

BAB II

LANDASAN TEORI

2.1. Pengertian Jaringan Komputer

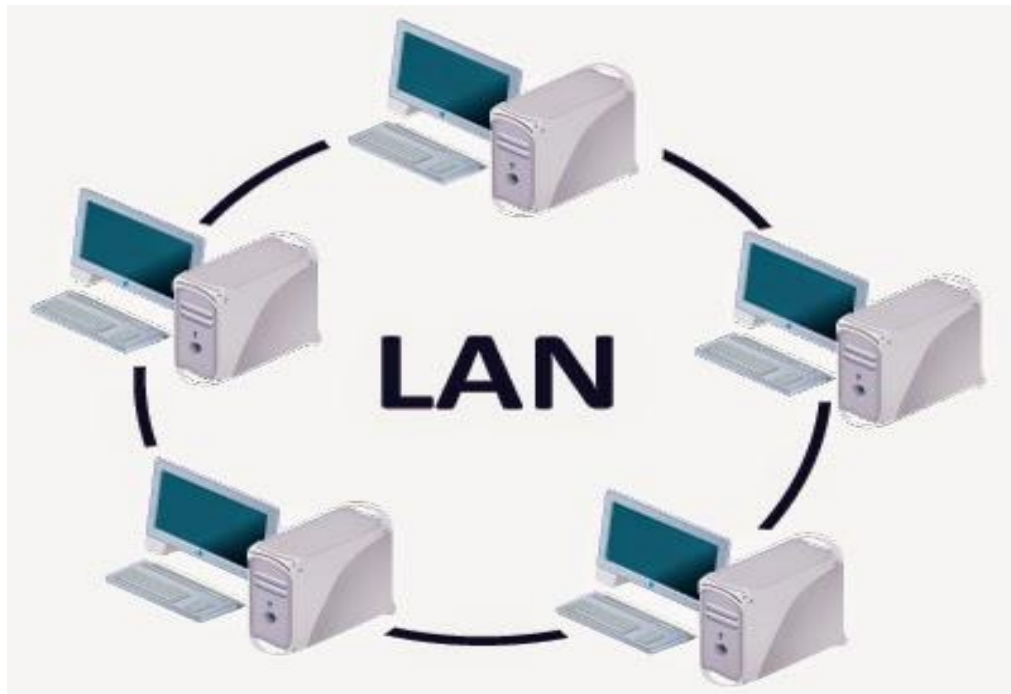
Menurut Sofana (2008:3) “Jaringan komputer adalah suatu himpunan interkoneksi sejumlah komputer autonomus. Dalam bahasa yang populer dapat dijelaskan bahwa jaringan komputer adalah kumpulan beberapa komputer (dan perangkat lain seperti *printer*, *hub*, dan sebagainya) yang saling terhubung satu sama lain melalui media perantar. 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 yang lain, sehingga masing-masing komputer yang terhubung tersebut bisa saling bertukar data atau berbagai perangkat keras”.

2.1.1 Berdasarkan Ruang Lingkup Geografis

Berdasarkan ruang lingkup geografisnya terdapat tiga jenis jaringan komputer, antara lain :

1. Local Area Network

Menurut sofana (2008:4) “Local Area Network adalah jaringan lokal yang dibuat area tertutup. Misalkan dalam satu gedung atau dalam suatu ruangan. Kadangkala jaringan lokal disebut juga jaringan *private*”. LAN biasa digunakan untuk jaringan kecil yang menggunakan *resource* bersama-sama, seperti pengguna *printer* secara bersama, penggunaan media penyimpanan secara bersama.



Sumber : <http://excellgroup.com/images/pic/LAN.jpg>

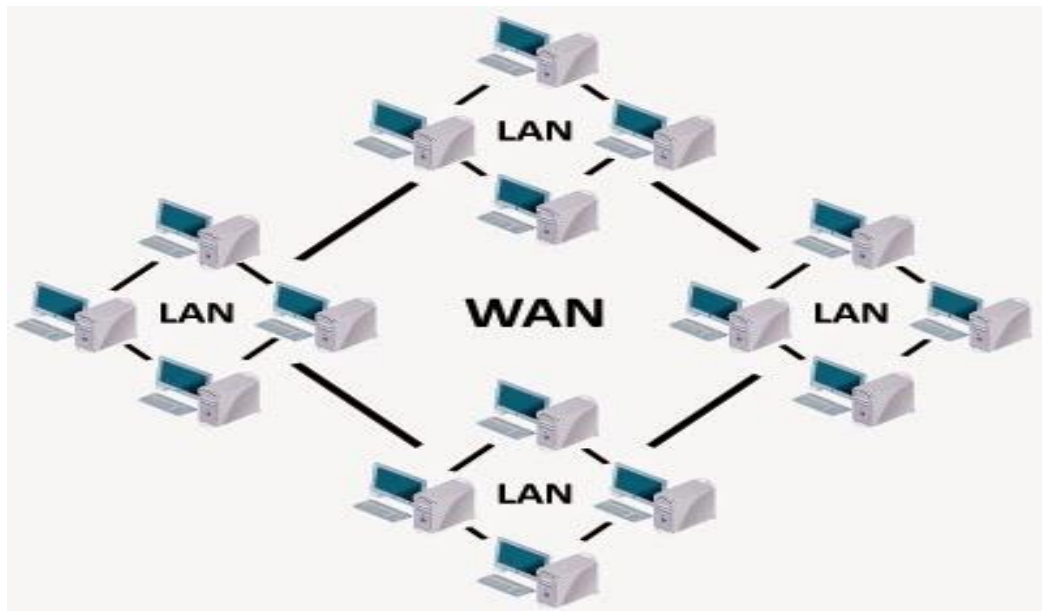
Gambar II.1
Skema Jaringan LAN

2. Metropolitan Area Network (MAN)

Menurut sofana (2008:4) mengatakan bahwa “Metropolitan Area Network menggunakan metode yang sama dengan LAN namun daerah cakupannya lebih luas”. Daerah cakupan MAN bisa satu RW, beberapa kantor yang berada dalam komplek yang sama, satu kota, bahkan satu provinsi. Dapat dikatakan MAN merupakan pengembangan dari LAN.

3. Wide Area Network (WAN)

Menurut Sofana (2008:4) mengatakan bahwa “Wide Area Network cakupannya lebih luas daripada MAN. Cakupan WAN meliputi kawasan, satu negara, satu pulau, bahkan satu benua. Metode yang digunakan WAN hampir sama dengan LAN dan MAN”.



sumber: <http://www.excellgroup.com/images/pic/WAN.jpg>

Gambar II.2
Wide Area Network (WAN)

4. Internet

Menurut Sofana (2008:5) “Internet adalah interkoneksi jaringan-jaringan komputer yang ada di dunia. Sehingga cakupannya sudah mencapai satu planet, bahkan tidak menutup kemungkinan mencakup antar planet”. Koneksi antar jaringan komputer dapat dilakukan berkat dukungan protokol yang khas, yaitu *Internet Protocol (IP)*. Dengan jarak $>10.000.000$ meter.

2.1.2 Berdasarkan Media Penghantar

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

1. *Wire Network*

Wire Network adalah jaringan komputer yang menggunakan kabel sebagai media penghantar. Jadi, data mengalir pada kabel. Kabel yang umum digunakan pada jaringan komputer biasanya menggunakan bahan dasar tembaga. Ada juga jenis kabel lain yang menggunakan bahan sejenis *fiber* optis atau serat optik. Biasanya bahan tembaga banyak digunakan pada LAN. Sedangkan untuk MAN atau WAN menggunakan gabungan kabel tembaga dan serat optik.

2. *Wireless Network*

Wireless Network adalah jaringan tanpa kabel yang menggunakan media penghantar gelombang radio atau cahaya *infrared*. Saat ini sudah semakin banyak *outlet* atau lokasi tertentu yang menyediakan layanan *Wireless Network*. Sehingga pengguna dapat dengan mudah melakukan akses *internet* tanpa kabel. Frekuensi yang digunakan pada radio untuk jaringan komputer biasanya menggunakan frekuensi 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*. Hal ini menyebabkan *infrared* tidak sepopuler gelombang radio.

2.1.3 Arsitektur Jaringan

Ada dua macam arsitektur jaringan, yaitu *Peer to Peer* dan *Client Server*. Masing-masing arsitektur memiliki perbedaan dalam derajat koneksinya, maupun bentuk hubungan antara *server* dengan antar *server* dengan terminalnya. Namun, semua sistem operasi tersebut berfungsi untuk menciptakan hubungan antar terminal yang ada.

1. *Peer to Peer*

Menurut Sofana (2008:6) “*Peer to peer* adalah jaringan komputer dimana setiap komputer bisa menjadi *server* sekaligus *client*. Setiap komputer dapat menerima dan memberikan *access* dari ke komputer lain. *Peer to peer* banyak diimplementasikan pada LAN. Walaupun dapat juga diimplementasikan pada MAN, WAN, atau Internet, namun hal ini kurang lazim. Salah satu alasannya adalah masalah manajemen dan *security*. Sulit sekali menjaga *security* pada jaringan *peer to peer* manakala pengguna komputer sudah sangat banyak”.

