

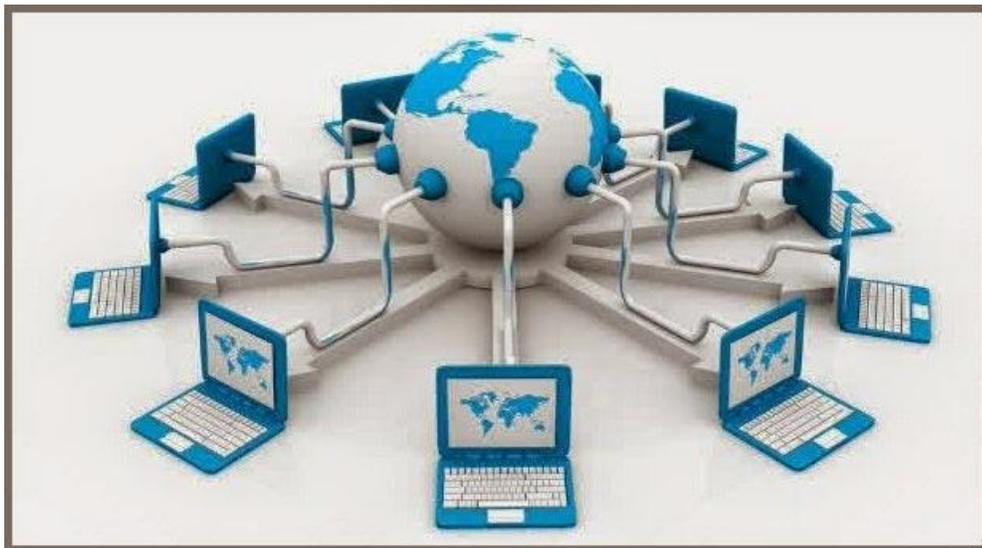
## **BAB II**

### **LANDASAN TEORI**

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

Menurut Sofana (2013:3) “Suatu himpunan interkoneksi sejumlah komputer *autonomous*. Dalam bahasa yang populer dapat dijelaskan bahwa jaringan komputer adalah kumpulan beberapa komputer (dan perangkat lain seperti *router*, *switch*, dan sebagainya) yang saling terhubung satu sama lain melalui media perantara”.

Sedangkan Menurut Irawan (2005:5) “Jaringan Komputer adalah sebuah *system* yang terdiri atas komputer dan perangkat jaringan lainnya yang berkerja bersama-sama untuk mencapai suatu tujuan yang sama”.



Sumber: <http://nesabamedia.com/pengertian-manfaat-dan-macam-macam-jaringan-komputer/>

**Gambar II.1**  
**Jaringan Komputer**

### 2.1.1 Jenis-jenis Jaringan Komputer

Berdasarkan Jangkauan area atau lokasi, jaringan di bedakan menjadi beberapa jenis yaitu:

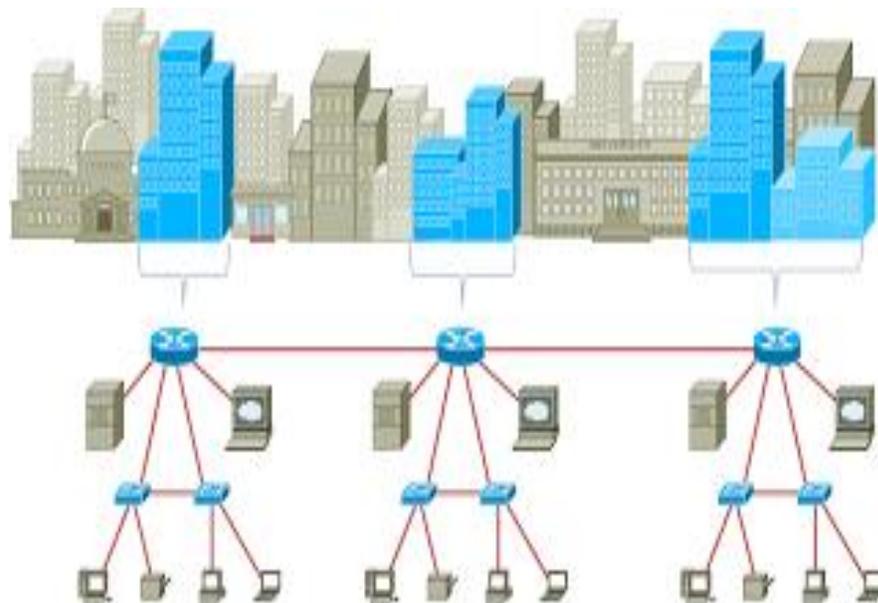
1. Menurut MADCOM (2015:3) *Personal Area Network (PAN)* yaitu saat anda menghubungkan komputer keperangkat lain seperti *handphone, personal digital assitant, keyboard, mouse, headset wireless*, kamera dan peralatan lain yang jarak nya cukup dekat sekita 4-6 meter, maka anda telah membentuk suatu sistem jaringan pribadi atau *Personal Area Network (PAN)*. Dalam hal ini yang paling penting adalah yang mengendalikan (*authority*) pada peralatan tersebut. *Personal Area Network (PAN)* juga sering dibentuk diteknologi *wireless* atau nirkabel seperti *bluetooth, infrared* atau *wifi*.



Sumber: <http://www.catatanteknisi.com/2012/05/jaringan-komputer-pan-lan-man-wan.html>

**Gambar II.2**  
***Personal Area Network (PAN)***

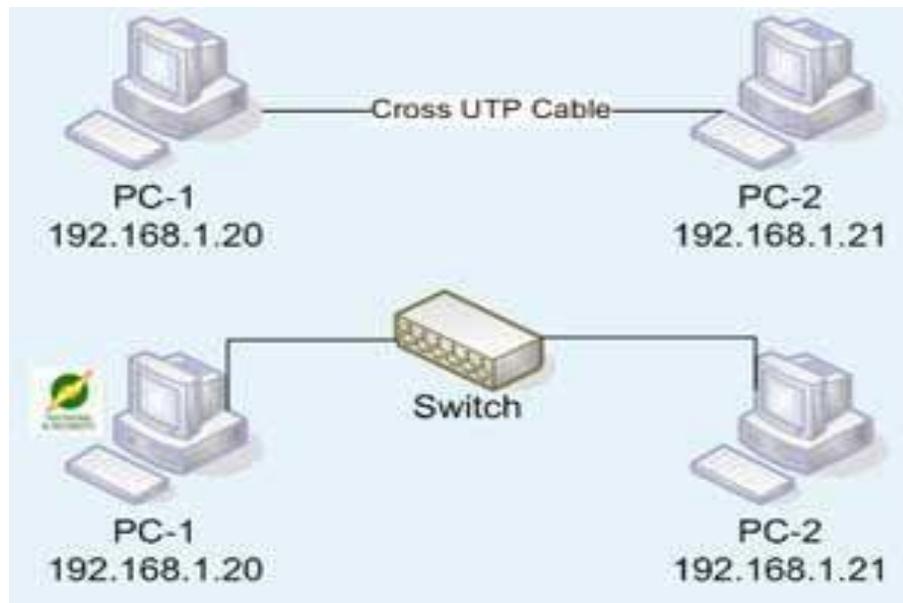
2. Menurut Sofana (2009:112) “*Metropolitan Area Network (MAN)* merupakan jaringan komputer yang meliputi area seukuran kota atau gabungan beberapa LAN (*Local Area Network*) yang dihubungkan menjadi sebuah jaringan besar, MAN (*Metropolitan Area Network*) dapat memanfaatkan jaringan TV kabel yang umumnya menggunakan kabel *coaxial* atau serat optik”.



Sumber:<http://tekaje.indonesiaz.com/pengertian-dan-fungsi-man-pada-jaringan.xhtml>

**Gambar II.3**  
**Jaringan MAN (*Metropolitan Area Network*)**

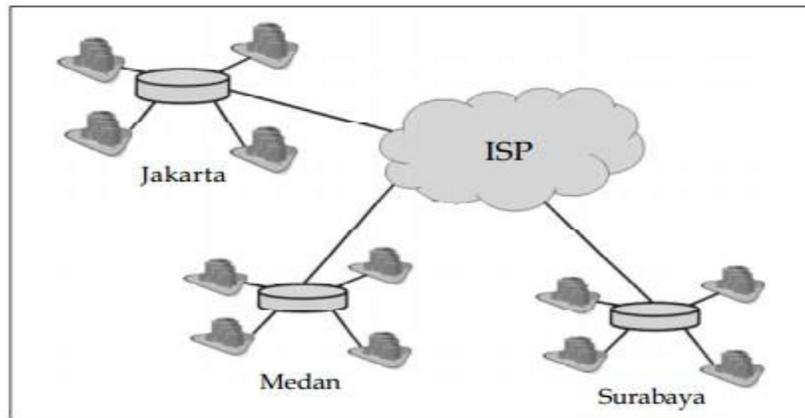
3. Menurut Sofana (2009:113) “LAN (*Local Area Network*) beberapa buah PC dapat membentuk *network*, berhubungan dengan area *network* yang berukuran relatif kecil. Oleh karena itu, LAN (*Local Area Network*) dapat dikembangkan dengan mudah dan mendukung kecepatan transfer data cukup tinggi”.



Sumber: <http://www.it-artikel.com/2012/10/skema-jaringan-komputer.html>

**Gambar II.4**  
**Jaringan LAN (*Local Area Network*)**

4. Menurut Sofana (2009:127) “WAN (*Wide Area Network*) memahami seluk beluk sebuah LAN (*Local Area Network*) merupakan langkah awal untuk memahami teknologi jaringan secara umum”. Manakala LAN (*Local Area Network*) dihubungkan dengan media komunikasi publik atau lainnya, seperti jaringan telepon dan melibatkan area geografis yang cukup besar, Seperti antarnegara antarbenua, maka model jaringan berskala besar disebut WAN (*Wide Area Network*).



