

## **BAB II**

### **LANDASAN TEORI**

#### **2.1. Pengertian Jaringan Komputer**

Menurut Irawan ( 2013 : 2 ) jaringan komputer adalah “ sebuah kelompok yang terdiri dari dua atau lebih komputer yang saling berbagi pakai ( *sharing* ) melalui perangkat lunak ataupun keras , serta menggunakan protokol yang sama ”.

Dan menurut Aripin ( 2011 : 9 ) jaringan komputer merupakan “ kumpulan dari beberapa komputer yang dihubungkan satu dengan yang lainnya dengan menggunakan protokol komunikasi , Jaringan ini memerlukan media transmisi tertentu untuk dapat saling berbagi informasi, program, dan penggunaan bersama perangkat keras ”.

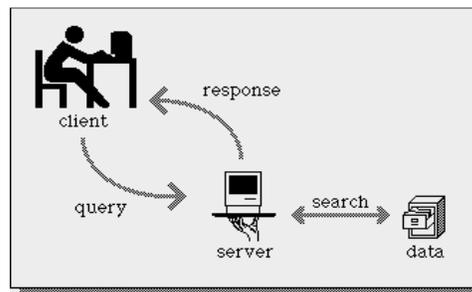
##### **2.1.1. Manfaat Jaringan Komputer**

Untuk mengetahui manfaat jaringan , dapat ditinjau dari mengapa orang tertarik menggunakan dan untuk apa jaringan tersebut dipakai?

Tinjauan tujuan utama dari jaringan , yaitu adalah berbagai pakai ( *resource sharing* ) yang bertujuan agar seluruh program, peralatan, khususnya data bisa digunakan setiap orang yang ada pada jaringan tanpa terpengaruh oleh lokasi *resource* dan pemakainya, hal ini merupakan usaha menghilangkan jarak.

Tinjauan kedua tujuan dari jaringan yaitu untuk mendapatkan keandalan tinggi dengan memiliki sumber – sumber alternatif yang tersedia. Sehingga jika ada mesin satu sibuk maka mesin lain dapat melayani permintaan, adanya *multiple* CPU sangat menguntungkan.

Tinjauan tujuan ketiga dari jaringan yaitu menghemat uang, komputer berukuran kecil mempunyai rasio harga / kinerja yang lebih baik dibanding komputer besar. Komputer *main frame* mempunyai kira – kira kecepatan sepuluh kali lipat komputer pribadi, tetapi harganya lebih mahal. Sehingga perancangan sistem memilih mengumpulkan komputer pribadi dalam sistem jaringan, dengan data utama disimpan pada satu atau lebih mesin *file server* yang dapat dipakai bersama – sama. Dalam model ini pengguna disebut model *client – server*.



Sumber : <http://jogjahostingterbaik.com/>

Gambar II. 1

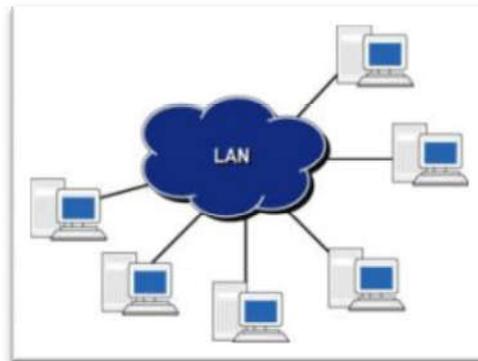
Client server

### 2.1.2. Jenis – Jenis Jaringan Komputer

Menurut Irawan ( 2013 : 6 ) “ Jaringan komputer dapat dibedakan menjadi beberapa macam, Secara umum jenis atau macam jaringan komputer dibedakan menjadi 3 macam, yaitu *Local Area Network* (LAN), *Metropolitan Area Network* (MAN) , *Wide Area Network* (WAN)”.

#### 1. *Local Area Network* ( LAN )

*Local Area Network* ( LAN ) adalah jaringan komputer dengan ruang lingkup terkecil, terdiri dari 2 komputer atau lebih yang saling berhubungan. Cakupan jaringan ini adalah lokasi dengan jangkauan dan area terbatas seperti warnet, kantor, atau laboratorium.



