PERANCANGAN *VOICE OVER INTERNET PROTOCOL* (VoIP) MENGGUNAKAN *VIRTUAL PRIVATE NETWORK* (VPN) PADA PT CARE TECHNOLOGIES

Rudiansyah[1] , Herlawati[2], Eka Puspita Sari [3]

[1,2] Jurusan Teknik Informatika, STMIK Nusa Mandiri Jakarta. Jl. Kramat Raya No. 25, Jakarta Pusat, 10420, Indonesia, [1]rudi.array@gmail.com, [2]herlawati@nusamandiri.ac.id

3 Jurusan Manajemen Informatika, AMIK BSI Jakarta Jl. Kramat Raya No. 18, Jakarta Pusat, 10420, Indonesia. eka.eps@bsi.ac.id

ABSTRACT

Current technological developments to make a change from several sides. As in telecommunications are now developed with incoming. One of them is VoIP. VoIP is a technology capable of passing voice in packet form. With this VoIP technology one can make telephone communication melaluit internet. To use this VoIP one can use the handphones are connected to lapop or PC. However, the use of VoIP has a disadvantage that can be done tapping at the time the conversation is being conducted. VPN (Virtual Private Network) is a way of creating a private network are using a public network / Internet. With a VPN network, a user as if connected by point to point that they are not. Consists of VPN-management protocols that can perform encryption and tunneling as PPTP (Point to Point Protocol), L2TP (Layer 2 Tunneling Protocol) and IPSec (Internet Protocol Security). With the capabilities of the VPN is expected that the wiretapping of conversations being conducted by the user can be prevented.

Keywords: *VoIP, VPN, Protocol*

I. Pendahuluan

VoIP (*Voice Over Internet Protocol*) atau yang disebut juga *IP Telephony* adalah teknologi yang mampu melewatkan traffic suara yang berbentuk paket melalui internet. Namun karena *Voip* ini menggunakan teknologi *IP* yang berhubungan dengan internet maka harus pula memperhitungkan *bandwidth*.

Pada jaringan komputer, keamanan jaringan juga merupakan hal yang sanagat penting. Menurut Pungkasanti (2010) "telah banyak terjadi kasus penyusupan data antara *client* dan *server* yang dituju sehingga penyerang dapat mengetahui informasi-informasi yang seharusnya rahasia". " Untuk menghindari serangan serupa maka dibuatlah sebuah sistem jaringan virtual dengan membuat sebuah tunnel atau terowongan untuk melewati proses transmisi data ini. Salah satu contohnya adalah dengan menggunakan *Virtual Private Network (VPN)"* (Pungkasanti, 2010). *VPN* ini tidak hanya digunakan untuk jaringan komputer biasa namun juga dapat digunakan pada *VoIP*, yang akan berguna untuk melindungi penyadapan terhadap paket suara.

Maksud yang ingin disampaikan oleh penulis adalah :

1. Berdasarkan latar belakang tersebut penulis mencoba menganalisa implementasi dan keamanan *Voip* pada PT Care Technologies.
2. Mengetahui cara kerja *softswitch* yang digunakan untuk *Voip*.
3. Mengetahui Topologi yang digunakan untuk *Voip*.

Ruang lingkup dari analisa ini yaitu bagaimana keamanan dari jaringan *VoIP*, *Hardware-Softw*are yang digunakan dalam *VoIP*, Arsitektur jaringan yang digunakan untuk *VoIP*, dan Penggunaan *VPN* pada *VoIP*.

II. Kajian Literatur

Jaringan komputer menurut Ramadhan (2006) adalah "suatu sistem yang menghubungkan komputer menggunakan suatu teknologi transmisi data". Secara lebih sederhana, jaringan komputer dapat diartikan sebagai sekumpulan komputer beserta mekanisme dan prosedurnya yang saling terhubung dan berkomunikasi. Komunikasi yang dilakukan oleh komputer tersebut dapat berupa transfer berbagai data, instruksi, dan informasi dari satu komputer ke komputer lain.

A. LAN

Rachman dan Yugianto (2008) mengemukakan *LAN* (*Local Area Network*) adalah "jaringan komunikasi data berkeceptan

tinggi dengan *fault-tolerant*, dengan cakupan area secara geografis relative lebih kecil (lokal)". Secara umum *LAN* biasanya menghubungkan beberapa *work station*, *personal computer*, printer dan peralatan lainnya.

