaan-perusahaan dengan jaringan komputer yang tersebar di beberapa cabang. Penyedia jasa keamanan jaringan seperti perusahaan pembuat *firewall* dan jasa-jasa internet lainnya juga memperoleh kemudahan serta jaminan keamanan dari PPTP.

Kalau diantara kita pernah mendengar mengenai *SecureSocketLayer* (SSL) yang menurut banyak pakar sangat memakan proses didalam CPU baik pada saat enkripsi maupun pada saat dekripsi, maka PPTP tidaklah demikian. Kebutuhan akan kerja prosesor yang kita lihat pada SSL biasanya terjadi karena faktor pemilihan algoritma enkripsi. RC4 memiliki overhead 14 instruksi per byte yang membuatnya lebih cepat jika dibandingkan dengan *stream chipper* yang tersedia.dalam RAS. Selain itu PPTP juga memiliki keunggulan bahwa enkripsi dilakukan pada tingkat kernel atau di dalam sistem operasi. SSL memiliki penurunan performansi karena dua hal, operasi kunci privat (*privatekeyoperation*) yang membutuhkan 85ms *waktu kerja CPU* untuk melakukan set up koneksi dan setelah itu, *streamencryption* dilakukan pada level aplikasi kemudian dimasukkan ke dalam *socket* layer, sebagai bagian dari proses transmisi data dan memungkinkan semua proses dilakukan pada tingkat kernel.

Fungsi VPN ada banyak. Beberapa diantaranya yaitu:

1. Menghubungkan kantor-kantor cabang melalui jaringan public. Dengan VPN maka perusahaan tidak perlu membangun jaringan sendiri. Cukup terhubung dengan jaringan public contohnya internet. Saat ini hampir semua kantor perusahaan pasti memiliki akses internet. Dengan demikin bisa dihemat anggaran koneksi untuk ke cabang-cabang.

Mobile working, dengan VPN maka karyawan dapat terhubung langsung dengan jaringan kantor secara private. Maka karyawan dapat melakukan pekerjaan

yang bisa dilakukan dari depan komputer tanpa harus berada di kantor. Hal ini menjadi solusi virtual office di jaman mobilitas tinggi seperti sekarang ini.

Securing your network. Saat ini beberapa vendor seperti telkom memberikan solusi VPN juga untuk perusahaan-perusahaan. Namun solusi ini masih kurang aman. Karena untuk terhubung tidak memerlukan authentikasi. Sehingga bila ada pengguna mengetahui settingan VPN perusahaan tersebut maka dia dapat terhubung ke jaringan perusahaan tapi harus login. Contohnya pada telkomsel VPN hanya dengan mengganti nama APN pada settingan network maka dia dapat langsung terhubung dengan jaringan dengan nama APN tersebut. Dengan memasang VPN lagi di jaringan VPN semi publik tersebut maka jaringan akan lebih aman karena sebelum masuk ke jaringan kantor maka user harus membuat tunnel dulu dan login ke VPN server baru bisa terhubung dengan jaringan kantor.

Mengamankan jaringan wireless. Jaringan wireless merupakan jaringan publik yang bisa diakses oleh siapa saja yang berada dijangkauan wireless tersebut. Walaupun wireless juga memiliki pengaman seperti WEP, WPA, WPA2 namun jaringan wireless masih saja bisa ditembus. Dengan menggunakan VPN maka user yang terhubung ke wireless harus membuat tunnel dulu dengan login ke VPN server baru bisa menggunakan resource jaringan seperti akses internet dan sebagainya.

1.10. Kebutuhan Non Fungsional

1.10.1. Analisis Kebutuhan Non Fungsional Server VoIP

Kebutuhan Non Fungsional dari server VoIP mencakup Hardware dan Software adalah sebagai berikut :

1.10.1.1.Hardware

Spesifikasi perangkat keras yang digunakan sebagai komputer *server* memiliki spesifikasi sebagai berikut :

a. Prosesor : Intel PENTIUM Dual CORE - 1,73 GHz

b. RAM : 1 GB DDR2

c. VGA : *Integrated* INTEL GMA 945, 256 MB

d. Sound Card : Realtek HD Audio

e. Ethernet : Realtek 8139 Ethernet

f. HDD : SATA 80 Gb

1.10.1.2.Software

Spesifikasi perangkat lunak yang digunakan pada *server* adalah sebagai berikut :

a. Sistem operasi : Linux CenOS

b. *Server VoIP* : Asterisk PBX

c. Analisis : Commview

1.10.2. Analisis Kebutuhan Non Fungsional *Server* VPN

Kebutuhan Non Fungsional dari server VoIP mencakup Hardware dan Software adalah sebagai berikut :

