

## **BAB II**

### **LANDASAN TEORI**

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

Menurut Arifin (2011:9) “Jaringan komputer adalah 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. Prinsip dasar jaringan komputer adalah terjadinya komunikasi 2 arah antara pengiriman dan penerimaan informasi. Keuntungan menggunakan jaringan komputer, diantaranya adalah:

1. Penggunaan bersama (*share*) peralatan, data, program, dan informasi.
2. Sebagai salah satu media komunikasi tanpa pulsa.
3. Sistem informasi yang terintegrasi.
4. Sangat menghemat waktu dan biaya transportasi, karena aliran informasi dan data yang cepat dengan jangkauan yang sangat luas.

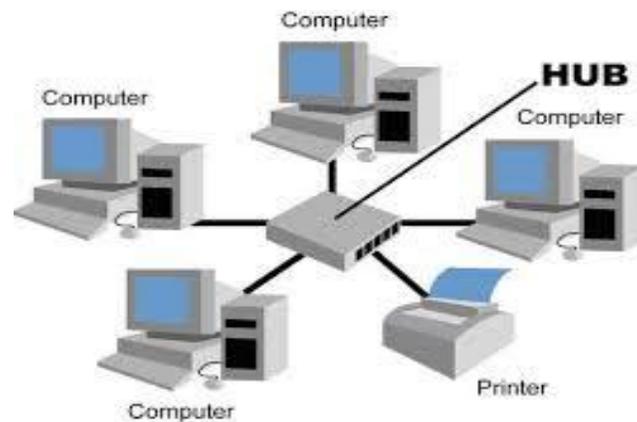
##### **2.1.1. Jaringan Komputer Berdasarkan Area**

Berdasarkan cakupan area, jaringan komputer terbagi menjadi:

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

Menurut Arifin (2011:9) mendefinisikan bahwa “*Local Area Network* adalah bentuk jaringan komputer lokal, yang luas areanya sangat terbatas”.Biasanya diterapkan untuk jaringan komputer rumahan, laboratorium komputer disekolah

dan kantor, dimana masing-masing komputer dapat saling berinteraksi, bertukar data dan dapat menggunakan peralatan bersama seperti printer. Media yang digunakan untuk LAN dapat berupa kabel (UTP atau BNC) maupun *wireless*. Contoh jaringan *Local Area Network* seperti Gambar 2.1 sebagai berikut:



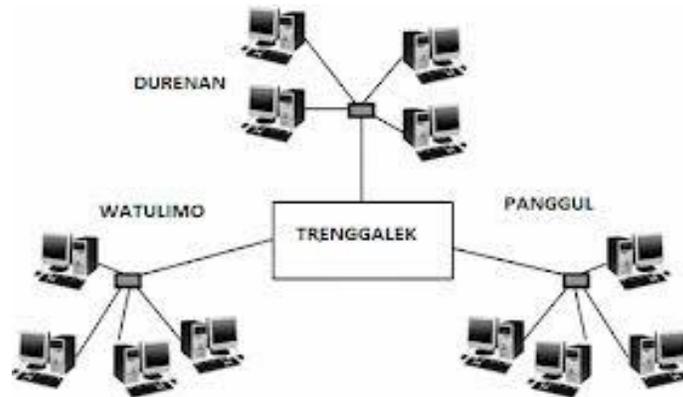
Sumber : <http://www.sman15-bdl.sch.id/2015/10>

Gambar II.1  
*Local Area Network (LAN)*

## 2. Metropolitan Area Network (MAN)

Menurut Utomo (2011:14) “*Metropolitan Area Network* merupakan jaringan yang mencakup area lokasi yang lebih luas, melibatkan kesatuan komputer yang lebih banyak”. komputer dengan skala yang lebih besar dari LAN, dapat berupa jaringan komputer antar kantor/perusahaan yang jaraknya berdekatan. MAN merupakan gabungan dari beberapa jaringan LAN atau dapat diartikan MAN merupakan pengembangan dari jaringan LAN.

Contoh jaringan *Metropolitan Area Network* seperti Gambar 2.2 sebagai berikut:



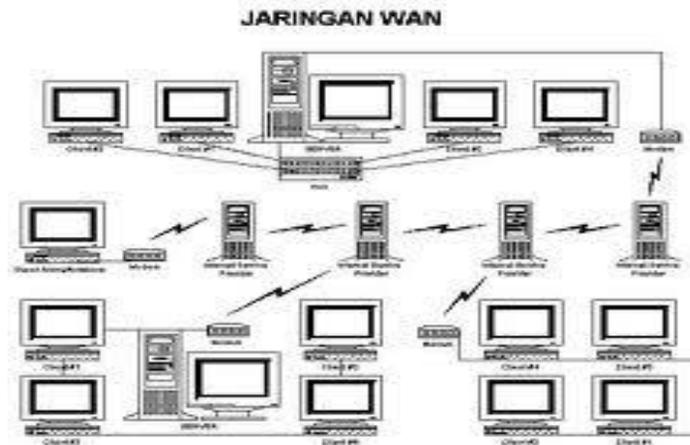
sumber : <http://www.sman15-bdl.sch.id/2015/10>

Gambar II.2  
*Metropolitan Area Network ( MAN )*

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

Menurut Kurniawan (2007:18) “*wide Area Network* merupakan bentuk yang terdiri dari LAN dan MAN. Jaringan WAN telah memenuhi berbagai kebutuhan sistem jaringan, seperti jaringan untuk publik, jaringan pada bidang perbankan, jaringan jual beli secara online di internet, jaringan penjualan jasa dan jaringan lainnya”. Media transmisi yang digunakan adalah satelit atau gelombang elektromagnetik.

Contoh jaringan *Wide Area Network* seperti Gambar 2.3 sebagai berikut:



Sumber : <http://www.sman15-bdl.sch.id/2015/10>

Gambar II.3  
*Wide area Network (WAN)*

#### 4. Internet

Menurut Sofana (2008:5) mendefenisikan bahwa “internet adalah interkoneksi jaringan-jaringan komputer yang ada di dunia”. Sehingga cakupannya sudah mencapai satu planet, bahkan tidak menutup kemungkinan mencakup antarplanet. Koneksi antar jaringan komputer dapat dilakukan berkat dukungan protokol yang khas, yaitu *internet Protocol (IP)*.

##### 2.1.2. Jaringan Komputer Berdasarkan Fungsi

Berdasarkan fungsinya jaringan komputer terbagi menjadi 2, yaitu:

##### 1. *Peer To Peer*

Menurut Arifin (2011:12) “*Peer To Peer* banyak digunakan pada jaringan dengan jumlah komputer yang sedikit, dimana masing-masing komputer memiliki status kedudukan yang sama dan tidak memerlukan sistem terpusat (server) “. Untuk lan

biasanya digunakan kabel UTP dengan menggunakan konektor RJ-45 sedangkan untuk MAN dan WAN biasanya menggunakan kabel serat optik.

