BAB III

TINJAUAN PUSTAKA

3.1 Teori Pendukung

3.2 Pengertian Jaringan Komputer

Jaringan komputer adalah suatu himpunan interkoneksi sejumlah komputer *autonomous*. Dalam bahasa yang popular dapat dijelaskan bahwa jaringan komputer adalah kumpulan beberapa komputer (dan perangkat lain seperti *printer*, *hub*, dan sebagainya) yang saling terhubung satu sama lain melalui media perantara. Media perantara ini bisa berupa media kabel ataupun media tanpa kabel (nirkabel). Informasi berupa data akan mengalir dari satu komputer ke komputer lainnya atau dari satu komputer ke perangkat lain, sehingga masing-masing komputer yang terhubung tersebut bisa saling bertukar data atau berbagi perangkat keras.

(Sofana, 2008:1).

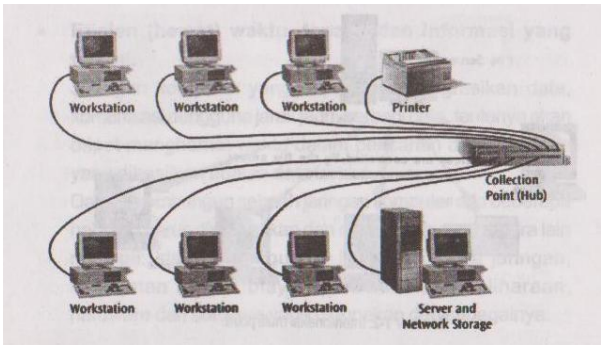
Disini penulis akan menjabarkan sedikit tentang jaringan komputer berdasarkan area, berdasarkan media dan berdasarkan fungsi , diantaranya adalah :

1. **Berdasarkan *Area***

   Berdasarkan skala atau area, jaringan komputer dapat dibagi menjadi 4 jenis, yaitu:

a. *Local Area Network* (LAN)

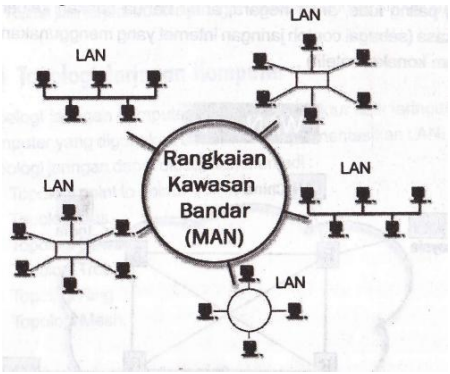
Menurut Sofana (2008:4), *Local Area Network* (LAN) adalah jaringan lokal yang dibuat pada area tertutup. Misalkan dalam satu gedung atau dalam satu ruangan. Kadangkala jaringan lokal disebut juga jaringan privat.



Gambar 3.1. *Local Area Network (*LAN*)*

b. *Metropolitan Area Network* (MAN)

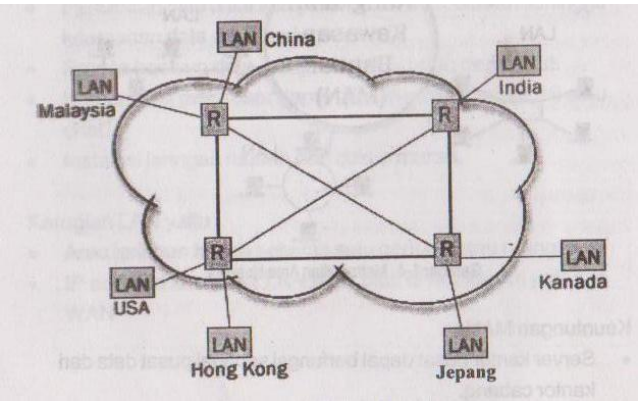
Menurut Sofana (2008:4), *Metropolitan Area Network* (MAN) menggunakan metode yang sama dengan LAN namun daerah cakupannya lebih luas, daerah cakupan MAN bisa satu RW, beberapa kantor yang berbeda dalam komplek yang sama, satu kota, bahkan satu provinsi.



Gambar 3.2. *Metropolitan Area Network* (MAN)

c. *Wide Area Network* (WAN)

Menurut Sofana (2008:4), *Wide Area Network* (WAN) Cakupannya lebih luas daripada MAN. Cakupan WAN meliputi satu kawasan, satu Negara, satu pulau, bahkan satu benua. Metode yang digunakan WAN hampir sama dengan LAN *dan* MAN.



Gambar 3.3. *Wide Area Network* (WAN)

d. *Internet*

Internet adalah interkoneksi jaringan-jaringan komputer yang ada di dunia. Sehingga cakupannya sudah mencapai satu planet, bahkan tidak menutup kemungkinan mencakup antar planet (Sofana, 2008:5).

2. Berdasarkan Media

Berdasarkan media penghantar, jaringan komputer dapat dibagi menjadi 2 jenis yaitu :

a. *Wire Network*

Adalah jaringan komputer yang menggunakan kabel sebagai media penghantar. Jadi, data mengalir pada 9 kabel. Kabel yang umum digunakan pada jaringan komputer biasanya menggunakan bahan dasar tembaga. Ada juga jenis kabel lain yang menggunakan bahan sejenis *fiber optic* atau serat optik (Sofana, 2008:6).

b. *Wireless Network*

Adalah jaringan tanpa kabel yang menggunakan media penghantar gelombang radio atau cahaya *infrared*. *Frequensi* yang digunakan pada radio untuk jaringan komputer biasanya menggunakan *frequensi* tinggi, yaitu 2.4 GHz dan 5.8 GHz. Sedangkan penggunaan *infrared* umumnya hanya terbatas untuk jenis jaringan yang hanya melibatkan dua buah komputer saja atau disebut *point to point* (Sofana, 2008:6).