1.10.2.1.Hardware

Spesifikasi perangkat keras yang digunakan sebagai komputer *server* memiliki spesifikasi sebagai berikut :

a. *Procesor* : Intel P4 2,4 GHz

b. *RAM* : 256 Mb DDR2

c. *VGA* : Onboard

d. *Ethernet* : - Onboard

: - DFE-528 TX Ethernet

: - DFE-528 TX Ethernet

e. *HDD* : ATA 40 Gb

f. *Monitor* : LG 710S

g. *Keyboard* : Standar

h. *Mouse* : Optic standar

i. *Optical disc* : CD Room

1.10.2.2.Software

Spesifikasi perangkat lunak yang digunakan pada *server* adalah sebagai berikut :

a. Sistem operasi : Linux

b. *Server VPN : Pfsense*

c. Analisis : Commview

1.10.3. Analisis kebutuhan Non Fungsional *client voip dan vpn*

Kebutuhan Non Fungsional dari server VoIP mencakup Hardware dan Software adalah sebagai berikut :

1.10.3.1.Software

Spesifikasi perangkat lunak yang dapat digunakan untuk *client* adalah sebagai berikut :

a. Sistem Operasi : Windows, Linux ataupun Apple

b. Client VPN : X-lite, 3CX, ataupun software yang suport SIP client

Hardware

Spesifikasi perangkat lunak yang dapat digunakan untuk client adalah sebagai berikut :

a. Processor : recommended P4 ++

b. RAM : recommended 256 ++

c. VGA : BEBAS

d. *Ethernet* : - Onboard(min)

e. *HDD* : BEBAS

f. *MONITOR* : BEBAS

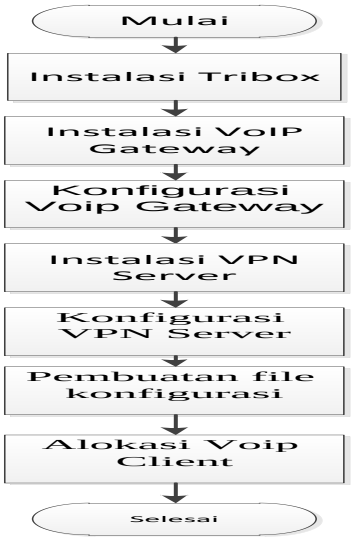
g. *Keyboard* : standart

h. *Mouse* : standar

i. *Headset* *:* bebas *(min : input mic)*

1.11. Kebutuhan Fungsional

1.11.1. *Konfigurasi Voice over internet protocol* (*VoIP*) dengan keamanan *Virtual Private Network* (VPN).



Gambar 3.7 Flowchart Perancangan VoIP dengan keamanan VPN

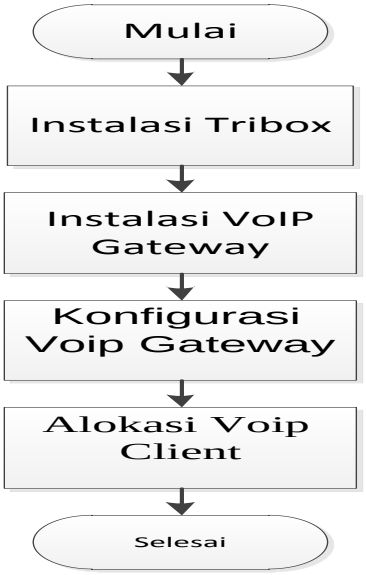
Proses pertama dalam perancangan *server* adalah instalasi *Trixbox* versi 2.8.0.4-i386 pada PC yang dikhususkan untuk VoIP *server*. Setelah selesai instalasi Trixbox, maka langkah selanjutnya adalah melakukan konfigurasi VOIP *gateway* yaitu dengan cara mengkonfigurasi networks address yang berada pada VOIP server tersebut. Konfigurasi Networks address meliputi input IP address, IP gateway, DNS server, dan Subnet Maks.

Selanjutnya pembuatan VPN *server* dilakukan dengan penambahan instalasi VPN serveragar dapat digunakan sebagai *security* terhadap VoIP. Implementasi *security* VPN bekerja pada *layer* 2 dan 3 referensi OSI. Setelah selesai proses instalasi VPN server, maka langkah selanjutnya adalah melalukan konfigurasi VPN *server* yaitu dengan cara megkonfigurasi netwoks address yang berada pada VPN VPN server tersebut. Konfigurasi Networks Address meliputi input address, IP gateway, DNS server dan Subnet Maks.

1.11.2. Konfigurasi pada sisi server VOIP

VoIP *server* menggunakan sistem operasi *linux server*. Penggunaan *Linux* disini menggunakan distributor (distro) *trixbox* yang khusus digunakan untuk menangani VoIP. Jenis distro ini dipilih dikarenakan atas kesetabilan dan kehandalan dari *trixbox* yang merupakan distro turunan dari *CentOS*.

Proses perancangan pada sisi server ada beberapa tahap. Tahap-tahap perancangan pada sisi *server* bisa dilihat pada Gambar 3.10.