2. *Client Server*

Menurut Sofana (2008:6) “*Client server* adalah jaringan komputer yang salah satu (boleh lebih) komputer difungsikan sebagai *server* atau induk bagi komputer 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. Namun LAN atau jaringan lain pun bisa mengimplementasikan *client server*. Hal ini sangat bergantung pada kebutuhan masing-masing.

Prinsip kerjanya, *server* akan menunggu permintaan dari *client*, memproses dan memberikan hasilnya kepada *client*. Sedangkan *client* akan mengirimkan permintaan ke *server*. Menunggu proses dan melihat visualisasi hasil prosesnya.

Tabel II.1.
Perbandingan jaringan *client server* dan *peer to peer*

Jaringan <i>Client Server</i>	Jaringan <i>Peer to Peer</i>
Lebih sulit dibuat dan konfigurasinya	Mudah dibuat dan konfigurasinya
Biaya instalasi lebih Mahal	Biaya instalasi Murah
Untuk client, penggunaan sistem operasi variatif. Untuk server, penggunaan sistem operasi lebih khusus, yaitu yang mendukung sistem jaringan komputer terpusat, misal, windows 2000 server, windows 2003 server, Linux, FreeBSD, dan lain-lain	Penggunaan sistem operasi lebih variatif
<i>Maintenance Software</i> lebih mudah dan memerlukan waktu yang lebih sedikit karena dapat dilakukan secara terpusat dari server.	Memerlukan waktu lebih untuk proses <i>maintenance software</i> , karena <i>software</i> pada masing-masing komputer bersifat individual.
Tingkat keamanan data lebih tinggi, dimana seluruh komputer <i>client</i> dapat dikontrol dari server, baik penghapusan data, perubahan <i>setting</i> , dan lain-lain.	Tingkat keamanan data lebih rendah/riskan.
Dapat digunakan dengan jumlah komputer yang tak terbatas.	Ideal digunakan dengan jumlah komputer maksimal 10 unit.

Memerlukan komputer <i>server</i>	Tidak memerlukan komputer <i>server</i> .
Memerlukan seorang administrator dengan kemampuan khusus dalam menangani jaringan.	Tidak memerlukan seorang administrator dengan kemampuan khusus untuk menangani jaringan

Sumber : Arifin (2011:13)

2.2 Topologi Jaringan Komputer

Menurut Sofana (2013:7) “topologi merupakan suatu aturan/*rules* bagaimana menghubungkan komputer (*node*) secara fisik”. Masing-masing topologi ini mempunyai khas, dengan kelebihan dan kekurangannya.

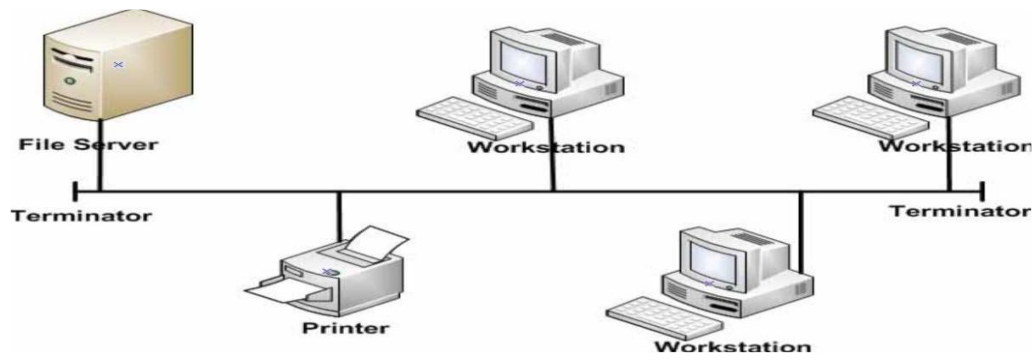
Penulis akan menjelaskan beberapa topologi jaringan, seperti: topologi Bus, topologi Ring dan topologi Star.

2.2.1. Topologi Bus

Menurut Kristanto (2009:2) mengatakan bahwa “*layout* ini termasuk *layout* umum. Satu kabel utama menghubungkan tiap simpul ke saluran tunggal komputer yang mengaksesnya ujung dengan ujung”. Masing-masing simpul dihubungkan ke dua simpul lainnya, kecuali komputer di salah satu ujung kebel, yang masing-masing hanya terhubung ke satu simpul lainnya.

Topologi ini seringkali dijumpai pada sistem *client/server*, di mana salah satu komputer pada jaringan tersebut difungsikan sebagai *file server*, yang berarti bahwa

komputer tersebut dikhususkan hanya untuk pendistribusian data dan biasanya tidak digunakan untuk pemrosesan informasi.



Sumber : Kristanto (2009:2)

Gambar II.3
Topologi Bus

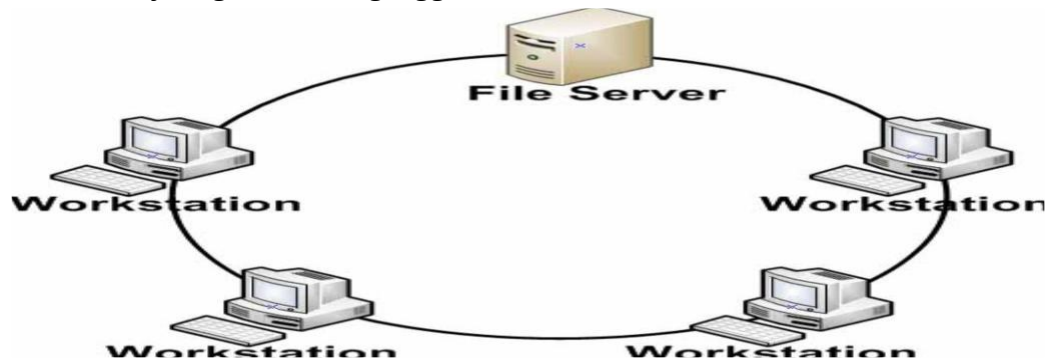
Table II.2
Keuntungan dan Kerugian Topologi Bus

Keuntungan	Kerugian
1. Hemat kabel 2. Layout kabel sederhana 3. Mudah dikembangkan	1. Deteksi dan isolasi kesalahan sangat kecil 2. Kepadatan lalu lintas 3. Bila salah satu client rusak, maka jaringan tidak bisa berfungsi 4. Diperlukan repeater untuk jarak jauh

Sumber : www.ilmukomputer.org

2.2.2. Topologi Ring

Menurut Kristanto (2009:3) mengemukakan bahwa “topologi ini mirip dengan *topologi Bus*, tetapi kedua terminal yang berada di ujung saling dihubungkan, sehingga menyerupai seperti lingkaran”. Setiap informasi yang diperoleh diperiksa alamatnya oleh terminal yang dilewatinya. Jika bukan untuknya, informasi akan dilewatkan sampai menemukan alamat yang benar atau yang di tuju. Setiap terminal dalam jaringan saling tergantung, sehingga jika ada kerusakan pada satu terminal maka seluruh jaringan akan terganggu.



Sumber : Kristanto (2009:3)

Gambar II.4
Topologi Ring

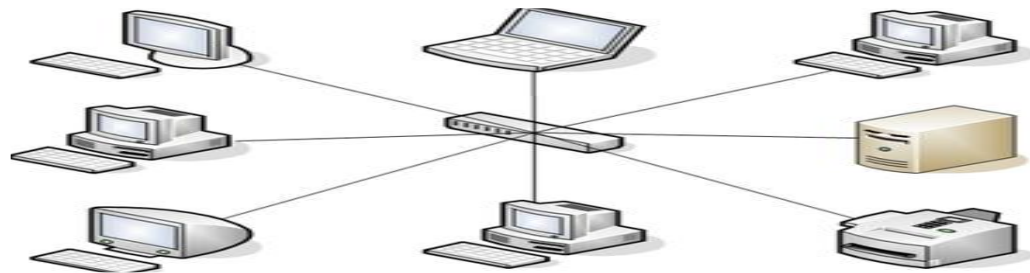
Table II.3
Keuntungan dan Kerugian Topologi Ring

Keuntungan	Kerugian
1. Hemat kabel	1. Peka kesalahan 2. Pengembangan jaringan lebih kaku.

Sumber : www.ilmukomputer.org

2.2.3. Topologi Star

Menurut Kristanto (2009:4) mengatakan bahwa “*topologi star* sebuah terminal pusat bertindak sebagai pengatur dan pengendali semua komunikasi data yang terjadi”. Terminal-terminal lain terhubung padanya dan pengiriman data dari satu terminal ke terminal lainnya melalui terminal pusat. Terminal pusat menyediakan jalur komunikasi khusus untuk dua terminal yang akan berkomunikasi. Dengan kata lain semua kontrol dipusatkan pada satu komputer yang dinamakan stasiun primer dan komputer lainnya dinamakan stasiun sekunder.