3. Berdasarkan Fungsi

Berdasarkan fungsinya, jaringan komputer dapat dibagi menjadi 2 jenis, yaitu:

a. *Client Server*

Client server dalah jaringan komputer yang satu (boleh lebih) komputer difungsikan sebagai *server* atau induk bagi

komputer yang lain. *Server* melayani komputer lain yang disebut *client*, layanan yang diberikan bisa berupa akses *Web, e-mail, file*, atau yang lain. *Client server* banyak dipakai pada internet (Sofana, 2008:6).

b. *Peer to peer*

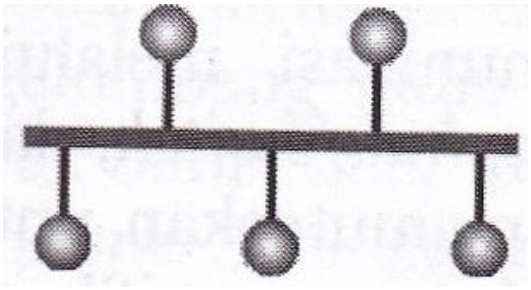
Peer to peer adalah jaringan komputer dimana setiap komputer bisa menjadi *server* sekaligus *client*. Setiap komputer dapat menerima dan memberikan akses dari komputer lain. *Peer to peer* banyak di implementasikan pada LAN. Walaupun dapat juga di implementasikan pada MAN, WAN, atau internet, namun hal ini kurang lazim. Salah satu alasanya adalah masalah *management* dan *security* (Sofana,2008:6).

3.3 Topologi Jaringan Komputer

Menurut Utomo (2006:21), Topologi Jaringan adalah gambaran dari struktur jaringan yang akan dibangun dan merupakan suatu aturan/*rules* bagaimana menghubungkan komputer satu sama lain secara fisik dan pola hubungan antara komponen-komponen yang berkomunikasi melalui media/peralatan jaringan, seperti: *server, workstation, hub/switch*, dan pengkabelannya.

Topologi jaringan komputer secara umum ada 5 (lima), topologi yang pertama adalah :

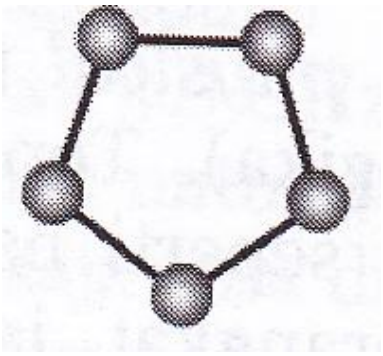
a. Topologi *Bus*



Gambar 3.4. Topologi *Bus*

Topologi ini adalah topologi yang awal di gunakan untuk menghubungkan komputer. Dalam topologi ini masing masing komputer akan terhubung ke satu kabel panjang dengan beberapa terminal, dan pada akhir dari kabel harus di akhiri dengan satu terminator. Topologi ini sudah sangat jarang digunakan dalam membangun jaringan komputer biasa karena memiliki beberapa kekurangan diantaranya kemungkinan terjadinya tabrakan aliran data, jika salah satu perangkat putus atau terjadi kerusakan pada satu bagian komputer maka jaringan langsung tidak akan berfungsi sebelum kerusakan tersebut di atasi. Topologi ini awalnya menggunakan kabel *Coaxial* sebagai media pengantar data dan informasi. Tapi pada saat ini topologi ini di dalam membangun jaringan komputer dengan menggunakan kabal serat *optic* (*fiber optic*) akan tetapi digabungkan dengan topologi jaringan yang lain untuk memaksimalkan performanya.

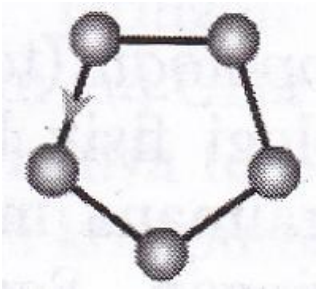
b. Topologi Cincin (*Ring*)



Gambar 3.5. Topologi *Ring* (Cincin)

Topologi cincin atau yang sering disebut dengan *ring* topologi adalah topologi jaringan dimana setiap komputer yang terhubung membuat lingkaran. Dengan artian setiap komputer yang terhubung kedalam satu jaringan saling terkoneksi ke dua komputer lainnya sehingga membentuk satu jaringan yang sama dengan bentuk cincin. Adapun kelebihan dari topologi ini adalah kabel yang digunakan bisa lebih dihemat. Tetapi kekurangan dari topologi ini adalah pengembangan jaringan akan menjadi susah karena setiap komputer akan saling terhubung.

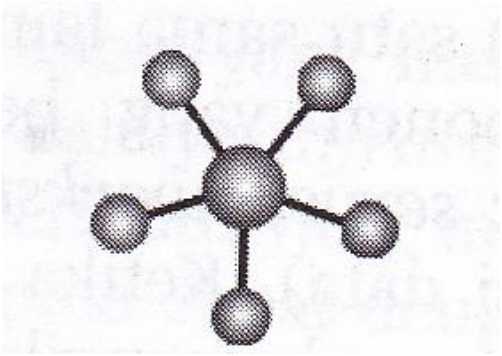
c. Topologi *Token Ring*



Gambar 3.6. Topologi *Token Ring*

Topologi ini hampir sama dengan topologi *ring* akan tetapi pembuatannya lebih di sempurnakan. Bisa di lihat dari perbedaan gambar. Didalam gambar jelas terlihat bagaimana pada *token ring* kabel penghubung di buat menjadi lingkaran terlebih dahulu dan nantinya akan di buatkan terminal-terminal untuk masing-masing komputer dan perangkat lain.

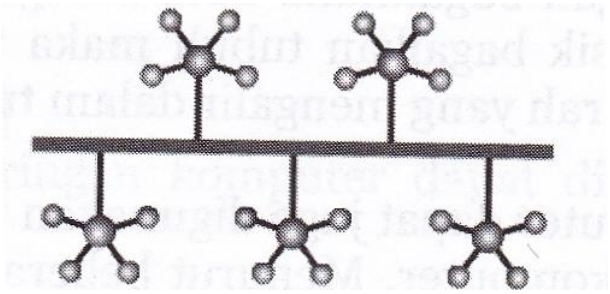
d. Topologi Bintang (*Star*)



Gambar 3.7. Topologi Bintang (*Star*)