Sumber: <http://www.it-artikel.com/2015/08/jaringan-berdasarkan-area-kerja.html>

**Gambar II.5**  
**Jaringan WAN (*Wide Area Network*)**

Teknologi yang biasanya dipakai dalam WAN, antara lain:

*Modem, ISDN (Integrated Services Digital Networks), framerelay, ATM (Asynchronous Transfer Mode), DSL (Digital Subscriber Line), T (US) dan E (Europe) Carrirer Series seperti T1, E1, T3, E3, SONET (Synchronous Optical Network)*

5. Menurut Sofana (2013:5) “*Internet* adalah interkoneksi jaringan komputer skala besar (mirip WAN), yang dihubungkan menggunakan protokol khusus. Jadi sebenarnya *Internet* merupakan bagian dari WAN (*Wide Area Netwrok*)”. Cakupan *Internet* adalah satu dunia bahkan tidak menutup kemungkinan antarplanet. Koneksi antarjaringan komputer dapat dilakukan berkat dukungan prokotel khas, yaitu TCP/IP(*Transmission Control Protocol / Internet Protocol*).

### 2.1.2 Tipe Jaringan Komputer Berdasarkan Pola Operasi

Menurut Sofana (2013:7) ”Berdasarkan pola operasi atau fungsinya, jaringan komputer dapat dibagi menjadi 2 (dua) jenis, yaitu”:

#### 1. *Client Server*

Menurut Sofana (2013:7) “*Client Server* adalah jaringan komputer yang mengharuskan salah satu (atau lebih) komputer difungsikan sebagai *server* atau *central*. *Server* melayani komputer lain disebut *client*”. Layanan yang diberikan bisa berupa *Web*, *e-mail*, *file* atau yang lain. *Client Server* banyak dijumpai pada jaringan *Internet*. Namun LAN (*Local Area Network*) atau jaringan lain pun bisa mengimplementasikan *client server*. Hal ini sangat bergantung pada kebutuhan masing-masing.

#### 2. *Peer To Peer*

Menurut Sofana (2013:7) “*Peer To Peer* adalah jaringan komputer dimana setiap komputer bisa menjadi *server* sekaligus *client*. Jadi tidak ada komputer yang ”lebih utama” dibandingkan komputer lain”. Setiap komputer dapat menerima dan memberikan *access* dari/ke komputer lain. *Peer To Peer* banyak di implementasikan pada LAN (*Local Area Network*). Walaupun dapat juga diimplementasikan pada MAN (*Metropolitan Area Network*), WAN (*Wide Area Network*), atau *Internet*, namun hal ini kurang lazim. Salah satu alasannya adalah masalah manajemen dan *security*. Cukup sulit menjamin *security* pada jaringan *Peer To Peer* manakala pengguna komputer sudah sangat banyak.

### 2.1.3 Tipe Jaringan Komputer Berdasarkan Media Penghantar

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

#### 1. *Wire Network*

Menurut Sofana (2013:6) “*Wire Network* adalah jaringan komputer yang menggunakan kabel sebagai media penghantar. Jadi, data mengalir pada kabel. Kabel yang umum digunakan pada jaringan komputer biasanya berbahan dasar tembaga”. Ada juga jenis kabel lain yang menggunakan bahan jenis *fiber* yang disebut *fiber optic* atau serat optik. Biasanya bahan tembaga banyak digunakan pada LAN (*Local Area Network*). Sedangkan untuk MAN (*Metropolitan Area Network*) atau WAN (*Wide Area Network*) menggunakan gabungan kabel tembaga dan serat optik. Serat optik saat ini sudah semakin populer.

#### 2. *Wireless Network*

Menurut Sofana (2013:6) “Jaringan tanpa kabel yang menggunakan media penghantar gelombang radio atau cahaya *infrared* atau LASER”. Saat ini sudah semakin banyak *public area* 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 dikisaran 2.4 GHz dan 5.8 GHz. Sedangkan penggunaan *infrared* dan LASER umumnya hanya terbatas untuk jenis jaringan yang hanya melibatkan dua buah komputer saja atau disebut *point to point*

#### 2.1.4 Manfaat Jaringan Komputer

Menurut Abdullah (2002:14) “Manfaat jaringan komputer bagi manusia adalah sebagai berikut”:

##### 1. *Resource sharing*

Menurut Abdullah (2002:14) “Bertujuan agar seluruh program, peralatan, khususnya data dapat digunakan oleh setiap orang yang ada pada jaringan tanpa terpengaruh oleh lokasi *resource* dan pemakai. Jadi *source sharing* adalah suatu usaha untuk menghilangkan kendala jarak”.

##### 2. Reliabilitas tinggi

Menurut Abdullah (2002:14) “Yaitu adanya sumber-sumber alternatif pengganti jika terjadi masalah pada salah satu perangkat dalam jaringan, artinya karena perangkat yang digunakan lebih dari satu jika salah satu perangkat mengalami masalah, maka perangkat yang lain dapat menggantikannya”.

##### 3. Skalabilitas

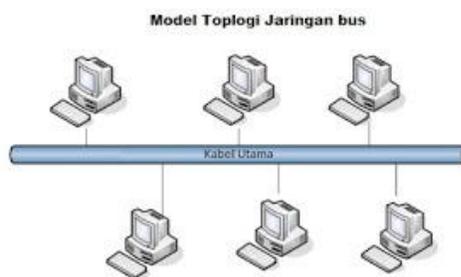
Menurut Abdullah (2002:14) “Yaitu kemampuan untuk meningkatkan kinerja sistem secara berangsur-angsur sesuai dengan bahan, hanya menambahkan sejumlah prosesor. Sejumlah jaringan komputer mampu bertindak sebagai media komunikasi yang bagi para pegawai yang terpisah jauh”.

## 2.2 Topologi Jaringan Komputer

Menurut Sofana (2013:7) “Topologi dapat diartikan sebagai layout atau arsitektur atau diagram jaringan komputer. Topologi merupakan suatu aturan/*rules* bagaimana menghubungkan komputer (*node*) secara fisik. Topologi berkaitan dengan cara komponen-komponen jaringan (seperti: *server*, *workstation* ,*switch*) saling berkomunikasi melalui media transmisi data”.

### 2.2.1 Topologi Jaringan Bus

Menurut Sofana (2013:10) “ Topologi *bus* Sering juga disebut *daisy chain* atau *ethernet bus topologies*. Sebutan terakhir diberikan karena pada topologi *bus* digunakan perangkat jaringan atau *network interface card* (NIC) bernama *ethernet*”. Jaringan yang menggunakan topologi *bus* dapat dikenali dari penggunaan kabel *backbone* (kabel utama) yang menghubungkan semua peralatan jaringan (*device*). Karena kabel *backbone* menjadi satu-satunya jalan bagi lalu lintas data maka apabila kabel *backbone* rusak atau terputus akan menyebabkan jaringan terputus total.



Sumber: <http://www.teorikomputer.com/2012/08/topologi-bus-pengertian-keuntungan-dan.html>

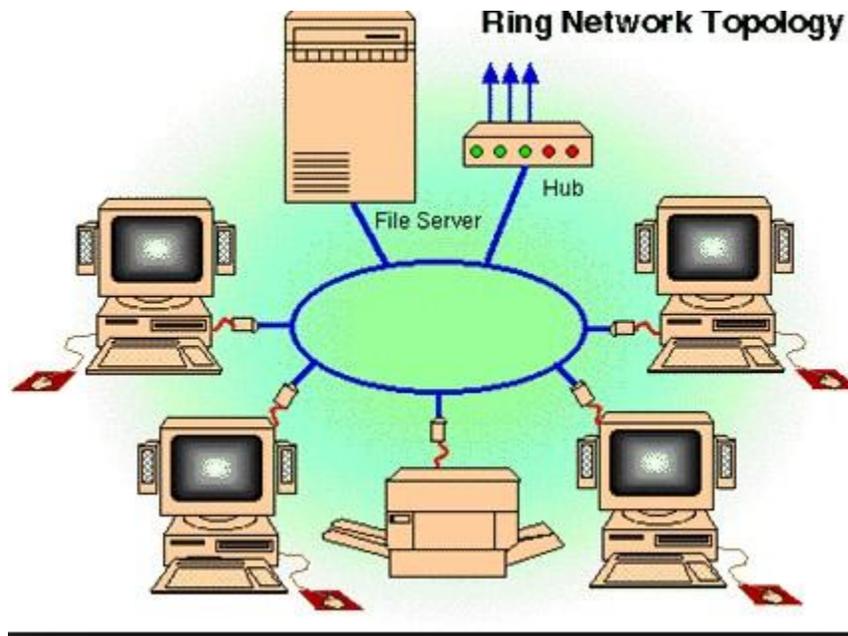
**Gambar II.6**  
**Topologi Bus**

Keuntungan topologi *bus* adalah hemat kabel, karena pada topologi *bus* hanya menggunakan kabel tunggal dan terpusat sebagai media transmisi sehingga tidak membutuhkan banyak kabel. *Layout* kabel sederhana, pada pemasangan topologi *bus* rancangan dan skema kabel yang digunakan sangat sederhana sehingga mudah dalam pemasangannya. Pengembangan jaringan komputer atau penambahan komputer baru baik sebagai *server* maupun *client* dapat dilakukan dengan mudah tanpa mengganggu komputer atau *workstation* yang lain.

Kerugian topologi *bus* adalah deteksi dan isolasi kesalahan sangat kecil sehingga jika jaringan mengalami gangguan, maka akan lebih sulit untuk mengidentifikasi kesalahan yang ada. Kepadatan lalu lintas pada jalur utama, karena topologi *bus* menggunakan kabel terpusat sebagai media transmisi maka lalu lintas data akan sangat padat pada kabel utama. Jika kabel utama mengalami gangguan maka seluruh jaringan akan mengalami gangguan pula. Diperlukan *repeater* sebagai penguat sinyal jika akan menambahkan *workstation* dengan lokasi yang jauh.

### **2.2.2 Topologi Jaringan *Ring***

Menurut Sofana (2013:22) “Topologi *ring* sangat berbeda dengan Topologi bus. Sesuai dengan namanya, jaringan yang menggunakan topologi ini dapat dikenali dari kabel *backbone* yang membentuk cincin. Setiap komputer terhubung dengan kabel *backbone*. Setelah sampai pada komputer terakhir maka ujung kabel akan kembali dihubungkan dengan komputer pertama”.



Sumber: <http://ahmadarib.com/topologi-jaringan-komputer-penjelasan-pengertian-jenisnya.html>

### **Gambar II.7** **Topologi Ring**

Kelebihan dari topologi *ring* mudah dirancang dan diimplementasikan, memiliki performa yang baik dari pada topologi *bus*, bahkan untuk aliran data yang berat sekalipun, mudah untuk melakukan konfigurasi ulang dan instalasi perangkat baru, mudah untuk melakukan pelacakan dan pengisolasian kesalahan dalam jaringan karena menggunakan *point to point*, hemat kabel, tidak akan terjadi tabrakan pengiriman data (*collision*), karena pada satu waktu hanya satu *node* yang dapat mengirimkan data.