Gambar 3.8 Flowchart Perancangan Server VoIP tanpa keamanan VPN

VOIP SERVER

Sistem Operasi : LINUX CenOs / Free PBX

Setting Network:

- IPv4 Address : Private Static (192.168.2.130)

- IPv4 Subnet Mask : 255.255.255.255.0
- IPv4 Default Gateway : 192.168.2.1

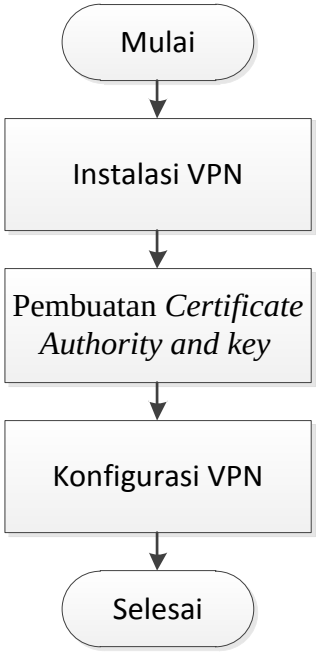
Tabel 3.*2 User* dan *Password Dial* VOIP *Client*

Tempat	User dial	Password	Alias Name
PT Neuronwoks Indonesia	10101	10101	VPN 101
	10102	10102	VPN 102
	10103	10103	VPN 103
Kantor Cabang	10201	10201	VPN 201
	10202	10202	VPN 202
	10203	10203	VPN 203
Cadangan/diluar kawasan kantor PT Neuronwoks Indonesia	10111	10111	VPN 111
	10112	10112	VPN 112
	10113	10113	VPN 113
Cadangan/ diluar kawasan kantor cabang	10211	10211	VPN 211
	10212	10212	VPN 212
	10213	10213	VPN 213

1.11.3. Konfigurasi Pada sisi Server VPN

Virtual Private Network (VPN) merupakan suatu cara untuk membuat sebuah jaringan bersifat private dan aman dengan menggunakan jaringan publik misalnya internet. VPN dapat mengirim data antara dua komputer yang melewati jaringan publik sehingga seolah-olah terhubung secara *point-to-point*. Sedangkan untuk mendapat koneksi yang bersifat private, data yang dikirimkan harus dienkripsi terlebih dahulu untuk menjaga kerahasiaannya sehingga paket yang tertangkap ketika melewati jaringan publik tidak terbaca karena harus melewati proses dekripsi. Proses enkapsulasi data tersebut sering disebut tunneling.Salah satu dari metode tunneling adari VPN adalah PPTP.PPTP adalah sebuah network protocol yang meng-enkapsulasi paket-paket PPP (Point-to-Point Protocol) kedalam IP datagram untuk ditransmisikan melalui Internet atau jaringan public berbasis TCP/IP lainnya. PPTP juga dapat digunakan dalam private LAN-to-LAN networking.Metode ini dipilih karena PPTP sangat cocok digunakan untuk membangun jaringan akses kepada LAN melalui intenet . Keunggulan-keunggulan utama pemakaian PPTP adalah:

1. lebih aman
2. tidak perlu melakukan perubahan pengalamatan jaringan internal
3. murah



Gambar 3.9 Flowchart Konfigurasi VPN

VPN SERVER

Setting Network :

- IPv4 Address : Private Static (192.168.2.125)
- IPv4 Subnet Mask : 255.255.255.255.0
- IPv4 Default Gateway : 192.168.2.1

Setting Database VPN client

UserName	Password
VPN01	VPN01
VPN02	VPN02
VPN03	VPN03

Tabel 3.10 *UserName* dan *Password* VPN *Client*

1.11.4. Konfigurasi pada sisi client

Perancangan pada sisi *client* dengan menyiapkan PC agar mampu melakukan dan menerima panggilan. Tahap – tahap perancangan ini dapat dilakukan dengan instalasi *softphone* , kemudian mengaktifkan *softphone* untuk melakukan registrasi ke *server* VoIP. *Softphone* yang dapat digunakan adalah X-Lite, Eye-Beam, serta Wengophone. Pada PC yang memerlukan keamanan lebih untuk melakukan panggilan, dapat ditambahkan VPN *client*. Diagram Alir pada sisi *client* dapat dilihat pada Gambar 3.14.