Topologi bintang atau yang lebih sering disebut dengan topologi *star*. Pada topologi ini kita sudah menggunakan bantuan alat lain untuk mengkoneksikan jaringan komputer. Contoh alat yang di pakai disini adalah *hub*, *switch*, dll. Pada gambar jelas terlihat satu *hub* berfungsi sebagai pusat penghubung komputer-komputer yang saling berhubungan. Keuntungan dari topologi ini sangat banyak sekali diantaranya memudahkan admin dalam mengelola jaringan, memudahkan dalam penambahan komputer atau terminal, kemudahan mendeteksi kerusakan dan kesalahan pada jaringan. Tetapi dengan banyak nya kelebihan bukan dengan artian topologi ini tanpa kekurangan. Kekurangannya diantaranya pemborosan terhadap kabel, kontrol yang terpusat pada hub terkadang jadi permasalahan kritis kalau seandainya terjadi kerusakan pada *hub* maka semua jaringan tidak akan bisa digunakan.

e. Topologi Pohon (*Tree*)



Gambar 3.8. Topologi Pohon (*Tree*)

Topologi pohon atau di sebut juga topologi *hirarki* dan bisa juga disebut topologi bertingkat merupakan topologi yang bisa di gunakan pada jaringan di dalam ruangan kantor yang bertingkat. Pada gambar bisa kita lihat hubungan antar satu komputer dengan komputer lain merupakan percabangan dengan *hirarki* yang jelas. Sentral pusat atau yang berada pada bagian paling atas merupakan sentral yang aktif sedangkan sentral yang ada di bawahnya adalah sentral yang pasif.

3.4 OSI 7 Layer

Model *Open Systems Interconnection* (OSI) diciptakan oleh *International Organization for Standardization* (ISO) yang menyediakan kerangka logika terstruktur bagaimana proses komunikasi data berinteraksi melalui jaringan. Standar ini dikembangkan untuk industri komputer agar komputer dapat berkomunikasi pada jaringan yang berbeda secara efisien. Model OSI terbagi 7 adalah sebagai berikut:

***Application Layer**:* Menyediakan jasa untuk aplikasi pengguna. *Layer* ini bertanggung jawab atas pertukaran informasi antara program komputer, seperti program *e-mail*, dan *service* lain yang jalan di jaringan, seperti *server printer* atau *aplikasi* komputer lainnya (Sofana, 2008:81).

Presentation Layer: Bertanggung jawab bagaimana data di konversi dan di *format* untuk *transfer* data. Contoh konversi *format text ASCII* untuk dokumen, .gif dan JPG untuk gambar. *Layer* ini membentuk kode konversi, *translasi* data, *enkripsi* dan konversi (Sofana, 2008:81).

Session Layer : Menentukan bagaimana dua terminal menjaga, memelihara dan mengatur koneksi, bagaimana mereka saling berhubungan satu sama lain. Koneksi di *layer* ini disebut "*session*" (Sofana, 2008:82).

Transport Layer : Bertanggung jawab membagi data menjadi segmen, menjaga koneksi logika "*end-to-end*" antar terminal, dan menyediakan penanganan *error* (Sofana, 2008:82).

Network Layer : Bertanggung jawab menentukan alamat jaringan, menentukan rute yang harus diambil selama perjalanan, dan menjaga antrian trafik di jaringan. Data pada layer ini berbentuk paket (Sofana, 2008:82).

Data Link Layer : Menyediakan link untuk data, memaketkannya menjadi *frame* yang berhubungan dengan "*hardware*" kemudian diangkut melalui media. komunikasinya dengan kartu jaringan, mengatur komunikasi *layer physical* antara sistem koneksi dan penanganan *error* (Sofana, 2008:82).

Physical Layer : Bertanggung jawab atas proses data menjadi bit dan mentransfernya melalui media, seperti kabel, dan menjaga koneksi fisik antar sistem (Sofana, 2008:83).

3.5 TCP/IP

TCP/IP (*Transmission Control Protocol/Internet Protocol)* adalah standar komunikasi data yang digunakan oleh komunitas internet dalam proses tukar-menukar data dari satu komputer ke komputer lain di dalam jaringan internet. Protokol ini tidaklah dapat berdiri sendiri, karena memang protokol ini berupa kumpulan protokol (*protocol suite*). Protokol ini juga merupakan protokol yang paling banyak digunakan saat ini. Data tersebut di implementasikan dalam bentuk perangkat lunak (*software*) di sistem operasi. Istilah yang diberikan kepada perangkat lunak ini adalah TCP/IP *stack.* Protokol TCP/IP dikembangkan pada akhir dekade 1970-an hingga awal 1980-an sebagai sebuah protokol standar untuk menghubungkan komputer-komputer dan jaringan untuk membentuk sebuah jaringan yang luas (WAN). TCP/IP merupakan sebuah standar jaringan terbuka yang bersifat independen terhadap mekanisme *transport* jaringan fisik yang digunakan, sehingga dapat digunakan di mana saja. Protokol ini menggunakan skema pengalamatan yang sederhana yang disebut sebagai alamat IP (IP *Address*) yang mengizinkan hingga beberapa ratus juta komputer untuk dapat saling berhubungan satu sama lainnya di internet. Protokol ini juga bersifat *routable* yang berarti protokol ini cocok untuk

menghubungkan sistem-sistem berbeda (seperti *Microsoft Windows* dan keluarga *UNIX*) untuk membentuk jaringan yang *heterogen*.

Protokol TCP/IP selalu berevolusi seiring dengan waktu, mengingat semakin banyaknya kebutuhan terhadap jaringan komputer dan internet. Pengembangan ini dilakukan oleh beberapa badan, seperti halnya *Internet Society* (ISOC), *Internet Architecture Board* (IAB), dan *Internet Engineering Task Force* (IETF). Macam-macam protokol yang berjalan di atas TCP/IP, skema pengalamatan, dan konsep TCP/IP didefinisikan dalam dokumen yang disebut sebagai *Request for Comments* (RFC) yang dikeluarkan oleh IETF (Sofana, 2008:88).

3.6 IP Address

Menurut Sofana (2008:93), *Internet Protocol* (IP) *address* adalah alamat numerik yang ditetapkan untuk sebuah komputer yang berpartisipasi dalam jaringan komputer yang memanfaatkan *Internet Protocol* untuk komunikasi antara node-nya. Walaupun alamat IP disimpan sebagai angka biner, mereka biasanya ditampilkan agar memudahkan manusia menggunakan notasi, seperti 208.77.188.166 (untuk IPv4), dan 2001: db8: 0:1234:0:567:1:1 (untuk IPv6). Peran alamat IP adalah sebagai berikut: "Sebuah nama menunjukkan apa yang kita cari. Sebuah alamat menunjukkan di mana ia berada. Sebuah route menunjukkan bagaimana menuju ke sana."