## 2. *Client Server*

Menurut Sofana (2008:6) “*client server* adalah jaringan komputer yang salah satu (boleh lebih) komputer difungsikan serbagai *server* atau induk bagi komputer lainnya. *Server* melayani komputer lain yang disebut *client* . layanan yang diberikan bisa berupa akses Web, *e-mail*, file atau yang lainnya”. *Server* tersebut bertugas melayani seluruh permintaan dari komputer *client*.

Berikut tabel perbandingan menggunakan jaringan peer-to-peer dan client/server.

Tabel II.1  
Peer-to-peer dan client server

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

Sumber : Arifin (2011:13)

### 2.1.3. Jaringan Komputer Berdasarkan Media Transmisi

Berdasarkan media transmisi jaringan komputer terbagi menjadi dua, yaitu:

#### 1. *Wire Network* (Kabel)

Menurut Sofana (2008:6) “*wire Network* adalah jaringan komputer yang menggunakan kabel sebagai media penghantar. Jadi data mengalir pada kabel”. Untuk LAN biasanya digunakan kabel *Unshielded Twisted Pair* (UTP) dengan menggunakan konektor RJ-45 sedangkan untuk MAN dan Wan biasanya menggunakan kabel secara optik.

#### 2. *Wireless Network* (Tanpa Kabel)

Menurut Arifin (2011:14) “*Wireless Network* adalah solusi yang tepat untuk mengatasi masalah lokasi. Pada beberapa wilayah yang memiliki hambatan dalam pengkabelan, seperti daerah gunung, bukit, sungai dan lainnya, teknologi ini sangat membantu dalam membangun jaringan”. Sehingga pengguna dapat dengan mudah mengakses internet tanpa kabel.

## 2.2. Topologi Jaringan

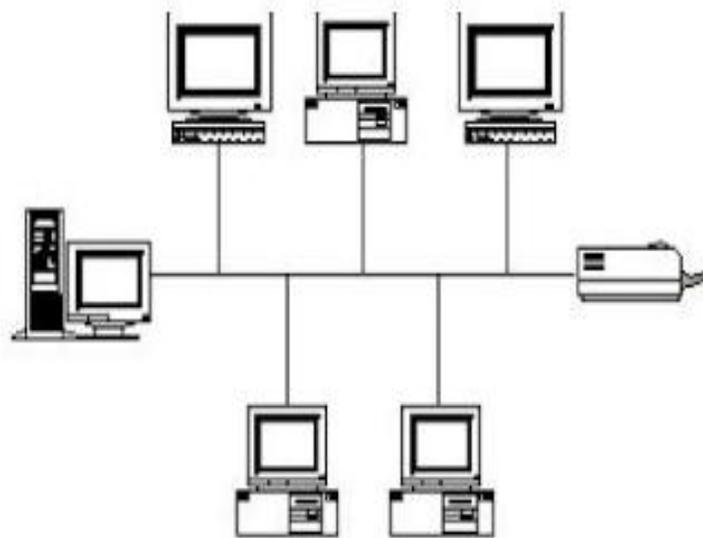
Jaringan komputer terbentuk dari beberapa komputer yang saling terhubung melalui media komunikasi baik kabel maupun nirkabel dan beberapa perangkat keras pendukungnya, cara menghubungkan *device* satu dengan topologi.

Menurut Sofana (2008:7) “Topologi adalah suatu aturan/*rules* bagaimana menghubungkan komputer (*node*) satu sama lain secara fisik dan pola hubungan antara komponen-komponen yang berkomunikasi melalui media/peralatan jaringan, seperti: *server*, *workstation*, *hub/switch*, dan pengabelannya (media transmisi data)”.

Topologi jaringan pada dasarnya terbagi menjadi dua yaitu topologi fisik dan topologi logika. Topologi fisik adalah topologi riil yang terdapat dalam sebuah jaringan sedangkan topologi logika adalah topologi mengenai aliran data yang terjadi pada topologi fisik. Topologi jaringan terbagi menjadi lima, yaitu:

#### 1. Topologi Bus

Jaringan yang menggunakan topologi bus dapat dikenali dari penggunaan sebuah kabel *backbone* (kabel utama) yang menghubungkan semua peralatan jaringan seperti komputer dan printer. komputer dan *device* yang lain dalam jaringan berkomunikasi dengan cara mengirim dan mengambil data melalui *bus*. Topologi bus sangat mudah untuk diimplementasikan, namun kelemahannya yaitu apabila kabel induk terputus pada satu titik atau rusak, maka dapat mempengaruhi komputer atau terminal selanjutnya. Contoh Topologi Bus seperti Gambar 2.4 sebagai berikut:

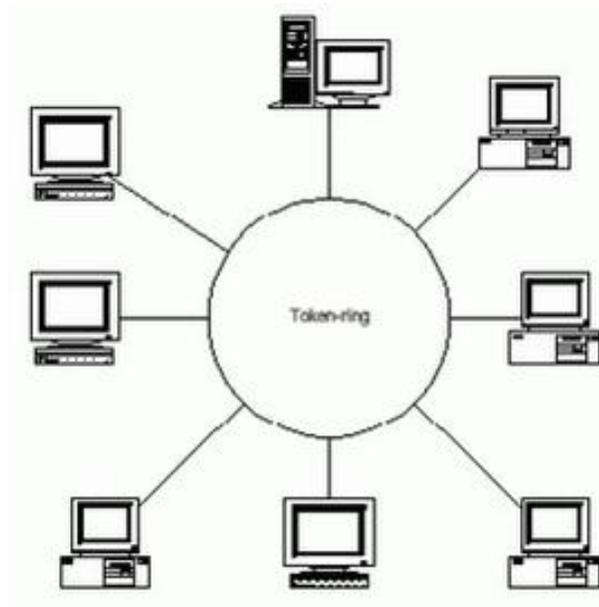


Sumber : <http://www.pintarkomputer.org/2015/08>

Gambar II.4  
Topologi Bus

## 2. Topologi Ring

Topologi ring sangat berbeda dengan topologi bus. Jaringan yang menggunakan topologi ini dapat dikenali dari kabel *backbone*, setelah sampai pada komputer terakhir maka ujung kabel akan kembali dihubungkan dengan komputer pertama sehingga terbentuk seperti lingkaran atau cincin. Pada topologi ini data mengalir satu arah, bias searah jarum jam atau berlawanan arah jarum jam. Karena mengalir satu arah jadi tidak mengakibatkan tabrakan data. Kelemahan topologi ini apabila kabel diputus pada satu titik maka akan sangat mempengaruhi kinerja jaringan. Contoh Topologi Ring seperti Gambar 2.5 sebagai berikut:



