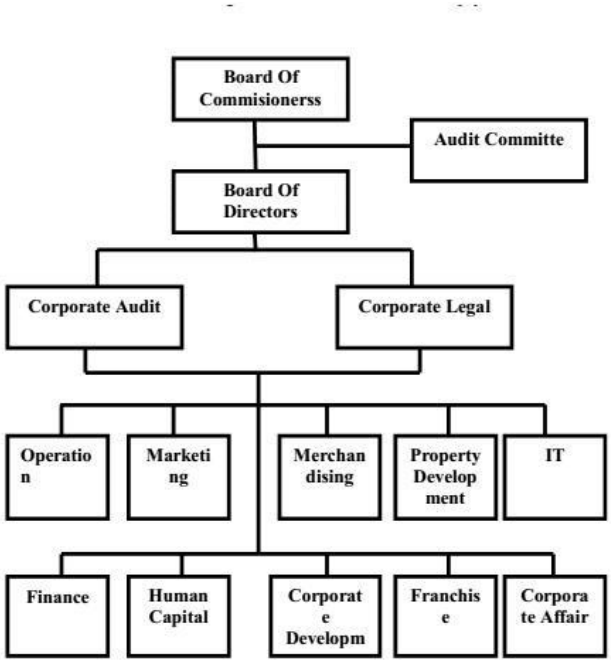
BAB 2

LANDASAN TEORI

2.1 Sejarah Instansi

XYZ Mart didirikan pada tahun 1989. Mengawali usahanya di bidang perdagangan dan distribusi, kemudian pada tahun 1999 mulai memasuki sektor minimarket. Ekspansi secara eksponensial dimulai perseroan pada tahun 2002 dengan mengakusisi 141 gerai XYZ Mart. Saat ini XYZ Mart merupakan salah satu yang terdepan dalam usaha ritel, dengan melayani lebih dari 2,1 juta pelanggan setiap harinya di hampir 10.600 gerai yang tersebar di Indonesia. XYZ Mart menyediakan barang-barang kebutuhan pokok dengan harga yang terjangkau, tempat belanja yang nyaman, serta lokasi yang mudah dijangkau. Didukung lebih dari 15.000 karyawan menjadikan XYZ Mart sebagai salah satu pembuka lapangan kerja terbesar di Indonesia.

2.1.1 Struktur Organisasi XYZ Mart



Gambar 2.1 Struktur Organisasi XYZ Mart

2.2 Jaringan Komputer

Jaringan komputer adalah interkoneksi antara 2 komputer *autonomous* atau lebih, yang terhubung dengan media transmisi kabel atau tanpa kabel (*wireless*).

Autonomous adalah apabila sebuah komputer tidak melakukan kontrol terhadap komputer lain dengan akses penuh, sehingga dapat membuat komputer lain, *restart, shutdowns*, kehilangan *file* atau kerusakan sistem.

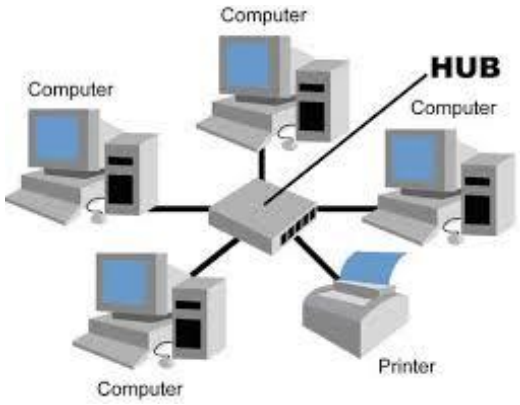
Dalam defenisi *networking* yang lain *autonomous* dijelaskan sebagai jaringan yang *independent* dengan manajemen sistem sendiri (punya admin sendiri), memiliki topologi jaringan, *hardware* dan *software* sendiri, dan dikoneksikan dengan jaringan *autonomous* yang lain. (Internet merupakan contoh kumpulan jaringan *autonomous* yang sangat besar.)

Dua unit komputer dikatakan terkoneksi apabila keduanya bisa saling bertukar data/informasi, berbagi *resource* yang dimiliki, seperti: *file, printer*, media penyimpanan (*hardisk, floppy disk*, cd-rom, *flash disk*, dll). Data yang berupa teks, audio maupun video, bergerak melalui media kabel atau tanpa kabel (*wireless*) sehingga memungkinkan pengguna komputer dalam jaringan komputer dapat saling bertukar file/data, mencetak pada printer yang sama dan menggunakan hardware/software yang terhubung dalam jaringan bersama-sama

Tiap komputer, printer atau periferal yang terhubung dalam jaringan disebut dengan *node*. Sebuah jaringan komputer sekurang-kurangnya terdiri dari dua unit komputer atau lebih, dapat berjumlah puluhan komputer, ribuan atau bahkan jutaan node yang saling terhubung satu sama lain.

Pada komputer terdapat pula beragam jenis jaringan komputer yang pembagiannya didasarkan pada besar kecilnya cakupan jaringan yang menghubungkan antar komputer. Jenis-jenis jaringan tersebut yaitu :

2.2.1 LAN (*Local Area Network*)



Gambar 2.2 Jaringan LAN

Local Area Network atau LAN, merupakan suatu Jenis Jaringan Komputer dengan mencakup wilayah lokal. Dengan menggunakan berbagai perangkat jaringan yang cukup sederhana dan populer, seperti menggunakan kabel UTP (*Unshielded Twisted-Pair*), Hub, Switch, Router, dan lain sebagainya.Contoh dari jaringan LAN seperti komputer-komputer yang saling terhubung di sekolah, di perusahaan, Warnet, maupun antar rumah tetangga yang masih mencakup wilayah LAN.

Keuntungan dari penggunaan Jenis Jaringan Komputer LAN seperti lebih irit dalam pengeluaran biaya operasional, lebih irit dalam penggunaan kabel, transfer data antar node dan komputer labih cepat karena mencakup wilayah yang sempit atau lokal, dan tidak memerlukan operator telekomunikasi untuk membuat sebuah jaringan LAN.

Kerugian dari penggunaan Jenis Jaringan LAN adalah cakupan wilayah jaringan lebih sempit sehingga untuk berkomunikasi ke luar jaringan menjadi lebih sulit dan area cakupan *transfer* data tidak begitu luas.

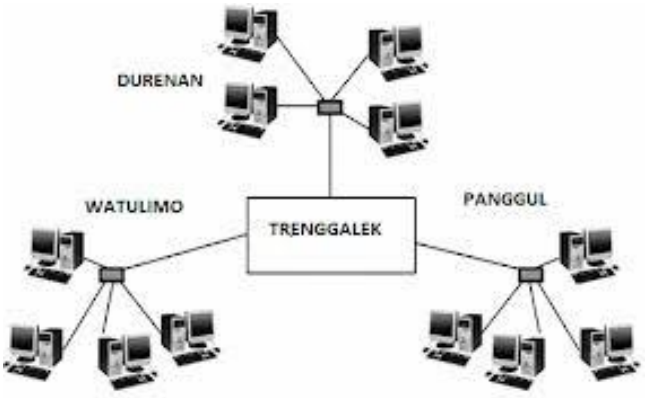
Pada sebuah LAN, setiap node atau komputer mempunyai daya komputasi sendiri, berbeda dengan konsep *dump terminal*. Setiap komputer juga dapat mengakses sumber daya yang ada di LAN sesuai dengan hak akses yang telah

diatur. Sumber daya tersebut dapat berupa data atau perangkat seperti printer. Pada LAN, seorang pengguna juga dapat berkomunikasi dengan pengguna yang lain dengan menggunakan aplikasi yang sesuai.

Berbeda dengan Jaringan Area Luas atau *Wide Area Network* (WAN), maka LAN mempunyai karakteristik sebagai berikut :

1. Mempunyai pesat data yang lebih tinggi
2. Meliputi wilayah geografi yang lebih sempit
3. Tidak membutuhkan jalur telekomunikasi yang disewa dari operator telekomunikasi.