Perancang awal dari TCP/IP menetapkan sebuah alamat IP sebagai nomor 32-bit, dan sistem ini, yang kini bernama *Internet Protocol Version 4*

(IPv4), masih digunakan hari ini. Namun, karena pertumbuhan yang besar dari internet dan penipisan yang terjadi pada alamat IP, dikembangkan sistem baru (IPv6), menggunakan 128 bit untuk alamat, dikembangkan pada tahun 1995 dan terakhir oleh standar RFC 2460 pada tahun 1998.

Internet Protocol juga memiliki tugas routing paket data antara jaringan, alamat IP dan menentukan lokasi dari node sumber dan node tujuan dalam topologi dari sistem routing. Untuk tujuan ini, beberapa bit pada alamat IP yang digunakan untuk menunjuk sebuah subnetwork. Jumlah bit ini ditunjukkan dalam notasi CIDR, yang ditambahkan ke Alamat IP, misalnya, 208.77.188.166/24. Dengan pengembangan jaringan pribadi / *private network*, alamat IPv4 menjadi kekurangan, sekelompok alamat IP *private* dikhususkan oleh RFC 1918. Alamat IP *private* ini dapat digunakan oleh siapa saja di jaringan pribadi / *private network*. Mereka sering digunakan dengan *Network Address Translation* (NAT) untuk menyambung ke internet umum global, IP juga terbagi menjadi 5 kelas seperti keterangan dibawah ini, diantaranya yaitu :

Kelas A

Oktet pertama dari 1-126,Alamat kelas A diberikan untuk jaringan skala besar. Nomor urut bit tertinggi di dalam alamat IP kelas A selalu diset dengan nilai 0 (nol). Tujuh bit berikutnya untuk melengkapi oktet pertama akan membuat sebuah *network identifier*. 24 bit sisanya (atau tiga oktet terakhir) merepresentasikan *host*

identifier. Ini mengizinkan kelas A memiliki hingga 126 jaringan, dan 16,777,214 host tiap jaringannya. Alamat dengan oktet awal 127 tidak diizinkan, karena digunakan untuk mekanisme *Interprocess Communication* (IPC) di dalam mesin yang bersangkutan (Sofana, 2008:106).

Kelas B

Oktet pertama dari 128-191,Alamat-alamat *unicast* kelas B dikhususkan untuk jaringan skala menengah hingga skala besar. Dua bit pertama di dalam oktet pertama alamat IP kelas B selalu diset ke bilangan biner 10. 14 bit berikutnya (untuk melengkapi dua oktet pertama), akan membuat sebuah *network identifier*. 16 bit sisanya (dua oktet terakhir) merepresentasikan *host identifier*. Kelas B dapat memiliki 16,384 *network*, dan 65,534 *host* untuk setiap *network* nya (Sofana, 2008:106).

Kelas C

Oktet pertama dari 192-223,Alamat IP kelas C digunakan untuk jaringan berskala kecil. Tiga bit pertama di dalam oktet pertama alamat kelas C selalu diset ke nilai biner 110. 21 bit selanjutnya (untuk melengkapi tiga oktet pertama) akan membentuk sebuah *network identifier*. 8 bit sisanya (sebagai oktet terakhir) akan merepresentasikan *host identifier*. Ini memungkinkan pembuatan total

2,097,152 buah *network*, dan 254 *host* untuk setiap *network* nya (Sofana, 2008:107).

Kelas D

Oktet pertama dari 224-239,Alamat IP kelas D disediakan hanya untuk alamat-alamat IP *multicast*, sehingga berbeda dengan tiga kelas di atas. Empat bit pertama di dalam IP kelas D selalu diset ke bilangan biner 1110. 28 bit sisanya digunakan sebagai alamat yang dapat digunakan 21 untuk mengenali *host*. Untuk lebih jelas mengenal alamat ini, lihat pada bagian alamat *Multicast* IPv4 (Sofana, 2008:107).

Kelas E

Oktet pertama dari 240-255 Oktet pertama dari 1,Alamat IP kelas E disediakan sebagai alamat yang bersifat "*eksperimental*" atau percobaan dan dicadangkan untuk digunakan pada masa depan. Empat bit pertama selalu diset kepada bilangan biner 1111. 28 bit sisanya digunakan sebagai alamat yang dapat digunakan untuk mengenali *host* (Sofana, 2008:108).

3.7 Perangkat *Network*

Menurut sumber yang didapat (Sofana, 2008:64). Perangkat *network* atau peralatan jaringan adalah sebuah perantara atau alat untuk menjalankan

sebuah jaringan komputer. Ada beberapa perangkat *network* standar yang sering digunakan untuk *internetworking*, seperti contoh dibawah ini :

a. *Hub*

Hub adalah sebuah perangkat jaringan komputer yang berfungsi untuk menghubungkan peralatan-peralatan dengan *ethernet* 10 BaseT atau serat optik sehingga menjadikannya dalam satu segmen jaringan. (Sofana, 2008:67).

b. *Switch*

Switch jaringan (switch untuk singkatnya) adalah sebuah alat jaringan yang melakukan *bridging transparan* (penghubung segementasi banyak jaringan dengan *forwarding* berdasarkan alamat MAC) (Sofana, 2008:71).

c. *Router*

Router adalah sebuah alat jaringan komputer yang mengirimkan paket data melalui sebuah jaringan atau internet menuju tujuannya, melalui sebuah proses yang dikenal sebagai *routing* (Sofana, 2008:69).

d. Modem

Modem berasal dari singkatan *MOdulator DEModulator*. *Modulator* merupakan bagian yang mengubah sinyal informasi kedalam sinyal pembawa (*carrier*) dan siap untuk dikirimkan, sedangkan *Demodulator* adalah bagian yang memisahkan sinyal informasi

(yang berisi data atau pesan) dari sinyal pembawa yang diterima sehingga informasi tersebut dapat diterima dengan baik. Modem merupakan penggabungan kedua-duanya, artinya modem adalah alat komunikasi dua arah. Setiap perangkat komunikasi jarak jauh dua-arah umumnya menggunakan bagian yang disebut "modem", seperti VSAT, Microwave Radio, dan lain sebagainya, namun umumnya istilah modem lebih dikenal sebagai Perangkat 23 keras yang sering digunakan untuk komunikasi pada komputer. Data dari komputer yang berbentuk sinyal digital diberikan kepada modem untuk diubah menjadi sinyal analog. Sinyal analog tersebut dapat dikirimkan melalui beberapa media telekomunikasi seperti telepon dan radio. Setibanya di modem tujuan, sinyal analog tersebut diubah menjadi sinyal digital kembali dan dikirimkan kepada komputer. Terdapat dua jenis modem secara fisiknya, yaitu modem *eksternal* dan modem *internal* (Utomo, 2006:70).