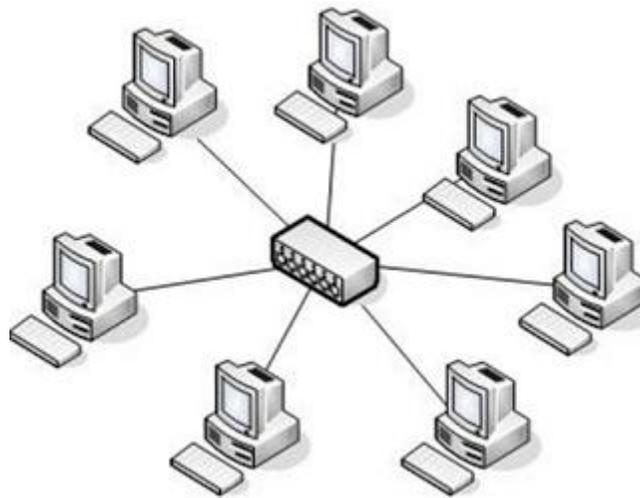
Sumber : <http://www.pintarkomputer.org/2015/08>

Gambar II.5  
Topologi Ring

### 3. Topologi Star

Pada topologi ini setiap komputer dan peralatan jaringan yang lain terhubung pada sebuah perangkat *hub* atau *switch*. *Switch* tersebut berfungsi sebagai pusat pengaturan lalu lintas data. Media koneksi yang digunakan adalah kabel UTP. Kelebihan dari topologi ini adalah mudah mendeteksi jika terjadi kerusakan jaringan dan apabila salah satu dari kabel putus tidak akan berpengaruh pada kinerja jaringan yang lain.

Sedangkan kelemahannya yaitu topologi ini lebih mahal karena memerlukan perangkat khusus yaitu *switch* atau *hub* dan lebih memerlukan banyak kabel karena setiap *device* terhubung dengan *switch* tersebut. Contoh Topologi Star seperti Gambar 2.6 sebagai berikut:

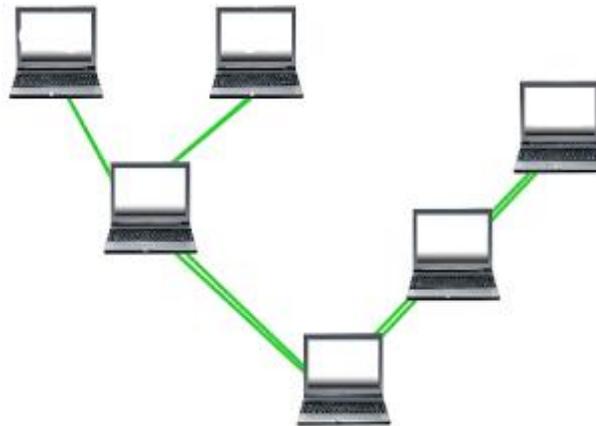


Sumber : <http://www.pintarkomputer.org/2015/08>

Gambar II.6  
Topologi Star

#### 4. Topologi Tree

Topologi *tree* merupakan gabungan beberapa topologi star yang dihubungkan dengan topologi bus. Topologi *tree* digunakan untuk menghubungkan beberapa LAN dengan LAN lainnya. Topologi *tree* dapat mengatasi kekurangan topologi bus yang disebabkan persoalan *broadcast traffic*, dan kekurangan topologi *star* yang disebabkan oleh keterbatasan kapasitas *port hub*. Contoh Topologi Tree seperti Gambar 2.7 sebagai berikut:



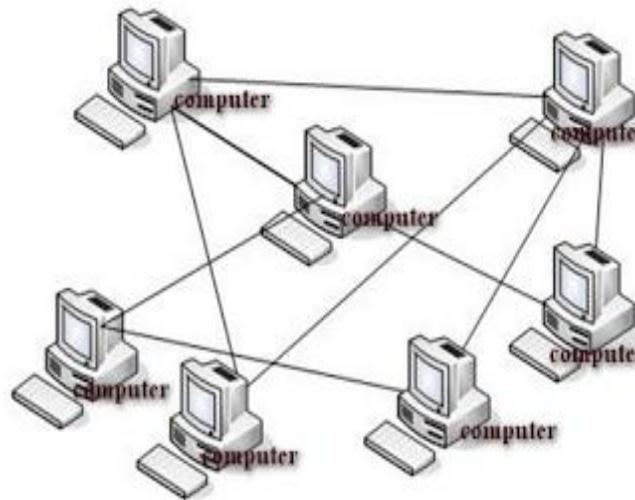
Sumber : <http://www.pintarkomputer.org/2015/08>

Gamabar II.7  
Topologi Tree

#### 5. Topologi Mesh

Pada topologi *mesh* semua titik terminal akan saling terhubung dengan titik yang lainnya, sehingga membentuk jaringan yang kompleks. Topologi ini sering disebut “*pure peer-to-peer*”, sebab merupakan implementasi suatu jaringan yang menghubungkan seluruh komputer secara langsung. Keuntungan topologi ini adalah kecil kemungkinannya terjadi kemacetan data atau gagal koneksi, sedangkan

kerugiannya adalah mahalnya biaya pemasangan karena setiap titik terminal dalam jaringan saling terhubung. Pada implementasinya untuk menekan biaya pemasangan biasanya tidak semua titik terminal dihubungkan, pada kasus seperti ini disebut topologi mesh dan jika semua titik dihubungkan disebut topologi *full mesh*. Contoh Topologi Mesh seperti Gambar 2.8 sebagai berikut:



Sumber : <http://www.pintarkomputer.org/2015/08>

Gambar II.8  
Topologi Mesh

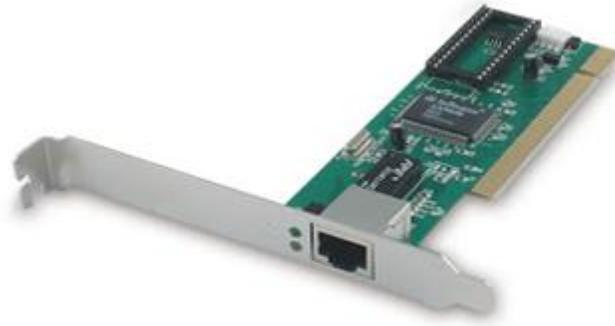
### 2.3. Perangkat Keras Jaringan

Untuk membangun sebuah jaringan komputer maka diperlukan beberapa perangkat dan peralatan, diantaranya:

#### 1. *Network Interface Card* (NIC)

*Network Interface Card* (NIC) Merupakan peralatan yang berhubungan langsung dengan komputer dan didesain agar komputer-komputer jaringan dapat saling berkomunikasi. *Network Interface Card* juga menyediakan akses ke media fisik

jaringan. *Network Interface Card* merupakan contoh perangkat yang bekerja pada *layer* pertama OSI atau *layer physical*. Contoh gambar *Network Interface Card* (NIC) seperti Gambar 2.9 sebagai berikut:



Sumber : <http://www.teorikomputer.com/2012/11/network-card.html>

Gambar II.9  
Network Interface Card (NIC)

## 2. *Hub*

*Hub* digunakan untuk menghubungkan komputer ke jaringan dengan jumlah klien yang lebih dari dua, maka diperlukan sebuah alat yang disebut dengan HUB. Dengan menggunakan HUB, maka akan dapat diperoleh beberapa keuntungan, antara lain dari sisi kecepatannya, harganya juga tidak terlalu mahal, simple dan praktis dalam penggunaannya.