2.2.2 MAN (Metropolitan Area Network)



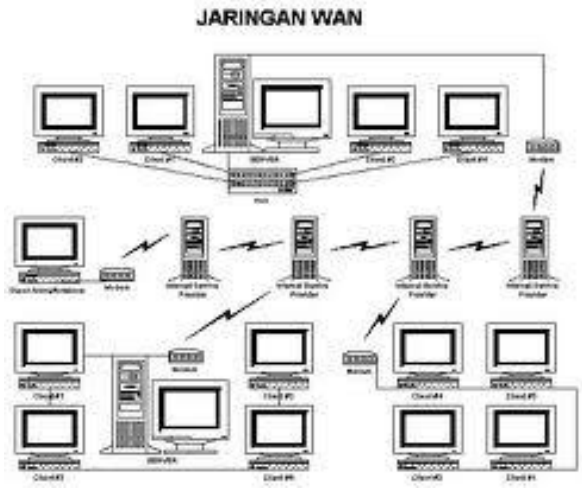
Gambar 2.3 Jaringan MAN

Metropolitan Area Network atau MAN, merupakan Jenis Jaringan Komputer yang lebih luas dan lebih canggih dari Jenis Jaringan Komputer LAN. Disebut Metropolitan Area Network karena Jenis Jaringan Komputer MAN ini biasa digunakan untuk menghubungkan jaringan komputer dari suatu kota ke kota lainnya. Untuk dapat membuat suatu jaringan MAN, biasanya diperlukan adanya operator telekomunikasi untuk menghubungkan antar jaringan komputer..

Keuntungan dari Jenis Jaringan Komputer MAN ini diantaranya adalah cakupan wilayah jaringan lebih luas sehingga untuk berkomunikasi menjadi lebih efisien, mempermudah dalam hal berbisnis, dan juga keamanan dalam jaringan menjadi lebih baik.

Kerugian dari Jenis Jaringan Komputer MAN seperti lebih banyak menggunakan biaya operasional, dapat menjadi target operasi oleh para *Cracker* untuk mengambil keuntungan pribadi, dan untuk memperbaiki jaringan MAN diperlukan waktu yang cukup lama..

2.2.3 WAN (Wide Area Network)



Gambar 2.4 Jaringan WAN

Wide Area Network atau WAN, merupakan Jenis Jaringan Komputer yang lebih luas dan lebih canggih daripada Jenis Jaringan Komputer LAN dan MAN. Teknologi jaringanWAN biasa digunakan untuk menghubungkan suatu jaringan dengan negara lain atau dari satu benua ke benua yang lainnya. Jaringan WAN bisa terdiri dari berbagai Jenis Jaringan Komputer LAN dan WAN karena luasnya wilayah cakupan dari Jenis Jaringan Komputer WAN. Jaringan WAN, biasanya

menggunakan kabel fiber optic serta menanamkannya di dalam tanah maupun melewati jalur bawah laut.

Keuntungan Jenis Jaringan Komputer WAN seperti cakupan wilayah jaringannya lebih luas dari Jenis Jaringan Komputer LAN dan MAN, tukar-menukar informasi menjadi lebih rahasia dan terarah karena untuk berkomunikasi dari suatu negara dengan negara yang lainnya memerlukan keamanan yang lebih, dan juga lebih mudah dalam mengembangkan serta mempermudah dalam hal bisnis.

Kerugian dari Jenis Jaringan WAN seperti biaya operasional yang dibutuhkan menjadi lebih banyak, sangat rentan terhadap bahaya pencurian data-data penting, perawatan untuk jaringan WAN menjadi lebih berat.

Lebih singkatnya WAN (*Wide Area Network*) merupakan jaringan komputer yang mencakup area yang besar sebagai contoh yaitu jaringan komputer antar wilayah, kota atau bahkan negara, atau dapat didefinisikan juga sebagai jaringan komputer yang membutuhkan *router* dan saluran komunikasi publik.

WAN digunakan untuk menghubungkan jaringan area lokal yang satu dengan jaringan lokal yang lain, sehingga pengguna atau komputer di lokasi yang satu dapat berkomunikasi dengan pengguna dan komputer di lokasi yang lain

2.2.4 Intranet

Intranet adalah sebuah jaringan komputer berbasis protokol TCP/IP seperti internet hanya saja digunakan dalam internal perusahaan, kantor, bahkan warung internet (WARNET) pun dapat di kategorikan Intranet. Antar Intranet dapat saling berkomunikasi satu dengan yang lainnya melalui sambungan Internet yang memberikan tulang punggung komunikasi jarak jauh. Akan tetapi sebetulnya sebuah Intranet tidak perlu

sambungan luar ke Internet untuk berfungsi secara benar. Intranet menggunakan semua protocol TCP/IP Protokol TCP/IP, alamat IP, dan protokol lainnya), klien dan juga server. Protokol HTTP dan beberapa protokol Internet lainnya (FTP, POP3, atau SMTP) umumnya merupakan komponen protokol yang sering digunakan. sebuah intranet dapat dipahami sebagai sebuah versi pribadi dari jaringan Internet, atau sebagai sebuah versi dari Internet yang dimiliki oleh sebuah organisasi.

2.2.5 Internet

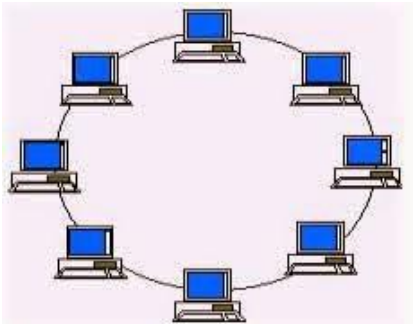
Interconnection network (internet) adalah sistem global dari seluruh jaringan komputer yang saling terhubung. Internet berasal dari bahasa latin "*inter*" yang berarti "antara". Internet merupakan jaringan yang terdiri dari milyaran komputer yang ada di seluruh dunia. Internet melibatkan berbagai jenis komputer serta topologi jaringan yang berbeda. Dalam mengatur integrasi dan komunikasi jaringan, digunakan standar protokol internet yaitu TCP/IP. TCP bertugas untuk memastikan bahwa semua hubungan bekerja dengan baik, sedangkan IP bertugas untuk mentransmisikan paket data dari satu komputer ke komputer lainya.

2.3 Topologi

Topologi menggambarkan struktur dari suatu jaringan atau bagaimana sebuah jaringan didesain. Pola ini sangat erat kaitannya dengan metode access dan media pengiriman yang digunakan. Topologi yang ada sangatlah tergantung dengan letak geofrapis dari masing-masing terminal, kualitas kontrol yang dibutuhkan dalam komunikasi ataupun penyampaian pesan, serta kecepatan dari pengiriman data. Dalam definisi topologi terbagi menjadi dua, yaitu topologi fisik (*physical topology*) yang menunjukan posisi pemasangan kabel secara fisik dan topologi logik (*logical topology*) yang menunjukan bagaimana suatu media diakses oleh host.

2.3.1 Topologi Ring

Pada topologi *ring* setiap komputer di hubungkan dengan komputer lain dan seterusnya sampai kembali lagi ke komputer pertama, dan membentuk lingkaran sehingga disebut ring, topologi ini berkomunikasi menggunakan data token untuk mengontrol hak akses komputer untuk menerima data, misalnya komputer 1 akan mengirim *file* ke komputer 4, maka data akan melewati komputer 2 dan 3 sampai di terima oleh komputer 4, jadi sebuah komputer akan melanjutkan pengiriman data jika yang dituju bukan *IP Address* dia.



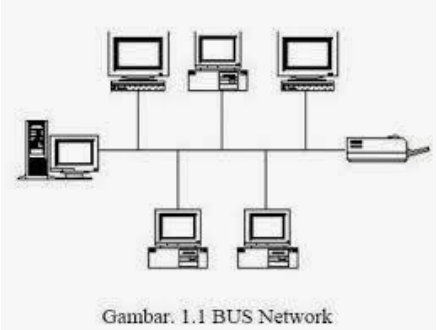
Gambar 2.5 Topologi Ring

- Kelebihan dari topologi jaringan komputer ring adalah pada kemudahan dalam proses pemasangan dan instalasi, penggunaan jumlah kabel lan yang sedikit sehingga akan menghemat biaya.
- Kekurangan paling fatal dari topologi ini adalah, jika salah satu komputer ataupun kabel nya bermasalah, maka pengiriman data akan terganggu bahkan *error*.