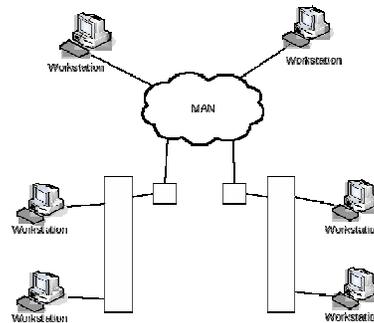
Sumber: <http://indoteknik.com>

Gambar II. 2

Skema jaringan LAN

## 2. *Metropolitan Area Network ( MAN )*

*Metropolitan Area Network ( MAN )* merupakan pengembangan dari LAN dengan cakupan yang lebih luas, seperti dalam satu kota besar beserta daerah setempat.



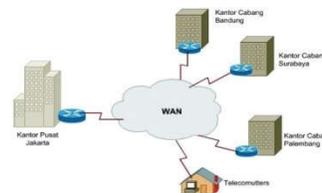
Sumber : <http://jakartaagungnetwork.com/>

Gambar II. 3

Skema jaringan MAN

## 3. *Wide Area Network ( WAN )*

*Wide Area Network ( WAN )* merupakan jaringan komputer dengan jangkauan paling luas, mencakup antar provinsi, negara, bahkan benua. Internet adalah jaringan WAN terbesar.



Sumber : <http://www.agashi86.com/>

Gambar II. 4

Skema jaringan WAN

## 2.2. Topologi

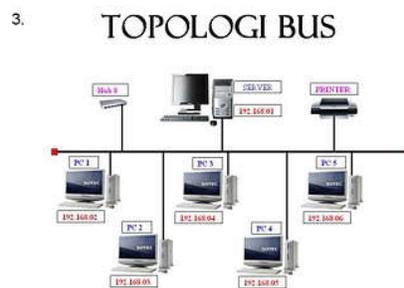
### 2.2.1. Topologi Jaringan

Menurut Irawan ( 2013 : 23 ) topologi jaringan adalah “ cara bagaimana menghubungkan komputer dengan komputer lainnya dalam sebuah jaringan ”.

Berikut jenis – jenis topologi dasar jaringan :

#### 1. Topologi *Bus*

Topologi *bus* yaitu menghubungkan beberapa komputer secara berantai pada sebuah kabel coaxial. Sebuah terminator di tempatkan pada tiap – tiap ujung *backbone*.



Sumber : <http://www.pintarkomputer.org>

Gambar II. 5

Topologi *bus*

Kelebihan :

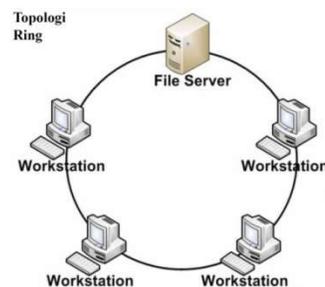
- a. Biaya relatif murah, hemat kabel.
- b. Jika sebuah komputer bermasalah, maka tidak akan mempengaruhi komputer lainnya.

Kekurangan :

- a. Jika kabel utama (*coaxial*) putus, maka komunikasi semua komputer yang terhubung pada kabel tersebut gagal.
- b. Semakin banyak komputer yang terhubung pada satu kabel utama menyebabkan lalu lintas data yang padat, kecepatan komunikasi bisa menurun.

## 2. Topologi *Ring*

Topologi *ring* merupakan jalur komunikasi satu arah, karena semua komputer dan *node* lainnya saling berhubungan seperti membentuk lingkaran. Data akan berputar dalam jaringan jika tidak ada terminal yang mengambil, beda dengan topologi *bus* yang menyerap data pada ujung *backbone* menggunakan terminator jika tidak ada yang mengambil.



Sumber : <http://www.pintarkomputer.org>

Gambar II. 6

Topologi *ring*

Kelebihan :

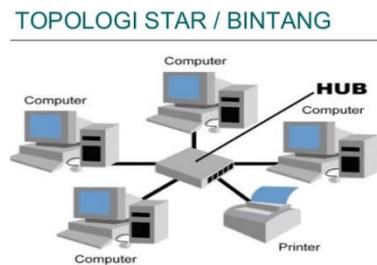
- a. Hemat kabel.
- b. Kegagalan koneksi karena gangguan media masih bisa diatasi dengan jalur lain yang masih terhubung.