Sumber : Kristanto (2009:4)

Gambar II.5
Topologi Star

Tabel II.4
Keuntungan dan Kerugian Topologi Star

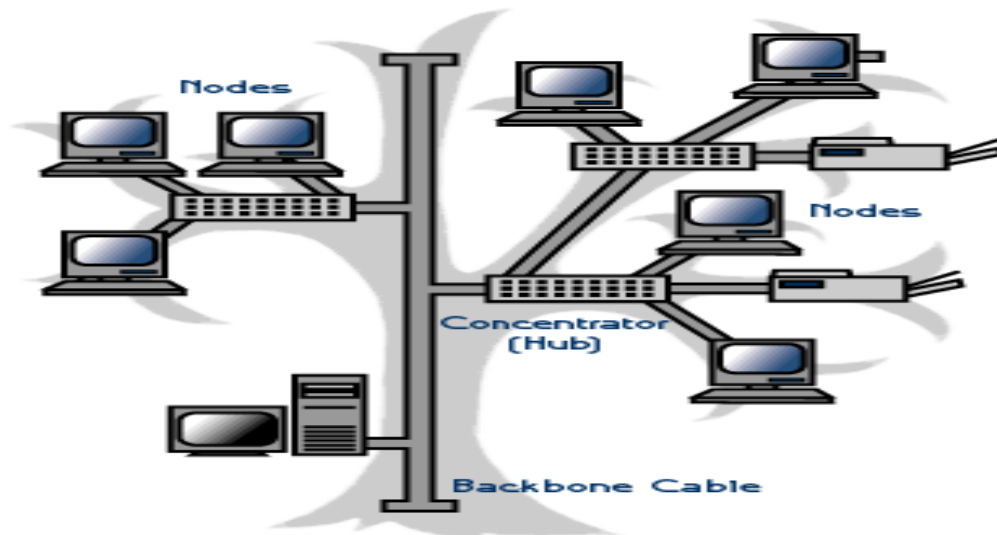
Keuntungan	Kerugian
1. Paling fleksibel 2. Pemasangan/perubahan status sangat mudah 3. Kontrol terpusat 4. Kemudahan deteksi dan	1. Boros kabel 2. Perlu penanganan khusus 3. Kontrol terpusat (HUB) jadi elemen kritis

isolasi kesalahan/kerusakan	
5. Kemudahan pengelolaan jaringan	

Sumber : www.ilmukomputer.org

2.2.4.Topologi Tree (Pohon)

Menurut Kristanto (2009:7) “topologi pohon adalah pengembangan atau generasi *topologi bus*. Media transmisi merupakan satu kabel yang bercabang namun loop tidak tertutup”. Topologi ini dimulai dari satu titik yang disebut “*headend*”. Dari *headend* beberapa kabel ditarik menjadi cabang, dan pada setiap cabang terhubung beberapa terminal dalam bentuk bus, atau dicabang lagi hingga menjadi rumit. Karena bercabang maka diperlukan cara untuk menunjukkan kemana data dikirim, atau kapan siapa transmisi data di tunjukan, dan perlu satu mekanisme untuk mengatur transmisi dari terminal-terminal dalam jaringan. *Active HUB* berfungsi tidak hanya sekedar sebagai penerus sinyal data dari satu komputer ke komputer lainnya, tetapi juga memiliki fungsi sebagai repeater. Sinyal data yang dikirimkan dari satu komputer ke komputer lainnya memiliki keterbatasan dalam hal jarak, setelah berjalan sekian meter maka sinyal tersebut akan melemah.



Sumber : www.pii.or.id/elektro

Gambar II.6
Topologi Tree

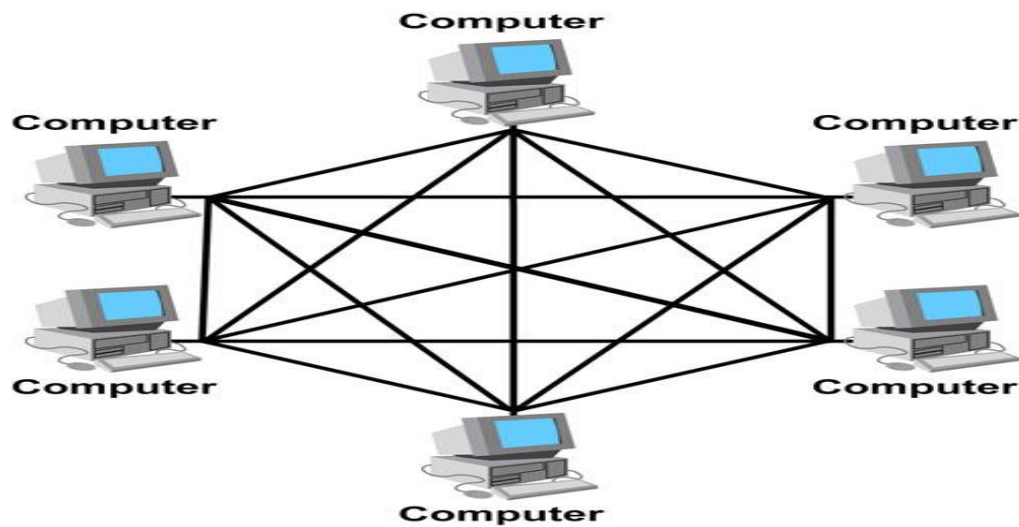
Tabel II.5
Keuntungan dan Kerugian Topologi Tree

Keuntungan	Kerugian
1. Mudah untuk dikembangkan 2. Semua data perusahaan dapat terpusat menjadi suatu area kerja	1. Dapat terjadi tabrakan file data 2. Bila terjadi kabel putus pada komputer tingkat diatas, komputer tingkat dibawahnya tidak dapat digunakan

Sumber : www.ilmukomputer.org

2.2.5. Topologi Mesh

Topologi mesh adalah suatu bentuk hubungan antara perangkat dimana setiap perangkat terhubung secara langsung ke perangkat lainnya yang ada di dalam jaringan. Akibatnya, dalam topologi mesh setiap perangkat dapat berkomunikasi langsung dengan perangkat yang ditutup.



Sumber : www.ilmukomputer.com

Gambar II.7
Topologi Mesh

Table II.6
Keuntungan dan Kerugian Topologi Mesh

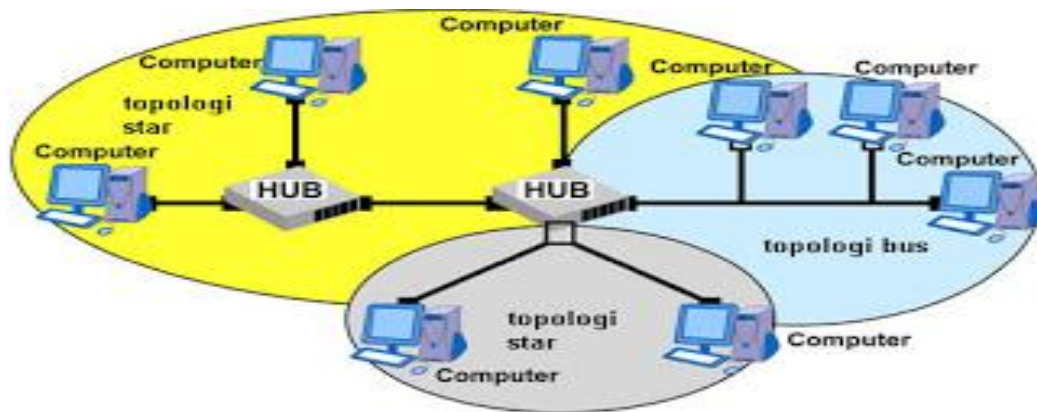
Keuntungan	Kerugian
1. Mampu menampung banyak pengguna yang aktif 2. Menjamin data langsung	1. Membutuhkan banyak kabel, sehingga mudah mengalami gangguan jaringan 2. Membutuhkan bnyak kabel da

dikirimkan ke komputer tujuan tanpa harus melalui komputer lainnya 3. Tidak mempengaruhi komputer lainnya jika salah satu kabel koneksi rusak 4. Memudahkan proses identifikasi permasalahan pada saat terjadi kerusakan koneksi antara computer	port
---	-------------

Sumber : www.ilmukomputer.org

2.2.6. Topologi Hybrid

Topologi *hybrid* adalah topologi yang tersusun dari beberapa topologi atau dapat dikatakan topologi *hybird* adalah topologi gabungan dari beberapa jenis topologi yang lainnya. Topologi *hybrid* terdiri dari kombinasi dua atau lebih topologi yang sedemikian rupa sehingga jaringan yang dihasilkan tidak menunjukkan salah satu dari standar topologi. Sebuah topologi *hybrid* selalu diproduksi ketika dua jaringan dasar yang berbeda terhubung. Dua contoh umum untuk jaringan hybrid adalah: jaringan bintang cincin dan jaringan bintang bus.