2.3.2 Topologi Bus

Topologi jaringan komputer bus tersusun rapi seperti antrian dan menggunakan cuma satu kabel *coaxial* dan setiap komputer

terhubung ke kabel menggunakan konektor BNC, dan kedua ujung dari kabel *coaxial* harus diakhiri oleh terminator.

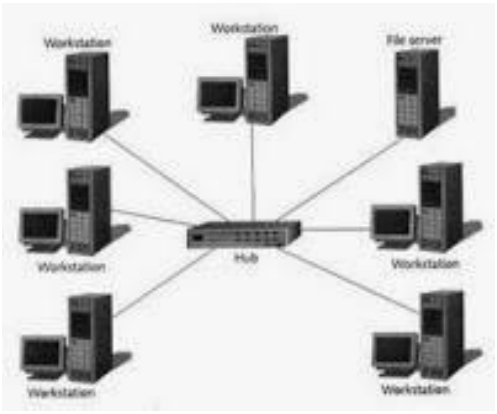


Gambar 2.6 Topologi Bus

- Kelebihan dari bus hampir sama dengan ring, yaitu kabel yang digunakan tidak banyak dan menghemat biaya pemasangan.
- Kekurangan topologi bus adalah jika terjadi gangguan atau masalah pada satu komputer bisa menggangu jaringan di komputer lain, dan untuk topologi ini sangat sulit mendeteksi gangguan, sering terjadinya antrian data, dan jika jaraknya terlalu jauh harus menggunakan repeater.

2.3.3 Topologi Star

Topologi ini membentuk seperti bintang karena semua komputer di hubungkan ke sebuah hub atau *switch* dengan kabel UTP, sehingga *hub/switch* lah pusat dari jaringan dan bertugas untuk mengontrol lalu lintas data, jadi jika komputer 1 ingin mengirim data ke komputer 4, data akan dikirim ke *switch* dan langsung di kirimkan ke komputer tujuan tanpa melewati komputer lain. Topologi jaringan komputer inilah yang paling banyak digunakan sekarang karena kelebihannya lebih banyak.

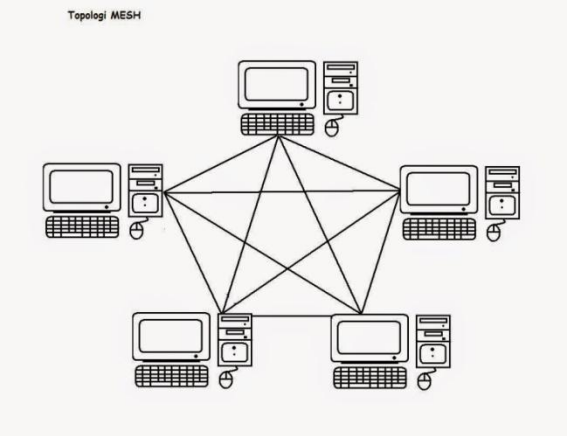


Gambar 2.7 Topologi Star

- Kelebihan topologi ini adalah sangat mudah mendeteksi komputer mana yang mengalami gangguan, mudah untuk melakukan penambahan atau pengurangan komputer tanpa mengganggu yang lain, serta tingkat keamanan sebuah data lebih tinggi, .
- Kekurangannya topologi jaringan komputer ini adalah, memerlukan biaya yang tinggi untuk pemasangan, karena membutuhkan kabel yang banyak serta *switch/hub*, dan kestabilan jaringan sangat tergantung pada terminal pusat, sehingga jika *switch/hub* mengalami gangguan, maka seluruh jaringan akan terganggu.

2.3.4 Topologi Mesh

Pada topologi ini setiap komputer akan terhubung dengan komputer lain dalam jaringannya menggunakan kabel tunggal, jadi proses pengiriman data akan langsung mencapai komputer tujuan tanpa melalui komputer lain ataupun *switch* atau hub.

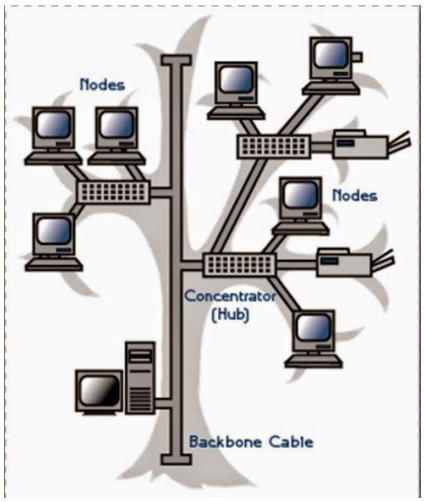


Gambar 2.8 Topologi Mesh

- Kelebihanya adalah proses pengiriman lebih cepat dan tanpa melalui komputer lain, jika salah satu komputer mengalami kerusakan tidak akan menggangu komputer lain.
- Kekurangan dari topologi ini sudah jelas, akan memakan sangat banyak biaya karena membutuhkan jumlah kabel yang sangat banyak dan setiap komputer harus memiliki *Port I/O* yang banyak juga, selain itu proses instalasi sangat rumit.

2.3.5 Topologi Tree

Topologi jaringan komputer Tree merupakan gabungan dari beberapa topologi star yang dihubungan dengan topologi bus, jadi setiap topologi star akan terhubung ke topologi star lainnya menggunakan topologi bus, biasanya dalam topologi ini terdapat beberapa tingkatan jaringan, dan jaringan yang berada pada tingkat yang lebih tinggi dapat mengontrol jaringan yang berada pada tingkat yang lebih rendah.



Gambar 2.9 Topologi Tree

- Kelebihan topologi tree adalah mudah menemukan suatu kesalahan dan juga mudah melakukan perubahan jaringan jika diperlukan.
- Kekurangan nya yaitu menggunakan banyak kabel, sering terjadi tabrakan dan lambat, jika terjadi kesalahan pada jaringan tingkat tinggi, maka jaringan tingkat rendah akan terganggu juga.

2.4 TCP/IP

TCP/IP (singkatan dari *Transmission Control Protocol*/*Internet Protocol*) adalah standarkomunikasi 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 diimplementasikan 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

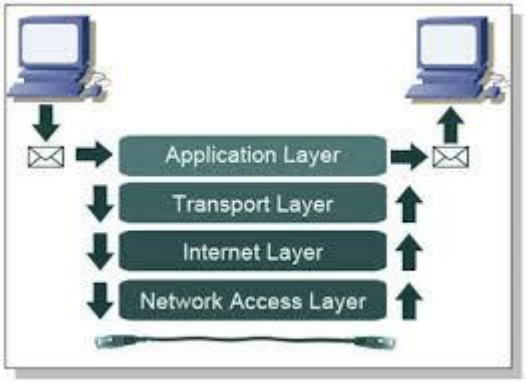
independen terhadap mekanisme transport jaringan fisik yang digunakan, sehingga dapat digunakan di mana saja. Protokol ini menggunakan skema pengalamatan yang sederhana yang disebut sebagai alamat IP (*IP Address*) yang mengizinkan hingga beberapa ratus juta komputer untuk dapat saling berhubungan satu 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.

TCP/IP pun mempunyai beberapa layer, layer-layer itu adalah :

1. IP (*internet protocol*) yang berperan dalam pentransmisian paket data dari node ke node. IP mendahului setiap paket data berdasarkan 4 byte (untuk versi IPv4) alamat tujuan (nomor IP). Internet authorities menciptakan range angka untuk organisasi yang berbeda. Organisasi menciptakan grup dengan nomornya untuk departemen. IP bekerja pada mesin gateaway yang memindahkan data dari departemen ke organisasi kemudian ke region dan kemudian ke seluruh dunia.
2. TCP (*transmission transfer protocol*) berperan didalam memperbaiki pengiriman data yang benar dari suatu klien ke server. Data dapat hilang di tengah-tengah jaringan. TCP dapat mendeteksi error atau data yang hilang dan kemudian melakukan transmisi ulang sampai data diterima dengan benar dan lengkap.