Kekurangan :

- a. *Transfer* data lebih lambat, karena harus melewati banyak komputer terlebih dahulu ( data harus berputar melewati semua komputer sampai menemukan komputer tujuan ).
- b. Pengembangan jaringan tidak fleksibel.

### 3. Topologi *Star*

Topologi *star* adalah sistem jaringan dengan komunikasi terpusat, yaitu beberapa komputer terhubung dengan sebuah terminal yang menjadi pusat jaringan.



Sumber : <http://www.pintarkomputer.org>

Gambar II. 7

Topologi star

Kelebihan :

- a. Kontrol dan pengelolaan mudah karena semua koneksi terpusat di satu tempat.
- b. Mudah untuk menelusuri jika terjadi masalah pada koneksi.

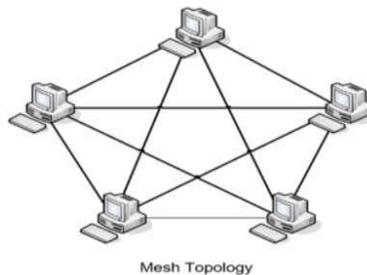
Kekurangan :

- a. Jika pusat koneksi gagal, maka semua komunikasi terputus.
- b. Kecepatan koneksi jaringan keseluruhan sangat bergantung dengan kualitas pusat koneksi.

#### 4. Topologi *Mesh*

Topologi *mesh* adalah topologi yang tidak memiliki aturan dalam koneksi.

Pada topologi ini setiap terminal terhubung secara langsung ke semua terminal – terminal yang lain.



Sumber : <http://www.pintarkomputer.org>

Gambar II. 8

Topologi *mesh*

Kelebihan :

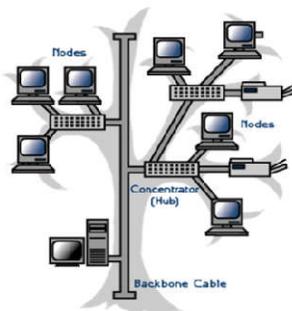
- a. Kegagalan koneksi antara 2 *workstation* tidak akan mempengaruhi dengan koneksi lainnya.
- b. Privasi dan keamanan lebih terjamin.

Kekurangan :

- a. Jika diterapkan pada jaringan kabel, akan membutuhkan banyak kabel dan sudah pasti biaya yang lebih mahal.
- b. Sulit untuk diorganisir karena kerumitan alur koneksi dalam jaringan.

#### 5. Topologi *tree*

Topologi *tree* atau topologi “pohon” bisa dikatakan sebagai kombinasi karakteristik antara topologi *star* dan topologi *bus*, Topologi ini terdiri atas kumpulan topologi *star* yang dihubungkan dalam satu topologi bus sebagai *backbone*.



Sumber : <http://www.pintarkomputer.org>

Gambar II. 9

Topologi *tree*

Kelebihan :

- a. Dapat membuat kelompok komputer dalam jaringan sesuai keinginan.
- b. Mudah untuk menelusuri jika terjadi masalah pada koneksi.

Kekurangan :

- a. Apabila simpul yang lebih tinggi tidak berfungsi maka akan mempengaruhi kinerja simpul – simpul dibawahnya.
- b. Perlu pengaturan khusus untuk mengatur jalur lalu lintas koneksi karena adanya percabangan.

## **2.3. Perangkat Keras Jaringan**

### **2.3.1. Komponen Perangkat Keras Jaringan**

#### **1. Kabel**

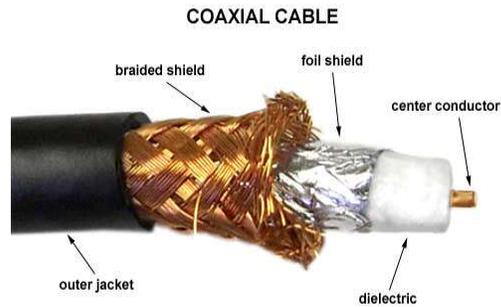
Menurut irawan ( 2013 : 8 ) kabel jaringan berfungsi “ sebagai media penghubung antara node di dalam jaringan. Meskipun saat ini teknologi jaringan nirkabel ( *wireless* ) sedang *trend*, namun media kabel masih banyak digunakan karena dari sisi kualitas dan kecepatan *transfer* data lebih baik dari *wireless* ”.