Contoh gambar *Hub* seperti Gambar 2.10 sebagai berikut:



Sumber : <http://www.cisco.com/2015.07>

Gambar II.10  
HUB

### 3. *Switch*

*Switch* berfungsi menghubungkan multiple komputer pada *layer* protokol jaringan level dasar. *Switch* beroperasi pada *layer* dua (data link layer) dalam *osi* model. *Switch* umumnya lebih cerdas dibandingkan dengan *hub*, memiliki performa yang lebih tinggi dan harganya relative lebih mahal dari *hub*. Contoh gambar *switch* seperti Gambar 2.11 sebagai berikut:



Sumber : <http://www.cisco.com/2015/07>

Gambar II.11  
Switch

#### 4. Router

*Router* merupakan perangkat jaringan yang lebih kompleks dan mahal jika dibandingkan dengan device yang lain. Dengan menggunakan informasi padamasing-masing paket data, *router* dapat melakukan *routing* dari satu LAN ke LAN yang lain, menentukan rute terbaik terbaik di antara jaringan”. *Router* juga digunakan untuk membagi jaringan yang besar menjadi beberapa jaringan yang kecil (*subnetwork*) dan membuat keputusan cara mengirim data tujuan data akan dikirim. Contoh gambar *router* seperti Gambar 2.12 sebagai berikut:



Sumber : <http://www.cisco.com/2015/07>

Gambar II.12  
Router

#### 5. Access Point

*Access Point* merupakan alat terpenting dalam membangun jaringan *wireless* maupun jaringan *hotspot*. Pada dasarnya *access point* merupakan hub untuk *wireless* dan *bridge* untuk jaringan LAN UTP. Oleh karena itu biasanya pada *access point* terdapat *port* untuk konektor RJ-45.

Contoh gambar *Access Point* seperti Gambar 2.13 sebagai berikut:



Sumber : <http://www.tp-link.co.id/2015/10>

Gambar II.13  
Access Point

#### 6. *Server*

*server* adalah sebuah atau beberapa komputer yang menghubungkan komputer lain serta perangkat elektronik secara bersama. Kegunaan server biasanya menyediakan data dan informasi. Media bertukar informasi ataupun sebagai media penyimpanan. Contoh gambar *Server* seperti Gambar 2.14 sebagai berikut:



Sumber : <http://www.satyasolusi.com/2015/10>

Gambar II.14  
Server

## 7. Modem

Menurut Utomo (2011:50) “Modem kependekan dari *modulator-modulator*, artinya modem bekerja mengkonversi informasi digital dari komputer anda kebentui sinyal analog yang ditransmisikan melalui kabel telepon. Kemudian modem pada komputer penerima akan mengkonversikan lagi sinyal analog tersebut kebentuk sinyal digital”. Biasanya digunakan untuk komunikasi komputer atau perangkat yang satu dengan komputer atau perangkat yang lain. Contoh gambar *modem* seperti Gambar 2.15 sebagai berikut:



Sumber : <http://www.dlink.com/2015/10>

Gambar II.15  
Modem

## 8. Kabel

Kabel merupakan komponen pokok pada sebuah jaringan komputer karena fungsinya sebagai penghubung antar komputer. Pada sebuah jaringan LAN digunakan sebuah media penghantar *transmisi* data berupa kabel yang akan terhubung dengan setiap NIC pada setiap komputer. Ada bermacam-macam jenis dan tipe kabel yang digunakan dalam jaringan komputer, setiap jenis kabel memiliki karakteristik dan kegunaannya sendiri. Jenis-jenis kabel tersebut yaitu:

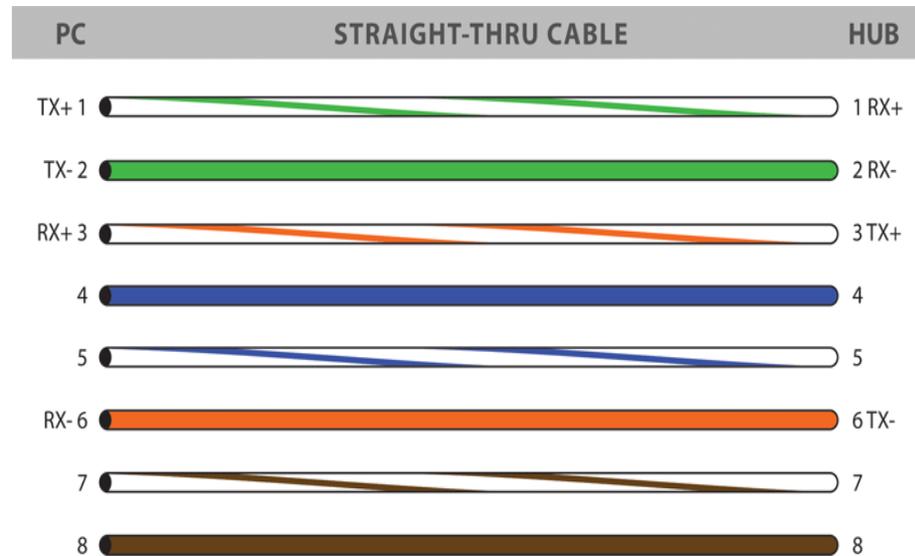
a. *Twisted Pair*

Merupakan salah satu kabel yang digunakan dalam jaringan komputer. Terdapat dua jenis kabel *twisted Pair* kabel dengan *shield* (pelindung) yang disebut UTP (*Shieldded Twisted Pair*). STP digunakan pada jaringan *Token Ring*. Terdiri dari dua *pair* (pasang) kabel yang dipilin dengan inti kawat tembaga berisolator dan memiliki kecepatan transmisi data 16 Mbps hingga jarak 100 meter. Kael yang banyak digunakan dalam jaringan yaitu kabel UTP, yang terdiri dari empat *pair* (pasang) kabel yang dipilin tanpa *shield*. Kabel UTP memiliki inti tembaga tunggal berisolator, dan memiliki kategori 1 hingga 6 yang disesuaikan dengan kecepatan transfer datanya. Berdasarkan fungsinya kabel UTP terbagi menjadi dua pengkabelan yaitu:

1) Pengkabelan *Straight*

Teknik pengkabelan *straight* UTP digunakan untuk menghubungkan komputer *client* dengan *hub* atau *switch* atau dengan kata lain kabel *straight* digunakan untuk menghubungkan dua perangkat yang berbeda. Teknik ini biasaya digunakan pada topologi *star*. Pada pembuatan kabel *straight* setiap ujung kabel dihubungkan dengan konektor RJ-45.