Operating System : Windows/ Linux/ Apple

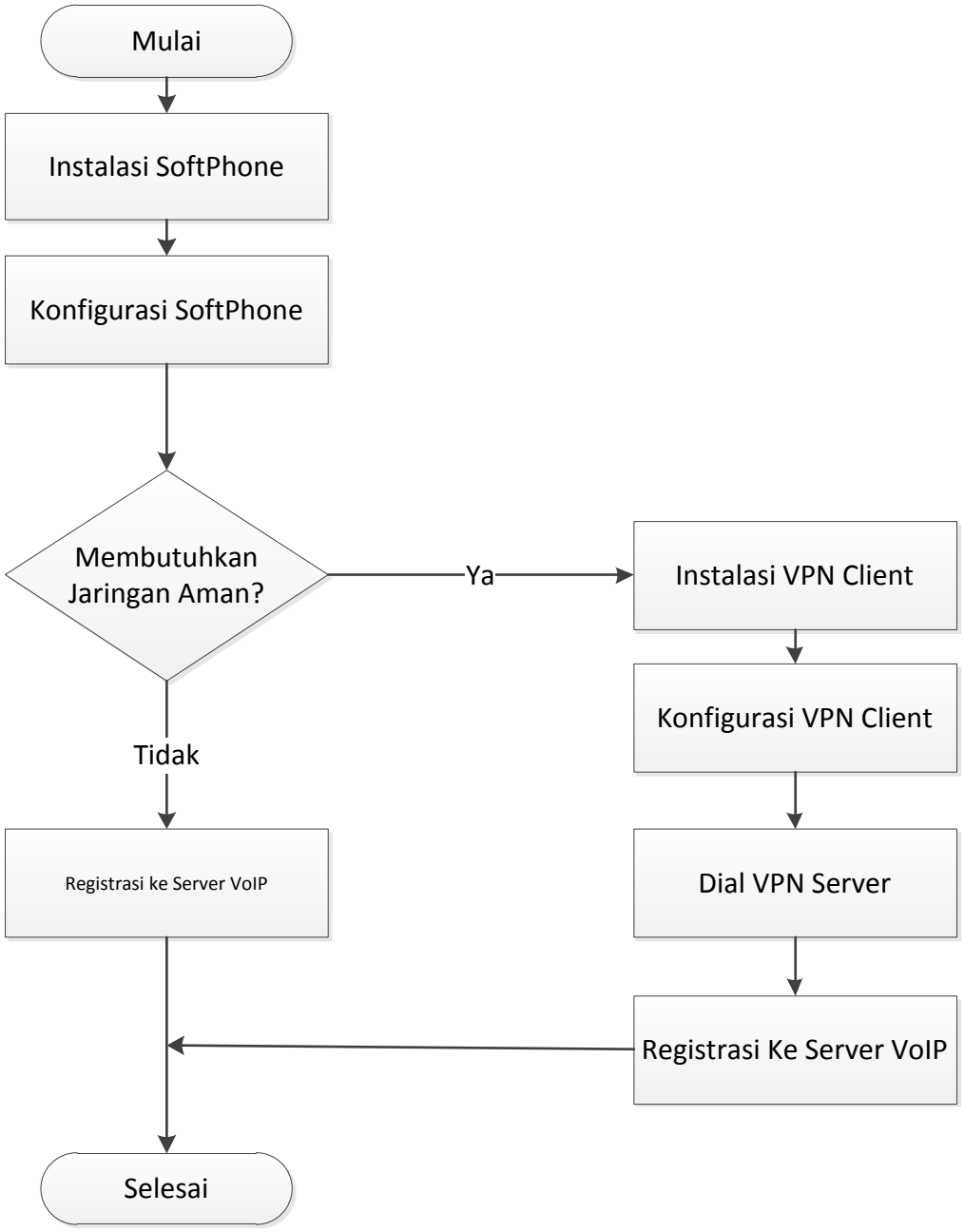
Setting Network :

VOIP Client PT. Neuronworks Indonesia:

- IPv4 Address 192.168.2.0/24 (DHCP – Private Dynamic)
- IPv4 Subnet Mask : 255.255.255.255.0
- IPv4 Default Gateway : 192.168.2.1

VOIP Client dan VPN client :

- IPv4 Address VPN client : 10.10.10.0/24 (DHCP – **Private static**)
- IPv4 Address Internet : Tergantung Provider (DHCP – Public dynamic)



Gambar 3.11 Flowchart Perancangan ada sisi VoIP client

1.12. Desain Sistem yang diusulkan

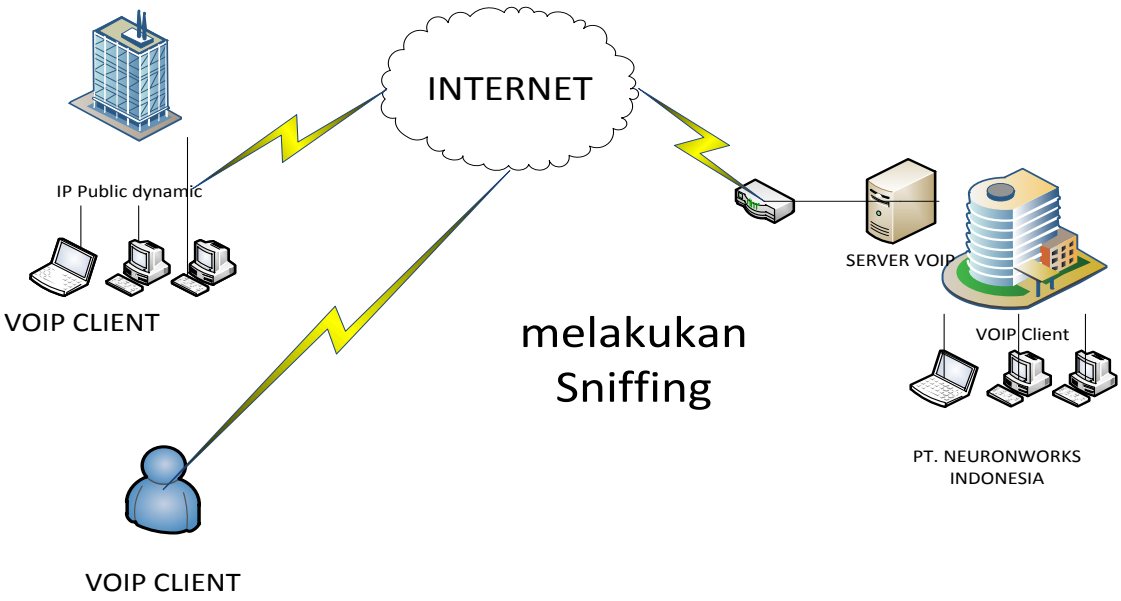
Rancang bangun sistem VoIP ini merupakan transportasi suatu pelewatan suara melalui jaringan komputer. Skenario VoIP ini terdiri dari tiga buah komponen utama yang saling berhubungan, yaitu VoIP server, VoIP Client, Voip Gateway, dan VPN server. Penggunaan VPN server , VoIP Gateway tergabung dalam satu perangkat dengan VoIP server.