Beberapa jenis yang menjadi standar dalam penggunaan komunikasi data dalam jaringan komputer adalah

- a. Kabel *coaxial* ( *wired network* )

Kabel ini dilindungi oleh dua lapis isolasi, yaitu lapisan pertama adalah yang paling dekat dengan konduktor tembaga dan lapisan kedua untuk melindungi bagian inti yang berada di tengah. Lapisan isolasi pertama dilapisi oleh serabut konduktor untuk melindungi dari bagian pengaruh elektromagnetik.

Lebar kabel *coaxial* bermacam – macam, beberapa jenis kabel *coaxial* ada yang lebih besar dari yang lain. Semakin besar kabel, maka semakin besar kapasitas datanya.



Sumber : <http://teknodaily.com/>

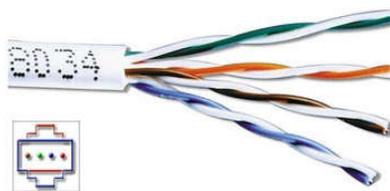
Gambar II. 10

Kabel *Coaxial*

*b. Unshielded Twisted Pair Cable (UTP)*

Kabel jaringan dengan bahan tembaga yang tidak dilengkapi pelindung. UTP merupakan jenis kabel yang paling banyak digunakan untuk membangun jaringan, khususnya jaringan lokal ( LAN ).

*Unshielded twisted pair (UTP)*



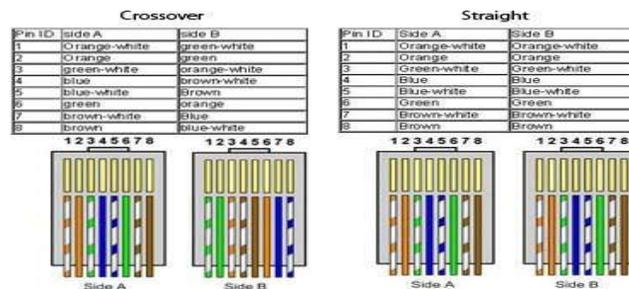
Sumber : <http://tech.dbagus.com/>

Gambar II. 11

Kabel UTP

Terdapat tipe penyambungan kabel jenis UTP, yaitu *straight cable* dan *crossover cable*. Perbedaannya, *straight cable* dipakai untuk menghubungkan beberapa *unit* komputer melalui perantara konsentrator maupun *repeater* sedangkan *crossover cable* digunakan untuk media komunikasi antar komputer.

Adapun pemasangan kabel *straight* dan *crossover* adalah :



Sumber : <http://emerer.com/>

Gambar II. 12

Kabel *straight* dan *crossover*

c. *Shielded twisted pair cable (STP)*

Kabel STP sama dengan kabel UTP, tapi memiliki pelindung ( *shield* ) lapisan *aluminium foil* untuk mencegah gangguan interferensi saat melakukan transmisi data.



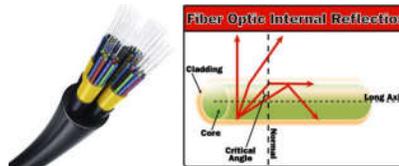
Sumber : <http://teknodaily.com/>

Gambar II.13

Kabel STP

d. Kabel serat optik (*fiber optic*)

Menggunakan serat kaca sebagai inti untuk mengirimkan cahaya dari satu tempat ke tempat lainnya. Kabel ini lebih cepat dari kabel apapun yang masih menggunakan tembaga, serta harganya sangat mahal.



Sumber : <http://www.syekhnurjati.ac.id>

Gambar II. 14

Kabel *fiber optic*

## 2. *Hub dan switch*

*Hub* adalah perangkat yang menyatukan kabel – kabel koneksi dari setiap workstation, server, serta perangkat lainnya. *Switch* memiliki fungsi yang hampir sama dengan *hub*, tapi *switch* mampu memeriksa paket data yang diterima, menentukan sumber dan perangkat tujuan masing – masing paket informasi, dan melanjutkan informasi serta data secara tepat.