Susunan warna harus sesuai dengan gambar II.16 sebagai berikut:



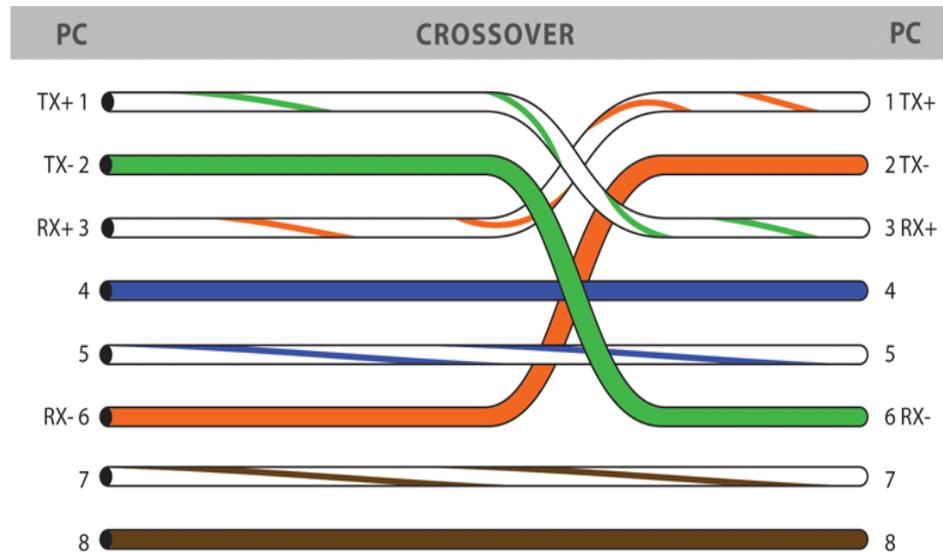
Sumber : <http://www.pintarkomputer.com/2015/08>

Gambar II.16  
Pengkabelan Straight

## 2) Pengkabelan *Cross-Over*

Teknik pengkabelan *Cross-Over* digunakan untuk menghubungkan dua perangkat yang berbeda secara langsung, antar komputer, *switch* dan *router*. Pada pembuatan kabel *Cross-Over* hamper sama dengan pembuatan kabel *straight* yaitu pada setiap ujung terhubung dengan konektor RJ-45, hanya saja susunan warna kabelnya berbeda.

Untuk susunan warna kabel *Cross-Over* seperti gambar 2.17 sebagai berikut:

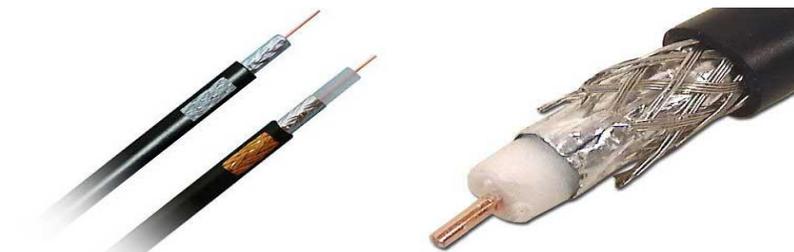


Sumber : <http://www.pintarkomputer.com/2015/08>

Gambar II.17  
Pengkabelan Cross-over

#### b. *Coaxial*

Kabel *Coaxial* biasa digunakan pada topologi *bus* dengan menggunakan konektor BNC dan paling banyak digunakan untuk instalasi jaringan *Ethernet* dan *Arenet*. Kabel jenis ini mudah dan murah dalam proses instalasinya sehingga dapat menekan biaya instalasi. Contoh kabel *Coaxial* seperti gambar 2.18 sebagai berikut:

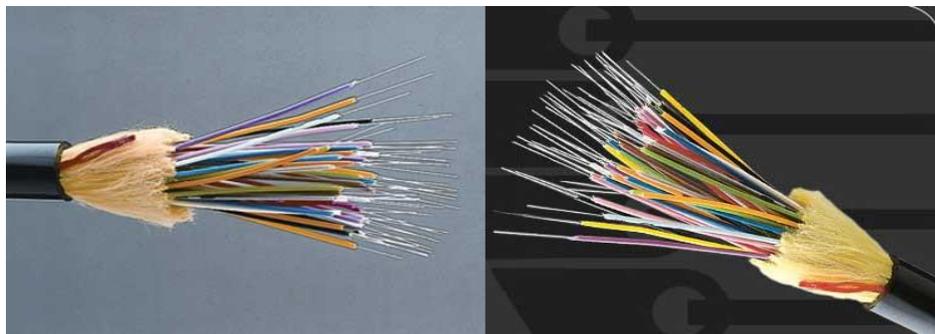


Sumber : <http://teknodaily.com/2015/08>

Gambar II.18  
Kabel Coaxial

### c. *Fiber Optic*

Kabel *Fiber Optic* merupakan suatu jenis kabel yang berisi serat optic yang sangat halus digunakan untuk mentransfer data pada jaringan komputer. Pada inti kabel terdapat serat sebagai inti (*core*) atau sering dinamakandengan *inner optic inner optic* ini dilapisi atau dilindungi oleh bahan gelas yang disebut dengan *cladding*. Contoh kabel *fiber optic* seperti gambar 2.19 sebagai berikut:



Sumber : <http://teknodaily.com/2015/08>

Gambar II.19  
Fiber Optik

## 2.4. Perangkat Lunak Jaringan

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*. Banyak sekali jenis sistem operasi yang biasa digunakan, akan tetapi pada penyusunan tugas akhir ini penulis hanya menjelaskan System Operasi dan mikrotik RouterOS sebagai *network router* sistem operasi sisi *client*. Perangkat lunak dalam jaringan komputer diantaranya yaitu:

## 1. System operasi

System operasi merupakan perangkat lunak (software) utama pada komputer. Sistem operasi mengatur dan mengendalikan semua operasi di komputer. Tanpa adanya sistem operasi, komputer hanyalah rakitan perangkat-perangkat keras yang tidak berfungsi. Sistem operasi dikelompokkan menjadi 2 yaitu *desktop* dan *server*. Sistem operasi *desktop* digunakan untuk komputer-komputer pribadi (PC), sedangkan sistem operasi desktop antara lain windows xp, windows vista, windows 7, MAC OS, dan beberapa produk linux server. Perbedaan antara sistem operasi desktop dan server adalah pada kemampuan dan layanan yang ditawarkan. Sistem operasi desktop lebih mengutamakan pada layanan perkantoran (office) dan multimedia. Sedangkan sistem operasi server lebih mengutamakan pada layanan-layanan jaringan, seperti *Active Directory*, DNS, DHCP, MAIL, *Proxy* dan sebagainya.

## 2. Mikrotik RouterOs

Dalam website Mikrotik Indonesia ([www.mikrotik.co.id](http://www.mikrotik.co.id)) dijelaskan “Mikrotik RouterOS adalah sistem operasi dan perangkat lunak yang dapat digunakan menjadikan komputer menjadi *router network* yang handal, mencakup berbagai fitur yang dibuat untuk *ip network* dan jaringan *wireless*”.