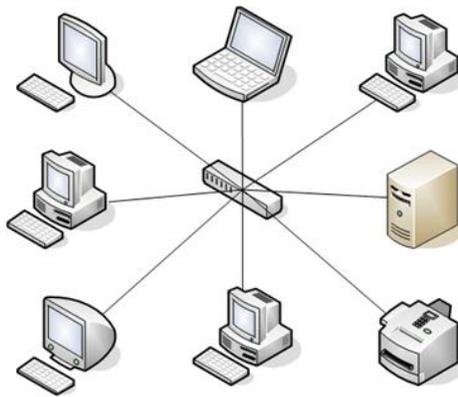
Kekurangan dari topologi *ring* peka kesalahan, sehingga jika terdapat gangguan di suatu *node* mengakibatkan terganggunya seluruh jaringan. Namun hal ini dapat diantisipasi dengan menggunakan cincin ganda (*dual ring*). Pengembangan

jaringan lebih kaku, karena memindahkan, menambah dan mengubah perangkat jaringan dan mempengaruhi keseluruhan jaringan.

Kinerja komunikasi dalam jaringan sangat tergantung pada jumlah titik/*node* yang terdapat pada jaringan. Lebih sulit untuk dikonfigurasi dari pada topologi *star*, diperlukan penanganan dan pengelolaan khusus *bundles*.

### 2.2.3 Topologi Jaringan *Star*

Meurut Sofana (2013:33) “Topologi *star* dikenali dengan keberadaan sebuah sentral berupa *hub* yang menghubungkan semua *node*. Setiap *node* menggunakan sebuah kabel UTP (*Unshielded Twisted Pair*) atau STP (*Shielded Twisted Pair*) yang di hubungkan melalui *ethernet card* ke *hub*. Banyak sekali jaringan rumah, sekolah pertokoan, laboratorium dan kantor yang menggunakan topologi ini. Topologi *star* tampaknya paling populer di antara semua topologi yang ada”.



Sumber:<http://www.pintarkomputer.com/ciri-karakteristik-kelebihan-dan-kekurangan-topologi-star/>

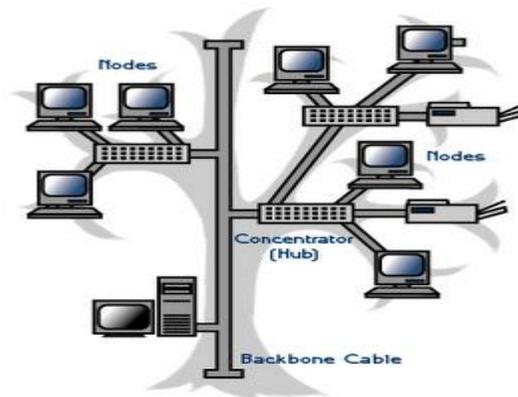
**Gambar II.8**  
**Topologi *Star***

Kelebihan topologi *star* Mudah untuk menambah atau mengembangkan koneksi. Termasuk mudah dalam melakukan *troubleshooting*. Jika terdapat masalah pada salah satu koneksi, maka tidak berdampak pada seluruh jaringan

Kekurangan topologi *star* seluruh koneksi bergantung pada terminal pusat, jika terjadi masalah pada terminal pusat maka akan terjadi kegagalan koneksi secara menyeluruh, boros dalam penggunaan kabel, biaya installasi termasuk mahal, salah satu penyebabnya karena kebutuhan kabel sebagai media penghubung yang banyak, satu koneksi butuh satu kabel.

#### **2.2.4 Topologi Jaringan *Tree***

Menurut Sofana (2013:54) “Topologi *tree* disebut juga topologi *star-bus* atau *star/bus hybrid*. Topologi *tree* merupakan gabungan beberapa topologi *star* yang dihubungkan dengan topologi *bus*. Topologi *tree* digunakan untuk menghubungkan beberapa LAN (*Local Area Network*) dengan LAN (*Local Area Network*) lain”. Hubungan antar-LAN dilakukan via *hub*. Masing-masing pohon (*tree*). Topologi *tree* dapat mengatasi kekurangan topologi *bus* yang disebabkan persoalan *broadcast traffic*, dan kekurangan topologi *star* yang disebabkan oleh keterbatasan kapasitas *port hub*.



Sumber : <https://www.utopiccomputers.com/model-topologi-jaringan-komputer-yang-sering-digunakan/>

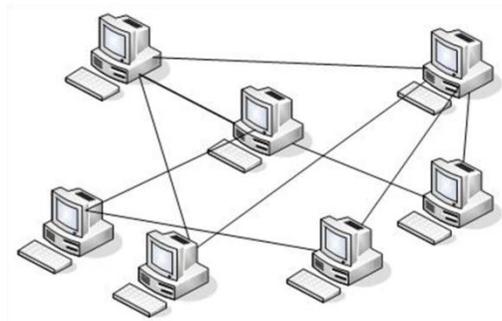
**Gambar II.9**  
**Topologi Tree**

Kelebihan topologi *tree* kelompok jaringan yang berada dibawah *hub* pusat dapat melakukan pengembangan atau penambahan *client* dengan mudah, *Scalable*. Komunikasi terjadi secara *point to point*, mengatasi keterbatasan dari topologi jaringan star yang memiliki keterbatasan pada titik koneksi *hub* dan keterbatasan lalu lintas yang diinduksi pada topologi *Bus*, karena dilakukan pengelompokan maka pendeteksian masalah jadi lebih mudah, jika salah satu *client* mati maka yang lain tidak akan terpengaruh (sifat topologi *star*).

Kekurangan Topologi *Tree* kinerja jaringan secara keseluruhan bergantung pada *hub* Pusat, apabila *hub* rusak maka jaringan akan terganggu (sifat topologi *star*), komunikasi yang tidak bisa dilakukan secara langsung antar komputer, melainkan harus melalui *hub* terlebih dahulu, karena melalui sebuah kabel utama maka lalu lintas data sangat padat, meskipun dari segi pendeteksian masalah lebih mudah, namun dari segi perawatan topologi ini cukup sulit.

### 2.2.5 Topologi Jaringan *Mesh*

Menurut Sofana (2013:55) “Topologi *mesh* dapat dikenali dengan hubungan *point to point* atau satu-satu ke setiap komputer. Setiap Komputer terhubung ke komputer lain melalui kabel, bisa menggunakan kabel *coaxsial*, *twisted pair*, bahkan serat optik”. Topologi *mesh* sangat jarang diimplementasikan, Selain rumit juga sangat boros kabel, apabila jumlah komputer semakin banyak maka instalasi kabel jaringan juga akan semakin rumit. Topologi *mesh* cocok digunakan pada jaringan yang sangat kritis. Pada awalnya jaringan *mesh* dikembangkan untuk keperluan militer, dan barangkali pusat kontrol senjata nuklir menggunakan topologi ini juga, apabila satu atau beberapa kabel putus masih tersedia *rute alternatif* melalui kabel lain.



Sumber : <https://www.utopicomputers.com/model-topologi-jaringan-komputer-yang-sering-digunakan/>

**Gambar II.10**  
**Topologi *Mesh***

## 2.3 Perangkat Jaringan Komputer

Menurut Irawan (2013:7) “Dalam membangun sebuah jaringan komputer dibutuhkan perangkat keras khusus yang berhubungan dengan kebutuhan jaringan yang akan dibangun. Berikut adalah beberapa peralatan jaringan yang umum digunakan untuk jaringan berbasis *nirkabel*”.

### 2.3.1 NIC

Menurut Sofana (2009:325) ”NIC (*Network Interface Card*) merupakan perangkat wajib yang harus dimiliki agar sebuah komputer dapat terhubung ke *network*. NIC menyediakan akses ke media fisik jaringan. Tegangan listrik, arus, gelombang elektromagnetik, dan besaran fisik lainnya dibentuk dan ditentukan oleh NIC. NIC berkerja pada *layer* pertama OSI atau *layer Physical*”. Jenis NIC yang lazim digunakan adalah *Ethernet Card*. Berdasarkan kecepatan Transmisi, *ethernet card* dibedakan menjadi beberapa, diantaranya:

1. 10BASE-T (*Standar Ethernet*) yang menyediakan kecepatan transmisi sampai dengan 10 Mbps.
2. 100BASE-T (*Fast Ethernet*) yang menyediakan kecepatan transmisi sampai dengan 100 Mbps.
3. 1000BASE-T (*Gigabit Ethernet*) yang menyediakan kecepatan transmisi sampai dengan 1 Gbps



Sumber: <http://www.newegg.com/Network-Interface-Cards/SubCategory/ID-27>

**Gambar II.11**  
***Ethernet Card***

### **2.3.2 Router**

Menurut Sofana (2009:58) “*Router* sering digunakan untuk menghubungkan beberapa *Network*. Baik *network* yang sama maupun yang berbeda dari segi teknologinya. *Router* secara cerdas dapat mengetahui kemana *route* perjalanan informasi (yang disebut *packet*) akan dilewatkan. *Router* juga digunakan untuk membagi *network* besar menjadi sebuah *subnetwork* (*network-network* kecil)”.



Sumber: <http://www.cisco.com/en/US/docs/routers/access/1700/1720/hardware/quick/guide/1700qsg.html>

**Gambar II.12**  
***Router Cisco Series 1700***

### 2.3.3 Bridge

Menurut Sofana (2009:67) “*Bridge* atau kadangkala disebut *transparent bridge* merupakan perangkat *network* yang digunakan untuk menghubungkan dua buah LAN (*Local Area Network*) atau membagi sebuah LAN (*Local Area Network*) menjadi dua buah segmen. Tujuannya adalah untuk mengurangi *traffic* sedemikian rupa sehingga dapat meningkatkan performa *network*”.



Sumber : <http://www.teorikomputer.com/2015/10/pengertian-dan-fungsi-bridge-pada.html>

**Gambar II.13**  
**Bridge**

### 2.3.4 Switch

Menurut Sofana (2009:70) “Cara kerja *Switch* mirip dengan *Bridge*, dan memang sesungguhnya *switch* adalah *bridge* yang memiliki banyak *port*. Sehingga *switch* disebut sebagai *multiport bridge*”. *Switch* berfungsi sebagai sentral atau kosentrator pada sebuah *network*. *Switch* dapat mempelajari alamat *hardware host* tujuan, sehingga informasi bisa langsung dikirim ke *host* tujuan. *Switch* yang lebih cerdas dapat mengecek *frame* yang *error* dan dapat mem-*block frame* yang *error* tersebut.