Sumber : <http://technet2u.com/>

Gambar II.15

*Hub dan switch*

### 3. *Repeater*

Berfungsi untuk menguatkan sinyal dari sebuah jaringan dengan koneksi kabel maupun gelombang.

Setiap media penghubung seperti kabel atau gelombang mempunyai batasan jarak agar kualitas sinyal tetap terjaga. Oleh karena itu untuk mencegah menurunnya kualitas sinyal, maka dibutuhkan *repeater* di antara koneksi.



Sumber : <http://www.synchrotech.com/>

Gambar II. 16

*repeater*

### 4. *Bridge*

Jika diartikan adalah “ jembatan “, berfungsi sebagai penghubung antara dua jaringan. *Bridge* dapat mengetahui masing – masing alamat dari tiap – tiap segmen komputer pada kedua jaringan yang dihubungkan. *Bridge* juga dapat dijadikan penghubung antara *network* dengan tipe kabel yang berbeda ataupun topologi yang berbeda.



Sumber : <http://www.teorikomputer.com>

Gambar II. 17

*bridge*

## 5. *Router*

*Router* merupakan perangkat yang dikhususkan untuk menangani koneksi antara dua atau lebih jaringan yang terhubung melalui *packet switching*. *Router* bekerja dengan melihat alamat asal dan alamat tujuan dari packet yang melewatinya dan memutuskan *route* yang akan dilewati paket tersebut untuk sampai ke tujuan.



Sumber : <http://www.catatanteknisi.com>

Gambar II. 18

*Router*

## 2.4. Perangkat Lunak Jaringan

### 2.4.1. Komponen perangkat lunak

Dalam jaringan komputer selain *hardware* (perangkat keras) dibutuhkan pula adanya *software* (perangkat lunak), jika tidak ada salah satu maka jaringan tersebut tidak akan bisa berjalan. Perangkat lunak (*software*) jaringan komputer umumnya berkaitan dengan sistem operasi yang digunakan oleh komputer *server* dan *client*.

Perangkat lunak dalam jaringan komputer diantaranya yaitu :

#### 1. Mikrotik

Mikrotik routerOS adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer menjadi *router network*, mencakup berbagai fitur yang dibuat untuk *ip network* dan jaringan *wireless*.





Sumber : <https://www.mikrotik.com/>

Gambar II. 20

Aplikasi *winbox*

### 3. Sistem operasi *windows 7*

Sistem operasi *windows 7* di luncurkan pada tanggal 22 oktober 2009 oleh perusahaan microsoft. *Windows 7* memiliki beberapa versi diantaranya *starter, home basic, home premium, enterprise, profesional, ultimate*. Adapun kelebihan dan kekurangan pada sistem operasi ini antara lain :

Kelebihan sistem operasi *windows 7* :

- a. Dapatkan akses lebih cepat ke semua program yang digunakan.
- b. Berbagi file dan printer diantara beberapa PC.
- c. Menjaga PC agar lebih terlindungi dengan hanya sedikit gangguan.
- d. Mengelola perangkat menjadi lebih mudah.
- e. *Multi – tasking* nya menjadi lebih mudah.

Kekurangan sistem operasi *windows 7* yaitu :

- a. Beberapa aplikasi belum bisa beroperasi di *windows 7*.
- b. *Bug* pada *windows player 12*.
- c. *Hardware* yang bisa langsung dikenali di *vista*, tapi tidak di *windows 7*.



Sumber : <http://www.nousis.com/>

Gambar II. 21

*Windows 7*

#### 4. Mikrotik *management bandwidth*

Mikrotik *management bandwidth* dasarnya dibedakan menjadi 2 sistem yaitu *simple queue* dan *queue tree*.

*Simple queue* sering digunakan sebagai *management bandwidth* dengan limit IP address ( *simple limite* ) sedangkan *queue tree* lebih spesifik lagi yaitu *content website* misalnya *extention* dan alamat *website*.