Mikrotik merupakan perangkat jaringan yang paling cerdas, terkadang saya sampai geleng-geleng kepala saat berhadapan dengan *router*, *router* bisa memahami betul bagaimana mengirimkan data dari suatu jaringan ke jaringan lain. Jarang sebuah *router* salah menyampaikan paket data. Kembali lagi ke mikrotik yang ternyata merupakan *router* yang memiliki *fitur* sangat lengkap, mudah di konfigurasi dan

tentunya harganya yang murah, walaupun ada juga *router mirotik* yang bias seharga sepeda motor ataupun seharga mobil bekas. Contoh Gambar Mikrotik RouterOS seperti Gambar 2.20 sebagai berikut:



Sumber:[http:// w.w.w.getintopc.com/software/operating-systems/netkit-4-free-download/](http://w.w.w.getintopc.com/software/operating-systems/netkit-4-free-download/)

Gambar II.20  
Mikrotik Router OS

## **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 protocol 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. Protocol 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) berf ungsi untuk menyampaikan paket data ke alamat yang tepat. *Address Resolution Protocol* (ARP) adalah protocol yang digunakan untuk menemukan alamat *hardware* dari *host*/komputer yang terletak pada *network* yang sama. *Internet Control Messange Protocol* (ICMP) adalah protocol yang digunakan untuk mengirimkan pesan dan melaporkan pengiriman data.

#### 3. *Transport Layer*

Berisi protocol yang bertanggung jawab untuk mengadakan komunikasi antara dua *host*/komputer. Kedua protocol 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. IP Address (*Internet Protocol Address*)**

Menurut Winarno (2013:63) “IP Address adalah identitas numeric yang diberikan kepada suatu alat seperti komputer, router atau printer yang terdapat dalam suatu jaringan komputer yang menggunakan internet protocol sebagai sarana komunikasi”.

Sebuah alamat IP yaitu berupa bilangan yang berjumlah 32 bit yang dipisahkan oleh tanda titik setiap 8 bitnya. Penulisan IP dalam bentuk biner adalah sebagai berikut 11000000.10101000,00000001.00000001 dan jika dituliskan dalam bentuk decimal maka menjadi 192.168.1.1.

Pada sebuah IP terdapat *network ID* dan *host ID* diaman *network ID* berfungsi untuk menunjukkan alamat sebuah jaringan dan *host ID* menunjukkan alamat *device* yang terdapat pada sebuah jaringan IP Address dikelompokkan menjadi lima kelas yaitu: A, B, C, D dan E. Pada umumnya yang sering digunakan adalah IP kelas A, B dan C sedangkan kelas D digunakan untuk jaringan *multicast* dan kelas E digunakan untuk keperluan eksperimen.

Berdasarkan sifat dan fungsinya IP address terbagi menjadi dua yaitu:

1. *Public IP* (IP Publik)

Sebuah alamat IP yang terhubung langsung ke internet dan telah ditetapkan oleh InterNIC dan berisi beberapa buah *network ID* dan tidak akan ada penggunaan dua buah IP yang sama.

2. *Private IP* (IP Khusus)

*Private IP* hanya dikenal oleh jaringan *local* yang digunakan untuk *client* di dalam jaringan *local* tersebut dan tidak dapat terhubung langsung ke internet. Untuk menghubungkan sebuah ip *private* dengan internet yaitu dengan menggunakan *Network Address Translation* (NAT).

### 2.5.3. Subnetting

Menurut Kurniawan (2007:73) “*subnetting* adalah pembagian suatu kelompok alamat IP menjadi beberapa *network ID* lain dengan jumlah anggota jaringan yang lebih kecil, yang disebut subnet (*subnetwork*)”. Tujuan dari dilakukan *subnetting* untuk membagi kelas IP Address atau menghemat IP, mengurangi *traffic* jaringan, memudahkan management, mengatasi perbedaan *hardware* dan topologi fisik. Pada *subnetting* digunakan subnet mask yang terdiri dari 32 bit angka biner untuk menentukan batas antara *host ID* dan *network ID*. Berikut contoh subnetmask kelas C dalam bentuk biner, 11111111.11111111.11111111.00000000. Bila ditulis dalam bentuk decimal adalah 255.255.255.0 Dimana angka 1 menunjukkan *network ID* dan angka biner 0 menunjukkan *host id*.

*Perhitungan subnetting mencakup empat hal yaitu:*

1. Subnetmask baru yang dihasilkan dari perhitungan *subnetting*.
2. Jumlah *subnet* yang akan terbentuk.
3. Jumlah *host* tiap *subnet* yang terbentuk.
4. Alamat *broadcast* tiap *subnet*.

Ada beberapa cara melakukan *subnetting* diantaranya yaitu:

a. *Classless Interdomain Domain Routing (CIDR)*

Salah satu cara untuk melakukan *subnet* berdasarkan *length previx* (panjang previks) yang ditulis dengan tanda *slash (I)*, *previx* ini menentukan jumlah bit dalam satu *subnetmask* terhitung dari sebelah kiri. Penulis *previx* ini diletakkan dibelakang *ip address*, contohnya 192.168,10/27.

Previks yang digunakan pada tiap kelas pun berbeda, penggunaan previks tiap kelas adalah sebagai berikut:

- 1) Kelas A: /9 sampai /30, perhitungan subnetting dilakukan pada octet 2,3 dan 4.
- 2) Kelas B: /17 sampai /30, perhitungan subnetting dilakukan pada octet 3, dan 4.
- 3) Kelas C: /25 sampai /30, perhitungan subnetting dilakukan pada octet 4, berikut contoh perhitungan *subnetting* pada kelas C dengan IP address 192.168.10.1/27.
  - a) Langkah pertama yaitu menentukan *subnetmask* dengan melihat CIDR, yaitu /27 yang berarti network ID terdiri dari 27 bit dan hoost ID 5 bit,

diperbolehkan dari jumlah keseluruhan bit 32 dikurangi network ID 27 bit yaitu 5 bit. Maka *subnetmasknya* dalam bentuk biner, 11111111.11111111.11111111.11100000 atau dalam desimalnya 255.255.255.128 dan ini adalah *subnetmask* baru yang terbentuk.

b) Langkah selanjutnya adalah menghitung jumlah subnet dengan menggunakan rumus  $2^n$ , n adalah jumlah bit *network ID* pada octet 4 yaitu 11111111.11111111.11111111.11100000 jadi jumlah n adalah 3 sehingga  $2^n=2^3$  hasilnya 8, jadi subnet yang terbentuk ada 8.

c) Selanjutnya menghitung jumlah *host* dengan rumus  $2^y-2$  dimana y merupakan bit *host ID* pada octet 4 yaitu 11111111.11111111.11111111.11100000 jadi jumlah y adalah  $2^y-2=2^5-2$  sehingga jumlah *host* yang terbentuk tiap subnet adalah 30.

d) Langkah terakhir adalah menentukan alamat IP *Broadcast* tetapi sebelumnya harus menghitung *blok subnet*, dari *blok subnet* tersebut dapat diketahui alamat IP *Broadcast* yaitu dengan menggunakan rumus  $256-\text{Range}$  dimana range tersebut merupakan nilai *network ID* yang terdapat pada octet 4 yaitu 224 sehingga  $256-224=32$ . Jadi blok subnet yang terbentuk adalah kelipatan 32 (0,32,64,128). Untuk menentukan alamat IP *Broadcast* yaitu dengan cara menambahkan rumus -1 pada *host* terakhir tiap *subnet* contohnya  $192.168.10.32-1=192.168.10.31$ , sehingga alamat *broadcast* yang terbentuk adalah 192.168.10.31, 192.168.10.32. 192.168.10.127.

b. *Variabel Length Subnet Mask (VLSM)*

VLSM merupakan salah satu teknik yang digunakan untuk melakukan *subnetting* berdasarkan jumlah *host*, dimana dalam satu *network* (jaringan) bias terbentuk *subnetmask* baru lebih dari satu sedangkan jika menggunakan CIDR dalam suatu *network* hanya terbentuk satu *subnetmask* saja.