B. WAN

WAN (*Wide Area Network*) adalah Jaringan komunikasi data yang mencakup area geografis yang relative luas menggunakan fasilitas transmisi yang disediakan "*common carriers*" seperti Telkom (Rachman dan Yugianto,2008).

C. VoIP

Menurut Munadi (2011) *voip* adalah teknologi pengiriman *voice* (dimungkinkan juga untuk tipe data multimedia yang lain) secara real time antara dua atau lebih user/partisipan dengan melewati jaringan yang menggunakan protocol-protokol internet, dan melakukan pertukaran informasi yang dibutuhkan untuk mengontrol pengiriman *voice* tersebut.

D. SIP

SIP (*Session Initiation Protocol*) adalah "protocol kontrol pada layer aplikasi untuk membangun, memodifikasi dan mengakihiri sebuah session dengan dua atau lebih partisipan" (Munadi, 2011). Cara kerja *SIP* sama dengan cara kerja protocol *HTTP* yaitu dengan metode *client-server* atau *request-response*.

E. Standar H.323

VoIP dapat berkomunikasi dengan system lain yang beroperasi pada jaringan *packet-swicth*. Untuk dapat berkomunikasi dibutuhkan suatu standar system komunikasi yang kompatibel satu sama lain. Salah satu standar komunikasi pada *VoIP* menurut rekomendasi *ITU-T* adalah H.323. Standar H.323 terdiri dari komponen, protocol dan prosedur yang menyediakan komunikasi multimedia melalui jaringan *packet-based*. Bentuk jaringan *packet-based* yang dapat dilalui antara lain jaringan internet, *Internet Packet Exchange (IPX)-based*, *Local Area Network* (*LAN)*, dan *Wide Area Network (WAN)*. H.323 dapat digunakan untuk layanan-layanan multimedia seperti komunikasi suara (*IP Telephony*), komunikasi video dengan suara (*video telephony*), dan gabungan suara, video dan data.

Standar H.323 terdiri dari 4 komponen fisik yang digunakan saat menghubungkan komunikasi multimedia point-to-point dan point-to-multipoint pada beberapa macam jaringan menurut Rendy (2011) yaitu:

1. Terminal
   Digunakan untuk komunikasi multimedia *realtime* dua arah. Terminal H.323 dapat berupa *personal computer* (*PC*) atau alat lain yang berdiri sendiri yang dapat menjalankan aplikai multimedia.
2. *Gateway*
   Sebuah gateway dapat memberikan banyak layanan, salah satunya yang paling penting adalah sebagai interface antara jaringan-jaringan lain, seperti jaringan PSTN dengan jaringan IP. *Gateway* dapat mendukung untuk komunikasi *real-time*, dan dapat melakukan komunikasi dua arah antar terminal H.323 pada jaringan IP dan terminal pada jaringan berbasis *Switched* atau dengan *Gateway* H.323 lain. *Gateway* pada *system* H.323 ini berfungsi sebagai translator.
3. *Gatekeeper*
   Gatekeeper merupakan *entity vital system* H.323 yang berfungsi untuk mengatur *system* H.323. Bertindak sebagai central point untuk semua call dalam zone H.323 dan menyediakan layanan pengontrol panggilan untuk me-*register endpoint*.
4. *Multipoint Control Unit* (MCU)
   Endpoint pada jaringan, yang menyediakan kemampuan untuk berpartisipasi melakukan multipoint conference antara tiga atau lebih terminal / Gateway. MCU terdiri dari :
   a. *MC* (*Multipoint Controler*)
      Yang menanngani persinyalan dan kontrol *message* yang diperlukan untuk *set-up* dan mengatur *conference*. *MC* juga menentukan kapabilitas terminal dengan menggunakan H.323 tetapi tidak melakukan *multiplexing* audio, video, dan data.
   b. *MP (Multipoint Processor)*
      Yang menerima *streams* dari *endpoint*, mereplesikannya, dan mem-*forward streams* tersebut ke *endpoint* yang berpartisipasi dalam *conference* tersebut. *Multiplexing stream* media ditangani oleh MP dbawah kendalai MC.