Sumber: <http://www.infoteknologi.com/perbedaan-hub-dan-switch/>

**Gambar II.14**  
*Switch*

### 2.3.5 Hub

Menurut Sofana (2009:75) “*Hub* mirip dengan *switch*, yaitu sebagai kosentrator. Namun, *hub* tidak secerdas *switch*. Jika informasi dikirim ke *host* target melalui *hub* maka informasi akan mengalir ke semua *host*. Kondisi semacam ini dapat menyebabkan beban *traffic* yang tinggi. Oleh sebab itu, sebuah *hub* biasanya hanya digunakan pada *network* berskala kecil”.



Sumber: <http://www.teorikomputer.com/2012/11/pengertian-dan-fungsi-hub.html>

**Gambar II.15**  
*Hub*

### 2.3.6 Repeater

Menurut Sofana (2013:69) ”*Repeater* merupakan salah satu contoh *active hub*. *Reapeater* merupakan peralatan yang dapat menerima sinyal kemudian memperkuat dan mengirim kembali *signal* tersebut ke tempat lain”. Sehingga *signal* dapat menjangkau tempat-tempat yang jauh karena *repeater* bekerja pada besaran fisik seperti tegangan listrik, arus listrik, gelombang elektromagnetik untuk itu *repeater* dalam kategori peralatan yang bekerja pada *layer physical*.



Sumber : <http://dosenit.com/jaringan-komputer/hardware-jaringan/fungsi-repeater>

**Gambar II.16**  
***Repeater***

### 2.3.7 Network Switch

Menurut Sofana (2013:72) “*Network Switch* selain *repeater*, *bridge*, dan *router* terdapat sejumlah peralatan *switching* yang dapat digunakan dalam membangun *internetwork*”. Peralatan *switch* didesain dengan tujuan yang berbeda dengan *repeater*, *bridge*, dan *router*. Jika perangkat jaringan yang terhubung pada sebuah LAN (*Local Area Network*) terlalu banyak, maka kebutuhan transmisi meningkat melebihi kapasitas yang mampu dilayani oleh media transmisi jaringan. Cara kerja *switch* mirip dengan *bridge*, sehingga kadangkala *switch* disebut sebagai *multiple*

*bridge* dan setiap *host* yang terkoneksi akan mendapatkan *full bandwidth*. *Switch* memiliki beberapa kelebihan dibandingkan *bridge* antara lain dalam hal *forwarding method* paket yang dilewatkan.



Sumber : <http://www.officeworks.com.au/shop/officeworks/p/netgear-prosafe-jgs516-switch-ngjgs516>

**Gambar II.17**  
**Network Switch**

### **2.3.8 Gateway**

Menurut Sofana (2013:73) “*Gateway* adalah sebuah perangkat yang digunakan untuk menghubungkan satu jaringan komputer dengan satu atau lebih jaringan komputer yang menggunakan protokol komunikasi yang berbeda sehingga informasi dari satu jaringan komputer dapat diberikan kepada jaringan komputer lain yang protokolnya berbeda”. Bekerja dan bertugas melewatkan paket antara jaringan dengan protokol yang berbeda, sehingga perbedaan tersebut tidak tampak pada lapisan aplikasi. Kadang kala *gateway* biasa disebut *IP router*. *Gateway* bekerja pada *layer application*. Istilah *gateway* merujuk kepada *hardware* atau *software* yang menjembatani dua aplikasi atau jaringan yang tidak kompatibel, sehingga data dapat ditransfer antar komputer yang berbeda-beda. Salah satu contoh penggunaan *gateway*

adalah pada *email*, sehingga pertukaran *email* dapat dilakukan pada sistem yang berbeda.

### **2.3.9 Access Point**

Menurut Irawan (2013:28) “*Access Point (AP)* adalah sebuah *node* yang telah dikonfigurasi secara khusus pada sebuah WLAN (*Wireless Local Area Network*). *Access Point* bertindak sebagai pusat pemancar dan penerima untuk sinyal-sinyal radio WLAN (*Wireless Local Area Network*)”. *Access Point* sering disebut juga *base station*. AP (*Access Point*) merupakan salah satu perangkat yang dapat mendukung akses jaringan tanpa kabel atau WLAN (*Wireless Local Area Network*). *Wireless devices* jenis AP (*Access Point*) menggunakan gelombang radio sebagai media transmisinya. Fungsi utama dari AP (*Access Point*) adalah sebagai pusat koneksi. AP (*Access Point*) dapat dikatakan mempunyai fungsi seperti *switch* pada jaringan transmisi kabel. AP (*Access Point*) menyediakan perangkat seperti radio penerima yang mampu menerima gelombang lain dari AP (*Access Point*) atau media *wireless* lain seperti USB *wireless*.

Selain itu AP (*Access Point*) juga menyimpan perangkat lunak yang mampu berkomunikasi dan mengenkripsikan data serta *port virtual* untuk menghubungkannya dengan jaringan *wired* (jaringan yang menggunakan kabel). *Interface* untuk mengatur setting AP (*Access Point*) dilakukan dengan memasukkan alamat IP perangkat AP (*Access Point*) melalui *browser*, beberapa konfigurasi dilakukan, diantaranya dengan:

1. Mengatur supaya AP(*Access Point*) dapat berfungsi sebagai DHCP (*Dynamic Host Configuration Protocol*)server.
2. Mencoba fitur *Wired Equivalent Privacy* (WEP) dan *Wi-Fi Protected Access* (WPA).
3. Mengatur akses berdasarkan *MAC Address devices* pengakses.



Sumber : <http://belajar-komputer-mu.com/pengertian-wireless-access-point-fungsi-access-point-penerapan-access-point/>

**Gambar II.18**  
*Access Point*

### 2.3.10 Kabel Jaringan

Menurut Irawan (2013:8)“Kabel jaringan berfungsi sebagai media penghubung antara *node* didalam 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*”. Berikut ini beberapa jenis kabel yang digunakan pada jaringan komputer:

#### 1. Kabel *Coaxial* (*Wired Network*)

Menurut Irawan (2013:8) “Kabel ini di lindungi 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 pengaruh elektromagnetik”.



Sumber: <http://tech.dbagus.com/fungsi-kabel-coaxial-beserta-kelebihan-dan-kelemahan>

**Gambar II.19**  
**Kabel Coaxial**

## 2. Kabel *Unshielded Twisted Pair* (UTP) , *Shielded Twisted Pair* (STP)

Menurut Irawan (2013:9) “Kabel jaringan dengan bahan tembaga yang tidak di lengkapi pelindung. UTP (*Unshielded Twisted Pair*) merupakan jenis kabel yang paling banyak digunakan untuk membangun jaringan, khususnya jaringan LAN (*Local Area Network*)”. Kabel UTP (*Unshielded Twisted Pair*) kategori 5e (cat5e) adalah salah satu yang paling banyak digunakan untuk membangun LAN (*Local Area Network*).

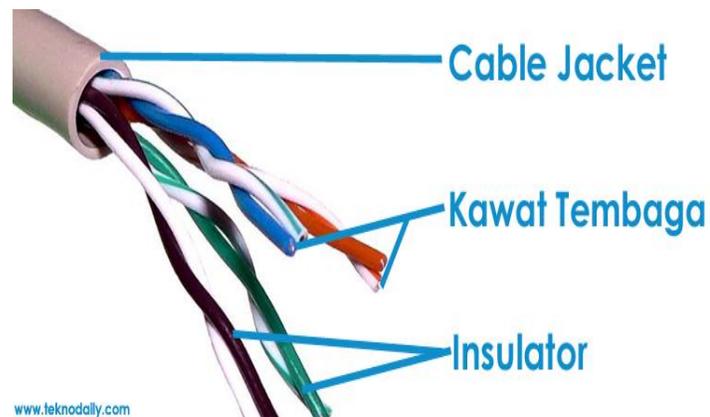
Menurut Irawan (2013:9) “Kabel STP (*Shielded Twisted Pair*) sama dengan kabel UTP (*Unshielded Twisted Pair*), tetapi memiliki pelindung (*shield*) lapisan aluminium foil untuk mencegah gangguan interferensi saat melakukan transmisi data”. Standar urutan kabel UTP (*Unshielded Twisted Pair*) sudah diatur oleh EIA/TIA (*Electronic Industries Alliance/ Telecommunication Industries Association*).

Standarisasi urutan kabel tersebut dibagi menjadi 2, dari tabel berikut ini

**Tabel II.1**  
**Standarisasi Kabel UTP**

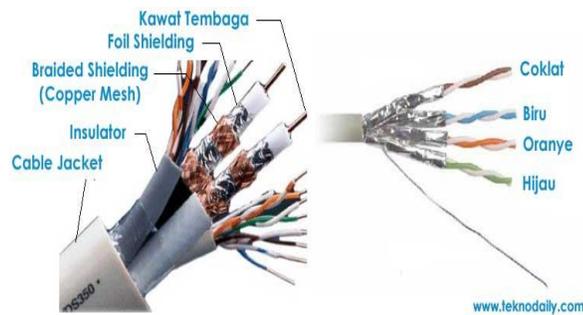
EIA/TIA 568A / T-568A		EIA/TIA 568B / T-568B	
1.	Putih Hijau	1.	Putih Orange
2.	Hijau	2.	Orange
3.	Putih Orange	3.	Putih Hijau
4.	Biru	4.	Biru
5.	Putih Biru	5.	Putih Biru
6.	Orange	6.	Hijau
7.	Putih Coklat	7.	Putih Coklat
8.	Coklat	8.	Coklat

Sumber: Irawan (2013:67) “Jaringan Komputer untuk Orang Awam Edisi Ke-2”



Sumber: <http://teknodaily.com/pengertian-kabel-jaringan-utp-kelebihan-dan-kekurangannya/>

**Gambar II.20 Kabel UTP**  
**(Unshielded Twisted Pair)**



Sumber : <http://teknodaily.com/pengertian-kelebihan-kekurangan-kabel-jaringan-stp/>

**Gambar II.21**  
**Kabel STP (*Shielded Twisted Pair*)**

Berikut ini tabel kategori kabel UTP dan STP :