##### a. *Simple queue*

*Simple queue* adalah cara sederhana melakukan limit data rate untuk IP address atau subnet. Adapun fitur yang dimiliki antara lain :

##### 1) *Peer to peer traffic shaping*

- a) Mengizinkan pembuatan aturan *queue* dengan pemilihan internal waktu.
- b) Menggunakan *multiple packet* dengan menggunakan *ip firewall mangle*.
- c) *Limit traffic* dari dua arah ( satu limit untuk untuk total *upload* dan *download*).

b. *Queue tree*

*Queue tree* merupakan limit *bandwidth* yang cukup kompleks karena proses limit dapat dikelompokkan berdasarkan protokol, *port*, atau kelompok *IP address*, sebelum melakukan proses limit, harus ditandai aliran paket menggunakan suatu tanda *mangle* agar paket tersebut dapat dikenal oleh *queue tree*. Hal ini bertujuan membedakan paket *downlink only* dan *uplink only* sehingga limit pada *bandwidth* dapat bekerja secara optimal.

## **2.5. TCP / IP DAN SUBNETTING**

### **2.5.1. TCP / IP**

Menurut Utomo ( 2011 : 24 ) menjelaskan “ TCP / IP merupakan sekumpulan protocol yang melakukan fungsi komunikasi data antara komputer dalam sebuah LAN atau WAN .”

Masing-masing protocol mempunyai tanggung jawab sendiri sehingga tugasnya menjadi jelas dan sederhana karena protocol yang satu tidak harus perlu mengetahui cara kerja protocol yang lain.sepanjang dapat melakukan komunikasi dengan baik, maka protocol tersebut telah dapat menjalankan tugas dan fungsinya masing-masing.

Sekumpulan protokol dari TCP/IP terbagi ke dalam empat layer yaitu:

1. *Network Interface Layer*

Bertanggung jawab mengirim dan menerima data dari media fisik. Media fisik bias berupa kabel, serat *optic*, atau bias gelombang radio.

Protokol ini harus mampu menerjemahkan sinyal listrik menjadi data digital yang bias dimengerti oleh komputer, yang berasal dari peralatan lain yang sejenis.

2. *Internet layer*

Bertanggung jawab dalam proses pengiriman paket ke alamat yang tepat. Pada *layer* ini terdapat tiga macam protocol, yaitu IP, ARP dan ICMP. *Internet Protocol* (IP) berfungsi untuk menyampaikan paket data ke alamat yang tepat. *Address Resolution Protocol* (ARP) adalah protokol yang digunakan untuk menemukan alamat *hardware* dari *host* / komputer yang terletak pada *network* yang sama. *Internet Control Messange Protocol* (ICMP) adalah protokol yang digunakan untuk mengirimkan pesan dan melaporkan pengiriman data.

3. *Transport Layer*

Berisi protokol yang bertanggung jawab untuk mengadakan komunikasi antara dua *host*/komputer. Kedua protokol tersebut adalah *Transmission Control Protocol* (TCP) dan *User Datagram Protocol* (UDP).

4. *Application layer*

*Application Layer* berfungsi menyediakan akses aplikasi terhadap jaringan TCP/IP. *Layer* ini menangani *high-level protocol*, dan dialog *control* yang memungkinkan terjadinya komunikasi antar aplikasi jaringan.

Pada *layer* ini *protocol* yang digunakan contohnya adalah *Simple Mail Transfer Protocol* (SMTP) digunakan untuk melayani pengiriman *email*, *File Transfer Protocol* (FTP) digunakan untuk *transfer* file, *Hyper Text Transfer Protocol* (HTTP) digunakan dalam aplikasi berbasis web, *Network News Transfer Protocol* (NNTP), *Telnet*, *Domain Name System* (DNS), *Dynamic Host Configuration* (DHCP).

### 2.5.2. Kelas – kelas *IP address*

*IP address* dibagi ke dalam kelas – kelas yang dibedakan berdasarkan *network ID* dan *host ID*. *Network ID* adalah bagian dari *IP address* yang menunjukkan lokasi jaringan komputer tersebut berada. Sedangkan *host ID* menunjukkan seluruh host TCP/IP yang lain dalam jaringan tersebut. Perbedaan pada tiap kelas tersebut adalah ukuran dan jumlahnya.