Sumber : www.ilmukomputer.com

Gambar II.8
Topologi Hybrid

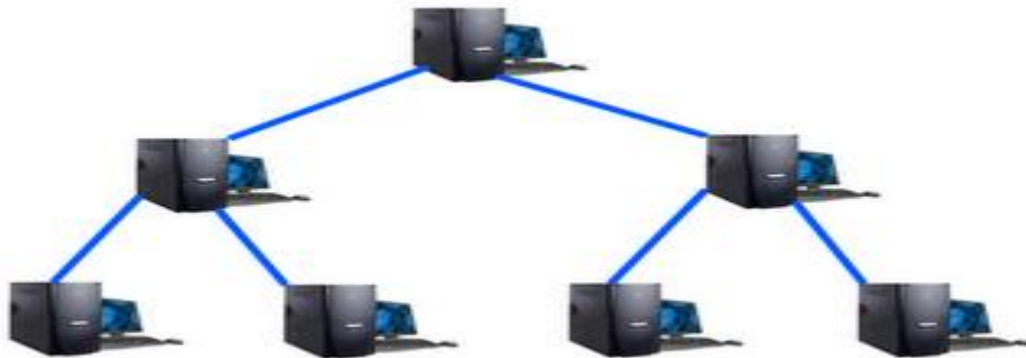
Table II.7
Keuntungan dan Kerugian Topologi *Hybrid*

Keuntungan	Kerugian
1. Fleksibilitas 2. Mengkombinasikan konfigurasi yang berbeda tapi dapat bekerja dengan sempurna untuk jumlah lalu lintas jaringan yang berbeda 3. Kecepatan konsisten	1. Pengelolaan topologi akan menjadi lebih sulit 2. Instalasi dan konfigurasi sangat sulit karena ada topologi yang berbeda yang harus dihubungkan satu sama lainnya

Sumber : www.ilmukomputer.org

2.2.7. Topologi Hierarki

Menurut Kristanto (2009:201) “topologi hierarki yaitu topologi berbentuk seperti pohon bercabang yang terdiri dari komputer induk (*host*) yang dihubungkan dengan simpul atau node lain secara berjenjang”. Topologi ini biasanya digunakan untuk interkoneksi antara sentral dengan hirarki yang berbeda. Topologi jaringan jenis ini cocok digunakan pada sistem jaringan komputer, terutama untuk jaringan WAN.



Sumber : www.ilmukomputer.org

Gambar II.9
Topologi Hierarki

Table II.8
Keuntungan dan Kerugian Topologi Hierarki

Keuntungan	Kerugian
1. Data terpusat secara hirarki sehingga manajemen data lebih baik dan mudah	1. Komputer dibawahnya tidak dapat dioperasikan apabila kabel pada komputer tingkat atasnya

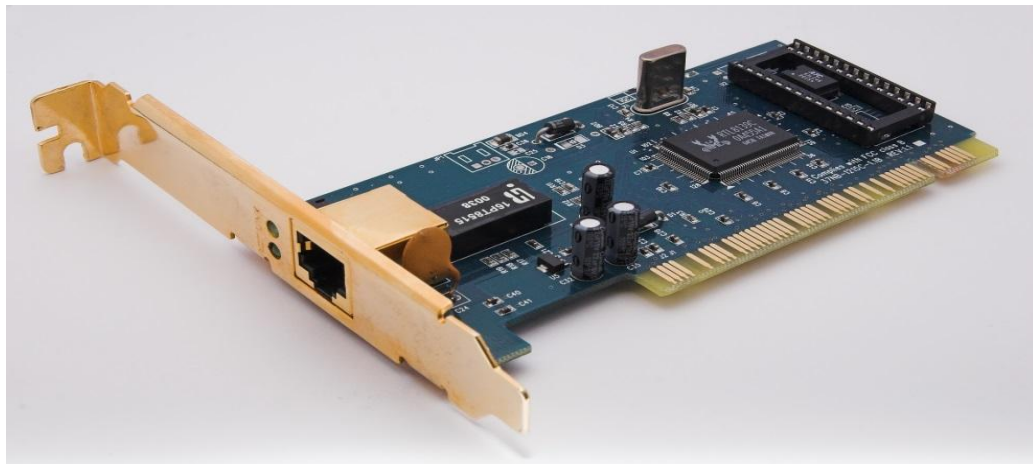
2. Mudah dikembangkan menjadi jaringan yang lebih luas	putus 2. Dapat terjadi tabrakan file
--	---

Sumber : www.ilmukomputer.org

2.3. Perangkat Keras Jaringan

2.3.1 Kartu Jaringan (LAN CARD)

Menurut Kurniawan (2007:38) “Kartu Jaringan merupakan perangkat paling utama yang harus terpasang pada komputer kita”. Setiap komputer dapat kita hubungkan dengan suatu jaringan melalui kartu jaringan. Dengan adanya kartu jaringan, proses tukar-menukar data atau informasi antara satu komputer dengan komputer yang lainnya dapat terjadi.



Sumber : www.jaringankomputer.org

Gambar II.10
Network Interface Card(NIC)

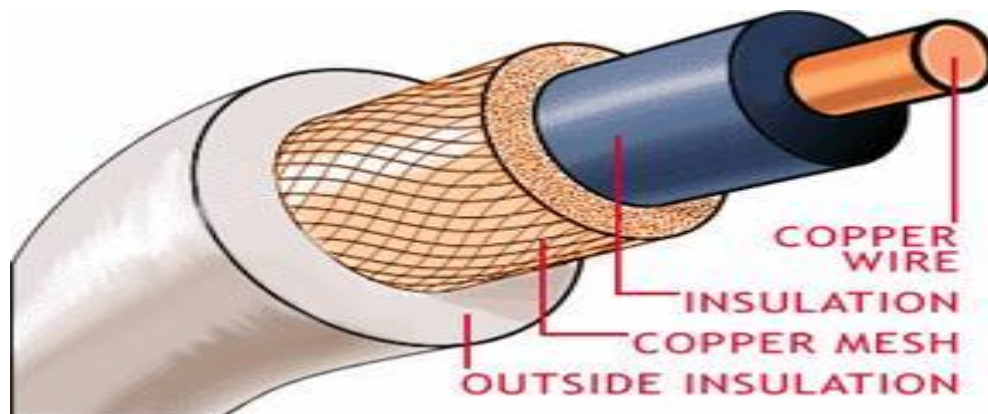
Kartu jaringan sering disebut juga LAN Card (*Local Area Network Card*), NIC Card (*Network Interface Card*), atau *Ethernet card*.

2.3.2 Kabel Jaringan

Komputer membutuhkan sebuah media transmisi untuk dapat terhubung dan melakukan segala bentuk kegiatan di jaringan. Berikut macam-macam bentuk kabel yang biasa digunakan dalam jaringan komputer :

A. Kabel Coaxial

Menurut Kurniawan (2007:39) “Kabel *coaxial* merupakan kabel yang hanya tersusun atas inti tembaga pada intinya, dan tertutup secara menyeluruh oleh bahan plastik insulator. Kabel *coaxial* dapat menghantarkan atau mengirimkan paket-paket data sampai jarak yang jauh menggunakan repeater”.



Sumber : www.sisilain.net

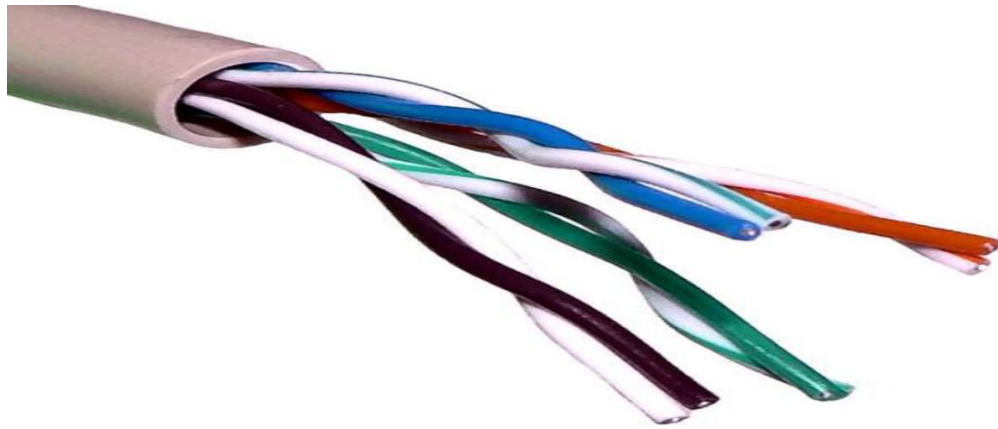
Gambar II.11
Kabel Coaxial

B. Kabel TP (Twisted Pair)

Menurut Kurniawan (2007:41) “Kabel TP (*Twisted Pair*) merupakan suatu kabel yang berintikan tembaga berukuran kecil”. Pada masing-masing kabel berisikan 8 buah kabel kecil dengan warna yang berbeda antara satu dengan yang lainnya. Pembedaan warna pada kabel bertujuan untuk mempermudah kita dalam memasukkannya pada konektor RG-45. Kabel TP terdiri dari dua macam, yaitu

1) Kabel UTP (*Unshielded Twisted Pair*)