**Tabel II.2**  
**Kategori Kabel UTP (*Unshielded Twisted Pair*)**

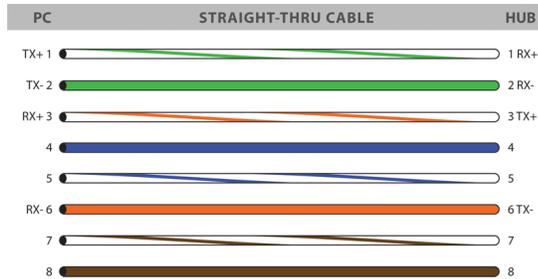
<b>Kategori</b>	<b>Date Rate Maksimum</b>	<b>Penggunaan</b>
Cat 1	1 Mbps	Analog Voice, ISDN
Cat 2	4 Mbps	Token Ring
Cat 3	16 Mbps	Voice dan data 10BaseT
Cat 4	20 Mbps	16 Mbps Token Ring
Cat 5	100 Mbps 1000 Mbps 4 (pasang)	ATM
Cat 5e	!000 Mbps	Ethernet
Cat 6	Mencapai 400 MHz	Super Fast Broadband
Cat 6e	Mencapai 500 Mhz	10G BaseT
Cat 7	Mencapai 1.2 GHz	Full Motion Video Teleradiology

Sumber : <http://www.materitkj.com/2015/12/pengertian-kabel-twisted-pair-lengkap.html>

Berdasarkan tipe kabel UTP (*Unshielded Twisted Pair*) dibedakan menjadi 3 yaitu:

### 1. Straight Trough Cable

Menurut Irawan (2013:68) “Urutan kabel ini digunakan untuk menghubungkan antara PC dengan *switch/hub* atau *router* dengan *switch/hub*”.

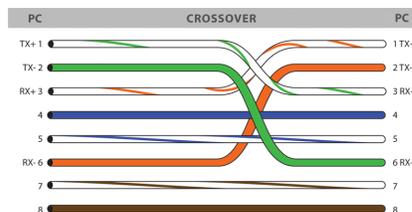


Sumber : <http://www.pintarkomputer.com/kabel-utp-penjelasan-dan-urutan-tipe-kabel-straight-trought-cross-over-dan-roll-over-cable/>

**Gambar II.22**  
*Straight Trought Cable*

### 2. Cross Over Cable

Menurut Irawan (2013:68) “Urutan kabel ini digunakan untuk menghubungkan antara perangkat *switch/hub* dengan *switch/hub*, PC dengan PC, *router* dengan *router*, PC dengan *router*”.



Sumber : <http://www.pintarkomputer.com/kabel-utp-penjelasan-dan-urutan-tipe-kabel-straight-trought-cross-over-dan-roll-over-cable/>

**Gambar II.23**  
*Cross Over Cabl*

### 3. Roll Over Cable

Menurut Irawan (2013:71) “Digunakan untuk menghubungkan 2 perangkat berbeda di jaringan seperti *switch* dengan printer atau komputer dengan *router* melalui *port console*”.

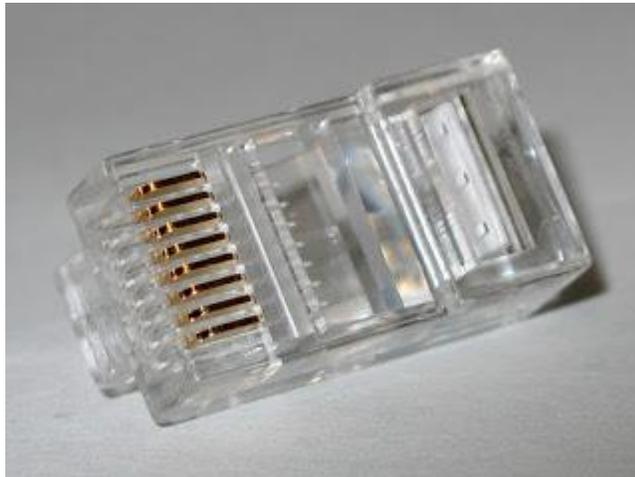
Router Pin name	Router Pin	Direction	Workstation Pin	Workstation Pin name
White-Orange	1	↔	8	Brown
Orange	2	↔	7	White-Brown
White-Green	3	↔	6	Green
Blue	4	↔	5	White-Blue
White-Blue	5	↔	4	Blue
Green	6	↔	3	White-Green
White-Brown	7	↔	2	Orange
Brown	8	↔	1	White-Orange

Sumber : <http://www.pintarkomputer.com/kabel-utp-penjelasan-dan-urutan-tipe-kabel-straight-trought-cross-over-dan-roll-over-cable/>

**Gambar II.24**  
**Roll Over Cable**

#### 2.3.11 Konektor

Menurut Irawan (2013:13) “Konektor merupakan sebagai penghubung antara kabel jaringan dengan *port* yang ada diperangkat keras jaringan. Konektor disesuaikan dengan jenis kabel yang digunakan”. Kabel UTP/STP menggunakan RJ45, *coaxial* menggunakan konektor BNC/T dan serat optik menggunakan banyak tipe konektor seperti SC (*Subscriber Connector*), ST (*Straight Tip*), FC (*Fiber Connector*), dan sebagainya. Konektor ST(*Subscriber Connector*), paling umum digunakan, karena mudah untuk dipasang dan dicabut.



Sumber : <http://www.ilmu-komputer.id/2016/04/perangkat-iaringan-komputer-kabel-coaxial-kabel-tp-kabel-fiber-optik-konektor-crimping-tool-lan-card-hub-switch-bridge-router-modem-repeater-accest-point-wireless-adapter.html>

**Gambar II.24**  
**RJ45**

### 2.3.12 Tang *Crimping*

Menurut Irawan (2013:13) “Tang *Crimping* untuk memasang konektor pada ujung kabel seperti UTP/STP atau coaxial. Pada tang terdapat bagian khusus yang berfungsi untuk “Menjepitkan” Konektor pada kabel”.



Sumber : <http://www.adalahcara.com/2013/06/cara-crimping-kabel-utp-ke-rg-45.html>

**Gambar II.25**  
**Tang *Crimping***

### 2.3.13 Kabel Tester

Menurut Irawan (2013:13) ”Alat yang digunakan untuk menguji hasil pemasangan konektor pada kabel. Apakah pemasangan konektor sudah benar atau belum”.



Sumber : <http://www.4xem.com/4xem-rj45-rj11-network-cable-tester/>

**Gambar II.26**  
**Kabel Tester**

### 2.4 Perangkat Lunak Jaringan

Menurut Simarmarta (2010:19) “Program komputer yang berfungsi sebagai sarana interaksi antara pengguna dan perangkat keras”. Perangkat lunak juga dapat dikatakan sebagai penerjemah perintah-perintah yang dijalankan pengguna komputer untuk diteruskan ke atau diproses oleh perangkat keras. Perangkat lunak ini dibagi menjadi 3, yaitu program aplikasi (*application program*, misalnya *microsoft excel*), sistem operasi (*operation system*, misalnya *linux*, *windows server 2008*), dan bahasa pemrograman( yang dibagi lagi atas bahasa pemrograman tingkat rendah yaitu rakitan , dan bahasa tinggi tinggi seperti pascal).

### 2.4.1 Windows Server 2008

Menurut Irawan (2013:132) “ Windows *server 2008* merupakan sistem operasi *Micosoft*. Merupakan pengembang dari versi sebelumnya yaitu *windows server 2003*”. *Windows server 2008* dibagi menjadi edisi sesuai dengan kebutuhan pengguna. Beberapa versi *windows server 2008* antara lain:

1. *Windowsserver 2008 Standard Edition*.
2. *Windowsserver 2008 Enterprise Edition*.
3. *Windows server 2008 Data center Edition*.
4. *Windows server 2008 Web Server Edition*.
5. *Windows server 2008 Itanium Edition*.

### 2.4.2 Mikrotik

Menurut MADCOM (2015:212) “Mikrotik adalah sebuah perusahaan yang bergerak di bidang produksi perangkat keras (*hardware*) dan perangkat lunak (*Software*) yang berhubungan dengan sistem jaringan komputer yang berkantor pusat di Latvia, bersebelahan dengan Rusia. Mikrotik didirikan pada tahun 1995 untuk mengembangkan router dan sistem ISP (*Internet Service Provider nirkabel*”. Pada tahun 1996 John dan Arnis memulai dengan sistem Linux dan MS DOS yang dikombinasikan dengan teknologi *Wireless LAN (W-LAN)* Aeronet berkecepatan 2Mbps di Moldova. Barulah kemudian melayani lima pelanggannya di Latvia, karena ambisi mereka adalah membuat satu peranti lunak *router* yang handal dan disebarakan ke seluruh dunia. Prinsip dasar Mikrotik bukan membuat *Wireless ISP (WISP)*, tapi membuat program *router* yang handal dan dapat dijalankan di seluruh dunia. Hingga

kini, MikroTik telah melayani sekitar empat ratusan juta pelanggannya Linux yang mereka gunakan pertama kali adalah Kernel 2.2 yang dikembangkan secara bersama-sama dengan bantuan 5 - 15 orang staff R&D Mikrotik yang sekarang menguasai dunia routing di negara-negara berkembang.



Sumber:<http://www.amplitude-rs.com/produit2.html>

**Gambar II. 27**  
**Mikrotik**

### 2.4.3 Jenis – jenis Perangkat Lunak

Suatu perangkat lunak dibangun atas kesatuan elemen-elemen yang terdiri dari:

#### 1. Sistem operasi(*operating system*)

Menurut Fathoni (2014:29) “Sistem operasi (*operating system*) adalah sistem operasi yaitu perangkat lunak yang bertugas mengontrol dan melakukan manajemen perangkat keras serta operasi-operasi dasar sistem, termasuk menjalankan perangkat lunak aplikasi seperti pengolah kata dan *browser web*”. Komputer tidak dapat menjalankan perangkat lunak aplikasi yang sangat kita butuhkan jika tidak memiliki sistem operasi di dalamnya. Dewasa ini, tersedia berbagai pilihan sistem operasi, misalnya *Linux, Unix, FreeBSD, Solaris, Macintosh* dan *Microsoft Windows*.