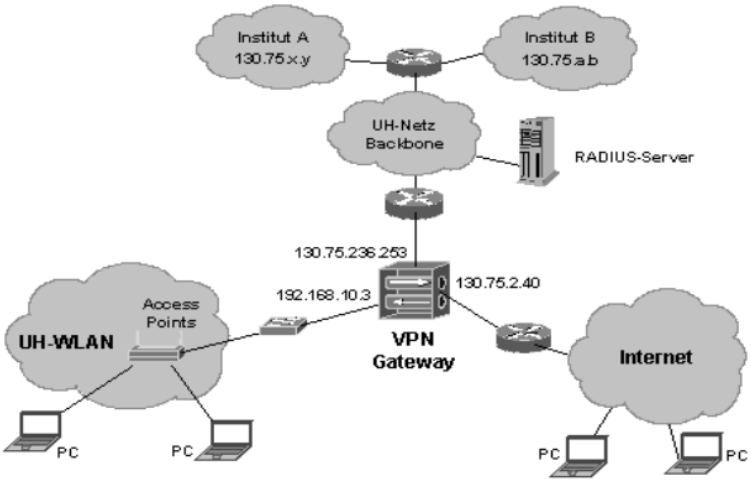
e. NIC

Kartu jaringan (*Network Interface Card* disingkat NIC atau juga *network card*) adalah sebuah kartu yang berfungsi sebagai jembatan dari komputer ke sebuah jaringan komputer. Jenis NIC yang beredar, terbagi menjadi dua jenis, yakni NIC yang bersifat fisik, dan NIC yang bersifat logis. Contoh NIC yang bersifat fisik adalah NIC *Ethernet*, *Token Ring*, dan lainnya, sementara NIC yang bersifat logis adalah *loopback* adapter dan *Dial-up* Adapter.

Disebut juga sebagai *Network* Adapter. Setiap jenis NIC diberi nomor alamat yang disebut sebagai *MAC address*, yang dapat bersifat statis atau dapat diubah oleh pengguna (Sofana, 2008:66).

3.8 *Virtual Private Network* (VPN)

Menurut Wendy & Ramadhan (2005:1), *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* sehingga data melewati jaringan publik dan dapat mencapai akhir tujuan.



Gambar 3.9 *Virtual Private Network* (VPN)

Menurut Rayszul Rivaldie, dkk (2011:35), *Virtual Private Network* (VPN) memiliki beberapa fungsi utama dalam penggunaannya, fungsi utama tersebut adalah sebagai berikut :

1. **Kerahasiaan**

   Teknologi VPN memiliki sistem kerja mengenkripsi semua data yang melewatinya. Dengan adanya teknologi enkripsi ini, maka kerahasiaan data menjadi lebih terjaga. Meskipun masih ada pihak yang dapat menyadap data, namun belum tentu pihak tersebut dapat membaca data itu dengan mudah karena data tersebut telah dienkripsi. Dengan menerapkan sistem enkripsi ini, maka tidak ada satupun orang yang dapat mengakses dan membaca isi jaringan data dengan mudah.

2. **Integritas Data**

   Ketika melewati jaringan internet, data sebenarnya sudah berjalan sangat jauh melintasi berbagai Negara. Di tengah perjalanannya, apapun bisa terjadi terhadap isi data tersebut, baik itu hilang, rusak, atau bahkan dimanipulasi isinya oleh orang lain. VPN memiliki teknologi yang dapat menjaga keutuhan data yang dikirim agar sampai ke tujuan tanpa cacat, hilang, rusak, ataupun dimanipulasi oleh orang lain.

3. **Autentikasi Sumber**

   Teknologi VPN memiliki kemampuan untuk melakukan autentikasi terhadap sumber-sumber pengirim data. VPN akan melakukan pemeriksaan terhadap semua data yang masuk dan mengambi informasi *source* datanya. Kemudian alamat *source* data ini akan disetujui jika proses autentikasinya berhasil. Dengan demikian,

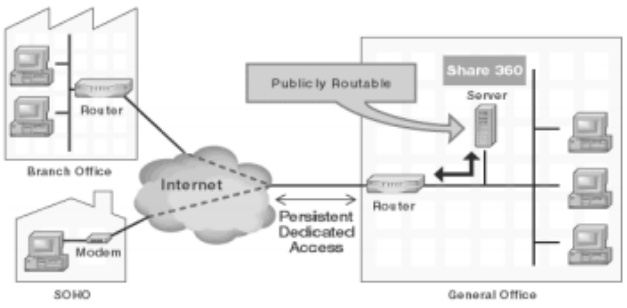
VPN menjamin semua data yang dikirim dan diterima berasal dari sumber yang seharusnya. Tidak ada data yang dipalsukan atau dikirimkan oleh pihak-pihak lain.

3.9 Jenis-jenis *Virtual Private Network* (VPN)

Menurut Rayszul Rivaldie, dkk (2011:36), Terdapat dua jenis yang ada pada VPN, diantaranya yaitu sebagai berikut :

1. ***Remote Access* VPN**

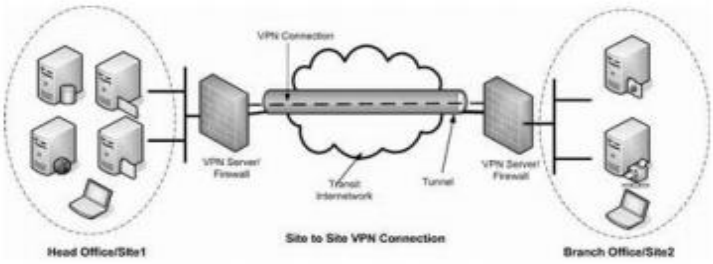
   Tipe VPN ini memungkinkan koneksi jarak jauh (*remote access*) bagi pegawai yang sedang bertugas diluar kantor, luar kota ataupun sedang diluar negeri untuk dapat mengakses ke LAN di kantor pusat menggunakan jaringan internet. Hal ini terutama sangat berguna untuk dapat menerima email yang tersedia di LAN kantor pusat. Selain itu, hal tersebut juga berlaku bagi kantor cabang yang tidak memiliki koneksi secara terus-menerus ke kantor pusat. Kantor cabang tersebut dapat melakukan koneksi *dial-up* ke suatu ISP dan setelah itu melakukan koneksi ke kantor pusat.