Kabel UTP sering digunakan pada jaringan untuk menghubungkan komputer. Kelebihan kabel UTP adalah kecepatan transfer paket data hingga mencapai 100 Mbps, harga kabel UTP lebih murah, pemasangannya sangat sederhana, sehingga tidak memerlukan keahlian khusus untuk memasangnya, biaya perawatan dan perbaikannya cukup murah sehingga biaya investasi dapat kita minimalkan. Kekurangan dari kabel UTP adalah untuk memakai kabel UTP, panjang maksimum yang diperbolehkan dalam jaringan adalah 100 meter dan apabila lebih dari 10 meter maka paket-paket data yang kita kirimkan akan hilang di jalan sehingga tidak akan sampai pada tujuannya, kabel UTP tidak tahan terhadap gangguan cuaca dalam jangka waktu yang lama, apabila kabel UTP kita gunakan pada suatu jaringan yang luas dan besar akan terjadi penumpukan kabel pada satu titik tempat hal ini akan menyebabkan tempat tersebut kurang rapi dan akan terlihat seperti gudang kabel



Sumber : www.sisilain.net

Gambar II.12
Kabel UTP

2) Kabel STP (*Shieldded Twisted Pair*)

Seperti halnya kabel UTP, penggunaan kabel STP juga digunakan pada jaringan komputer. Kelebihan kabel STP adalah memilih kecepatan transfer paket data mencapai 155 Mbps, koneksinya lebih tahan lama terhadap gangguan elektrik daripada kabel UTP. Walaupun kabel STP lebih unggul dibandingkan dengan kabel UTP, tetapi kabel STP juga mempunyai beberapa kekurangan, di antaranya harganya lebih mahal dibandingkan kabel UTP, jarang ditemui di pasaran sehingga agak susah mendapatkannya, panjang maksimum yang diperbolehkan sama dengan kabel UTP, yaitu 100 meter, membutuhkan suatu konektor khusus untuk grounding-nya, kurang dapat mengatasi penyadapan dari pihak luar.



Sumber : www.sisilain.net

Gambar II.13
Kabel STP

Berdasarkan cara pemasangannya dengan LAN Card, kabel twisted pair dapat kita hubungkan dengan dua macam cara yaitu :

a. Metode straight

Metode *straight* digunakan untuk menghubungkan peralatan jaringan yang jenisnya berbeda, misalnya antara komputer dengan *hub/switch*. Pemasangannya atau pengkabelannya sama dengan kabel standar. Pemasangan kabel antara warna ujung satu dengan ujung yang lain sama dengan warna dari ujung kabel standart, tidak ada yang perlu kita ubah.

Tabel II.9
Penggunaan dan Pemasangan Kabel Straight

PIN Kabel	Ujung kabel A	Ujung Kabel B
1	Putih – Orange	Putih – Orange
2	Orange	Orange

3	Putih – Hijau	Putih – Hijau
4	Biru	Biru
5	Putih – Biru	Putih – Biru
6	Hijau	Hijau
7	Putih – coklat	Putih – coklat
8	Coklat	Coklat

Sumber : Modul LAB Teknik II

b. Metode Crossover

Metode *crossover* digunakan untuk menghubungkan peralatan jaringan yang sejenis, misalnya antar komputer dengan komputer, *hub* dengan *hub*. Kabel yang digunakan dalam jaringan hanya empat pin saja. Pin-pin kabel yang di pakai pin 1, pin 2, pin 3, dan pin 6. Dengan demikian pemasangan kabel crossover hanya dengan menyilangkan 4 buah pin tersebut, sedangkan kabel yang lainnya kita pasang sesuai dengan kabel standart.

Tabel II.10
Penggunaan dan Pemasangan Kabel Crossover

PIN Kabel	Ujung kabel A	Ujung Kabel B
1	Putih – Orange	Putih – Hijau
2	Orange	Hijau
3	Putih – Hijau	Putih – Orange
4	Biru	Biru
5	Putih – Biru	Putih – Biru

6	Hijau	Orange
7	Putih – coklat	Putih – coklat
8	Coklat	Coklat

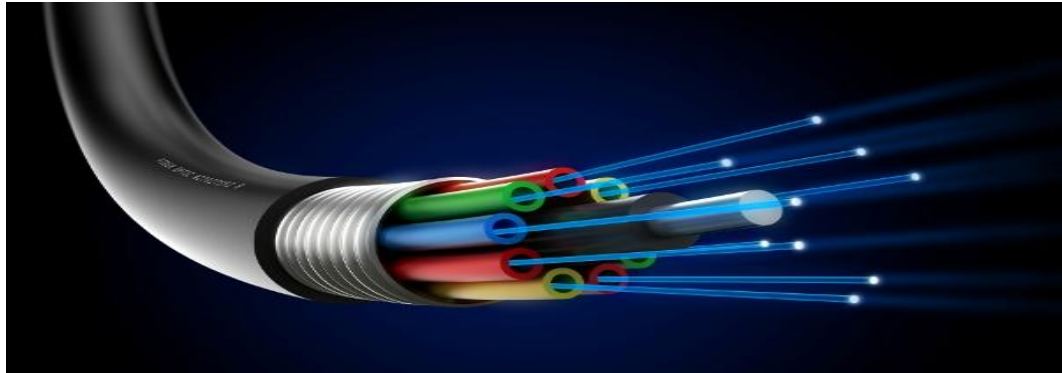
Sumber : Modul LAB Teknik II

C. Kabel Fiber Optik

Menurut Kurniawan (2007:47) Mengatakan bahwa “Kabel fiber optik suatu jenis kabel yang berisi serat optik yang sangat halus digunakan untuk mentransfer data pada jaringan komputer”. Pada inti kabel terdapat serat sebagai inti (*core*) atau sering dinamakan dengan *inner optik*. Inner optik ini dilapisi atau dilindungi oleh bahan gelas yang disebut dengan *cladding*. Pada fiber optik terdapat dua jenis sumber cahaya yang dapat digunakan untuk melakukan pensignalan, yaitu *Semiconductor Laser* dan *LED*. Kecepatan transfer kabel fiber optik dapat mencapai ratusan mega bit per detik (Mbps).

Keuntungan menggunakan kabel fiber optik adalah sangat stabil dan konstan dalam mengakses paket data, apabila terdapat suatu hambatan dalam pengiriman paket data biasanya kendala tersebut sangat kecil dan bukan hambatan yang berarti, kecepatan akses paket data sangat tinggi dapat mencapai 1 Gbps, apabila dalam suatu jaringan membutuhkan suatu *bandwith* dalam proses transmisi datanya maka fiber optik dapat dijadikan sebagai backbone. Dan kerugian menggunakan fiber optik adalah pemasangan dan pemeliharaan kabel memerlukan keahlian khusus, harganya lebih mahal dibandingkan kabel TP (*twisted pair*) maupun kabel *coaxial*, pemeliharaan kabel lebih sulit karena berada diluar ruangan

dan jarak yang jauh, perawatan kabel membutuhkan biaya investasi yang tidak sedikit sehingga pengguna rumahan jarang memakai fiber optik untuk media akses jaringannya.



Sumber : www.jaringankomputer.org

Gambar II.14
Kabel Fiber Optik

D. HUB

Menurut Kurniawan (2007:50) “*Hub* merupakan alat yang mempunyai fungsi sebagai tempat untuk menerima file-file dari komputer untuk kemudian meneruskannya ke komputer atau tempat lain pada suatu jaringan. Hub biasanya digunakan pada jaringan bertopologi star”. Batas maksimum paralel antar *hub* adalah tiga buah *hub*. Apabila jumlah paralel antar *hub* lebih dari tiga buah, maka untuk menghubungkan jaringan kita membutuhkan sebuah router. *Hub* kita hubungkan ke komputer menggunakan kabel UTP dengan konektor RJ-45 yang terpasang pada ujung-ujungnya.



Sumber : www.jaringankomputer.org

Gambar II.15
HUB

E. Switch

Menurut Kurniawan (2007:51) mengatakan bahwa “*Switch* adalah alat yang hampir sama dengan *hub*”. Akan tetapi keduanya memiliki perbedaan yaitu kecepatan akses *switch* lebih besar dibanding *hub*, *switch* hanya mentransfer data yang diterimanya kemudian meneruskan hanya pada port yang dituju saja dan adapun *hub* membroadcast data yang masuk pada semua port yang dimilikinya.

Untuk jaringan yang lebih luas seperti internet, *switch* masih tetap membutuhkan router untuk dapat meneruskan paket-paket data, sebagaimana *hub*. *Switch* juga mampu melakukan fungsi routing, sehingga dinamakan dengan IP *switch*. Namun demikian hanya beberapa *switch* saja yang melakukan hal ini.



Sumber : www.jaringankomputer.org

Gambar II.16
Switch

F. Repeater

Menurut Kurniawan (2007:52) “*Repeater* merupakan alat yang dapat menerima sinyal digital dan memperkuatnya untuk diteruskan kembali. *Repeater* juga dapat memperjauh jarak transmisi data”. Di samping itu, repeater dapat memperkecil *noise* pada sinyal transmisi yang datang. *Repeater* bekerja pada level *Physical Layer* dalam model jaringan OSI. Tugas utama dari *repeater* adalah menerima sinyal dari satu kabel LAN dan memancarkannya kembali ke kabel LAN yang lain.