#### 2. Program utility

Menurut Fathoni (2014:29) “*Program utility* adalah perangkat lunak yang ditujukan untuk melengkapi kinerja sistem operasi dan meningkatkan kinerja komputer”. Salah satu contoh program *utility* adalah *antivirus*. Sistem operasi biasanya tidak dilengkapi dengan antivirus. Karena itu kita harus menambahkan sendiri program *utility* ini. Contoh lain program *utility* adalah program untuk mempartisi *hardisk* dan merapikan file-file yang tersebar di *hardisk* (disebut defragmentasi).

#### 3. Bahasa pemrograman

Menurut Fathony (2014:29) “Bahasa pemrograman yaitu intruksi dan aturan yang tertuang dalam bentuk kode-kode yang diberikan pada komputer untuk melaksanakan suatu tugas”. Manusia memberikan instruksi yang dimengerti

komputer melalui bahasa pemrograman, dan komputer akan menerjemahkannya. Berdasarkan levelnya, bahasa pemrograman dibagi menjadi 3 kelompok, yaitu: *low level language* (contohnya bahasa *Assembly*), *middle level language* (contohnya bahasa C dan C++), dan *high level language* (contohnya bahasa BASIC dan Pascal).

## **2.5 Transmission Control Protocol (TCP) / Internet Protocol (IP)**

Menurut Irawan (2013:18) “TCP merupakan singkatan dari *Tranmission Control Protocol* sedangkan IP ialah *Internet Protocol*. TCP / IP merupakan protokol standar yang dimiliki oleh semua sistem operasi”. Protokol adalah prosedur yang mengatur beberapa fungsi yang ada pada setiap komputer. Protokol mengizinkan adanya hubungan antar komputer sehingga dapat saling bertukar informasi atau saling berkirim data. Tugas protokol adalah mengatur hubungan/komunikasi data saat komunikasi data itu dimulai sampai berakhir.

Menurut Irawan (2013:18) “Ada beberapa protokol yang saling berhubungan dengan internet” :

1. UDP (*User Datagram Protocol*) yaitu protokol yang bersifat *connectionless*, dan bersifat kebalikan dari TCP yang berorientasi *connection*.
2. FTP (*File Transfer Protokol*) yaitu protokol yang digunakan untuk melakukan transfer data. Pengambilan data dari *server* disebut *Download* dan pengiriman data ke *server* disebut *Upload*.
3. HTTP (*Hyper Text Transfer Protokol*) yaitu protokol yang digunakan untuk mentransfer halaman web di *internet*.
4. SMTP (*Simple Mail Transfer Protokol*) yaitu protokol yang digunakan untuk mengirim data *e-mail*.

5. DHCP (*Dynamic Host Configuration Protocol*) yaitu protokol yang dapat menentukan nomor IP pada setiap komputer yang terhubung padanya.

Selain itu TCP / IP adalah sebuah sistem dengan 4 (empat) buah lapisan yaitu :

1. Menurut Irawan (2013:16) "*Link layer* disebut juga data-link layer atau *network interface layer* yang terdiridari *device driver* dalam sistem operasi dan *network interface card* yang terdapat dalam komputer. Bersama-sama menangani seluruh detail perangkat keras dari penghubung fisik dengan kabel atau media komunikasi lainnya yang digunakan".
2. Menurut Irawan (2013:16) "*Network layer* disebut juga *Internet layer* menangani perpindahan paket diseputar jaringan, mengarahkan paket (*routing*). Merupakan protokol yang bertanggung jawab dalam proses pengiriman paket ke alamat yang tepat dan bersifat *unreliable* dan *connectionless*".
3. Menurut Irawan (2013:16) "*Transport layer* menyediakan sebuah aliran data antar dua komputer untuk *application layer* diatasnya. TCP (*Transmission Control Protocol*) bersifat *reliable* dan *connection oriented*, Sedangkan UDP (*Unit Datagram Protocol*) bersifat *connectionless* dan *unreliable*".
4. Menurut Irawan (2013:16) "*Application layer* menangani aplikasi yang ada secara detail. Merupakan lapisan teratas yang berisi semua aplikasi berbasis TCP & IP dan berhubungan langsung dengan pemakai. Aplikasi tersebut misalnya FTP, HTTP dan Telnet"

## 2.6 IP Address

Menurut Irawan (2013:32) “IP (*Internet Protocol*) *address* adalah alamat yang digunakan pada perangkat yang terhubung dengan jaringan, seperti komputer, printer, dan sebagainya. IP *address* yang sudah banyak digunakan adalah IP versi 4 dengan kapasitas 32 bit, jika sudah penuh akan digantikan IP versi 6 dengan kapasitas 128 bit”.

Menurut Sofana(2013:105) “IPv4 merupakan *IPaddress* yang terdiri dari sekumpulan bilangan biner sepanjang 32 bit, yang dibagi atas 4 segmen dan setiap segmen terditias atas 8 segmen”.

Nilai paling tinggi dari biner 8 *bit* adalah 255. Angka ini dihitung dari bilang biner 2 berpangkat. Contoh:

$$\begin{aligned} 11111111 &= 2^7 + 2^6 + 2^5 + 2^4 + 2^3 + 2^2 + 2^1 + 2^0 \\ &= 128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 \\ &= 255 \end{aligned}$$

Nilai dari angka 2 berpangkat hanya di hitung jika biner bernilai 1. Jika biner bernilai 0, maka nilainya juga sama dengan 0. Dengan demikian nilai terbesar dari 32 *bit* IP *address* adalah:

11111111.11111111.11111111.11111111

Atau sama dengan:

255.255.255.255

**Tabel II.3**  
**Rumus Biner ke Desimal**

Bilangan	1 Octet IP versi 4								Total
Binner	1	1	1	1	1	1	1	1	8 bit
Desimal	128	64	32	16	8	4	2	1	255

Sumber: Irawan (2013:34) "Jaringan Komputer untuk Orang Awam Edisi Ke-2"

Berikut ini penulis akan mencoba merubah *bit* bilangan biner IP *address* dibawah ini menjadi bilangan desimal menggunakan tabel diatas

11000000.10101000.01100100.00000001

**Tabel II.4**  
**Mengubah Bilangan Biner ke Desimal**

Bilangan	Octet Pertama								Total
Binner	1	1	0	0	0	0	0	0	192
Desimal	128	64	32	16	8	4	2	1	
	Octet Kedua								
Binner	1	0	1	0	1	0	0	0	168
Desimal	128	64	32	16	8	4	2	4	
	Octet Ketiga								
Binner	0	1	1	0	0	1	0	0	100
Desimal	128	64	32	16	8	4	2	1	
	Octet Keempat								
Binner	0	0	0	0	0	0	0	1	1
Desimal	128	64	32	16	8	4	2	1	

Sumber: Irawan (2013:34) "Jaringan Komputer untuk Orang Awam Edisi Ke-2"

Berdasarkan tabel II.4 maka nilai desimal untuk alamat IP 11000000 . 10101000 . 01100100 . 00000001 adalah 192.168.100.1

### 2.6.1 Kelas IP Address

Menurut Sofana (2013:108)“Untuk memudahkan pengaturan IP *address* seluruh pengguna Internet, dibentuklah suatu badan yang mengatur pembagian IP *address*. Badan tersebut bernama InterNIC (*Internet Network Information Center*)”.

#### 1. Kelas A

Menurut Sofana (2013:108) “Jika *bit* pertama di IP *address* adalah 0 maka IP *address* termasuk dalam *network* kelas A. *Bit* ini dan 7 *bit* ( 8 *bit* pertama) merupakan *bit-bit network (network bit)* dan boleh bernilai berapa saja (kombinasi angka 1 dan 0), sedangkan 24 bit terakhir merupakan *bit host*. Ingatlah , IP *address* harus di konversikan dari bentuk biner ke bentuk desimal”. Dengan demikian, hanya ada 128 *network* kelas A, yakni dari nomor 0.xxx.xxx.xxx sampai 127.xxx.xxx.xxx. Setiap *network* dapat menampung lebih dari 16 juta (2563) *host* (xxx adalah variabel, nilainya dari 0. Sampai dengan 255).

#### 2. Kelas B

Menurut Sofana (2013:108) “Jika *bit* pertama di IP *address* adalah 10, maka IP *address* tersebut termasuk dalama *network* kelas B. Dua *bit* ini dan 14 *bit* berikutnya (16 *bit* pertama) merupakan *bit network* dan boleh bernilai berapa saja (kombinasi angka 1 dan 0), sedangkan 16 bit terakhir merupakan *bit host*”. Jika bentuk biner dikonversikan ke bentuk desimal maka terdapat lebih dari 16 ribu *network* kelas B, yakni 128.xxx.xxx hingga 191.255.xxx.xxx. Setiap *network* kelas B mampu menampung lebih dari 65 ribu *host* (2562).

#### 3. Kelas C

Menurut Sofana (2013:109) “Jika 3 *bit* pertama di *IP address* adalah 110, maka *IP address tersebut* termasuk dalama *network* kelas C. Tiga *bit* ini dan 21 *bit* berikutnya (24 *bit* pertama) merupakan *bit network* dan boleh bernilai berapa saja (kombinasi angka 1 dan 0), sedangkan 8 bit terakhir merupakan *bit host*”. Jika bentuk biner dikonversikan ke bentuk desimal maka terdapat lebih dari 2 juta *network* kelas C, yakni 192.xxx.xxx hingga 223.255.255.xxx. Setiap *network* kelas C mampu menampung lebih dari 256 *host*.

#### 4. Kelas D

Menurut Sofana (2013:109) “Jika 4 *bit* pertama di *IP address* adalah 1110, maka *IP address tersebut* termasuk dalama *network* kelas D. *IP address* kelas D digunakan untuk *multicast address*, yakni sejumlah komputer yang memakai bersama suatu aplikasi. Salah contoh pengguna *multicast address* adalah *video confrence* yang melibat lebih dari 2 *host(multipoint)*, menggunakan *Multicast Backbone(Mbone)*”.

#### 5. Kelas E

Menurut Sofana (2013:110) “*IP address* kelas E masih bersifat percobaan. Jika bit pertama adalah 1111 (atau sisa dari seluruh kelas) maka *IP address* termasuk dalam kategori kelas E”.

### 2.6.2 Aturan Dasar Pemilihan *Network ID* dan *Host ID*

Menurut Abdul (2015:19) “Berikut adalah aturan-aturan dasar dalam menentukan *network ID* dan *host ID* yang digunakan :

#### 1. *Network ID* tidak boleh sama dengan 127

*Network ID* 127 secara *default* digunakan sebagai alamat *loopback* yakni *IP address* yang digunakan oleh suatu komputer untuk menunjuk dirinya sendiri.