F. Proxy Server

Proxy server ini sama dengan *proxy-proxy server* pada umumnya, yang membedakan adalah kegunaan dari *server* yaitu untuk kebutuhan *VoIP*. *Proxy server* ini menggunakan *softwitch*. Dengan menggunakan

softswitch ini sebuah mesin akan menjadi sebuah *PBX* yang mengatur alur komunikasi. Contoh softswitch yang sering digunakan adalah Asterisk, OpenSER, Briker, TrixboxCE, dan YATE.

G. VPN

VPN menurut Wijaya (2011) adalah fasilitas yang memungkinkan koneksi jarak jauh (*remote accses*) yang aman dengan menggunakan jaringan internet untuk akses ke *LAN* Kantor". Menurut sakiwan dalam (Putranto, 2009) "*VPN* merupakan jaringan *public* yang menekankan pada keamanan data dan akses global melalui internet". Hubungan ini dibangun melalui suatu *tunnel* (terowongan) *v*irtual antara 2 (dua) *node*. Dengan menggunakan jaringan publik, *user* dapat bergabung dalam jaringan local, untuk mendapatkan hak dan pengaturan yang sama ketika user berada di kantor.

Pada umumnya jaringan *VPN* dikelompokan menjadi 2 yaitu *remote accses VPN* dan *site to site*.

1. *Remote accses* adalah *virtual private dial-up network* (*VPDN*) yang menghubungkan antara pengguna mobile dengan jaringan *Local Area Network (LAN)*. Jenis ini dapat digunakan oleh perusahaan yang terhubung ke jaringan khusus perusahaannya dari beberapa lokasi yang jauh (*remote*) dari perusahaanya. Biasanya digunakan oleh instansi pemerintah maupun swasta yang ingin membuat *VPN*, tipe ini akan bekerjasama dengan *enterprise service provider (ESP)*. *ESP* akan memberikan *network access server* (*NAS*) bagi perusahaan tersebut.
2. *Site to site VPN* yaitu suatu jaringan *VPN* yang menghubungkan 2 buah kantor atau lebih yang letaknya berjauhan.

Teknologi VPN menyediakan tiga fungsi utama untuk penggunaannya. Ketiga fungsi utama tersebut antara lain sebagai berikut (Ardiyansyah, 2008) :

a. *Confidentially* (kerahasiaan)
   Dengan digunakannya jaringan public yang rawan pencurian data, maka teknologi VPN menggunakan system kerja dengan cara mengenkripsi semua data yang lewat melaluinya. Dengan teknologi enkripsi 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 system enkripsi ini, tidak ada satupun orang yang dapat mengakses dan membaca isi jaringan data dengan mudah.
b. *Data Integrity (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.
c. *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.
d. *Non-repudiation*
   Yaitu mencegah dua perusahaan dari menyangkal bahwa mereka telah mengirim atau menerima sebuah file mengakomodasi perubahan
e. *Kendali akses*
   Menentukan siapa yang diberikan akses kesebuah sistem atau jaringan, sebagaimana informasi apa dan seberapa banyak seseorang dapat menerima.

H. TCP/IP

TCP atau "*Tranmision Control Protocol*" adalah "suatu *protocol* atau perantara yang dapat mentransmisikan data per segmen, artinya paket data dipecah dalam jumlah yang sesuai dengan besaran paket, kemudian dikirim satu persatu hingga selesai" (Rachman dan Yugianto, 2008). Selain dari itu *TCP* bertugas menangani pengiriman "message" ukuran sembarang yang handal dan juga mendefinisikan suatu mekanisme pengiriman dari semua jenis data pada suatu jaringan.

Sedangkan "*Internet Protocol*" (*IP*) adalah "*Protocol* yang mengatur Routing dari pentransmisian melewati jaringan antara pengirim dan penerima, termasuk juga isu yang terkait dengan pengalamatan jaringan dan computer, sehingga dapat dikatakan bahwa *IP* (*Internet Protocol*) merupakan perantara komunikasi antar komputer dengan menggunakan "*IP-Address*" sebagai suatu

identitas dari jaringan maupun komputer" (Rachman dan Yugianto, 2008).

Pengiriman data akan dikemas dalam pkaet dengan label berupa "*IP-Address*" si pengirim dan si penerima paket data. Apabila si penerima melihat pengiriman paket tersebut dengan identitas (*IP-Address*), maka paket data tersebut akan diambil dan disalurkan ke *TCP* melalui *port*, dimana aplikasi menunggu. Sehingga dapat disimpulkan bahwa *TCP* adalah Protocol level tertinggi yang disebut sebagai protocol aplikasi. Layer ini bertugas untuk komunikasi antar aplikasi *user-visible interface* pada *TCP/IP*.