Gambar 3.10 *Remote Access* VPN

2. *Site-to-Site* VPN

Site-to-Site VPN memungkinkan suatu *private network* diperluas melintasi jaringan internet atau layanan *public network* lainnya dengan cara yang aman. *Site-to-Site* VPN kadang disebut juga sebagai LAN-to-LAN VPN. *Site-to-Site* VPN merupakan suatu alternatif dari infrastruktur WAN yang biasa menghubungkan kantor-kantor cabang, kantor pusat, atau partner bisnis ke seluruh jaringan yang terdapat di perusahaan.



Gambar 3.11 *Site-to-Site* VPN

3.10 Keamanan *Virtual Private Network* (VPN)

Menurut Rayszul Rivaldie, dkk (2011:39), *Virtual Private Network* menggunakan sistem keamanan untuk menjaga kerahasiaan data dan keamanan pada jaringan VPN itu sendiri. Berikut ini penjabaran dari tipe keamanan pada teknologi VPN :

1. Enkripsi

Enkripsi merupakan salah satu cara yang dapat digunakan .untuk mengubah data asli (sebenarnya) menjadi bentuk sandi

(*chipper text*) yang mana sandi-sandi tersebut hanya dapat dimengerti oleh pihak pengirim dan penerima data sehingga data tersebut tidak dapat dibaca oleh orang luar yang tidak mempunyai hak akses untuk melihat data tersebut. Untuk mengubah sandi (*chipper text*) tersebut ke bentuk semula maka digukanan teknik yang dinamakan dekripsi. Terdapat dua cara untuk melakukan proses enkripsi, yaitu enkripsi kunci simetrik dan enkripsi kunci asimetrik.

2. Autentikasi

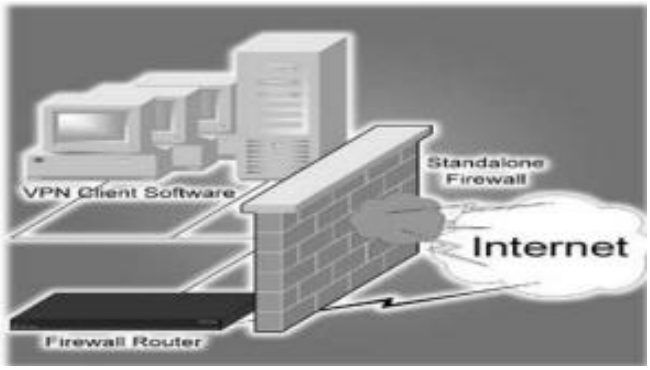
Autentikasi merupakan salah satu proses untuk mengindetifikasi pengguna sehingga data yang dikirim akan menjadi jelas isi dan siapa pengirimnya. Biasanya dalam proses autentikasi, diperlukan *username* dan *password* sebagai alat verifikasinya. *Username* dan *password* ini dimaksudkan agar tidak sembarang orang dapat mengakses, mengirim ataupun mengambil data yang bersifat private.

3. Autorisasi

Autorisasi adalah pencarian apakah orang yang sudah diidentifikasi, diizinkan untuk memanipulasi sumber daya atau data tertentu di jaringan VPN tersebut. Proses autorisasi inilah yang menentukan apakah pengguna tersebut dapat melakukan perintah atau tugas yang dikehendakinya pada jaringan VPN tersebut.

4. Firewall

Firewall merupakan suatu cara atau mekanisme yang diterapkan baik terhadap hardware, software maupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi, atau bahkan menolak suatu atau semua hubungan atau kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan lingkupnya. Segmen tersebut dapat merupakan sebuah *workstation, server, router,* dan *local area network* (LAN). *Firewall* merupakan sebuah perangkat yang diletakkan antara *internet* dengan jaringan internal. Informasi yang keluar atau masuk harus melalui *firewall* ini. Tujuan utama dari *firewall* adalah untuk menjaga agar orang yang tidak berwenang tidak dapat melakukan akses, baik ke dalam maupun keluar.



Gambar 3.12 *Firewall*

Firewall memiliki prinsip kerja dalam menjalankan tugasnya, berikut ini adalah prinsip kerja yang dijalankan *Firewall* :

1. *Service Control* (Kendali Terhadap Layanan)

   Prinsip kerja berdasarkan tipe-tipe layanan yang digunakan di *internet* dan boleh diakses baik untuk ke dalam maupun keluar *firewall. Firewall* akan mengecek nomor IP *address* dan nomor *port* yang digunakan, baik pada *protocol* TCP dan UDP. *Firewall* bisa dilengkapi *software proxy* untuk menerima dan menterjemahkan setiap permintaan atas suatu layanan sebelum mengizinkannya. Selain itu, *server* juga bisa menggunakan *software,* misalnya untuk layanan web atau mail. (Rayszul Rivaldie, dkk, 2011:42-43)

2. *Direction Control* (Kendali Terhadap Arah)

   Prinsip kerja berdasarkan arah dari berbagai permintaan (*request*) terhadap layanan. Layanan akan dikenali dan diizinkan melewati *firewall.* (Rayszul Rivaldie, dkk, 2011:43)

3. *User Control* (Kendali Terhadap Pengguna)

   Prinsip kerja berdasarkan pengguna atau *user* untuk dapat menjalankan suatu layanan. Dengan demikian, ada user yang dapat menjalankan suatu *service* dan ada yang tidak. *User* tidak dapat menjalankan *service* karena tidak di izinkan untuk melewati *firewall.* Prinsip ini biasa digunakan untuk membatasi akses keluar user jaringan lokal, namun bisa juga

diterapkan untuk membatasi akses terhadap pengguna dari luar. (Rayszul Rivaldie, dkk, 2011:43)