#### 2. *Network ID* dan *host id* tidak boleh sama dengan 255

*Network ID* atau *host ID* 255 akan diartikan sebagai alamat *broadcast*. ID ini merupakan alamat yang mewakili seluruh jaringan.

3. *Network ID* dan *host ID* tidak boleh sama dengan 0

IP *address* dengan *host ID* 0 diartikan sebagai alamat *network*. Alamat *network* digunakan untuk menunjuk suatu jaringan bukan suatu *host*.

4. *Host ID* harus unik dalam suatu *network*.

Dalam suatu *network* tidak boleh ada dua *host* yang memiliki *host ID* yang sama”.

### **2.6.3 Network Address**

Menurut Sofana (2013:110) “*Network address* adalah setiap *network* yang tergabung di Internet haruslah memiliki ID yang unik, yang disebut alamat *network* atau *network address*”. Kita sudah melihat bahwa IP *address* kelas A,B, dan C selalu dapat dibagi menjadi 2 bagian, yaitu bagian *network* dan *host*. *Network address* ini didapat dengan membuat *bit host* menjadi 0, pada IP *address* kelas B panjang *bit network* dan *bit host* masing-masing adalah 16 *bit*. Misalkan untuk *host* dengan IP *address* kelas B, contoh 167.205.9.35, maka *network address* dari *host* tersebut adalah 167.205.0.0.

### **2.6.4 Broadcast Address**

Menurut Sofana (2013:113) “ *Broadcast address* adalah IP *address* khusus yang digunakan untuk mengirim/menerima informasi yang harus diketahui oleh seluruh *host* pada suatu *network*. Setiap datagram IP memiliki *header* berisi IP *address* alamat tujuan”. Dengan adanya alamat ini, maka hanya *host* tujuan yang dapat memproses datagram tersebut, sedangkan *host* lain akan mengabaikannya”. *Broadcast address* diperoleh dengan membuat *bit-bit* menjadi 1. Hal ini kebalikan

dengan *network address*, dimana seluruh *bit host* menjadi 0. Untuk *host IP address* 167.205.9.35, *broadcast address*-nya adalah 167.205.255.255. Proses konversi dapat diilustrasikan sebagai berikut.

167 . 205 . 9 . 35  
 10100111.11001101.00001001.000000101  
 10100111.11001101.11111111.111111111  
 167 . 205 . 255 . 255

### 2.6.5 Private IP Address

Menurut Irawan (2013:38) “*IP private* adalah alamat yang masih termasuk dalam rentang IP untuk jaringan lokal atau LAN”.

**Tabel II.5**  
**Private IP Address**

<b>Kelas</b>	<b>IP Address</b>
<b>A</b>	<b>10.0.0.0 – 10.255.255.255</b>
<b>B</b>	<b>169.254.0.1 -169.254.255.254 APIPA</b> <b>172.16.0.0 – 172.31.255.255</b>
<b>C</b>	<b>192.168.0.0 – 192.168.255.255</b>

Sumber :Irawan (2013:38) “”Jaringan Komputer untuk Orang Awam Edisi Ke-2”

Menurut Irawan (2013:38) “**APIPA (Automatic Private IP Address)**, merupakan fitur milik sistem *Microsoft windows* yang secara otomatis mendaftarkan perangkat dalam jaringan dengan alamat 169.254.0.1 -169.254.255.254”.

### 2.6.6 Public IP Address

Menurut Irawan (2013:38) “Alamat IP yang digunakan pada perangkat yang terhubung dengan internet. IP *Public* biasanya diberikan oleh penyedia layanan internet yang digunakan. Setiap perangkat yang tersambung dengan Internet dan jaringan akan memiliki dua alamat jaringan, yaitu IP *Private* dan IP *Public*”.

### 2.6.7 Subnet Mask

Menurut Irawan (2013:39) “ Alamat yang terdiri dari susunan angka biner 32 bit yang digunakan untuk mengelompokan alamat berdasarkan *netwrok* ID dan *host* ID”.

**Tabel II.6**  
**Subnet Mask**

<b>KELAS</b>	<b>Subnet Mask</b>	<b>Biner</b>
A	255.0.0.0	11111111.00000000.00000000.00000000
B	255.255.0.0	11111111.11111111.00000000.00000000
C	255.255.255.0	11111111.11111111.11111111.00000000

Sumber :Irawan (2013:39) “Jaringan Komputer untuk Orang Awam Edisi Ke-2”

### 2.7 Subnetting

Menurut Sofana(2013:117) “*Subnetting* adalah proses membagi atau memecah sebuah *network* menjadi yang lebih kecil (*subnet-subnet*). Esensi dari *subnetting* adalah “memindahkan” garis pemisah bagian *network*, sehingga beberapa *bit* *host* digunakan untuk *bit* tambahan *network*”.

*Subnetting* dilakukan dengan beberapa alasan diantaranya:

1. Untuk efisiensi *IP address*, alokasi *IP address* berdasarkan pembagian kelas kurang efisien. Sebagai contoh, sebuah *network A* menyediakan *IP address* untuk sekitar 16 juta *host*. Saat ini *IP address* bukanlah barang “gratis”. Sanggupkah organisasi kecil membeli sebuah *network* dan membayar 16 juta *IP address*?. Lebih baik jika *network* kelas A dibagi menjadi beberapa *subnet*. Barulah setiap *subnet* dialokasikan menjadi LAN (*Local Area Network*).
2. Untuk menjembatani perbedaan topologi fisik sering kali digunakan *router*. *Router* bekerja dengan cara meneruskan paket antar-*network* yang berbeda. Ingatlah, perbedaan *network* dalam “kacamata” TCP/IP ditentukan dari *network address*-nya. Sehingga untuk mengatasinya harus membagi sebuah *network* menjadi beberapa *subnet* yang kemudian dihubungkan dengan *router*.
3. Untuk mengisolasi *traffic*. Manakala suatu *host* berkomunikasi dengan *host* lain pada *subnet* yang sama, pesan *broadcast* cukup disebar di antara anggota *subnet* dan tidak akan diteruskan ke *subnet* lain.

Suatu *subnet* didefinisikan dengan mengimplementasikan masking bit (*subnet mask*) kepada *IP address*. Struktur subnet mask sama dengan struktur *IP address*, yakni terdiri dari 32 bit yang dibagi atas 4 segmen. Bit-bit dari *IP address* yang “ditutupi” (*masking*) oleh bit-bit *subnet mask* yang aktif dan bersesuaian akan diinterpretasikan sebagai network bit. Bit 1 pada subnet mask berarti mengaktifkan *masking* (*on*), sedangkan bit 0 tidak aktif (*off*). Sebagai contoh kasus, penulis mengambil satu *IP address* kelas A dengan nomor 44.132.1.20. Ilustrasinya dapat dilihat tabel berikut:

**Tabel II.7**  
**Subnetting 16 Bit IP Address Kelas A**

44	132	1	20
00101100	10000100	00000001	00010100
<b>IP Address</b>			
255	255	0	0
11111111	11111111	00000000	00000000
<b>Subnet Mask</b>			
44	132	0	0
00101100	10000100	00000000	00000000
<b>Network Address</b>			
44	132	255	255
001011000	10000100	11111111	11111111
<b>Broadcast Address</b>			

Sumber : Sumber :Irawan (2013:49) ”Jaringan Komputer untuk Orang Awam Edisi Ke-2”

Dengan aturan standar, nomor *network IP address* ini adalah 44 dan nomor *host* adalah 132.1.20. *Network* tersebut dapat menampung maksimum lebih dari 16 juta *host* yang terhubung langsung. Misalkan pada *address* ini akan diimplementasikan *subnet mask* sebanyak 16 bit 255.255.0.0 (Hexa = FF.FF.00.00 atau Biner = 11111111.11111111.00000000.00000000 ). Perhatikan bahwa pada 16 bit pertama dari *subnet mask* tersebut berharga 1, sedangkan 16 bit berikutnya 0. Dengan demikian, 16 bit pertama dari suatu *IP address* yang dikenakan *subnet mask* tersebut akan dianggap sebagai *network bit*. Nomor *network* akan berubah menjadi 44.132 dan nomor *host* menjadi 1.20. Kapasitas maksimum *host* yang langsung terhubung pada *network* menjadi sekitar 65 ribu *host*.

*Subnet mask* di atas identik dengan standard *IP address kelas B*. Dengan menerapkan *subnet mask* tersebut pada satu *network kelas A*, dapat dibuat 256

*network* baru dengan kapasitas masing-masing *subnet* setara *network* kelas B. Penerapan *subnet* yang lebih jauh seperti 255.255.255.0 (24 *bit*) pada kelas A akan menghasilkan jumlah *network* yang lebih besar (lebih dari 65 ribu *network*) dengan kapasitas masing-masing *subnet* sebesar 256 *host*. *Network* kelas C juga dapat dibagi-bagi lagi menjadi beberapa *subnet* dengan menerapkan subnet mask yang lebih tinggi seperti untuk 25 *bit* (255.255.255.128), 26 *bit* (255.255.255.192), 27 *bit* (255.255.255.224) dan seterusnya.

*Subnetting* dilakukan pada saat konfigurasi *interface*. Penerapan *subnet mask* pada IP *address* akan mendefinisikan 2 buah *address* baru, yakni *network address* dan *broadcast address*. *Network address* didefinisikan dengan menset seluruh bit host berharga 0, sedangkan *broadcast address* dengan menset bit host berharga 1. Seperti yang telah dijelaskan pada bagian sebelumnya, *network address* adalah alamat *network* yang berguna pada informasi *routing*. Suatu *host* yang tidak perlu mengetahui *address* seluruh *host* yang ada pada *network* yang lain. Informasi lain dibutuhkannya hanyalah *address* dari *network* yang akan dihubungi serta *gateway* untuk mencapai *network* tersebut. Ilustrasi mengenai *subnetting*, *network address* dan *broadcast address* dapat dilihat pada tabel di bawah. Dari tabel dapat disimpulkan bagaimana nomor *network standard* dari suatu IP *Address* diubah menjadi nomor *subnet / subnet address* melalui *subnetting*.