Tabel II. 1

#### *Class IP address*

IP address Classes				
Class	# Network Bits	# Hosts Bits	Decimal Address Range	Subnet mask
Class A	8 bits	24 bits	1-126	255.0.0.0
Class B	16 bits	16 bits	128-191	255.255.0.0
Class C	24 bits	8 bits	192-223	255.255.255.0
Class D	Reserved for Multicasting		224-239	N/A
Class E	Reserved for R. & D		240-255	N/A

Sumber : <http://bangbiw.com/>

1. Kelas A

*IP address* yang terdiri dari 8 bit untuk *network ID* dan 24 bit untuk *host ID*, sehingga *IP address* kelas A ini digunakan untuk jaringan dengan jumlah *host* sangat besar.

Rentang IP: 1.x.x.x – 127.x.x.x

Contoh : 10.1.2.54

Angka 10 masuk ke rentang 0 – 127 sehingga masuk ke kelas A.

2. Kelas B

*IP address* terdiri dari 16 bit untuk *network ID* dan 16 bit untuk *host ID*, sehingga *IP address* kelas B di gunakan untuk jaringan dalam jumlah *host* tidak terlalu besar.

Rentang IP : 128.1.x.x – 191.255.x.x

Contoh : 170.1.2.254

Angka 170 berada di antara 128 – 191, sehingga masuk ke kelas B.

3. Kelas C

*IP address* yang terdiri dari 24 bit untuk *network ID* dan sisanya 8 bit untuk *host ID*, sehingga IP kelas C digunakan untuk jaringan yang berukuran kecil. Kelas C biasanya digunakan untuk jaringan *local area network* atau LAN.

Rentang IP : 192.1.x.x – 223.255.255.x

Contoh : 192.10.1.1

Angka 192 berada di antara 192 – 223, sehingga termasuk kelas C.

#### 4. Kelas D dan E

Selain ketiga kelas *IP address* diatas,terdapat pula kelas *IP address* D dan E, namun kedua kelas ini tidak digunakan untuk alokasi IP secara normal tetapi digunakan untuk *IP multicasting* dan untuk eksperimental. Oktaf pertama untuk *IP address* kelas D berada pada *range* 224 – 239 dan untuk *IP address* kelas E berada pada *range* 240 – 255.

#### 2.5.3. Subnetting

*Item* kedua yang diperlukan agar TCP/IP bekerja adalah *subnet mask* . *Subnet mask* digunakan oleh protokol TCP/IP untuk menentukan apakah sebuah *host* ada pada *subnet* yang lokal atau pada jaringan *remote*. Di TCP/IP, bagian dari alamat penyuratan IP yang digunakan sebagai jaringan dan *host* alamat penyuratan tidak tetap, sehingga jaringan dan host alamat di atas tidak dapat ditentukan kecuali jika anda memiliki informasi lebih lanjut. Informasi ini disediakan dalam nomor 32 bit lain yang disebut *subnet mask*.

Dalam contoh ini *subnet mask* adalah 255.255.255.0 . Hal ini tidak jelas apa artinya ini nomor kecuali anda tahu bahwa 255 dalam notasi biner sama dengan 11111111 jadi, *subnet mask* adalah : 11111111.11111111.11111111.00000000

Berbaris IP alamat penyuratan dan *subnet mask* bersama – sama, jaringan dan bagian host alamat penyuratan dapat dipisahkan contoh:

11000000.10101000. 01111011.10000100 *IP address* (192.168.132.132)

11111111.11111111.11111111.00000000 *Subnet mask* ( 255.255.255.0)

24 bit pertama ( jumlah yang di *subnet mask* ) diidentifikasi sebagai alamat penyuratan jaringan dengan 8 bit terakhir ( jumlah sisa nol dalam *subnet mask* ) diidentifikasi sebagai alamat penyuratan *host*. contoh :

11000000. 10101000. 01111011.00000000 *Network address* ( 192.168.123.0 )

00000000.00000000.00000000.10000100 *Host address* ( 000.000.000.132 ).

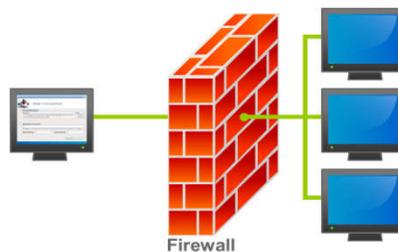
## 2.6. Sistem keamanan jaringan

### 2.6.1. Contoh system keamanan jaringan

#### 1. *Firewall*

Menurut thowijhojo ( 2013 :15 ) *firewall* adalah “ keamanan jaringan dengan menentukan paket apa saja yang bisa masuk ataupun keluar dari jaringan tersebut. Untuk menentukan paket mana yang akan diterima atau dibuang, *firewall* akan memeriksa *header* dari sebuah IP paket.