4. *Behavior Control* (Kendali Terhadap Perlakuan)

   Prinsip kerja berdasarkan seberapa banyak layanan itu telah digunakan, Misallnya, *firewall* dapat melakukan *filter* email untuk menanggulangi atau mencegah spam. (Rayszul Rivaldie, dkk, 2011:43)

3.11 *Tunneling*

Tunneling merupakan metode untuk transfer data dari satu jaringan ke jaringan lain dengan memanfaatkan jaringan *internet* secara terselubung. Disebut *tunnel* atau saluran karena aplikasi yang memanfaatkannya hanya melewati dua *end point* atau ujung, sehingga paket yang lewat pada tunnel hanya akan melakukan satu kali lompatan atau hop. (Wendy, Ramadhan, 2005:9)

3.12 Protokol-Protokol VPN

Virtual private network (VPN) memiliki beberapa protokol, beberapa protokol yang digunakan untuk pengembangan VPN adalah sebagai berikut :

1. *Point-to-Point Tunneling Protocol* (PPTP)

   PPTP memberikan sarana terselubung (*Tunneling*) untuk berkomunikasi melalui internet. Salah satu kelebihan yang membuat

PPTP ini terkenal adalah karena protokol ini mendukung protokol *non*-IP seperti IPX/SPX, NetBEUI, *Appletalk* dan sebagainya. Protokol ini merupakan protokol standar pada enkapsulasi VPN yang digunakan oleh *Windows Virtual Private Network*. Protokol ini bekerja berdasarkan PPP protokol yang digunakan pada *dial-up connection*. (Wendy, Ramadhan, 2005:7)

2. Layer 2 Tunneling Protocol (L2TP)

   L2TP memberikan sarana enkripsi dan selubung untuk berkomunikasi melalui *internet*. L2TP merupakan kominasi dari dua buah protokol *Cisco* yaitu L2F dan PPTP. Seperti PPTP, L2TP juga mendukung protokol-protokol *non*-IP. L2TP lebih banyak digunakan pada VPN *non-internet* atau *frame relay*, ATM, dan sebagainya. (Wendy, Ramadhan, 2005:7)

3. IPSEC (*Internet Protocol Security*)

   IPsec merupakan protokol standar yang digunakan untuk memberikan keamanan untuk berkomunikasi melalui jaringan IP dengan menggunakan layanan enkripsi keamanan (*Crypto-graphic Security Services*). Protokol ini merupakan protokol populer kedua setelah PPTP, IPSEC sebenarnya merupakan kumpulan dari beberapa protokol yang berhubungan dan mendukung format enkripsi yang lebih kuat dibandingkan dengan PPTP. Kunci kekuatan IPSEC

terletak pada metode baik antara *endpoint* VPN. Fitur ini tidak didukung oleh PPTP dan L2TP. (Wendy, Ramadhan, 2005:8)

4. PPTP Over L2TP

   PPTP *Over* L2TP memberikan sarana PPTP menggunakan protokol L2TP. (Wendy, Ramadhan, 2005:8)

5. IP-IN-IP

   IP-*in*-IP menyelubungi IP datagram dengan IP *header* tambahan. IP-*in*-IP berguna untuk meneruskan paket data melalui jaringan dengan *policy* yang berbeda. IP-*in*-IP juga dapat digunakan untuk meneruskan *multicast audio* dan video data melalui *router* yang tidak mendukung *multicast routing*. (Wendy, Ramadhan, 2005:8)

3.13 *Samba Server*

Menurut Wilfridus Bambang Triadi Handayana, dkk (2010:99), *Samba* merupakan salah satu aplikasi di mesin UNIX dan turunannya yang mengimplementasikan protokol SMB atau *Server Message Block.* Pada mayoritas sistem operasi, protokol SMB digunakan dalam jaringan *client-server*, sehingga memungkinkan antar sistem operasi yang berbeda tersebut dapat saling berkomunikasi, seperti misalnya bertukar data, akses *printer* secara bersama, hingga digunakan sebagai jalur *login* ke suatu *server domain.*

Samba server memiliki beberapa fungsi pada sebuah jaringan *client-server*, beberapa fungsi yang disediakan *samba server* yaitu sebagai berikut :

1. *Sharing file* atau *direktori* antar *Unix/Linux* dengan *windows client*
2. *Sharing printer* pada *samba server* dengan *windows client*
3. Memudahkan proses *network browsing*
4. Menyediakan proses autentikasi komputer *windows client* ketika *login* ke *windows domain*
5. Menyediakan dan membantu proses *netbios name resolution* dengan *Windows Internet Name Service* (WINS) *name-server resolution*

Samba Primary Domain Controller (PDC) berfungsi dimana setiap *user* atau *user* sistem *linux* yang terdaftar sebagai *user samba server* akan memiliki *folder* atau *direktory* masing-masing di *samba server* yang dapat diakses dari jaringan melalui komputer *windows*, dan juga setiap *user* dapat melakukan *logon* ke *domain* melalui komputer *windows* dalam jaringan *windows* tersebut.

3.14 Hasil Penelitian Terdahulu

Tabel 3.1 Hasil Penelitian Terdahulu

No.	Judul	Nama	Metodologi	Keterangan
1	Perancangan dan Implementasi *Remote Access* VPN pada PT. Buana Centra Swakarsa	1. Rayszul Rivaldie (1100009096) 2. Lodeweyk Andri (1100040970) 3. Khairul Fahmi (1100041014)	1. Melakukan wawan cara dengan pihak perusahaan. 2. Melakukan studi kepustakaan mengenai teknologi-teknologi jaringan, serta pengumpulan informasi dan materi yang berkaitan dengan masalah teknologi VPN. 3. Melakukan	1. Penggunaan *Zentyal* sebagai VPN *server* dan *software routing* pada sebuah PC harus dilengkapi dengan 2 buah *Network Interface Card* (NIC). 2. *Advertised network* pada *Zentyal* diperuntukkan untuk menentukan jaringan internal perusahaan yang dapat diakses oleh VPN *client* melalui *tunnel* VPN. 3. Konfigurasi VPN *server* menggunakan protokol TCP. Aplikasi VPN *remote access* diperlukan untuk