3. Sockets yaitu merupakan nama yang diberikan kepada subrutin paket yang menyediakan akses ke TCP/IP pada kebanyakan sistem.



Gambar 2.10 TCP/IP Layer

2.5 *IP Address*

IP Address adalah bilangan biner yang secara unik mengidentifikasi komputer dan perangkat lain pada TCP / IP network. Terdapat dua jenis Ip address yaitu *ip address private* yang digunakan pada jaringan area lokal (LAN) dan ip address publik yang digunakan di Internet.



Gambar 2.11 Public dan Private IP

Ada Dua standar pengalamatan *IP address* yang digunakan saat ini. Standar IPv4 yang paling familiar bagi masyarakat dan mendukung di hampir semua perangkat jaringan komputer saait ini,dan standar IPv6 secara bertahap

menggantikan Ipv4. Alamat IPv4 terdiri dari empat byte (32 bit), sedangkan alamat IPv6 adalah 16 byte (128 bit).

Ip address dirancang untuk memungkinkan satu komputer (atau perangkat digital lainnya) untuk berkomunikasi dengan yang lain melalui Internet maupun intranet. Ip address memungkinkan miliaran perangkat digital terhubung Internet dan di bedakan satu sama lain. Dalam arti yang sama bahwa seseorang membutuhkan alamat Anda untuk mengirimkan surat, begitu juga komputer membutuhkan alamat IP untuk berkomunikasi dengan komputer yang lain.

IP singkatan dari Internet Protokol, sehingga alamat IP adalah alamat Internet Protokol. Internet Protokol adalah seperangkat aturan yang mengatur aktivitas internet dan memfasilitasi penyelesaian berbagai tindakan pada *World Wide Web*. Oleh karena itu alamat Internet Protokol adalah bagian sistematis ditata jaringan interkoneksi yang mengatur komunikasi online dengan mengidentifikasi kedua perangkat memulai dan berbagai tujuan Internet, sehingga memungkinkan kedua perangkat dapat saling berkomunikasi.

2.5.1 Sistem Pengalamatan IP

Deretan angka biner antara 32-bit sampai 128-bit yang dipakai sebagai alamat identifikasi untuk tiap komputer host dalam jaringan Internet. Panjang dari angka ini adalah 32-bit (untuk IPv4 atau IP versi 4), dan 128-bit (untuk IPv6 atau IP versi 6) yang menunjukkan alamat darikomputer tersebut pada jaringan Internet berbasis TCP/IP.

Sistem pengalamatan IP ini terbagi menjadi dua, yakni:

2.5.1.1 IPV4

Alamat IP versi 4 umumnya diekspresikan dalam notasi desimal bertitik (*dotted-decimal notation*), yang dibagi ke dalam empat buah octet berukuran 8-bit. Dalam beberapa buku referensi, format bentuknya adalah w.x.y.z. Karena setiap oktet berukuran 8-bit, maka nilainya berkisar antara 0 hingga 255 (meskipun begitu, terdapat beberapa pengecualian nilai). Alamat IP yang dimiliki oleh sebuah host dapat dibagi dengan menggunakan subnet mask jaringan ke dalam dua buah bagian, yakni:

- *Network Identifier/NetID* atau *Network Address* (alamat jaringan) yang digunakan khusus untuk mengidentifikasikan alamat jaringan di mana host berada.

- *Host Identifier/HostID* atau *Host address* (alamat host) yang digunakan khusus untuk mengidentifikasikan alamat host (dapat berupa *workstation*, *server* atau sistem lainnya yang berbasis teknologi TCP/IP) di dalam jaringan. Nilai *host identifier* tidak boleh bernilai 0 atau 255 dan harus bersifat unik di dalam *network identifier*/segmen jaringan di mana ia berada.

2.5.2 Class IP Address

IP address dikelompokan dalam lima kelas, yaitukelas A, B, C, D, dan E. Perbedaannya terletak pada ukuran dan jumlah. *IP address* kelas Ajaringan*IP address* Kelas B digunakan untuk jaringan berukuran besar dan sedang. *IP address* Kelas C untuk pembagian jaringan yang banyak, namun masing-masing jaringan memiliki anggota yang sedikit. *IP address* Kelas D dan E juga didefinisikan, tetapi tidak digunakan dalam penggunaan normal, kelas d diperuntukan bagi jaringan multicast, dan E untuk Eksperimental. Pembagian kelas-kelas *IP address* didasarkan pada dua hal, yaitu *Network ID* dan Host ID dari suatu *IP address* Setiap *IP address* selalu merupakan pasangan *network ID* (Identitas Jaringan) dan Host ID (Indentitas host

dalam suatu jaringan). Masing-masing komputer/router di suatu jaringan host ID-nya harus Unik (harus berbeda dengan komputer yang lain).

2.5.2.1 Class A

Format	0nnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh (n = Net ID, h = Host ID)
Bit Pertama	0
Panjang Net ID	8 bit (1oktet)
Panjang Host ID	24 bit (3 oktet)
Oktet Pertama	0 – 127
Range ***IP address***	1.xxx.xxx.xxx.sampai 126.xxx.xxx.xxx (0 dan 127 dicadangkan)
Jumlah Network	126
Jumlah ***IP address***	16.777.214

IP kelas A untuk sedikit jaringan dengan host yang sangat banyak. cara membaca ***IP address*** kelas A misalnya 113.46.5.6 ialah : Network ID :113, Host ID = 46.5.6

2.5.2.2 Class B

Format	10nnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh (n = Net ID, h = Host ID)
2 Bit Pertama	10
Panjang Net ID	16 bit (2 oktet)
Panjang Host ID	16 bit (2 oktet)

Oktet Pertama	128 – 191
Range ***IP address***	128.0.0.xxx sampai 191.255.xxx.xxx
Jumlah Network	16.384
Jumlah ***IP address***	65.534

Biasa digunakan untuk jaringan besar dan sedang. dua bit pertama selalu di set 10. 16 bit selanjutnya, network IP kelas B dapat menampung sekitar 65000 host.

2.5.2.3 Class C

Format	110nnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh (n = Net ID, h = Host ID)
3 Bit Pertama	110
Panjang Net ID	24 bit (3 oktet)
Panjang Host ID	8 bit (1 oktet)
Oktet Pertama	192 – 223
Range ***IP address***	192.0.0.xxx sampai 255.255.255.xxx
Jumlah Network	2.097.152
Jumlah ***IP address***	254

Host ID adalah 8 bit terakhi, dengan IP kelas C, dapat dibentuk sekitar 2 juta network yang masing-masing memiliki 256 ***IP address*** Tiga bit pertama ***IP address*** kelas C selalu berisi 111 dengan 21 bit berikutnya. Host ID ialah 8 bit terakhir.

2.5.2.4 Class D

Format	1110mmmm.mmmmmmmm.mmmmmmmm.mmmmmmmm
4 Bit Pertama	10
Bit Multicast	28 bit
Byte Inisial	224-247
Deskripsi	Kelas D adalah ruang alamat multicast

Kelas ini digunakan untuk keperluan Multicasting. 4 bit pertama 1110, bit-bit berikutnya diatur sesuai keperluan multicast group yang menggunakan ***IP address*** ini. Dalam multicasting tidak dikenal network bit dan host bit.

2.5.2.5 Class E

Format	1111rrr.rrrrrrrr.rrrrrrrr.rrrrrrrr
4 Bit Pertama	1111
Bit Cadangan	28 bit
Byte Inisial	248-255
Deskripsi	Kelas E adalah ruang alamat yang dicadangkan untuk keperluan eksperimental.