Contoh perhitungan *subnetting* dengan menggunakan VLSM untuk IP 150.10.10.0/19.

1) Langkah awal dalam perhitungan VLSM yaitu dengan menghitung jumlah subnet dahulu dengan menggunakan CIDR yaitu 11111111.11111111.11100000.00000000 =/20. Dengan menggunakan rumus  $2^n=2^3$  hasilnya adalah 8 subnet. Jadi blok tiap subnet adalah:

- a) Blok subnet ke-1=150.10.10.0/19
- b) Blok subnet ke-2=150.10.18.0/19
- c) Blok subnet ke-3=150.10.26.0/19
- d) Blok subnet ke-4=150.10.34.0/19
- e) Blok subnet ke-5=150.10.42.0/19
- f) Blok subnet ke-6=150.10.50.0/19
- g) Blok subnet ke-7=150.10.58.0/19
- h) Blok subnet ke-1=150.10.66.0/19

Sehingga didapat *subnetmask* baru yaitu 255.255.224.0

2) Langkah selanjutnya adalah mengambil blok subnet ke-2 dari hasil CIDR di atas yaitu 150.10.18.0. kemudian dipecah menjadi 8 subnet dimana nilai 8 yaitu hasil dari perhitungan subnet yang pertama. Selanjutnya untuk nilai subnet

menggunakan /17 dengan rumus  $2^x=2^1$  hasilnya 2 yang kemudian digunakan sebagai kelipatan ip pada octet 3. sehingga didapat 8 *blok subnet* baru yaitu:

- a) Blok subnet ke-1.1=150.10.18.0/22
- b) Blok subnet ke-1.2=150.10.20.0/22
- c) Blok subnet ke-1.3=150.10.22.0/22
- d) Blok subnet ke-1.4=150.10.24.0/22
- e) Blok subnet ke-1.5=150.10.26.0/22
- f) Blok subnet ke-1.6=150.10.28.0/22
- g) Blok subnet ke-1.7=150.10.30.0/22
- h) Blok subnet ke-1.8=150.10.34.0/22

Sehingga terbentuk *subnetmask* ke-2 yaitu 255.255.128.0

3) Selanjutnya *blok subnet* dipecahkembali menjadi  $8:2=4$  blok subnet. Dengan menggunakan blok subnet 1.1 yaitu 150.10.18.0 akan tetapi pada octet 4 perlu diubah pula menjadi 4 blok kelipatan 8 sehingga didapat:

- a) Blok subnet 2-1=150.10.18.0/27
- b) Blok subnet 2-2=150.10.18.0/27
- c) Blok subnet 2-3=150.10.26.0/27
- d) Blok subnet 2-4=150.10.34.0/27
- e) Blok subnet 2-5=150.10.42.0/27
- f) Blok subnet 2-6=150.10.50.0/27
- g) Blok subnet 2-7=150.10.58.0/27
- h) Blok subnet 2-1=150.10.66.0/27

Sehingga didapat kembali *subnetmask* ke-3 yaitu 255.255.255.224.

## 2.6. Sistem Keamanan Jaringan

Menurut Sukmaaji dan Rianto (2008:158) “Sistem keamanan jaringan adalah proses untuk mencegah dan mengidentifikasi penggunaan yang tidak sah pada jaringan komputer”. Di dalam sebuah jaringan, keamanan sangat diperlukan untuk memberikan perlindungan terhadap jaringan tersebut agar terindar dari berbagai macam ancaman dari luar jaringan itu sendiri. Ancaman tersebut dapat berupa seorang pengguna yang tidak sah dari luar yang berusaha memasuki jaringan itu sendiri. Keamanan jaringan yang dilakukan meliputi keamanan berupa fisik dan *logic*, keamanan jaringan secara fisik yaitu meliputi segala hal yang berhubungan dengan perangkat dengan perangkat keras *server* maupun *client*, dan juga penempatan *server* yang aman dari pihak yang tidak memiliki wewenang sedangkan keamanan jaringan secara *logic* yaitu meliputi pencegahan terhadap hilang atau rusaknya data komputer dan juga aplikasi yang berjalan didalam jaringan mmisalnya dengan menggunakan *firewall* dan *proxy server*.

### 2.6.1. Contoh Keaman Jaringan dan Aspek Keamanan Jaringan

#### 1. Contoh Keamanan Jaringan

##### a. *Firewall*

*Firewall* memiliki banyak fungsi dalam keamanan jaringan yaitu:

- 1) Mengontrol dan mengawasi paket data yang mengalir di jaringan *firewall* harus dapat mengaatur, mem*filter* dan mengontrol lalu lintas data yang diizinkan untuk mengakses jaringan *private* yang dilindungi *firewall*. *Firewall* harus dapat melakukan pemeriksaan terhadap paket data yang akan

melewati jaringan *private*. Beberapa criteria yang dilakukan *firewall* apakah memperbolehkan paket data lewati atau tidak, antara lain:

- a) Alamat IP dari komputer sumber
  - b) Port TCP atau UDP sumber dari sumber
  - c) Alamat IP dari komputer tujuan
  - d) Port TCP atau UDP tujuan data pada komputer tujuan
  - e) Informasi dari header yang disimpan dalam paket data
- 2) Melakukan *autentifikasi* terhadap akses
  - 3) Aplikasi *firewall* mampu meriksa lebih dari sekedar *header* dari paket data, kemampuan ini menuntut *firewall* untuk mampu mendeteksi protokol aplikasi tertentu yang spesifikasi.
  - 4) Mencatat setiap transaksi kejadian yang terjadi di *firewall*, sehingga memungkinkan berperan sebagai pendeteksi dini akan penjeblolan jaringan.

Cara kerja *firewall*:

*Firewall* menggunakan beberapa metode untuk mengatur lalu lintas keluar atau masuknya suatu data, diantaranya:

a) *Packet Filtering*

Pada metode ini paket-paket atau potongan-potongan data akan dianalisis dan difilter dengan menggunakan sekumpulan pengaturan yang dilakukan oleh *administrator firewall*, dan hanya paket yang sesuai dengan peraturan yang akan lolos menuju tujuannya dan yang tidak sesuai akan dibuang.

b) *Stateful Inspeksi*

Metode ini merupakan metode baru yang tidak menyelrksi isi dari setiap paket akan tetapi membandingkan *key* dari setiap paket tersebut dengan suatu *database* yang terpercaya, jika sesuai dengan yang ketentuan dari *database* tersebut maka paket akan dilanjutkan ketujuan jika tidak maka akan dibuang.

b. *Proxy*

Fungsi dari *proxy* yakni sebagai berikut:

1) *Connecting Sharing*

Fungsi *proxy* disinipenghubung atau perantara pengambilan data dari suatu IP dan dihantarkan ke ip lain ataupun ke ip komputer kita.