I. OSI Layer

Untuk menyelenggarakan komunikasi berbagai macam vendor komputer diperlukan sebuah aturan baku yang standar dan disetujui berbagai pihak. Seperti halnya dua orang yang berlainan bangsa, maka untuk berkomunukasi memerlukan penerjemah/interpreter atau satu bahasa yang dimengerti kedua belah pihak. Dalam dunia komputer dan telekomunikasi interpreter identik dengan Protokol. Untuk itu maka badan dunia yang menangani masalah standarisasi ISO (*Internasional Standarization Organization*) membuat aturan baku yang dikenal dengan nama model referensi OSI (*Open System Interconnection*). Dengan demikian diharapkan vendor perangkat telekomunikasi haruslah berpedoman dengan model referensi ini dalam mengembangkan protokolnya.

Model OSI tidak membahas secara detail cara kerja dari lapisan-lapisan OSI, melainkan hanya memberikan suatu konsep dalam menentukan proses apa yang harus terjadi, dan protokol-protokol apa yang dipakai disuatu lapisan tertentu.

1. Lapisan Application

Lapisan ini merupakan lapisan ke-7 model OSI, bertugas memberikan sarana-sarana pelayanan pada jaringan komputer untuk aplikasi-aplikasi pemakai dan mengadakan komunikasi dari program ke program. Jika akan mencari suatu file dari file server untuk digunakan sebagai aplikasi pengolah kata, maka proses ini bekerja melalui aplikasi ini. Demikian pula pada saat mengirim email, browse ke internet dan bulletin board, membuka telnet session atau menjalankan FTP, semua proses tersebut terjadi dilapisan ini.

2. Lapisan *Presentation*

Lapisan ini merupakan ke-6 model OSI, bertanggung jawab untuk presentasi grafik dan visual image. Lapisan ini memberikan sarana-sarana pelayanan untuk konversi, format, dan enkripsi data-data. Lapisan *presentation* bekerja dengan file format seperti *ASCII, EBCDIC, JPEG, MPEG, TIFF, PICT, MIDI*, dan *Quick Time*.

3. Lapisan *Session*

Lapisan ini membuka, mengatur, dan menutup suatu session antara aplikasi-aplikasi. Protokol yang berfungsi pada lapisan ini antara lain *NFS, NETBEUI, RPC, SQL, X Windows System, Apple Talk Session Protocol (ASP), Digital Architechture Session Control Program (DNASCP).*

4. Lapisan *Transport*

Lapisan transport bertanggung jawab atas keutuhan dari transmisi data. Lapisan ini sangat penting karena bertugas memisahkan lapisan tingkat atas dengan tingkat bawah. Pada lapisan ini diubah menjadi segmen atau data stream.

5. Lapisan *Network*

Lapisan *Network* ini berfungsi meneruskan paket-paket dari satu node lain dalam jaringan komputer. Lapisan ini juga berguna untuk pengaturan pemberian alamat untuk peralatan jaringan dan memilih jalur yang terbaik dalam meneruskan paket dijaringan. Pada lapisan ini segmen-segmen diubah menjadi paket-paket dengan menambah informasi mengenai alamat logika atau *IP Address* yang dituju, dan alamat asal dari paket. Router bekerja pada lapisan ini.

6. Lapisan *Data Link*

Lapisan ini mengatur topologi jaringan, *error notification* dan *flow control*. *Switch* dan *bridge* bekerja di lapisan *data link* ini. Lapisan ini mengolah paket dari lapisan diatasnya menjadi frame, dengan menambahkan informasi mengenai alamat *hardware* atau *MAC Address* yang dituju serta alamat asal.