G. Router

Menurut Kurniawan (2007:54) “*Router* merupakan suatu alat atau program aplikasi yang berfungsi menentukan pada titik mana suatu paket data harus diteruskan ke jaringan yang lain”. *Router* akan memilih jalan terdekat untuk melewati paket aplikasi data. Aplikasi-aplikasi yang berada pada *router*, jika

telah terinstall pada sebuah komputer dinamakan *PC Router*. *Router* bekerja pada level *network layer* pada model jaringan OSI. *Router* dapat kita gunakan untuk menghubungkan sejumlah LAN, sehingga trafik yang dibangkitkan oleh sebuah LAN akan terisolasi dengan baik dari trafik LAN lain. Fungsi utama *router* adalah untuk m-routing-kan paket-paket data dengan suatu segmen jaringan yang berbeda. Pada hubungan jaringan yang lebih global seperti internet, diperlukan adanya *router*. *Router* dapat berfungsi ganda, salah satunya adalah sebagai *firewall*.

Keuntungan menggunakan *router* yaitu dapat digunakan pada topologi jaringan apapun, dalam *router* terdapat suatu trafik *broadcast* yang dapat memperkecil beban *network*, *router* tidak peka terhadap masalah kelambatan waktu seperti yang dialami jika menggunakan *bridge*, *router* dapat menentukan jalur optimal antar dua sistem dan mengatur prioritas antar protokol. Dan kerugian dari *router* adalah pada lapisan *network OSI* hanya mampu meneruskan trafik yang sesuai dengan protokol yang diimplementasikan padanya saja, penggunaan tabel *routing* statik menyebabkan beberapa sistem dapat terjangkau oleh sistem yang lain, *router* lebih kompleks dan pemrosesan pada *router* lebih besar daripada *bridge*, sehingga keluaran yang dihasilkan dapat lebih rendah daripada *bridge*, apabila memindahkan suatu jaringan LAN ke jaringan LAN yang lain maka alamat *network* tersebut juga berubah.



Sumber : www.jaringankomputer.org

Gambar II.17
Router

H. Modem

Menurut Kurniawan (2007:55) “Modem merupakan kependekan dari *Modulator Demodulator*. Alat ini memungkinkan PC, *mini Computer*, atau *mainframe* untuk menerima dan mengirimkan paket data dalam bentuk digital melalui saluran telepon. Modem digunakan untuk menghubungkan PC dengan internet. Cara menghubungkan PC dengan internet ada beberapa macam, yaitu dengan menggunakan line telepon, kabel modem , satelit, ADSL (*Asymmetric DigitalSubscriber Line*) dan lain sebagainya. Terdapat dua macam modem yang dapat kita gunakan, yaitu modem internal dan modem eksternal.

Modem internal berupa sebuah kartu yang dapat kita pasangkan pada salah satu slot komputer dan menggunakan *power supply* dari PC. Sedangkan, Modem eksternal biasanya terletak di dalam case tersendiri, menggunakan *power supply* terpisah , dan pada umumnya memiliki adaptor. Modem eksternal tersambung pada komputer menggunakan kabel serial yang terkoneksi pada port serial di bagian belakang PC



Sumber : www.computer.howstuffworks.com

Gambar II.18
Modem

I. Access Point

Menurut Kurniawan (2007:58) “*Access Point* merupakan alat terpenting dalam membangun jaringan *wireless* maupun jaringan *hostpot*”. Pada dasarnya *access point* merupakan *hub* untuk *wireless* dan *bridge* untuk jaringan LAN UTP. Oleh karena itu, biasanya pada *access point* terdapat port untuk konektor RJ-45.

Untuk menghindari *collision* atau tabrakan antar data baik yang diterima maupun yang dikirim, *access point* menggunakan media *access Carrier Sense Access With Collision Avoidance* atau biasa disebut dengan *CSMA/CA*. Secara standarisasi, *access point* bekerja pada lapisan *Data Link* dan lapisan fisik dari standarisasi *OSI*, sehingga protokol komunikasi atau transfer datanya masih memakai protokol TCP/IP.



Sumber : www.jaringankomputer.org

Gambar II.19
Access Point

3.4. Perangkat Lunak Jaringan

3.4.1 Virtual Private Network

Menurut Wijaya (2011:177) Mengatakan bahwa “*Virtual Private Network* (VPN) adalah fasilitas yang memungkinkan koneksi jarak jauh (remote akses) yang aman dengan menggunakan jaringan internet untuk akses ke LAN di kantor”.

VPN menggunakan jaringan internet sehingga koneksi dengan fasilitas VPN dapat dilakukan dengan koneksi internet yang sudah tersedia, seperti ADSL atau fasilitas *broadband* lainnya. Penggunaan VPN menjadi sangat populer saat ini karena VPN memberikan jaminan keamanan yang hampir sama dengan jaringan pribadi. Penggunaan VPN menjamin keamanan yang tinggi karena koneksi dengan VPN dilakukan dengan peralatan yang menerapkan metode autentikasi untuk memberi

identitas kepada pemakai dan data yang dikirimkan lewat VPN dienkripsikan. Berbagai metode *enkripsi* dan autentikasi yang dapat dipakai, seperti *IPSEC*, *IKE*, dan *ISAKMP*.

a. Enkripsi dan Autentikasi

1) IPSEC

Menurut Wijaya (2011:180) Mengatakan bahwa “*IPSec* menyediakan jalur *enkripsi* yang menggunakan *Security Association (SA)* antara *remote IPSec peer* menggunakan sejumlah protokol yang bekerja pada lapisan *network OSI* untuk menjaga keamanan data”. SA tersebut menentukan protokol dan algoritma yang akan diterapkan pada paket data yang dikirimkan. *IPSec* menyediakan dua protokol *security*, yaitu *Authentication Header (AH)* dan *Encapsulation Security Payload (ESP)*. Pada dasarnya *IPSec* bekerja berdasarkan konsep “*shared secret*” (rahasia bersama) antara dua peralatan yang ingin saling bertukaran informasi dengan aman. *IPSec* beroperasi dalam dua phase :

- a) Phase-1 mengatur negosiasi parameter *security* yang diperlukan untuk membina jalur aman antara kedua *IPSec peer*.
- b) Phase-2 menggunakan jalur aman yang telah dibina pada phase-1 untuk melakukan pertukaran parameter *security* yang akan dipakai untuk mengirim data lewat jalur aman VPN tersebut.

2) IKE dan ISAKMP

Fungsi *Internet Key Exchange (IKE)* adalah untuk memungkinkan peralatan saling menukar informasi yang diperlukan guna komunikasi yang aman. Ini termasuk penggunaan kunci yang dienkripsi (*cryptographic keys*) untuk membuat kode (*encoding*) autentikasi informasi.

Menurut Wijaya (2011:181) Mengatakan bahwa “*IKE* adalah protokol *security* yang mempergunakan *IPSec* sehingga memungkinkan peralatan yang mendukung *IPSec* untuk saling menukar *Security Association (SA)* menggunakan protokol AH dan ESP”. *Internet Security Association and Key Protocol (ISAKMP)* yang menyediakan bingkai kerja (*frame work*) untuk pertukaran *encryption key* dan *security association*. *ISAKMP* menentukan prosedur untuk pembuatan, perundingan, perubahan dan penghapusan *security association*. Untuk pertukaran *encryption key*, *ISAKMP* menggunakan kombinasi protokol *Oakley dan Skeme*.

3) DES dan 3Des

Menurut Wijaya (2011:181) Mengatakan bahwa “*Data Encryption Standart (DES)* dan *3DES* adalah dua metode enkripsi yang sering dipergunakan pada koneksi dengan VPN”. DES mempergunakan algoritma enkripsi 56-bit untuk mengenkripsi data. DES merupakan metod enkripsi yang sangat matang sehingga banyak dipergunakan. *3DES* mempergunakan algoritma enkripsi 168-bit untuk mengenkripsi data, sehingga memberikan tingkat keamanan yang tinggi. Tetapi *3DES* memiliki keburukan karena memerlukan waktu yang lebih lama dan memerlukan sumber daya yang lebih tinggi untuk memproses data.

b. Tipe Koneksi dengan VPN

Dilihat dari cara koneksinya, VPN dapat dibagi atas dua tipe :

1. Site to Site VPN

Tipe VPN ini membuat jalur aman dan tetap antar *site* dengan *site*, misalnya antar kantor pusat dengan kantor-kantor cabang lewat jalur internet.

2. Remote User VPN

Tipe VPN ini memungkinkan koneksi dari jauh oleh *remote user*, misalnya pegawai yang sedang bertugas di luar kota atauluar negri untuk dapat akses ke LAN di kantor pusat menggunakan jaringan internet. Hal ini terutama sangat berguna untuk dapat menerima email yang tersedia di LAN kantor pusat.

3.4.2 Operating System

Perangkat Lunak merupakan program-program yang ada dalam komputer yang berguna untuk menjalankan suatu pekerjaan sesuai dengan yang dikehendaki. Salah satunya yaitu *Operating System* (OS). Menurut SP Hariningsih (2006:1) “*Operating System* atau sistem operasi ialah bagian dari system software yang umumnya terdiri dari program aplikasi, penerjemah bahasa. Disebut sebagai penerjemah karena dalam sistem komputer hanya mengenal bahasa mesin yang biasa disebut dengan kode bit 1 dan bit 0”.