Umumnya yang akan diperiksa pada *header* adalah IP address pengirim, IP address tujuan, jenis protokol, port pengirim, port tujuan , bahkan *fragmentation* yang terjadi pada paket juga dpat diperiksa oleh *firewall*.



Sumber : <http://berbagicatatn.web.id/>

Gambar II. 22

*Firewall*

## 2. *Proxy*

*Proxy Server* adalah server yang diletakkan antara suatu aplikasi client dan aplikasi server yang dihubungi. Aplikasi *client* dapat berupa *browser web*, *client FTP*, dan sebagainya. Sedangkan aplikasi server dapat berupa *server web*, *server FTP* dan sebagainya.

*Proxy Server* merupakan pihak ketiga yang menjadi perantara antara kedua pihak yang saling berhubungan, dalam hal ini adalah jaringan lokal dan jaringan internet. Secara prinsip pihak pertama dan pihak kedua tidak langsung berhubungan, akan tetapi masing-masing berhubungan dengan pihak ketiga yaitu *proxy*.

Tiga fungsi utama *proxy server* adalah:

### a. *Connection sharing*

Bertindak sebagai *gateway* yang menjadi batas antara jaringan lokal dan jaringan luar. *Gateway* juga bertindak sebagai titik dimana sejumlah koneksi dari pengguna lokal akan terhubung kepadanya dan koneksi jaringan luar juga terhubung kepadanya. Dengan demikian koneksi dari jaringan lokal ke internet akan menggunakan sambungan yang dimiliki oleh *gateway* secara bersama-sama (*connection sharing*).

### b. *Filtering*

Bekerja pada layar aplikasi sehingga berfungsi sebagai *Firewall* paket *filtering* yang digunakan untuk melindungi jaringan lokal terhadap gangguan atau serangan dari jaringan luar. Dapat dikonfigurasi untuk menolak situs web tertentu pada waktu-waktu tertentu.

### c. *Caching*

*Proxy Server* memiliki mekanisme penyimpanan obyek-obyek yang sudah diminta dari server-server di internet. Mekanisme *caching* akan menyimpan obyek-obyek yang merupakan permintaan dari para pengguna yang di dapat dari internet.

### 2.6.2. **Macam – macam ancaman sistem keamanan jaringan**

Terdapat banyak ancaman yang mungkin terjadi terhadap sistem keamanan jaringan , diantaranya :

1. Pencurian perangkat keras komputer atau perangkat keras jaringan.
2. Kerusakan pada komputer atau perangkat komunikasi jaringan.
3. Kerusakan pada sistem operasi atau aplikasi yang disebabkan oleh virus.
4. *Sniffing* yaitu kegiatan memonitor proses yang sedang berlangsung di jaringan.
5. *Spoofing* yaitu penggunaan komputer untuk meniru, dengan cara menimpa identitas (*MAC address* ) atau alamat IP.
6. *Phreaking* yaitu perilaku menjadikan sistem pengamanan komunikasi melemah.
7. *Remote attack* yaitu segala bentuk serangan terhadap suatu sistem dimana penyerangnya tidak memiliki kendali terhadap suatu mesin tersebut karena dilakukan dari jarak jauh di luar sistem jaringan.
8. *Hole* yaitu suatu kondisi dari *software* atau *hardware* yang bisa diakses oleh pemakai yang tidak memiliki otoritas atau meningkatnya tingkat pengaksesan tanpa melalui proses otorisasi.

9. *Hacking* merupakan kegiatan yang dilakukan secara diam – diam bertujuan mempelajari sistem yang biasanya sukar dimengerti untuk kemudian mengelola dan membagi hasil uji coba yang dilakukannya tanpa merusak sistem yang ada.
10. *Cracking* merupakan kegiatan yang serupa dengan *hacking* dengan tujuan jahat bahkan biasanya merusak sistem yang ada.