7. Lapisan *Phisycal*

Lapisan ini bertanggung jawab untuk megatifkan dan mengatur *physical interface* jaringan komputer. Pada lapisan ini hubungan antara *interface-interface* dari perangkat keras diatur seperti hubungan DTE dan DCE. *Interface-interface* yang didefinisikan pada lapisan ini antara lain 10BaseT, 100BaseTX, V.35, X.21, dan *High Speed Serial Interface (HSSI).*

Peralatan Pendukung yang digunakan yaitu:

A. Topologi Jaringan

"Denah bagaimana cara menghubungkan komputer satu dengan lain disebut topologi jaringan" (Wijaya, 2003). Bentuk topologi jaringan dalam LAN secara umum terbagi atas 4 (empat) macam menurut Rachman dan Yugianto yaitu :

1. Topologi bus
2. Topologi star
3. Topologi Ring

B. *Hub*

Menurut Rachman dan Yugianto (2008) Hub merupakan "peralatan layer fisik yang menghubungkan peralatan melalui *"dedicated cable"* ". Interkoneksi elektrik tercapai dalam Hub. Hub digunakan untuk menciptakan topologi "*star*" secara fisik, topologi "*bus*" secara logik.

C. Ethernet Card

Ehternet bekerja berdasarkan *broadcast network*, di mana setiap node menerima transmisi data yang dikirim oleh sebuah node. Menggunakan metode CSMA/CD (*carrier sense multiple accses/collision detection*) *baseband*. Setiap *PC* dihubungkan ke *LAN* dengan perantara *Network Interface Card* (dalam hal ini *Ehternet Card*) yang cocok untuk digunakan dengan kabel *coax, twisted pair,* atau *fiber optic*.

D. Twisted Pair

Twisted Pair Cable ini ada dua jenis yaitu *Shielded* dan *Unshielded*. *Shielded* adalah jenis kabel yang memiliki selubung pembungkus sedangkan *unshielded* tidak mempunyai selubung pembungkus. *Twisted-pair* (dikenal juga sebagai 10Base T) cocok untuk jaringan kecil, sedang maupun besar yang membutuhkan fleksibilitas dan kapasitas untuk berkembang sesuai dengan pertumbuhan pemakai *network*. Ada dua macam tipe pengkabelan untuk kabel *UTP* yaitu *Stright-through* dan *Crossed*. Tipe *Stright-through* digunakan untuk menghubungkan komputer ke *hub / switch* sedangkan kabel *Crossed* digunakan untuk menghubungkan *Hub* ke *Hub* atau *Switch* ke *Switch*.

E. Coaxial Cable

Media ini paling banyak digunakan sebagai media *LAN* meskipun lebih mahal dan lebih sukar penggunaannya dibandingkan *twisted pair*. Kabel ini memiliki *bandwith* yang lebar, sehingga bsia digunakan untuk komunikasi *broadband*. Thick Coaxial biasa digunakan untuk kabel *backbone* pada jaringan instalasi *Ethernet* antar gedung.

Thin coax (dikenal juga sebagai 10 base2) adalah cocok untuk *network* rumah atau kantor, dengan dua atau tiga komputer. Kabel ini mirip seperti kabel antenna tv, harganya tidak terlalu mahal dan mudah pemasangannya. Kabel ini pemasangannya menggunakan konektor BNC. Pada jaringan jenis ini untuk menyambung ke masing-masing komputer menggunakan konektor T (*T-Conncetor*) dan setiap ujungnya menggunakan terminator atau penutup (50 ohm) jika tidak menggunakan hub.

F. Fiber Optik

Jaringan yang menggunakan *F/O* ini memang sangat jarang digunakan. Biasanya hanya perusahaan besar saja yang menggunakan jaringan dengan media *F/O*. Karena harganya relative mahal dan proses pemasangannya lebih sulit. Namun demikian, jaringan yang menggunakan *F/O* ini dari segi kehandalan dan kecepatan tidak diragukan lagi. Kecepatan pengiriman data dengan media *F/O* ini lebih dari 100 *Mbps* dan bebas dari pengaruh lingkungan (*noise*).

III. Metode Penelitian

Analisis Penelitian yang dilakukan terdiri dari:

a. Analisa kebutuhan

Dalam analisa kebutuhan ini penulis mencoba menyiapkan analisa kebutuhan seperti:

1. Jurnal
2. *Software* yang digunakan seperti *wireshark, packet tracer,*dan *3CX Phone*
3. Hardware yang dibutuhkan seperti *HeadPhone*

b. Desain

Dalam metode ini penulis membuat analisa desain jaringan yang digunakan untuk penerapan *VPN*.

c. Testing

Penulis melakukan testing yang digunakan sebagai bahan dalam penulisan skripsi ini. Testing yang dilakukan adalah bagaimana perbandingan dari penerapan *Voip* dengan *VPN* dan tanpa *VPN*.

d. Impementasi

Penulis mencoba melakukan implementasi sebagain bahan percobaan penerapan jaringan *VPN* pada *VoIP*.