VoIP *server* merupakan pusat penangan proses , registrasi dan panggilan VoIP *client*. VoIP *server* ini terdapat empat buah *client* SIP dengan menggunakan PC (*Personal Computer*) konvensional yang telah terinstall *softphone*.

VPN *server* merupakan *server* yang digunakan untuk pelayanan jalur komunikasi SIP yang lebih aman. Penggunaan VPN *server* ini secara fisik menjadi satu dengan VoIP *server*, hanya melakukan penambahan instalasi pada VoIP *server* agar mampu bekerja sebagai VPN *server*.

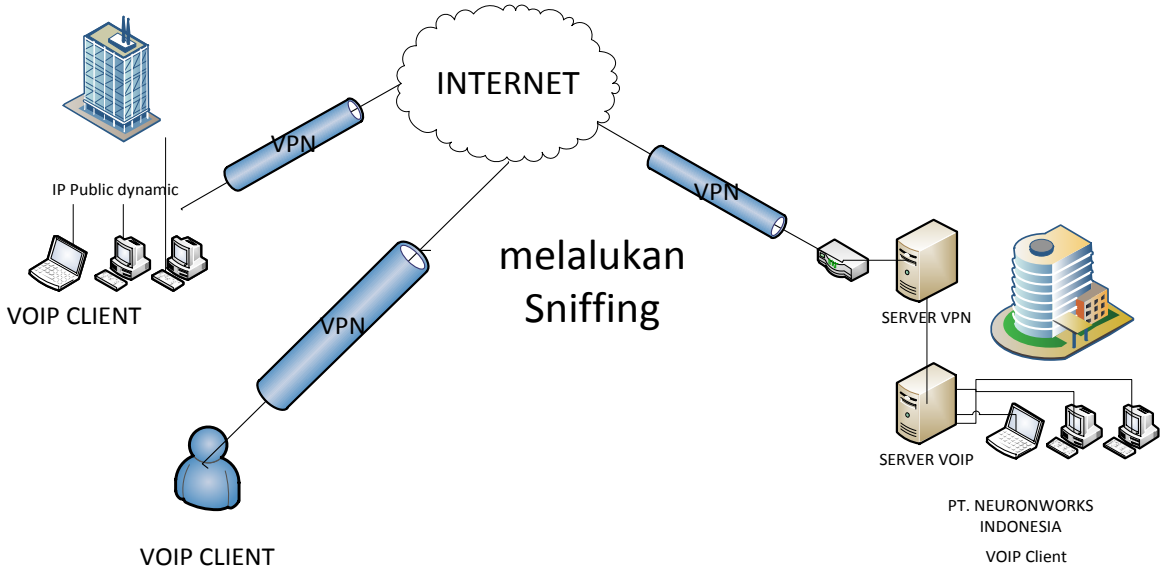
VoIP *client* disini adalah PC konvensional yang telah ditambahkan *softphone* agar mampu melakukan registrasi ke SIP *server* agar dapat melakukan panggilan terhadap VoIP *client* yang lainnya yang telah teregister ke SIP *server*.