Jika sistem komputer terbagi dalam lapisan-lapisan, maka Sistem Operasi adalah penghubung antara lapisan *hardware* dan lapisan *software*. Lebih dari itu,

sistem operasi melakukan semua tugas-tugas penting dalam komputer, dan menjamin aplikasi-aplikasi yang berada dapat berjalan secara bersamaan dengan lancar. Sistem operasi menjamin aplikasi *software* lainnya menggunakan memori, melakukan *input* dan *output* terhadap peralatan lain, dan memiliki akses kepada sistem file. Apabila beberapa aplikasi berjalan secara bersamaan, maka sistem operasi mengatur *schedule* yang tepat, sehingga mungkin semua proses yang berjalan mendapatkan waktu yang cukup untuk menggunakan *prosesor* (CPU) serta tidak saling mengganggu. Beberapa contoh sistem operasi adalah DOS, Linux, Windows.

3.4.3 Mikrotik

Menurut Athailah (2013:18) Mengatakan bahwa “Mikrotik adalah sebuah perangkat lunak pada sebuah perangkat jaringan yang mana digunakan untuk mengontrol jaringan, mengatur bandwidth dan untuk routing”. Dari pada perkembangannya sistem operasi mikrotik ini mempunyai fitur-fitur yang sangat lengkap, diantaranya:

1. *Firewal* dan NAT
2. *Routing-Static Routing*
3. *Hostpot*
4. *Point-to-o\point tunneling protocols (PPTP)*
5. *Simple Tunnels*
6. *IPSec*
7. *DHCP*

8. Dan *tools* jaringan lainnya

Itulah yang fitur-fitur atau *service* yang paling banyak digunakan pada saat ini. Pada perkembangannya sekarang Mikrotik juga membuat perangkat router yang diberi nama RouterBoard Mikrotik dan juga di install pada sebuah PC, dikenal menjadi PC Router Mikrotik. Jika dibandingkan dengan vendor lain RouterBoard Mikrotik jauh lebih ekonomis dengan fitur-fitur yang sama dengan vendor lain.

3.5 TCP/IP dan Subnetting

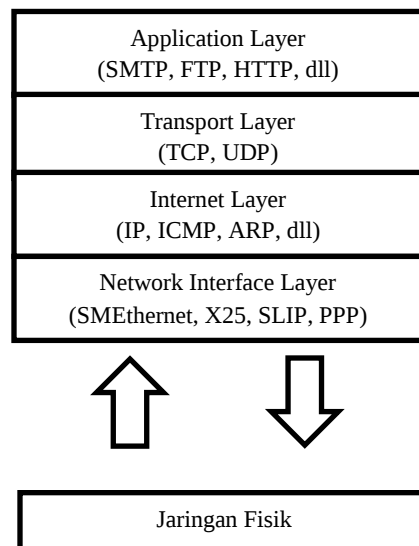
1. TCP/IP

protokol TCP/IP dikembangkan pada akhir dekade 1970-an hingga 1980-an sebagai sebuah protokol standar untuk menghubungkan komputer-komputer dan jaringan untuk membentuk sebuah jaringan yang luas. TCP/IP merupakan sebuah standar jaringan terbuka yang bersifat independen terhadap mekanisme *transport* jaringan fisik yang digunakan, sehingga dapat digunakan di aman 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 *heteogen*.

TCP/IP adalah standar komunikasi data yang digunakan oleh komunitas internet dalam proses tukar menukar data dari satu komputer ke komputer lain 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.

Menurut Kurniawan (2007:6) Mengatakan bahwa “TCP/IP (*Transport Control Protocol/Internet Protocol*) adalah salah satu protokol atau standar aturan jaringan yang sering digunakan pada jaringan berskala besar dan luas. TCP/IP dipakai karena bersifat fleksible dan mudah digunakan”. TCP/IP terdiri dari beberapa lapisan protokol.



Sumber : Kurniawan (2007:7)

Gambar II.20
Layer TCP/IP

Table II.11
Layer TCP/IP

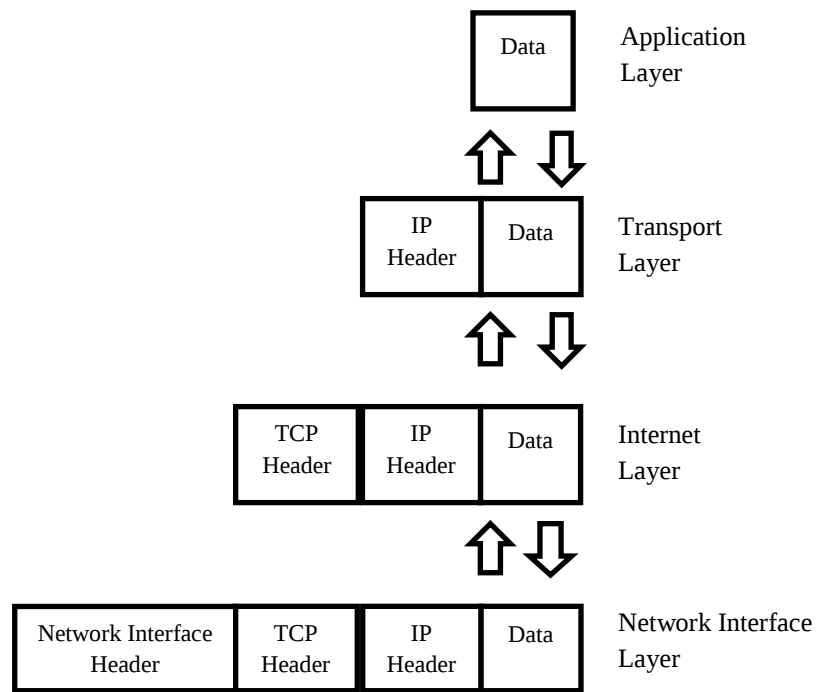
Lapisan ke-	Nama Lapisan	Keterangan

1	Application Layer	Bertanggung jawab untuk menyediakan akses kepada aplikasi terhadap layanan jaringan TCP/IP. Protokol ini mencakup protokol <i>Dynamic Host Configuration Protocol(DHCP)</i> , <i>Domain Name System (DNS)</i> , <i>Hypertext Transfer Protocol (HTTP)</i> , <i>File Transfer Protocol (FTP)</i> , <i>Telnet</i> , <i>Simple Mail Transfer Protocol (SMTP)</i> , <i>Simple Network Management Protocol (SNMP)</i> , dan masih banyak protokol lainnya. Dalam beberapa implementasi stack protokol, seperti halnya <i>Microsoft TCP/IP</i> , protokol-protokol lapisan aplikasi berintraksi dengan menggunakan antarmuka <i>Windows Sockets (winsock)</i> atau <i>NetBIOS over TCP/IP (NetBT)</i> .
2	Transfer Layer	Berguna untuk membuat komunikasi menggunakan sesi koneksi yang bersifat <i>connection-oriented</i> atau <i>broadcast</i> yang bersifat <i>connectionless</i> . Protokol dalam lapisan ini adalah <i>Transmission Control Protocol (TCP)</i> dan <i>User Datagram Protocol (IGMP)</i> .
3	Internet Layer	Bertanggung jawab untuk melakukan pemetaan (<i>routing</i>) dan <i>enkapsulasi</i> paket-paket dan jaringan

		menjadi paket-paket IP. Protokol yang bekerja dalam lapisan ini adalah <i>Internet Control Message Protocol (ICMP)</i> , dan <i>Internet Group Message Protocol (IGMP)</i> .
4	Network Interface Layer	Bertanggung jawab untuk meletakkan <i>frame-frame</i> jaringan di atas media jaringan yang digunakan. TCP/IP dapat bekerja dengan banyak teknologi <i>transport</i> , mulai dari teknologi <i>transport</i> dalam LAN (seperti halnya <i>Ethernet</i> dan <i>Token Ring</i>).

Sumber : Kurniawan (2007:6)

Dalam TCP/IP, terjadi penyampaian data dari protokol yang berbeda di satu *layer* ke protokol yang berada di *layer* yang lain. Setiap protokol memperlakukan informasi yang diterimanya dari protokol lain sebagai data. Jika suatu protokol menerima data dari protokol lain di *layer* atasnya dan ia akan menambahkan informasi tambahan miliknya ke data tersebut. Jika data ini dianggap valid, protokol akan melepas informasi tambahan tersebut, untuk kemudian meneruskan data itu ke protokol lain yang berada pada *layer* di atasnya.



Sumber : Kurniawan (2007:8)

Gambar II.21
Pergerakan data dalam layer TCP/IP

Menurut Waloea (2012:65) Mengatakan bahwa “IP Address adalah deretan angka biner antara 32-bit sampai 128-bit yang di pakai sebagai alamat identifikasi untuk tiap komputer host dalam jaringan internet”. Panjang angka ini adalah 32-bit untuk IP versi 4 dan 128-bit IP versi 6. Jumlah IP Address yang tersedia secara teoritis adalah $255 \times 255 \times 255 \times 255$ atau sekitar 4 milyar lebih yang harus dibagikan ke seluruh pengguna jaringan internet di seluruh dunia, karena jumlahnya yang banyak itulah maka di perlukan pembagian kelas untuk mempermudah alokasi IP Address, baik untuk host atau jaringan dan untuk keperluan tertentu. Perbedaan tiap kelas terletak pada ukuran dan jumlahnya. Contohnya IP kelas A di pakai oleh sedikit jaringan namun jumlah host yang dapat ditampung oleh tiap jaringan sangat besar.