Metode pengumpulan data yang digunakan sebagai berikut:

1. Observasi

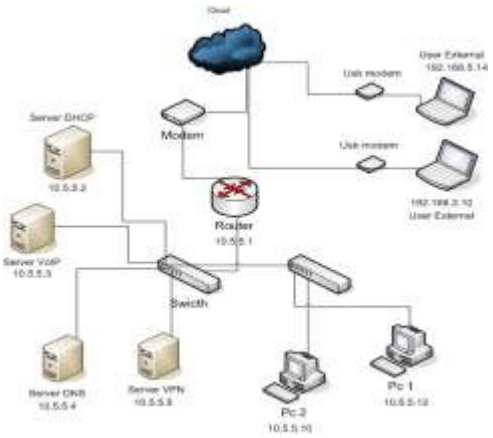
Penulis melakukan Observasi yang digunakan sebagai bahan dalam penulisan skripsi ini.

2. **Wawancara**
   Penulis mengadakan wawancara langsung kepada pihak-pihak terkait yang berhubungan dengan sistem jaringan atau IT jaringan pada PT Care Technologies.
3. **Studi Pustaka**
   Metode pengumpulan data dengan cara mempelajari beberapa buku, sarana perpustakaan, catatan-catatan kuliah dan mengunjungi situs-situs yang yang diajukan sebagai bahan analisa penulis.

IV. Pembahasan

1. Rancangan Jaringan Usulan

Rrancangan gambar jaringan usulan dari penulis adalah :



Gambar 1. Rancangan Jaringan Usulan
Sumber : Penulis dan IT PT Care Technologies

2. Rancangan Layer

VPN (Virtual Private Network) Menurut Prasetyo (2008) adalah "koneksi secara logical yang menghubungkan dua node melalui *public network*". Koneksi logical tersebut bisa merupakan layer 2 ataupun layer 3 dalam basis *OSI Layer*. *ATM*, dan *Frame Relay* adalah contoh *Layer* 2 *VPN*. *GRE, L2TP, MPLS,* dan *IPSec* adalah contoh dari *layer* 3 *VPN*. Sedangkan untuk *VoIP* berjalan pada layer *Transport* dan layer *Network*. Maka dari itu yang digunakan oleh penulis dalam pembuatan skirpsi ini adalah 2 Layer yaitu Layer *Transport* dan Layer *Network.*

1) Layer Transport

Pada lapisan ini digunakan untuk membuat dan menjaga hubungan komunikasi antara dua peralatan komputer, serta memberikan garansi bahwa data yang dikirim akan sampai ke tujuan dengan baik. Protokol yang berkerja pada lapisan ini adalah *TCP* , *UDP* dan *SPX*.

2) Layer Network

Lapisan ini berfungsi meneruskan paket-paket dari satu node ke node yang lain dalam jaringan komputer. Dalam meneruskan paket ini digunakan alamat dan alamat ini yang sering disebut *IP Address*. Data yang dikirimkan dalam lapisan ini dibetuk kedalam paket yang memuat informasi mengenai alamat asal dan alamat tujuan. Dengan bantuan *IP Address* ini paket dapat dikirimkan pada jaringan yang jauh dan berbeda dengan bantuan peralatan yaitu Router.

3. Rancangan Keamanan Jaringan

Rancangan sistem keamanan jaringan dari skema jaringan adalah dengan menggunakan *VPN (Virtual Private Network)*. Karena jaringan *VPN* ini dapat melakukan enkripsi data sehingga data yang dikirimkan lebih aman dan dengan menggunakan jaringan *VPN* ini penyadapan pada saat user melakukan komunikasi melalui *VoIP* tidak dapat dilakukan.