SKENARIO 1

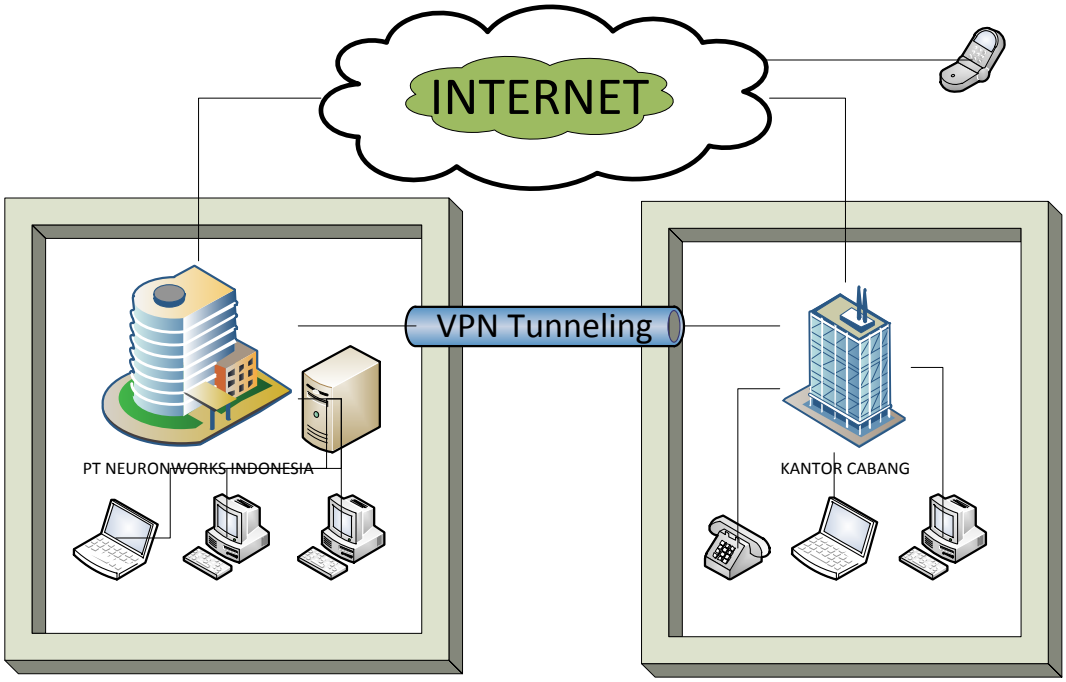


Gambar 3.12 Melakukan Komunikasi dengan VoIP tanpa VPN langsung ke server VoIP

Skenario 2



Gambar 3.13 Melakukan Komunikasi VoIP dengan VPN dengan perantara server VPN

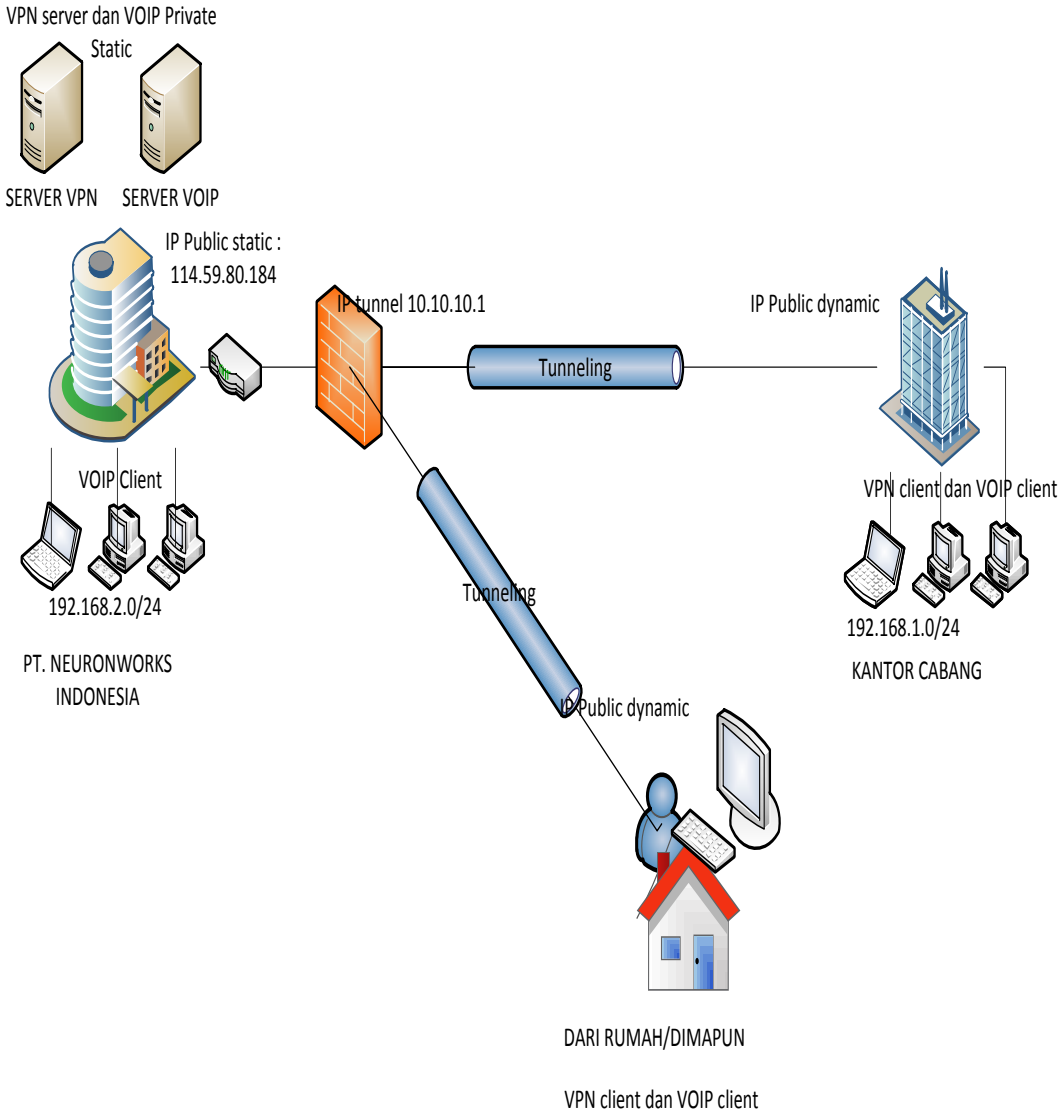


Gambar 3.14 Topologi VOIP Dengan keamanan VPN

Cara kerja client VoIP dengan VPN tunneling adalah

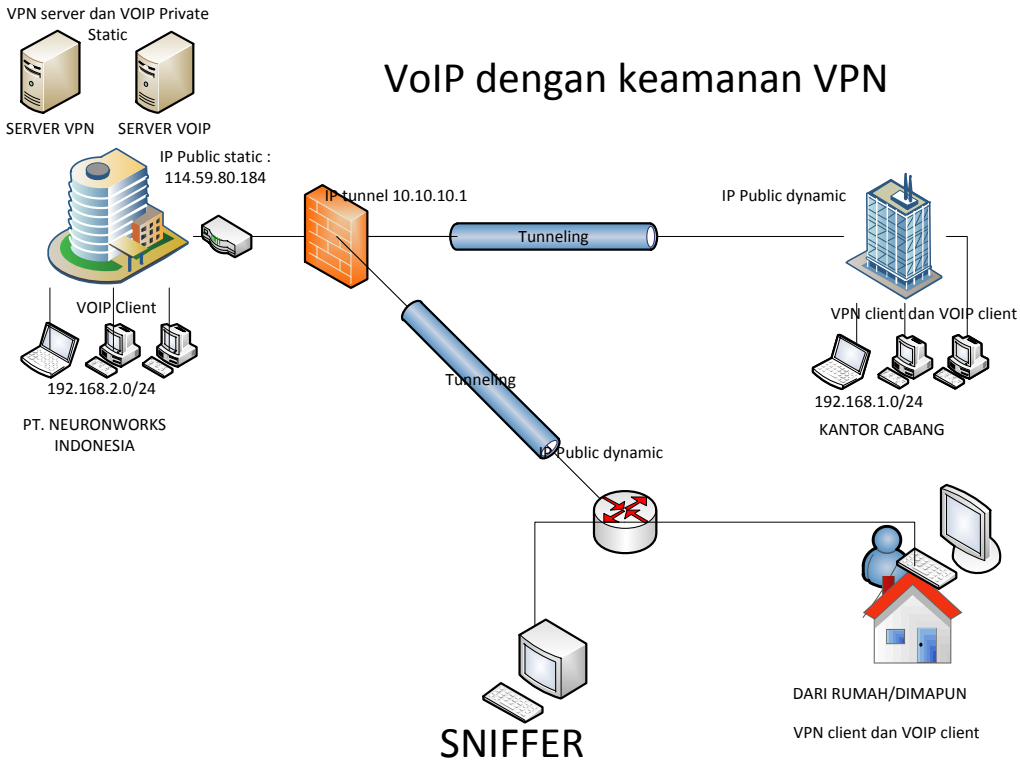
1. Client pada PT. Neuronwoks Indonesia melakukan autentifikasi terhadap Server Voip yang berada yang diberikan hak user untuk dapat dial kedalam server VoIP, setelah itu user Client siap untuk melakukan panggilan VoIP dengan client lain ataupun menerima panggilan dari client lainnya.
2. Client yang diluar server PT. Neuronworks Indonesia ataupun pada kantor cabang, hal pertama yang dilakukan adalah melakukan dial ataupun autentifikasi terhadap server VPN yang berada di PT. Neuronworks Indonesia dengan cara input alamat server IP Public STATIC yang ada pada ROUTER nya PT. Neuronwoks Indonesia. Setelah itu Router akan melakukan FORWARDING kedalam jaringan LAN yang ada di perusahaan tersebut

tepatnya adalah ke alamat IP Private STATIC yang telah di setting sebelumnya untuk dapat memberikan hak akses ke dalam jaringan local yang berada disekitarnya. Selah client VPN melakukan autentifikasi ke dalam VPN server maka VPN server akan memberikan alamat IP VPN serta memberikan jalur langsung terhadap jaringan yang ada didalam PT. Neuronworks Indonesia. Jalur tersebutlah yang disebut jaringan Tunneling sehingga paket yang nantinya akan di kirim akan di enkripsi dengan beberapa header yang ikut serta dalam pengiriman data tersebut. Setelah itu client VPN dapat dial kedalam VoIP SERVER dengan User ID dan Password yang telah diinputkan sebelumnya kedalam server VoIP. Setelah selesai Dial ke dalam maka komputer bekerja sebagai VoIP client dengan keamanan VPN dan dapat memalukan panggilan ataupun menerima panggilan dari client VoIP server lainnya tanpa harus takut adanya penyadapan terhadap pembicaraaan yang sedang berlangsung.