2.5.3 Jenis IP Address

IP address dibagi menjadi empat jenis, yaitu:

2.5.3.1 Public Address

Public Address adalah IP Address yang digunakan untuk komunikasi pada jaringan di internet, sebagai contoh pada saat kita pertama kali mengakses URLhttp://www.google.co.id, maka secara otomatis computer kita akan melakukan koneksi menuju alamat 72.14.203.147. Angka tersebut dapat kita lihat pada baris status di *browser* (Internet Explorer/Mozilla Firefox) yang terletak pada sebelah kiri bawah. Nomor 72.14.203.147 adalah *IP address* yang digunakan di jaringan internet dan digolongkan sebagai *Public Address*.

2.5.3.2 *Private Address*

Private Address adalah *IP Address* yang digunakan untuk komunikasi yang tidak terhubung langsung dengan internet atau berada pada sebuah area lokal. Dengan menggunakan *Private Address* ini, computer tidak dapat terhubung dengan internet. Hanya dapat bertukar informasi dengan computer lainnya yang juga terhubung pada jaringan yang sama (intranet). Private IP ini biasanya digunakan pada suatu perkantoran. Nomor yang digunakan biasanya dimulai dengan 192.168.0.1 sampai seterusnya sebanyak komputer yang ada.

2.5.3.3 *IP Dynamic*

IP Dynamic adalah ip yg diberikan dari server DHCP (isp) biasanya akan berubah setiap kamu terputus, lalu *connect*-ulang (*restart* komputer, dan lain-lain) tidak perlu configurasi tambahan, cukup *set config* koneksi kamu dari ip sampai dns ke mode-otomatis.

2.5.3.4 *IP Static*

IP Static adalah IP yg dialokasikan dan diberikan secara langsung dari pihak ISP. kamu perlu memasukkan IP yg dialokasikan dari ISP ke *config* koneksi kamu. sehingga waktu kamu terputus dan *connect*-ulang (*restart* komputer, ip tidak akan berubah*) ip dynamic* biasanya digunakan oleh kebanyakan user rumahan dan soho (*small office, home office*) ip statik biasanya digunakan oleh kebanyakan user *professional, server, dan enterprise*.

2.6 Subneting

Subnetting adalah teknik pengaturan jaringan yang bertujuan untuk mengefisiensikan pengelolaan dan penggunaan *IP Address* dalam sebuah jaringan. Adakalanya tatacara penulisan *IP Address* 32 bit seperti : 192.168.1.1, tapi juga terkadang dapat pula ditulis 192.168.1.1/24. Apa maksudnya ? Untuk memahaminya, bisa menggunakan tabel *subnetting* yang ada di atas. Dimulai dari urutan angka yang paling atas sampai ke bawah (diurutkan berdasarkan baris tabel):

1. Binary
2. Bits
3. Subnets
4. Jumlah Network
5. Jumlah Hosts
6. Jumlah Network yang dipinjam
7. Jumlah Bit Host yang di pinjam
8. Masks (CIDR)

Untuk CIDR (*Classless Inter-Domain Routing*) **/24** (kolom pertama, baris terakhir), dengan bilangan biner 256. Maka subnet mask-nya 255.255.255.**0**. Dengan **0** terakhir diambil dari tabel baris ke 3 kolom pertama. Sehingga host yang mungkin adalah berjumlah 254 Host (Bilangan biner 256-2=254, 2 adalah

jumlah host yang dipinjam untuk digunakan sebagai IP Subnet (IP Awal) dan IP Broadcast (IP Akhir)). Contoh lainnya adalah: CIDR /**26** (kolom ke tiga, baris terakhir), mulai dari Bilangan Biner 64. Disitulah subnetnya. Kita punya 4 buah jaringan, dimana masing-masing memiliki 62 host/komputer (64-2 =126). Jadi pada intinya, dalam sebuah kasus *Subnetting*, ada 4 hal yang biasanya perlu diketahui:

1. **Jumlah Subnet**. Berada pada baris ke empat. Misal: 192.168.1.0/26, akan mempunyai 4 buah subnet.
2. **Jumlah Host/Komputer per Subnet**. Berada pada baris ke lima. Untuk IP 192.168.1.0/26, jumlah host per subnet adalah 62 hosts (64-2=62). Contoh: Range IP Host salah satu subnet adalah 192.168.1.**1**-192.168.1.**62**. Dimana 192.168.1.0 digunakan untuk Subnet pertama, dan 192.168.1.63 digunakan sebagai IP Broadcast.
3. **Blok Subnet**. Berada pada baris pertama. Sehingga untuk CIDR /26, blok-blok subnet nya adalah:
   192.168.1.**0,**192.168.1.**64,** 192.168.1.**128,** dan 192.168.1.**192** (Kelipatan 64 bit sejumlah 4 subnet).
4. **IP Host dan IP Broadcast yang valid**. Seperti yang telah dijelaskan pada nomor 2, Jumlah subnet akan berpengaruh terhadap jumlah IP Address yang dapat digunakan. Pada tiap-tiap subnet, IP Awal dikenal dengan IP Subnet, sedangkan IP Akhir dikenal sebagai IP Broadcast. Sedangkan IP sisanya, adalah IP yang dapat digunakan untuk host.

2.7 *Firewall*

Secara umum, *firewall filtering* biasanya dilakukan dengan cara mendefinisikan IP address, baik itu src-address maupun dst-address. Misalnya Anda ingin blok komputer client yang memiliki ip tertentu atau ketika melakukan blok terhadap web tertentu berdasarkan ip web tersebut. *Firewall* tidak hanya digunakan untuk melakukan blok client agar tidak dapat mengakses *resource* tertentu, namun juga digunakan untuk melindungi jaringan local dari ancaman luar, misalnya virus atau serangan *hacker*. Biasanya serangan dari internet ini

dilakukan dari banyak IP sehingga akan sulit bagi kita untuk melakukan perlindungan hanya dengan berdasarkan IP. Nah, sebenarnya ada banyak cara *filtering* selain berdasar *IP Addres*, misalnya berdasar protokol dan port. Berikut contoh implementasi dengan memanfaatkan beberapa parameter di fitur *firewall filter*.

2.8 NAT (*Network Address Translation*)

NAT adalah pengalihan suatu alamat IP ke alamat yang lain. Dan apabila suatu paket dialihkan dengan NAT pada suatu link, maka pada saat ada paket kembali dari tujuan maka link ini akan mengingat darimana asal dari paket itu, sehingga komunikasi akan berjalan seperti biasa.

2.8.1 *Source NAT*

Untuk melakukan Source NAT anda harus merubah asal dari koneksi. Hal ini dilakukan di *chain postrouting*, sebelum keluar. Hal ini sangat penting, dikarenakan berarti *tools* lain yang di dalam router itu (*routing, packet filtering*) akan melihat paket itu tidak berubah. Hal ini juga berarti opsi '-o' (*outgoing interface*) juga bisa digunakan.

Source dispesifikasikan dengan menggunakan '-j SNAT', dan juga opsi '--to-source' untuk menspesifikasikan sebuah alamat IP, range alamat IP dan port atau range port (hanya untuk protokol UDP dan TCP) yang sifatnya optional.

2.8.2 *Masquerading*

Terdapat kasus yang khusus untuk *Source* NAT yang disebut masquerading, sebaiknya hanya digunakan untuk alamat IP yang dinamik, seperti menggunakan dialup secara standar (untuk alamat IP yang statis, gunakan SNAT si atas). Anda tidak perlu menempatkan

alamat asal apabila anda menggunakan masquerading, dikarenakan alamat asal akan memakai alamat dari *interface* tempat paket itu keluar. Hal ini akan memudahkan apabila ada penggantian alamat IP dari *interface* tersebut, sehingga kesalahan data dihindari.

2.8.3 *Destination NAT*

Destination NAT dilakukan pada chain PREROUTING, pas ketika paket masuk, hal ini berarti semua tools di dalam router akan melihat paket akn pergi ke tujuan yang sebenarnya . Hal ini juga berarti bahwa opsi '-i' (*incoming interface*) bisa digunakan.