"Mengapa VPN aman,karena system keamanan di VPN menggunakan beberapa lapisan…." menurut Setyawan, et al (2004). Adapun metode keamanan VPN diantaranya menurut Setyawan, et al (2004) yaitu :

1. Metode tunneling (terowongan), membuat terowongan virtual diatas jaringan publik menggunakan protocol seperti *Point to Point Protocol* (PPTP), *Layer 2 Tunneling Protocol* (L2TP), *Generic Routing Encapsulution* (GRE) atau *IPSec*. PPTP dan L2TP adalah layer 2 tunneling protocol. Keduanya melakukan pengbungkusan payload pada frame *Point to Point Protocol* (PPP) untuk dilewatkan pada jaringan, IPSec berada di layer 3 yang menggunakan packet, yang akan melakukan pembungkusan IP header sebelum dikirim jaringan.
2. Metode Enkripsi untuk Encapsulation (membungkus) paket data yang lewat di dalam tunneling, dimana data akan dienkripsi pada saat dilewatkan. Data disini akan dirubah dengan metode algoritma cripthography tertentu seperti DES, 3DES, atau AES.
3. Metode Otentikasi User, karena banyak user yang akan mengakses dari banyak titik maka digunakan beberapa metode protocol otentikasi user tertentu, seperti Remote Accses Dial In User Service (RADIUS) dan Digital Certificate.

Server *VPN* dapat dibuat dari router atau server terpisah seperti pc mikrotik, *windows*

server sampai *windows seven*. Untuk konfigurasi *VPN* pada *windows server 2008* adalah sebagai berikut :

1. Lakukan login ke server
2. Lalu klik start→ administrative tools → server manager
3. Pada windos Server Manager, pada bagian sebelah kanan lakukan scroll kebawah hingga menemukan Role Summary dan klik Add Roles.
4. Lalu pada window Add Roles Wizard, pilih Server Roles dan pada bagian Roles berikan checklist "Network Policy And Access Service" lalu next
5. Kemudian klik next kembali pada Window Network Policy and Access service
6. Kemudian pada bagian Select Role Service, pilih Remote Accsess Service lalu next
7. Pada bagian Confirm Instalation klik Install
8. Tunggu hingga proses selesai dan klik close
9. Klik start lalu pilih administrative tolls → Routing and Remote Access
10. Lalu pada bagian window Routing and Remote Access klik kanan pada "nama server" (local) dan klik Configure and Enable Routing and Remote Access lalu Next
11. Pada bagian Configuration pilih Remote Access (dial-up or VPN) dan klik next
12. Pada bagian remote access pilih VPN dan klik next
13. Pada bagian VPN Connection pilih alamat IP Public (IP dari ISP) lalu klik next
14. Pada bagian IP Address Assigment pilih from a spesicified range of address lalu klik next
15. Kemudian klik new untuk membuat range IP address dan jumlah member lalu klik ok dan pada bagian address range assignment klik next
16. Setelah itu pilih No, use Routing and Remote Access to authentication connection request dan klik next
17. Lalu klik finish dan klik ok pada kotak dialog DHCP Relay Agent

Setelah konfigurasi *VPN server* selesai dibuat, lalu buat user untuk mengakses *VPN* tersebut, adapun langkahnya adalah :

1. Login ke server
2. Lalu klik *start*→ *administrative tools* → *server manager*
3. Kemudian klik *configuration* → *local user and Groups*
4. Klik kanan pada bagian *users* → *new user*
5. Isi nama *user*, *password*, dan *description* kemudian beri *checklist* pada *password never expired*
6. Setelah selesai klik *create*

Setelah konfigurasi server *VPN* selesai dibuat maka, untuk sisi client dapat melakukan akses dengan melakukan konfigurasi sebagai berikut (konfigurasi *windows seven*) :

1. Klik menu *start* → *control panel*
2. Klik pada *Network and Sharing Center*
3. Klik *Set Up a new connection or network*
4. Klik *connect to a workplac*e lalu klik next
5. Pilih *use my Internet Connection* (VPN) lalu klik *next*
6. Kemudian pilih *I'll set up an Internet connection later*, klik *next*
7. Lalu masukan *IP server VPN* dan *Name*, kemudian klik *next*
8. Masukan Nama *user* dan *password* yang telah dibuat pada *server* lalu klik create
9. Tunggu hingga proses selesai maka akan terbentuk koneksi *VPN*
10. Klik *connect* pada koneksi *VPN* yang telah dibuat, dan proses koneksi pun akan terbuat

Setelah proses koneksi ke server telah selesai maka, langkah selanjutnya mencoba melakukan komunikasi melalui *VoIP*.