Perangkat lunak internet protokol menentukan pembagian jenis kelas ini dengan menguji beberapa bit pertama dari *IP Address*. Penentuan kelas ini dilakukan dengan cara berikut :

Bit pertama *IP Address* kelas A adalah 0, dengan panjang *network ID* 8 bit dan panjang *host ID* 24 bit. Jadi bit pertama *IP Address* kelas A mempunyai range dari 0-127, jadi pada kelas A terdapat 127 *network* dengan tiap *network* dapat menampung sekitar 16 juta *host* ($255 \times 255 \times 255$). *IP Address* kelas A diberikan untuk jaringan dengan *host* yang sangat besar, IP kelas ini dapat dilukiskan pada gambar berikut :

IP Address terdiri dari 32 bit angka biner yang dapat dituliskan sebagai empat kelompok angka desimal yang dipisahkan oleh titik, seperti 192.168.0.1.

Tabel II.12
Contoh *IP Address*

Network ID			Host ID
192	168	0	1

Sumber : http://mikrotik.co.id/artikel_lihat.php?id=64

IP Address terdiri atas dua bagian yaitu *network ID* dan *host ID*. *Network ID* menentukan alamat jaringan komputer, sedangkan *host ID* menentukan alamat *host* (komputer, *router*, *switch*). Jika kita mempunyai 2 atau 3 komputer, maka pada *host ID* dapat dituliskan 192.168.0.1 kemudian 192.168.0.2 dan 192.168.0.3. oleh sebab itu, *IP Address* memberikan alamat lengkap suatu *host* beserta alamat jaringan di mana *host* itu berada.

Untuk mempermudah pemakai maka *IP Address* dibagi dalam tiga kelas. Namun untuk jaringan LAN, protokol yang digunakan biasanya adalah kelas C. Berikut adalah tabel pembagian kelas *IP Address*.

Tabel II.13
Pembagian kelas *IP Address*

Kelas	Dari	Sampai
A	0.0.0.0	127.255.255.255
B	128.0.0.0	191.255.255.255
C	192.0.0.0	223.255.255.255

Sumber : http://mikrotik.co.id/artikel_lihat.php?id=64

IP Address kelas A diberikam untuk jaringan dengan jumlah *host* yang sangat besar. Range IP-nya 1.xxx.xxx.xxx – 126.xxx.xxx.xxx, terdapat 16.777.214 (16 juta) *IP Address* pada kelas A. Pada *IP Address* kelas A, *network ID* ialah 8 bit pertama, sedangkan *host ID* ialah 24 bit berikutnya, Dengan demikian, cara membaca *IP Address* kelas A, misalnya 111.77.77.8 ialah :

Network ID = 111

Host ID = 77.7.8

Sehingga *IP Address* di atas berarti *Host ID*-nya adalah 77.7.8 sedangkan 111 merupakan *Network ID*-nya.

IP Address kelas B biasanya dialokasikan untuk jaringan berukuran sedang dan besar. Pada *IP Address* kelas B, *network ID* ialah 16 bit pertama, sedangkan *host ID*

ialah 16 bit berikutnya. Dengan demikian, cara membaca *IP Address* kelas B, misalnya 135.92.127.1

Network ID = 135.92

Host ID = 127.1

Sehingga *IP Address* di atas berarti *Host ID*-nya 127.1 sedangkan *network ID*-nya adalah 135.92. *Network* dengan *IP Address* kelas B dapat menampung sekitar 65000 *host*. *Range IP* 128.0.xxx.xxx – 191.155.xxx.xxx.

IP Address kelas C awalnya digunakan untuk jaringan berukuran kecil (LAN). *Host ID* ialah 8 bit terakhir. Dengan konfigurasi ini, bisa dibentuk sekitar 2 juta *network* dengan masing-masing *network* memiliki 256 *IP Address*. *Range IP* 192.0.0.xxx – 223.255.255.xxx. pengalokasian *IP Address* pada dasarnya ialah proses memiliki *network ID* dan *host ID* yang tepat untuk suatu jaringan. Tepat atau tidaknya konfigurasi ini tergantung dari tujuan yang hendak dicapai, yaitu mengalokasikan *IP Address* seefisien mungkin.

2. Subnetting

Menurut Kurniawan (2007:75) Mengatakan bahwa “*Subnetting* adalah pembagian suatu kelompok alamat IP menjadi beberapa *networkID* lain dengan jumlah anggota jaringan yang lebih kecil, *subnet* (Subnetwork)”.

Subnetting merupakan proses yang dilakukan guna memudahkan administrator jaringan dan akan meningkatkan kinerja kerja. Hal ini berkaitan dengan cakupan

jaringan yang tadinya luas telah di kelompok-kelompokan menjadi kecil, dan juga tidak membebankan jaringan dengan alamat-alamat yang tidak digunakan.

Table II.14
Renteng IP Address Setiap Kelas

Kelas	Alamat Awal	Alamat Akhir
A	XXX.0.0.1	XXX.255.255.255
B	XXX.XXX.0.1	XXX.XXX.255.255
C	XXX.XXX.XXX.1	XXX.XXX.XXX.255

Sumber : www.jaringankomputer.org

Tujuan dalam melakukan *subnetting* adalah

- Membagi suatu kelas *network* atas sejumlah *subnetwork* dengan membagi suatu kelas jaringan menjadi bagian-bagian yang lebih kecil.
- Menempatkan suatu *host*, apakah berada dalam suatu jaringan atau tidak.
- Untuk mengatasi masalah perbedaan *hardware* dengan topologi fisik jaringan agar pengguna *IP Address* lebih efisien.

Tabel II.13
Jumlah Network ID dan Host ID

Kelas	Rentang IP Address	Jumlah Jaringan	Jumlah Host Jaringan
A	1 s.d. 126	126	16.777.214
B	128 s.d. 191	16.384	65.534
C	192 s.d. 223	2.097.152	254

Sumber : www.jaringankomputer.org

Table II.14
Subnet Mask untuk Internets Address Kelas

Kelas	Alamat Awal	Alamat Akhir
A	11111111.00000000.00000000.00000000	255.0.0.0
B	11111111.11111111.00000000.00000000	255.255.0.0
C	11111111.11111111.11111111.00000000	255.255.255.0

Sumber : www.jaringankomputer.org

3.6 Sistem Keamanan Jaringan

Satu hal yang perlu diingat bahwa tidak ada jaringan yang anti sadap atau tidak ada jaringan komputer yang benar-benar aman. Sifat dari jaringan adalah melakukan komunikasi. Setiap komunikasi dapat jatuh ke tangan orang lain dan di salah gunakan, sistem keamanan membantu mengamankan jaringan tanpa menghalangi penggunaannya dan menempatkan antisipasi ketika jaringan berhasil di tembus. Salah satu sistem keamanan jaringan komputer adalah *firewall*.

Menurut Waloea (2012:81) Mengatakan bahwa “*Firewall* adalah sebuah sistem atau perangkat untuk mengizinkan lalu lintas jaringan yang dianggap aman dan mencegah lalu lintas jaringan yang dianggap tidak aman. *Firewall* adalah suatu mekanisme untuk melindungi keamanan jaringan komputer dengan menyaring paket data yang keluar dan masuk di jaringan”. Paket data yang “baik” diperbolehkan untuk melewati jaringan dan paket yang dianggap “jahat” tidak di perbolehkan melewati jaringan. *Firewall* bekerja dengan mengamati paket IP atau *Internet Protocol* yang

melewatinya. Berdasarkan konfigurasi dari *firewall* maka akses dapat diatur berdasarkan *IP address*, *port*, dan arah informasi. Detail dari konfigurasi bergantung kepada masing-masing *firewall*. *Firewall* dapat berupa perangkat lunak atau perangkat keras untuk memfilter paket data.

Firewall juga terbagi menjadi dua jenis, yaitu:

1. Personal Firewall

Personal *firewall* didesain untuk melindungi sebuah komputer yang terhubung ke jaringan dari akses yang tidak dikehendaki. *Firewall* jenis ini seiring waktu berevolusi menjadi sebuah kumpulan program yang bertujuan untuk mengamankan komputer secara total dengan ditambahkannya beberapa fitur pengaman tambahan, semacam perangkat proteksi terhadap virus, anti-spyware, anti-spam, dan lainnya. Personal *Firewall* secara umum hanya memiliki dua fitur utama, yakni *packet filtering firewall* dan *stateful firewall*.

2. Network Firewall

Network *Firewall* di desain untuk melindungi jaringan secara keseluruhan dari berbagai serangan. Umumnya di jumpai dalam dua bentuk, yakni sebagai perangkat yang terdedikasi atau sebagai sebuah perangkat lunak yang diinstalasikan dalam sebuah server. *Network Firewall* secara umum memiliki beberapa fitur utama, yakni Personal *Firewall* (*packet filter firewall* dan *stateful firewall*), *circuit Level Gateway*, *Application Level Gateway*, dan *NAT Firewall*.