Destination NAT dispesifikasikan dengan menggunakan '-j DNAT' dan opsi '--to-destination' menspesifikasikan sebuah alamat IP, range alamat IP dan range dari port (hanya untuk protokol UDP dan TCP) yang sifatnya optional.

2.9 VLAN (*Virtual Local Area Network*)

VLAN (Virtual LAN) adalah suatu model jaringan yang tidak terbatas pada lokasi fisik seperti LAN, hal ini mengakibatkan suatu *network* dapat dikonfigurasi secara virtual tanpa harus menuruti lokasi fisik peralatan. Penggunaan VLAN akan membuat pengaturan jaringan menjadi sangat fleksibel karena dapat dibuat segmen yang bergantung pada organisasi, tanpa bergantung lokasi *workstations*.

VLAN diciptakan untuk menyediakan layanan segmentasi secara tradisional disediakan oleh router di konfigurasi LAN. VLAN menangani masalah-masalah seperti skalabilitas, keamanan, dan manajemen jaringan.

VLAN diklasifikasikan berdasarkan metode (tipe) yang digunakan untuk mengklasifikasikannya, baik itu menggunakan port, *MAC address*, dsb. Semua informasi yang mengandung penandaan/pengalamatan suatu VLAN (*tagging*)

disimpan pada suatu database, jika penandaannya berdasarkan port yang digunakan maka database harus mengindikasi port-port yang digunakan VLAN.

Untuk mengaturnya maka biasanya digunakan *switch* yang bisa diatur. *Switch/bridge* inilah yang bertanggung jawab menyimpan semua informasi dan konfigurasi suatu VLAN dan dipastikan semua *switch* memiliki informasi yang sama.

Kesimpulannya, VLAN membuat kita dapat mengontrol pola lalu lintas dan bereaksi cepat untuk relokasi.VLAN memberikan fleksibilitas untuk beradaptasi dengan perubahan dalam persyaratan jaringan dan memungkinkan untuk administrasi disederhanakan.

2.10 *Routing*

Routing digunakan untuk proses pengambilan sebuah paket dari sebuah alat dan mengirimkan melalui network ke alat lain disebuah network yang berbeda. Jika network Anda tidak memiliki router, maka jelas Anda tidak melakukan routing. Untuk bisa melakukan routing paket, ada hal-hal yang harus diketahui :

• Alamat tujuan
• Router-router tetangga dari mana sebuah router bisa mempelajari tentang network remote
• Route yang mungkin ke semua network remote
• Route terbaik untuk setiap network remote

Router menyimpan routing table yang menggambarkan bagaimana menemukan network-network remote. Jenis-jenis routing adalah :
• Routing statis
• Routing default
• Routing dinamis

Proses routing IP dapat dijelaskan dengan menggunakan gambar berikut ini :

Default gateway dari host 172.16.10.2 (Host_A) dikonfigurasi ke 172.16.10.1. Untuk dapat mengirimkan paket ini ke default gateway, harus diketahui dulu alamat hardware dari *interface Ethernet* 0 dari *router* (yang dikonfigurasi dengan alamat IP 172.16.10.1 tersebut). Mengapa demikian? Agar paket dapat diserahkan ke *layer Data Link*, lalu dienkapsulasi menjadi *frame*, dan dikirimkan ke *interface router* yang terhubung ke network 172.16.10.0. Host berkomunikasi hanya dengan alamat hardware pada LAN lokal. Penting untuk memahami bahwa Host_A, agar dapat berkomunikasi dengan Host_B, harus mengirimkan paket ke alamat MAC dari *default gateway* di jaringan lokal.

2.10.1 Routing Statis

Routing statis terjadi jika Admin secara manual menambahkan route-route di *routing table* dari setiap router.

Routing statis memiliki kentungan-keuntungan berikut:

- Tidak ada *overhead* (waktu pemrosesan) pada CPU router (router lebih murah dibandingkan dengan routeng dinamis)
- Tidak ada bandwidth yang digunakan di antara router.
- Routing statis menambah keamanan, karena administrator dapat memilih untuk mengisikan akses routing ke jaringan tertentu saja.

Routing statis memiliki kerugian-kerugian berikut:

- Administrasi harus benar-benar memahami internetwork dan bagaimana setiap router dihubungkan untuk dapat mengkonfigurasikan router dengan benar.

- Jika sebuah network ditambahkan ke internetwork, Administrasi harus menambahkan sebuah route kesemua router—secara manual.
- Routing statis tidak sesuai untuk network-network yang besar karena menjaganya akan menjadi sebuah pekerjaan *full-time* sendiri.

2.10.2 Routing Default

Routing default digunakan untuk mengirimkan paket-paket secara manual menambahkan router ke sebuah network tujuan yang tidak ada di *routing table*, ke *router hop* berikutnya. Bisanya digunakan pada jaringan yang hanya memiliki satu jalur keluar.

2.10.3 Routing Dinamis

Routing dinamis adalah ketika *routing protocol* digunakan untuk menemukan *network* dan melakukan update routing table pada router. Dan ini lebih mudah daripada menggunakan routing statis dan *default*, tapi ia akan membedakan Anda dalam hal proses-proses di CPU router dan penggunaan *bandwidth* dari link jaringan

Routing protokol-protokol ini digunakan untuk merawat *routing table* pada router-router. Contoh dari routing protokol diantaranya OSPF, RIP, BGP, IGRP, dan EIGRP

RIP (**Routing Information Protocol)** *distance vector protocol* – merawat daftar jarak tempuh ke network-network lain berdasarkan jumlah hop, yakni jumlah router yang harus lalui oleh paket-paket untuk mencapai address tujuan. RIP dibatasi hanya sampai 15 *hop*. Broadcast di-update dalam setiap 30 detik untuk semua RIP router guna menjaga integritas. RIP cocok dimplementasikan untuk jaringan kecil.

OSPF (**Open Shortest Path First**) *Link state protocol*—menggunakan kecepatan jaringan berdasarkan metric untuk menetapkan path-path ke jaringan lainnya. Setiap router merawat map sederhana dari keseluruhan jaringan. Update-update dilakukan via multicast, dan dikirim. Jika terjadi perubahan konfigurasi. OSPF cocok untuk jaringan besar.

EIGRP (**Enhanced Interior Gateway Routing Protocol**) Distance vector protocol—merawat satu set metric yang kompleks untuk jarak tempuh ke jaringan lainnya. EIGRP menggabungkan juga konsep link state protocol. Broadcast-broadcast di-update setiap 90 detik ke semua EIGRP router berdekatan. Setiap update hanya memasukkan perubahan jaringan. EIGRP sangat cocok untuk jaringan besar.

2.11 Port

Dalam protokol jaringan TCP/IP, sebuah ***port*** adalah mekanisme yang mengizinkan sebuah komputer untuk mendukung beberapa sesi koneksi dengan komputer lainnya dan program di dalam jaringan. Port dapat mengidentifikasikan aplikasi dan layanan yang menggunakan koneksi di dalam jaringan TCP/IP. Sehingga, port juga mengidentifikasikan sebuah proses tertentu di mana sebuah server dapat memberikan sebuah layanan kepada klien atau bagaimana sebuah klien dapat mengakses sebuah layanan yang ada dalam server. Port dapat dikenali dengan angka 16-bit (dua byte) yang disebut dengan **Port Number** dan diklasifikasikan dengan jenis protokol transport apa yang digunakan, ke dalam **Port TCP** dan **Port UDP**. Karena memiliki angka 16-bit, maka total maksimum jumlah port untuk setiap protokol transport yang digunakan adalah 65536 buah.