V. Penutup

Kesimpulan yang dapat diuraikan penulis adalah VPN (*Virtual Private Network*) ini memiliki keamanan yang mumpuni karena menggunakan metode *tunneling* (terowong) serta penerapan autentikasi dan untuk penggunaan pada *client* juga mudah dilakukan dengan menggunakan software atau fasilitas bawaan dari operating system seperti windows XP atau windows 7. Dan Penerapan *VoIP* pada PT Care Technologies membuat komunikasi antar devisi lebih mudah dan tidak harus beranjak dari tempat bekerja untuk menerima telepon.

Adapun saran yang dapat diuraikan penulis adalah :

1. Dalam keamanan tidak hanya digunakan *VPN* saja akan tetapi penggunaan *firewall* juga diperlukan untuk menjaga keamanan system.
2. Untuk *server VPN* tidak selalu harus dibuat terpisah karena disesuaikan dengan kondisi jaringan pada Perusahaan.
3. Diharapkan untuk penelitian selanjutnya tidak hanya menggunakan *PC* / laptop namun juga digunakan sebuah handphone untuk menggunakan fasilitas *VoIP* ini.

Daftar Pustaka

Agoes, Suhartati dan Adi Putranto. 2007. Simulasi Kualitas Layanan VoIP

Menggunakan Metode Antrian Paket CBQ Dengan Mekanisme Link Sharing. Jakarta: JETri. Vol. 7, No1 :41-64.

Jiwa P.,Agus Aan. Membangun Jaringan Komputer Berbasis Multipoint dengan Memanfaatkan Switch (studi kasus: laboratorium komputer SMK TI Bali Global). Diambil dari : http://ilmukomputer.org/2011/03/04/membangun-jaringan-komputer-berbasis-multipoint-dengan-memanfaatkan-switch/ (28 mei 2012).

Kurniawan, Davit. 2007. Metode IP Address Lanjutan VLSM. Diambil dari : http://www.ilmukomputer.org/wp-content/uploads/2007/12/metode-ip-address-lanjutan-vlsm.pdf (5 Juni 2012).

Nurhaetati,Sitti. 2008. Fungsi Hash. Makasar : Makalah keamanan komputer.

Munadi, Rendy. 2011. Teknik Switching. Bandung : Informatika Bandung.

Pungkasanti, Prind Triajeng. 2010. Jaringan VPN Untuk Sistem Informasi Koleksi Buku pada Perpustakaan Anggota Jasapusperti Jawa Tengah. Semarang : Jurnal Transformatika. Vol. 7, No2 :59-67.

Prastyo, Heri Bayu. 2008. IPSec VPN Pada Cisco Router. Diambil dari : http://ilmukomputer.org/wp-content/uploads/2008/05/herry-bayu-vpncisco1.pdf (5 Juni 2012)

Rachman, Oscar dan Gin gin Yugianto. 2008. TCP/IP Dalam Dunia Informatika dan Telekomunikasi. Bandung: Infromatika Bandung.

Sakiawan. 2010. Kajian Virtual Private Network (VPN) LAPAN dan Pemanfaatannya Dalam Mendukung Pengembang E-Government. Berita Dirgantara. Jakarta : Berita Dirgantara. Vol 2, No. 4 :145-152

Setiawan, Deris dan Dian Palupi Dini. 2009. Optimalisasi Interkoneksi Virtual Private Network (VPN) Dengan Menggunakan Hardware Based dan lix (Indonesia Exchange) sebagai Alternatif Jaringan Skala luas (WAN). Palembang : Jurnal Ilmiah generic. Vol 4, No 1:57-68

Sugeng, Winarno. 2008. Membangun Telepon Berbasis VOIP. Bandung : Informatika Bandung.

Suryani, Erma dan Nur Roy Honey. 2007. Implementasi Virtual Private Network – WAN Dalam Dunia Bisnis. Surabaya : JUTI. Vol 6, No. 1: 31-38

Tutang. 2002. Membangun Jaringan Sendiri LAN Local Area Network. Jakarta : Datakom.

Wijaya, Hendra. 2003. Belajar Sendiri Cisco Switch. Jakarta : PT Elex Media Komputindo.

Yuhefizar,2003. Tutorial Komputer dan Jaringan. Diambil dari : http://ilmukomputer.com (31 juli 2012).

Zimbra Indonesia. 2010. Instalasi Dan Konfigurasi DNS. Diambil dari : http://buaya.klas.or.id/zimbra/docs/InstalasiKonfigurasiDNS.pdf (1 Juni 2012).