			observasi dan survei pada jaringan jaringan komputer yang berjalan, menganalisis masalah yang sedang dihadapi perusahaan serta mengidentifikasi aplikasi yang diperlukan untuk mendukung proses bisnis perusahaan. 4. Merancang jaringan yang dibutuhkan berdasarkan	meningkatkan kinerja perusahaan karena dibutuhkan ketersediaan data bagi direksi dan *manager* yang cepat, aman dan dapat diakses dimana saja. 4. Berdasarkan perancangan yang dibuat pada perusahaan maka dilakukan implementasi berupa instalasi dan konfigurasi menggunakan openVPN sebagai *software* pada jaringan VPN sesuai kebutuhan perusahaan. 5. Perangcangan VPN menggunakan Zentyal 2.0-3 pada *server* tidak membutuhkan biaya dikarenakan Zentyal merupakan produk *open-*

			pada hasil identifikasi masalah yang dihadapi, seperti dalam hal keamanan pada pertukaran data perusahaan yang bersifat rahasia. 5. Menetapkan topologi dan teknologi jaringan yang akan digunakan sesuai hasil identifikasi. 6. Konfigurasi jaringan dengan teknologi dan topologi yang	*source* dan juga sudah terintegrasi dengan openVPN di dalamnya. 6. Penggunaan dan konfigurasi *Zentyal* 2.0-3 serta *open*VPN relatif mudah karena tampilannya yang user *friendly* dan dilengkapi juga dengan *Graphic User Interface* (GUI). 7. Aplikasi VPN dengan menggunakan *open*VPN berdasarkan hasil evaluasi dapat berjalan dengan baik, sukses dan data yang dikirimkan dapat ter*enkripsi* dengan baik sehingga dapat menghindari ancaman yang dapat merugikan perusahaan dan mengganggu aktifitas

			telah diterapkan. 7. Pengujian dan evaluasi terhadap jaringan yang telah di implementasikan.	kerja.
2.	Penerapan Sistem Samba Server Menggunakan Ubuntu 8.04 di SMA Swasta Insani Binjai	Isminaldi	1. Observasi, yaitu mengadakan pengamatan langsung ke SMA insani untuk mengaplikasikan atau mengkonfigurasi *samba server* 2. Wawancara, yaitu bertanya	1. *Samba server* mempunyai kelebihan sebagai *server* dan memiliki fungsi yang lengkap sebagai *server, tool* yang disediakan banyak. 2. Sistem *samba server* merupakan *server* yang handal, dengan *server* sebagai *linux*, dan *client* meggunakan *windows* karena siswa lebih

			langsung kepada instruktur serta staff-staff sekaligus pegawai SMA insani. 3. Studi Dokumen, yaitu untuk memudahkan dalam pengumpulan data, penulis meneliti dokumen yang mendukung penelitian. 4. Studi Literatur, yaitu mempelajari atau mengunjungi	familiar menggunakan *windows.* 3. *Samba* adalah alat yang bisa membuat hubungan antara *linux* yang handal dan *windows* yang familiar, sehingga keamanan dan kemudahan bisa didapatkan dari *samba.* 4. Perawatan terhadap server tetap harus dilakukan secara terus menerus, karena aplikasi *server* makin bertambah canggih. 5. Sistem *samba server* merupakan sistem yang terbaik untuk digunakan dan sangat cocok untuk sekolah seperti SMU. Hal ini dilandasi oleh siswa yang banyak tapi

			website-website yang menyediakan tutorial serta artikel-artikel mengenai *samba server*.	mereka bisa memiliki hak akses tersendiri.

Adapun isi dari tabel penelitian terdahulu diatas dapat disimpulkan sebagai berikut :

1. **Perancangan dan Implementasi *Remote Access* VPN pada PT. Buana Centra Swakarsa**

   Penggunaan *Zentyal* sebagai VPN *server* dan *software routing* pada sebuah PC harus dilengkapi dengan 2 buah *Network Interface Card* (NIC) yang bertujuan 1 NIC untuk ke *Internet Service Provider* (ISP) dan 1 NIC untuk ke jaringan lokal.

   Berdasarkan perancangan yang dibuat pada perusahaan untuk membangun VPN *server* dengan menggunakan *Zentyal* sebagai sistem operasi, maka dilakukan implementasi berupa instalasi dan konfigurasi menggunakan openVPN sebagai *software* pada jaringan VPN sesuai kebutuhan perusahaan.

   Dengan menggunakan sistem operasi *Zentyal* 2.0-3 pada server, maka tidak membutuhkan biaya dikarenakan *Zentyal* merupakan produk

open-source dan juga sudah terintegrasi dengan *open*VPN di dalamnya. Penggunaan dan konfigurasi *Zentyal* 2.0-3 serta *open*VPN relatif mudah karena tampilannya yang user friendly dan dilengkapi juga dengan *Graphic User Interface* (GUI).

Selain dilengkapi dengan *Graphic User Interface* (GUI), pada sistem operasi *Zentyal* 2.0-3 sudah tersedia aplikasi VPN *server* yaitu *open*VPN. Berdasarkan hasil evaluasi dapat berjalan dengan baik, sukses dan data yang dikirimkan dapat ter*enkripsi* dengan baik sehingga dapat menghindari ancaman yang dapat merugikan perusahaan dan mengganggu aktifitas kerja.

2. Penerapan Sistem Samba Server Menggunakan Ubuntu 8.04 di SMA Swasta Insani Binjai

Samba server mempunyai kelebihan sebagai *server* dengan memiliki fungsi yang lengkap sebagai *server* untuk melakukan *sharing* data maupun *sharing printer*, sehingga dapat memudahkan *admin* jaringan untuk membangun dan mengatur *server* data.

Dengan menggunakan *samba server* sebagai pusat untuk *sharing* data dan *sharing* printer, data yang tersimpan di samba *server* lebih aman dari ancaman virus dikarenakan *samba server* menggunakan sistem operasi *linux* dikarenakan berbeda dengan sistem operasi *windows* yang rentan terinfeksi *virus*.

Menggunakan *samba server* sebagai pusat penyimpanan data dan *sharing* data dengan metode *Primary Domain Controller* (PDC), siswa dapat memiliki tempat penyimpanan data sendiri yang mempunyai hak akses masing-masing sehingga data yang disimpan tidak dapat dihapus atau diambil oleh siswa lain yang tidak mempunyai hak akses untuk data tersebut.