Dilihat dari penomorannya, port UDP dan TCP dibagi menjadi tiga jenis, yakni sebagai berikut:

- ***Well-known Port***: yang pada awalnya berkisar antara 0 hingga 255 tapi kemudian diperlebar untuk mendukung antara 0 hingga 1023. Port number yang termasuk ke dalam well-known port, selalu merepresentasikan layanan jaringan yang sama, dan ditetapkan oleh *Internet Assigned Number Authority (IANA)*. Beberapa di antara port-port yang berada di dalam range Well-known port masih belum ditetapkan dan direservasikan untuk digunakan oleh layanan yang bakal ada pada masa depan. *Well-known port*didefinisikan dalam RFC 1060.
- ***Registered Port***: Port-port yang digunakan oleh vendor-vendor komputer atau jaringan yang berbeda untuk mendukung aplikasi dan sistem operasi yang mereka buat. Registered port juga diketahui dan didaftarkan oleh IANA tapi tidak dialokasikan secara permanen, sehingga vendor lainnya dapat menggunakan port number yang sama. Range registered port berkisar dari 1024 hingga 49151 dan beberapa port di antaranya adalah *Dynamically Assigned Port*.
- ***Dynamically Assigned Port***: merupakan port-port yang ditetapkan oleh sistem operasi atau aplikasi yang digunakan untuk melayani request dari pengguna sesuai dengan kebutuhan. Dynamically Assigned Port berkisar dari 1024 hingga 65536 dan dapat digunakan atau dilepaskan sesuai kebutuhan.

2.12 Protocol

Protokol adalah sebuah aturan atau standar yang mengatur atau mengijinkan terjadinya hubungan, komunikasi, dan perpindahan data antara dua atau lebih titik komputer. Protokol dapat diterapkan pada perangkat keras, perangkat lunak atau kombinasi dari keduanya. Pada tingkatan yang terendah, protokol mendefinisikan koneksi perangkat keras.

Protokol perlu diutamakan pada penggunaan standar teknis, untuk menspesifikasi bagaimana membangun komputer atau menghubungkan peralatan perangkat keras. Protokol secara umum digunakan pada komunikasi *real-time* dimana

standar digunakan untuk mengatur struktur dari informasi untuk penyimpanan jangka panjang.

Sangat susah untuk *menggeneralisir* protokol dikarenakan protokol memiliki banyak variasi di dalam tujuan penggunaanya. Kebanyakan protokol memiliki salah satu atau beberapa dari hal berikut:

- Melakukan deteksi adanya koneksi fisik atau ada tidaknya komputer atau mesin lainnya.
- Melakukan metode "jabat-tangan" (*handshaking*).
- Negosiasi berbagai macam karakteristik hubungan.
- Bagaimana mengawali dan mengakhiri suatu pesan.
- Bagaimana format pesan yang digunakan.
- Yang harus dilakukan saat terjadi kerusakan pesan atau pesan yang tidak sempurna.
- Mendeteksi *rugi-rugi* pada hubungan jaringan dan langkah-langkah yang dilakukan selanjutnya
- Mengakhiri suatu koneksi.

2.12.1 PPP (*Point to Point*)

Point to Point Protocol atau yang biasa disingkat PPP merupakan enkapsulasi multiprotokol datagram dalam jaringan yang sering digunakan pada jaringan WAN, *Point to Point Protocol* menggunakan arsitektur berlapis dengan model logis dan desain yang membantu komunikasi diantara lapisan interkoneksi. *Point to Point Protocol* juga menyediakan enkapsulasi datagram melalui jalur *point to point* dan menggunakan lapisan data link untuk mengetes koneksi. *Point to Point Protocol* terdiri dari 2 sub protokol, yaitu:

- ***Link Control Protocol*** yang berfungsi untuk membangun jalur *point to point*. *Link Control Protocol* berada diatas lapisan *physical layer*

dan digunakan untuk membangun, mengkonfigurasi dan mengetes koneksi data link.

- ***Network Control Protocol*** yang berfungsi untuk konfigurasi berbagai *protocol network layer*.

Point to Point Protocol juga menggunakan *link Control Protocol* untuk menyetujui pilihan format enkapsulasi seperti: *Authentication, Compression, error detection, multilink* dan PPP *callback*. *Point to Point Protocol* mengizinkan berbagai *protocol network layer* untuk beroperasi pada jalur komunikasi yang sama. Untuk setiap *protocol network layer* yang digunakan disediakan pula *Network Control Protocol* yang berbeda. sebagai contoh: *Internet Protocol*(IP) menggunakan *Internet Protocol Control Protocol*(IPCP) dan yang lainnya.

2.13 Gateway

Gateway adalah sebuah perangkat yang digunakan untuk menghubungkan satu jaringan komputer dengan satu atau lebih jaringan komputer yang menggunakan kaidah komunikasi yang berbeda sehingga informasi dari satu jaringan komputer dapat dialirhantarkan ke jaringan komputer yang lain dengan kaidah jaringan berbeda. Pengartian tersebut adalah arti utama istilah gerbang jaringan.

Seiring dengan merebaknya Internet, pengartian gerbang jaringan sering kali bergeser. Tidak jarang pula pemula menyamakan "gerbang jaringan" dengan "penghala" (*router*) yang sebetulnya tidak benar.

Kadangkala, kata "gerbang jaringan" digunakan untuk memerikan perangkat yang menghubungkan jaringan komputer besar dengan jaringan komputer besar lainnya. Hal ini muncul karena kerap kali perbedaan kaidah komunikasi dalam jaringan komputer hanya terjadi di tingkat jaringan komputer yang besar.

2.14 Bridge

Bridge adalah sebuah komponen jaringan yang digunakan untuk memperluas jaringan atau membuat sebuah segmen jaringan. Bridge jaringan beroperasi di dalam lapisan data-link pada model OSI. Bridge juga dapat digunakan untuk menggabungkan dua buah media jaringan yang berbeda, seperti halnya antara media kabel *Unshielded Twisted-Pair* (UTP) dengan kabel serat optik atau dua buah arsitektur jaringan yang berbeda.

Koneksi internet digunakan pada 1 PC saja, atau koneksi internet di-share dengan beberapa PC menggunakan *server/access point*. Koneksi internet menggunakan pilihan paket kuota, sehingga tidak selalu terhubung ke internet selama 24 jam.

Menginginkan kerja modem yang lebih ringan, karena jika koneksi di-share maka modem tidak dijadikan sebagai server untuk membagi *bandwidth*, sehingga modem lebih awet. Namun konsekuensinya, untuk membagi bandwidth diperlukan tambahan *server/access point*. Dapat memisahkan jaringan yang luas menjadi sub jaringan yang lebih kecil. Dapat mempelajari alamat, meneliti paket data dan menyampaikannya. Dapat mengoleksi dan melepas paket-paket diantara dua segmen jaringan. Dapat mengontrol broadcast ke jaringan. Dapat merawat *address table*.

2.15 Switch

Switch merupakan perangkat jaringan yang berfungsi menghubungkan Hub untuk membentuk jaringan yang lebih besar atau menghubungkan komputer - komputer yang membutuhkan *bandwith* yang besar.

Switch merupakan perangkat keras jaringan yang hampir sama dengan Hub, bedanya switch sedikit lebih pintar walaupun dengan harga sama atau sedikit lebih mahal. Switch bekerja dengan cara menerima paket data pada suatu port lalu melihat alamat MAC tujuan dan membagun sebuah koneksi logika dengan port

yang terhubung dengan node/perangkat tujuan, sehingga port - port selain port yang dituju tidak akan menerima paket data yang dikirim dan mengurangi terjadinya tabrakan data (*collision*). Setiap Perangkat yang tersambung ke port tertentu, *MAC addressnya* akan dicatat pada *MAC address table* yang disimpan di memori *cache switch.*

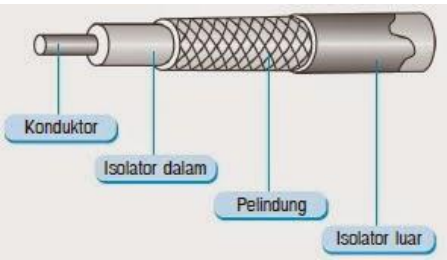
2.16 Jenis Kabel

Kabel jaringan merupakan salah satu media transmisi yang digunakan pada jaringan komputer agar setiap komputer/perangkat yang tergabung didalamnya bisa saling berkomunikasi. Selain menggunakan kabel, terdapat juga media transmisi yang tidak menggunakan kabel yang lebih sering kita sebut wireless. Pada OSI Layer, media komunikasi menempati posisi paling bawah yaitu Physical Layer.