Gambar 3.15 VoIP dengan VPN Tunneling

Perancangan Snifer

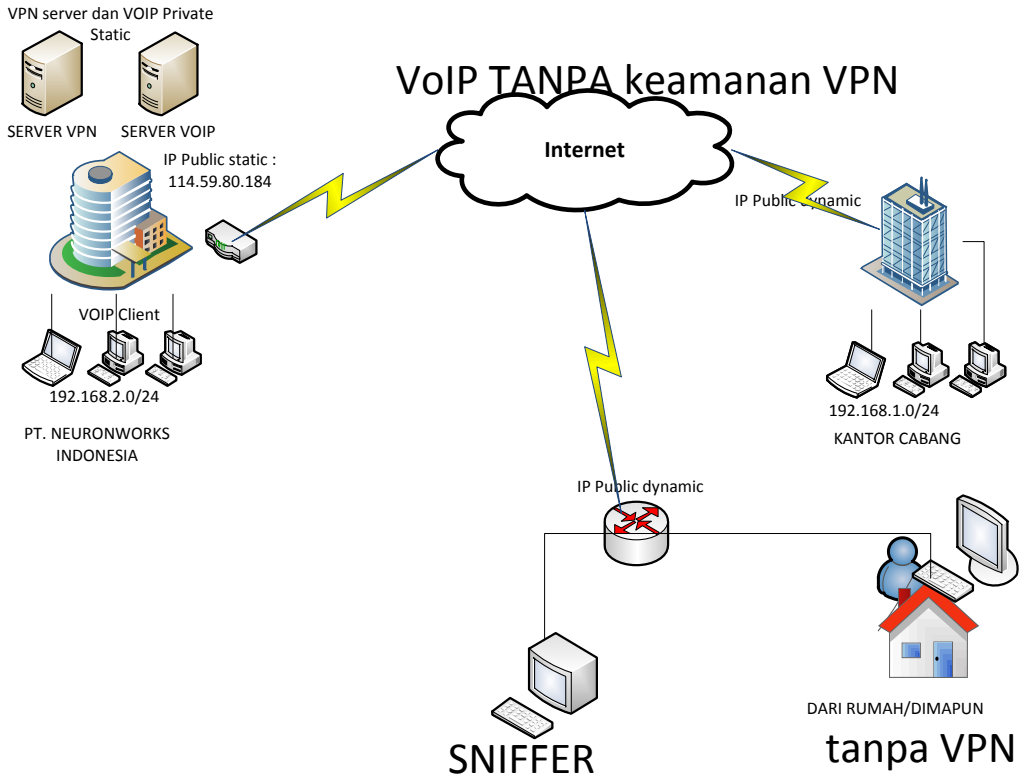


Gambar 3.16 Perancangan Proses Sniffing pada VoIP dengan VPN

Wireshark

Wireshark adalah program yang berfungsi untuk mengetahui kejadian yang terjadi pada saat kita melakukan interaksi pada suatu jaringan komputer. Wireshark merupakan salah satu *network analysis tool*, atau disebut juga dengan *protocol analysis tool* atau *packet sniffer*. Wireshark dapat digunakan untuk *troubleshooting* jaringan, analisis, pengembangan software dan protokol, serta untuk keperluan edukasi.

Wireshark mampu menangkap paket-paket data atau informasi yang berjalan dalam suatu jaringan yang dimonitor. Hampir semua jenis paket informasi dalam berbagai format protokol dapat ditangkap dan dianalisa.



Gambar 3.17 Perancangan Proses Sniffing pada VoIP tanpa VPN

Perancangan Skenario

Setelah semua yang diperlukan untuk membangun sistem VoIP selesai, maka ada beberapa skenario yang akan dilakukan untuk melakukan pengujian terhadap celah keamanan dan performansi dari jaringan VoIP over VPN.

1. Perancangan VoIP tanpa Keamanan VPN

Skenario Pertama Pada skenario pertama dibangun sebuah panggilan antara client VoIP 1 ke Client VoIP 2 menggunakan softphone Xlite. Untuk codec digunakan beberapa codec sebagai perbandingan yaitu codec G.711 dengan bitrate 64 Kbps codec G729 yang memiliki bitrate 8 Kbps codec GSM yang memiliki bit rate 13 Kbps. *Bandwith* jaringan dibatasi menjadi tiga buah *rate* yang berbeda. 256, 128, 96, 64, dan 32 Kbps dengan utilitas 20%. Ketika client 1 dan 2 telah berkomunikasi maka pembicaraan yang terjadi akan di *capture* (tapping), dan dianalisis data yang ada di dalamnya dan di *play* (di mainkan ulang) dengan software untuk mengetahui apakah suara dari pembicara di client 1 dan client 2 dapat disadap. Setelah itu akan data yang ditangkap juga dianalisis performansinya di dalam jaringan. Berapa QoS dari sistem tersebut. Hal ini dapat diketahui dengan menganalisa *delay, jitter, paket loss* dan *troughput*. Setelah didapatkan data tersebut, akan dianalisa manakah bagaimana tingkat keamanan dan performansi dari codec tersebut.

2. Perancangan VoIP dengan Keamanan VPN

Pada skenario kedua dibangun jaringan VoIP over VPN. VPN digunakan untuk mengamankan jaringan *backbone* dari router 1 ke router 2. kunci *enkripsi* yang digunakan adalah 3DES 128 bit. Untuk kali client akan kembali berkomunikasi dan data yang lewat akan disadap menggunakan ethereal dan di *play* untuk didengar hasilnya. Setelah itu dianalisa besar paket dan isi paket yang di*capture*. Apakah isi paket tersebut terdapat perbedaan dengan paket yang ditangkap pada skenario pertama. Selain itu dihitung pula QoS dari sistem tersebut. Seberapa baik performansi

yang dihasilkan dari jaringan VoIP over VPN untuk menghasilkan QoS yang sebaik mungkin.