**Tabel II.9**  
**Beberapa kombinasi IP Address**

<i>IP Address</i>	<i>Network Address Standar</i>	<i>Subnet Mask</i>	<i>Interpretasi</i>	<i>Broadcast Address</i>
44.132.1.20	44.0.0.0	255.255.0.0 (16 bit)	Host 1.20 pada subnet 44.132.0.0	44.132.255.255
80.50.2.3	81.0.0.0	255.255.255.0 (24 bit)	Host 3 pada subnet 80.50.2.0	80.50.2.255
192.168.2.100	192.168.0.0	255.255.255.128 (25 bit)	Host 100 pada subnet 192.168.2.0	192.168.2.127
192.168.2.130	192.168.0.0	255.255.255.192 (26 bit)	Host 130 pada subnet 192.168.2.128	192.168.2.191

Sumber :Irawan (2013:48) ”Jaringan Komputer untuk Orang Awam Edisi Ke-2”

### 2.7.1 CIDR

Menurut Irawan (2013:50) “CIDR (*Classless Inter-Domain Routing*) menghindari cara pemberian IP address tradisional menggunakan Kelas A, B, dan C. CIDR (*Classless Inter-Domain Routing*) menggunakan “*network prefix*” dengan panjang tertentu”. *Prefix-length* menentukan jumlah “*bit* sebelah kiri” yang akan digunakan sebagai *network ID*. Jika suatu IP address memiliki 16 bit sebagai *network ID*, maka IP address tersebut akan diberikan *prefix-length* 16 bit yang ditulis sebagai /16 dibelakang IP address, contoh: 202.152.0.1/18. Oleh karena tidak mengenal kelas, CIDR (*Classless Inter-Domain Routing*) dapat mengalokasikan kelompok IP address dengan lebih efektif. Seperti contoh, jika satu blok IP address 202.91.8.26 dialokasikan untuk sejumlah *host* (komputer) yang akan dibagi dalam beberapa

jaringan (*subnet*), maka setiap bagian (segmen/*subnet*) akan menerima porsi IP *address* yang sama satu sama lain”

*Subnet 1 = 62 host – network address = 202.91.8.0/26*

*Subnet 2 = 62 host – network address = 202.91.8.64/26*

*Subnet 3 = 62 host – network address = 202.91.8.128/26*

*Subnet 4 = 62 host – network address = 202.91.8.192/26*

*Subnet Mask = 255.255.255.192*

Bila salah satu *subnet* masih ingin memecah jaringannya menjadi beberapa bagian, misal *subnet 4* masih akan dibagi menjadi 2 jaringan (*subnet*), maka 62 IP yang sebelumnya akan dialokasikan buat *host subnet 4* akan dipecah menjadi 2 *subnet* lagi dengan *host* yang sama.

*Subnet 4 = 30 host – network address = 202.91.192/27*

*Subnet 5 = 30 host – network address = 202.91.224/27*

*Subnet Mask = 255.255.255.224*

Jika pada penalokasian IP *address classfull*, suatu *network ID* hanya memiliki satu *subnetmask*, maka sisa *host* masing-masing *subnet* yang baru hanya 30 *host*, dikarenakan 1 IP sebagai identitas alamat jaringan (*network ID*) dan 1 IP lainnya (yang terakhir) digunakan sebagai IP *broadcast subnet* tersebut.

## **2.7.2 VLSM**

Menurut Irawan (2013:53) “VLSM (*Variable Length Subnet Mask*) menggunakan metode yang berbeda, yakni dengan memberikan suatu alamat jaringan (*network address*) lebih dari satu *subnet mask*. Contoh: satu blok IP *address* 169.254.0.0/20 dibagi menjadi 16”.

*Subnet 1 = 4094 host – Net address = 169.254.0.0/20*

*Subnet 2 = 4094 host – Net address = 169.254.16.0/20*

*Subnet 3 = 4094 host – Net address = 169.254.32.0/20*

.....

.....

*Subnet 16 = 4094 host – Net address = 169.254.240.0/20*

*Subnet Mask = 255.255.240.0*

Berikutnya *subnet 2* akan dibagi menjadi 16 *subnet* lagi yang lebih kecil, maka:

*Subnet 2.1 = 254 host – Net address = 169.254.16.0/24*

*Subnet 2.2 = 254 host – Net address = 169.254.17.0/24*

*Subnet 2.3 = 254 host – Net address = 169.254.18.0/24*

.....

.....

*Subnet 2.16 = 254 host – Net address = 169.254.31.0/24*

*Subnet Mask = 255.255.255.0*

Bila *subnet 2.1* akan dipecah lagi menjadi beberapa *subnet*, misalnya 4 *subnet*, maka:

*Subnet 2.1.1 = 62 host – Net address = 169.254.16.0/24*

*Subnet 2.1.2 = 62 host – Net address = 169.254.16.64/24*

*Subnet 2.1.3 = 62 host – Net address = 169.254.16.128/24*

*Subnet 2.1.4 = 62 host – Net address = 169.254.16.192/24*

*Subnet Mask = 255.255.255.192*

Jika diperhatikan, CIDR (*Classless Inter-Domain Routing*) dan metode VLSM (*Variable Length Subnet Mask*) mirip satu sama lain, yaitu blok *network address*

dapat dibagi lebih lanjut menjadi sejumlah blok IP *address* yang lebih kecil. Perbedaannya adalah CIDR (*Classless Inter-Domain Routing*) merupakan sebuah konsep untuk pembagian blok IP *Public* yang telah didistribusikan dari IANA (*Internet Assigned Number Authority*) yaitu badan yang memiliki *resources Internet*, sedangkan VSLM (*Variable Length Subnet Mask*) merupakan implementasikan pengalokasian blok IP yang dilakukan oleh pemilik jaringan (*network administrator*) dari blok IP yang telah diberikan kepadanya tetapi bersifat lokal dan tidak dikenal di Internet.

## **2.8 Firewall dan Pendahuluan Security**

Menurut Sofana (2013:167) “ Mengingat pentingnya perlindungan informasi yang ada pada komputer, maka orang telah mengembangkan berbagai teknik untuk melindungi komputernya dari berbagai serangan seperti enkripsi data, pengembangan metode otentikasi, proteksi biometri, *firewalling*, dan sebagainya”.

### **2.8.1 Security**

Menurut Sofana (2013:168) “keamanan komputer atau *computer security* mencakup empat aspek”, yaitu :

#### *1. Integrity*

Menurut Sofana (2013:168) “ Aspek *integrity* berhubungan dengan keutuhan informasi. Inti utama aspek *integrity* adalah bagaimana menjaga informasi agar tidak diubah tanpa izin pemilik informasi”. *Virus, trojan horse*, atau pemakaian lain dapat mengubah informasi tanpa izin, ini merupakan contoh serangan terhadap aspek ini. Sebuah *e-mail* dapat saja “ditangkap” ditengah jalan, diubah isinya, kemudian diteruskan ke alamat yang dituju. Penggunaan enkripsi dan

*digital signature* dapat mengatasi masalah ini.

## 2. *Privacy*

Menurut Sofana (2013:168) “Aspek *privacy* berhubungan dengan kerahasiaan informasi. Inti utama aspek *privacy* adalah bagaimana menjaga informasi dari orang yang tidak berhak mengaksesnya”.

## 3. *Authentication*

Menurut Sofana (2013:168) “Aspek *authentication* berhubungan dengan identitas atau jati diri atau kepemilikan yang sah. Sistem harus mengetahui bahwa suatu informasi dibuat atau diakses oleh pemilik yang sah. Ada dua masalah yang terkait dengan aspek ini, yang pertama pembuktian keaslian informasi atau dokumen, yang kedua adalah *access control*”.

## 4. *Availability*

Menurut Sofana (2013:169) “Aspek *availability* berhubungan ketersediaan informasi. Contoh serangan terhadap aspek ini yaitu, ”*denial of service attack*”, dimana *server* dikirim permintaan palsu yang bertubi-tubi sehingga tidak dapat melayani permintaan lain”.

### 2.8.2 Serangan

Menurut Sofana (2013:169) ”Serangan terhadap *security* atau *security attack* merupakan segala bentuk gangguan terhadap keamanan sistem informasi. Berikut ini kemungkinan serangan terhadap *security*”.

#### 1. *Interruption*

Menurut Sofana (2013:169) ”Serangan jenis ini ditujukan terhadap ketersediaan (aspek *availability*) informasi. Sistem dapat dirusak, baik

*software* maupun *hardware*, sedemikian rupa sehingga informasi tidak dapat diakses lagi”.

## 2. *Interception*

Menurut Sofana (2013:169)”Serangan jenis ini ditujukan terhadap aspek *privacy* dan *authentication*. Pihak yang tidak berwenang dapat mengakses informasi. Contoh serangan ini adalah *wiretapping*”.

## 3. *Modification*

Menurut Sofana (2013:170)”Serangan jenis ini ditujukan terhadap aspek *privacy*, *authentication*, dan *integrity*. Pihak yang tidak berwenang dapat mengakses dan mengubah informasi”.

## 4. *Fabrication*

Menurut Sofana (2013:170)”Serangan jenis ini ditujukan terhadap aspek *privacy*, *authentication*, dan *integrity*. Pihak yang tidak berwenang dapat menyisipkan objek palsu ke dalam sistem seperti jaringan komputer”.

### 2.8.3 Firewall

Menurut Sofana (2013:168) Sebuah *firewall* digunakan untuk melindungi jaringan komputer, khususnya LAN (*Local Area Network*) dari berbagai serangan (*intrusions*) yang dapat menyebabkan data *corrupt* atau *service* menjadi macet. Sebuah *firewall* dapat berupa komputer biasa yang telah di konfigurasi menggunakan *software* tertentu, bisa juga *hardware* atau *device* khususnya. Sekurang-kurangnya *firewall* memiliki 2 buah *interface*. Salah satu *interface* dihubungkan dengan jaringan *private* (yang akan dilindungi, biasanya LAN), sedangkan *interface* yang lain dihubungkan dengan jaringan *public* (biasanya *Internet*). Umumnya *firewall* menjadi satu dengan *router* atau NAT (*Network Address Translation*) *router*, namun *firewall* memiliki fitur-fitur lebih lengkap dibandingkan *router*. *Firewall* dapat menyeleksi setiap data yang keluar/masuk, kemudian membandingkannya dengan kriteria atau *policy* tertentu. Manakala sesuai *policy* maka data akan diteruskan. Jika tidak sesuai, data akan di *-block* atau *-drop*.