Dibandingkan media tanpa kabel, media kabel lebih memiliki kecepatan dan stabilitas yang tinggi serta jangkauan yang lebih jauh. Dalam artikel ini, saya akan membahas jenis-jenis kabel apa saja yang ada pada jaringan komputer. Ada tiga jenis kabel yang digunakan dalam media komunikasi via Kabel, yaitu Coaxial, Twisted Pair, dan Fiber Optik. Berikut Penjelasan Lengkap Jenis-jenis Kabel Jaringan Komputer

2.16.1 Kabel Coaxial

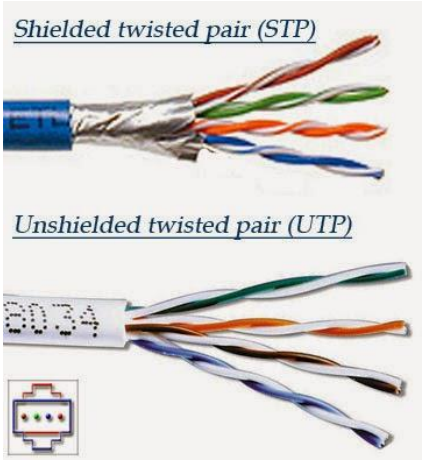
Kabel coaxial adalah jenis kabel yang terdiri atas dua penghantar di mana salah satu penghantarnya berada di tengah kabel dan dikeliling oleh penghantar satunya lagi dengan pola melingkar. Prinsip kerja Coaxial dengan cara menghantarkan arus atau sinyal listrik dari sumber ke tujuan.



Gambar 2.12 Kabel Coaxial

2.16.2 Kabel Twisted Pair

Kabel twisted pair merupakan kabel jaringan yang didalamnya terdiri atas beberapa kabel yang saling berpasangan. Sama seperti kabel coaxial, cara kerja dari kabel Twisted Pair adalah dengan mengahantarkan arus atau sinyal listrik dari sumber ke tujuan. Kabel twisted pair ini terbagi atas jenis, yaitu STP (Shielded Twisted Pair) dan UTP (Unshielded Twisted Pair).

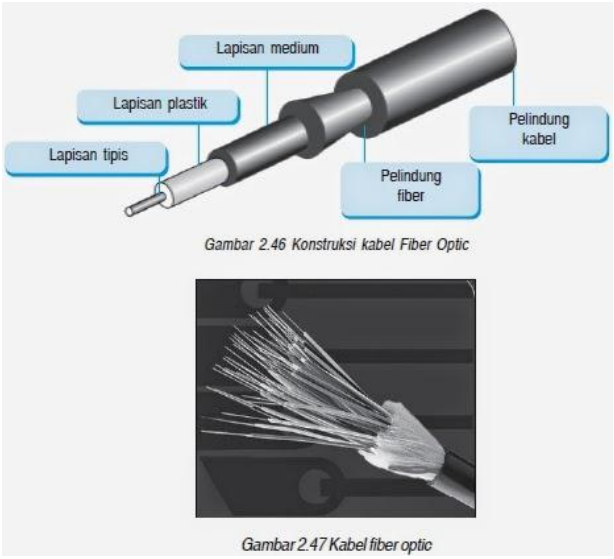


Gambar 2.13 Kabel Twistet Pair

2.16.3 Kabel Fiber Optik

Tidak seperti dua kabel sebelumnya yang menggunakan tembaga sebagai media penghantarnya. Kabel fiber optik ini tebuat dari serat kaca atau plastik yang sangat tipis. Karena terbuat dari kaca, sinyal yang dikirim oleh FO ini berupa cahaya dari sumber ke tujuan.

Makanya tidak heran bila transmisi kabel ini lebih cepat dibandingkan dengan dua kabel sebelumnya. Salah satu kelemahan kabel ini adalah gangguan (noise) yang sering terjadi apabila tertekuk walaupun hanya sedikit.



Gambar 2.14 Kabel Fiber Optic

2.17 Wireless

Wireless merupakan jaringan tanpa kabel yang menggunakan udara sebagai media transmisinya untuk menghantarkan gelombang elektromagnetik. Perkembangan wireless sebenarnya telah dimulai sejak lama dan telah dibuktikan secara ilmiah oleh para ilmuan dengan penemuan radio dan kemudian dilanjutkan dengan penemuan radar. Kemudian dengan perkembangan kebutuhan informasi bagi manusia, maka penggunaan wireless semakin banyak dan tidak hanya untuk penggunaan radio dan radar saja.

2.18 Converter

Converter adalah perangkat jaringan sederhana yang memungkinkan untuk menghubungkan dua jenis jaringan yang berbeda media seperti twisted pair dengan kabel fiber optik. *Fiber Optic Media Converter* diperkenalkan ke industri

hampir dua dekade lalu, *Fiber Optic Media Converter* berperan penting dalam proses interkoneksi anatara jaringan berbasis sistem fiber optik dengan jaringan yang berbasis tembaga, dalam sistem kabel terstruktur. Fiber Optik Media *Converter* juga digunakan dalam akses MAN dan layanan data transportasi ke pelanggan perusahaan.

2.19 Mikrotik

Mikrotik adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer manjadi *router network* yang handal, mencakup berbagai fitur yang dibuat untuk ip network dan jaringan *wireless*, cocok digunakan oleh ISP dan *provider hotspot*.

Untuk instalasi Mikrotik tidak dibutuhkan piranti lunak tambahan atau komponen tambahan lain. Mikrotik didesain untuk mudah digunakan dan sangat baik digunakan untuk keperluan administrasi jaringan komputer seperti merancang dan membangun sebuah sistem jaringan komputer skala kecil hingga yang kompleks sekalipun.

Mikrotik dibuat oleh MikroTikls sebuah perusahaan di kota Riga, Latvia. Bagi yang belum tau, Latvia adalah sebuah negara yang merupakan "pecahan" dari negara Uni Soviet dulunya atau Rusia sekarang ini. Dengan nama merek dagang Mikrotik mulai didirikan tahun 1995 yang pada awalnya ditujuka untuk perusahaan jasa layanan Internet (PJI) atau *Internet Service Provider* (ISP) yang melayani pelanggannya menggunakan teknologi nirkabel atau wireless. Saat ini MikroTikls memberikan layanan kepada banyak ISP nirkabel untuk layanan akses Internet dibanyak negara di dunia dan juga sangat populer di Indonesia.

Mikrotik pada standar perangkat keras berbasiskan Personal Computer (PC) dikenal dengan kestabilan, kualitas kontrol dan fleksibilitas untuk berbagai jenis paket data dan penanganan proses rute atau lebih dikenal dengan istilah routing. Mikrotik yang dibuat sebagai router berbasiskan PC banyak bermanfaat untuk sebuah ISP yang ingin menjalankan beberapa aplikasi mulai dari hal yang

paling ringan hingga tingkat lanjut. Contoh aplikasi yang dapat diterapkan dengan adanya Mikrotik selain routing adalah aplikasi kapasitas akses (*bandwidth*) manajemen, *firewall*, *wireless access point* (WiFi), *backhaul link*, sistem hotspot, *Virtual Private Network* (VPN) server dan masih banyak lainnya.

2.20 Quality Of Service (Simple Bandwith Management)

Dalam mengelola jaringan, sangat penting untuk mengendalikan pemakaian bandwith yang akan digunakan oleh komputer user. Jika anda tidak mengendalikannya, maka akan terjadi pemakaian bandwith secara berlebihan oleh satu atau beberapa user. Pemakaian yang berlebihan tersebut akan menyebabkan komputer user-user yang lain tidak lagi mendapatkan alokasi bandwith. Pada akhirnya, jaringan anda tidak dapat memberikan layanan (service) secara maksimal kepada seluruh user yang ada. Keadaan ini akan bertambah parah jika jaringan anda ternyata hanya memiliki alokasi bandwith internet yang terbatas dan pengguna jaringan anda “arkus” akan aktifitas download file-file besar dari internet.