2) *Filtering*

Beberapa *proxy* dilengkapi juga dengan *firewall* yang mampu memblokir atau menutup alamat suatu IP yang tidak diinginkan, sehingga beberapa *website* tidak bias diakses dengan menggunakan *proxy* tersebut.

3) *Caching*

Artinya menyimpan *proxy* juga dilengkapi media penyimpanan data suatu *website* dari *query* atau permintaan akses pengguna, jadi misalkan permintaan akses suatu *website* biasa lebih cepat apabila sudah terdapat permintaan akses ke suatu *website* pada pengguna *proxy* sebelumnya.

Cara kerja *proxy*:

Ketika sebuah *pc client* mengakses sebuah *website* dalam sebuah jaringan LAN maka *pc client* akan mengirimkan *request* kepada *proxy server* melalui Ethernet 1 dan

kemudian diteruskan oleh *proxy server* melalui Ethernet 0 dan diteruskan ke *pc client* dan akhirnya terhubung dengan *website* yang *direquest*.

### c. Enkripsi

Suatu enkripsi sangat erat dengan sistem keamanan pada suatu jaringan termasuk dalam jaringan WLAN adalah:

#### 1) *Wired Equivalent Privacy* (WEP)

Teknik enkripsi yang meniru cara kerja teknologi *wired*, karena pada komunikasi dengan teknologi *wired* dirasa lebih aman dibandingkan dengan *wireless*. prinsip kerja WEP yaitu menggunakan *shared key* secara bersama baik untuk proses enkripsi maupun deskripsi. Namun prinsip kerja inilah yang menjadi WEP.

#### 2) *Wi-Fi Protected Access* (WPA)

Teknologi ini merupakan pengembangan dari teknologi yang sebelumnya yaitu WEP. Pada teknologi ini *shared key* tetap digunakan akan tetapi akan dirotasi dengan tujuan menyulitkan *cracker* menangkap *shared key* yang digunakan. Proses otentikasinya menggunakan 802.1x dan *Extensible Authentication Protocol* (EAP), dimana user akan terotentikasi jika akan bergabung dengan jaringan *wireless* dan diberlakukan *mutual authentication* sehingga user tidak akan bias bergabung tanpa kesengajaan. Pada perangkat *wi-Fi* umumnya sudah mendukung WPA.

#### 3) *Wi-Fi Protected access 2* (WPA2)

Teknologi WPA2 merupakan pengembangan dari WPA, dengan tujuan meningkatkan performa *client* saat mengakses *access point*. Proses otentikasinya

menggunakan algoritma AES dan 802.1x sehingga menjamin keamanan data dan *control access* lebih baik dari teknologi sebelumnya.

## 2. Aspek Keamanan Jaringan

Aspek keamanan komputer meliputi aspek-aspek di antaranya:

### a. Authentication

Agar penerima informasi dapat memastikan keaslian pesan tersebut datang dari orang yang dimintai informasi, dengan kata lain informasi tersebut benar-benar dari orang yang dikehendaki.

### b. Integrity

Keaslian pesan yang dikirim melalui sebuah jaringan dan dapat dipastikan bahwa informasi yang dikirim tidak dimodifikasi oleh orang yang tidak berhak dalam perjalanan informasi tersebut.

### c. Nonrepudiation

Merupakan hal yang bersangkutan dengan sipengirim, sipengirim tidak dapat mengelak bahwa dia lah yang mengirim informasi tersebut

### d. Authority

Informasi yang berada pada sistem jaringan tidak dapat dimodifikasi oleh pihak yang tidak berhak atas akses tersebut.

### e. Confidentiality

Merupakan usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. Confidentiality biasanya berhubungan dengan informasi yang diberikan ke pihak lain

f. Privacy

Merupakan lebih kearah data-data yang sifatnya privat (pribadi)

g. Availability

Aspek availability atau ketersediaan berhubungan dengan ketersediaan informasi ketika dibutuhkan. Sistem informasi yang diserang atau dijebol dapat menghambat atau meniadakan akses ke informasi.

h. Access Control

Aspek ini berhubungan dengan cara pengaturan akses kepada informasi. Hal ini biasanya berhubungan dengan masalah authentication dan juga privacy. Access control seringkali dilakukan dengan menggunakan kombinasi user id dan password atau dengan menggunakan mekanisme lainnya.

## 2.6.2. Jenis Gangguan Keamanan Jaringan

### 1. Hacking

*Hacking* adalah kegiatan menerobos komputer milik orang lain/pihak lain, pengrusakan pada infrastruktur jaringan yang sudah ada, misalnya pengrusakan pada sistem dari suatu server. Memiliki keahlian membuat dan membaca program tertentu dan terobsesi mengamati keamanan (*security*)-nya.

### 2. Phising

*Phising* adalah suatu bentuk penipuan yang dicirikan dengan percobaan untuk mendapatkan informasi peka seperti, kata sandi dan kartu kredit, dengan menyamar sebagai orang atau bisnis yang terpercaya dalam sebuah komunikasi elektronik resmi, seperti surat elektronik atau pesan instan. Istilah *phising* dalam

bahasa inggris berasal dari kata *fishing* (“memancing”), dalam hal ini berarti memancing informasi keuangan dan kata sandi pengguna.

### 3. *Deface*

Perubahan terhadap tampilan suatu website secara illegal. *Carding*, pencurian data terhadap identitas perbankan seseorang, misalnya pencurian nomor kartu kredit, digunakan untuk memanfaatkan saldo yang terdapat pada rekening tersebut untuk keperluan belanja online.

### 4. *Carding*

*Carding* merupakan pencurian data terhadap identitas perbankan seseorang, misalnya pencurian nomor kartu kredit, digunakan untuk memanfaatkan saldo yang terdapat pada rekening tersebut untuk keperluan belanja *online*.

### 5. *Spoofing*

*Spoofing* adalah pemalsuan *IP address* untuk menyerang sebuah *server* di internet yaitu dengan cara menggunakan alamat email seseorang atau tindakan penyusupan dengan menggunakan identitas resmi secara ilegal. Dengan menggunakan identitas tersebut, penyusup akan dapat mengakses segala sesuatu, dalam jaringan ini biasanya para *hacker/cracker* sering menggunakan cara ini. *Spoofing* merupakan teknik yang digunakan untuk memperoleh akses yang tidak sah kesuatu komputer atau informasi, dimana penyerang berhubungan dengan pengguna dengan pura-pura memalsukan bahwa mereka adalah *host* yang dapat dipercaya.

### 6. *Password cracker*

*Password cracker* adalah sebuah program yang dapat membuka *enkripsi* sebuah password atau sebaliknya malah untuk mematikan sistem pengaman password.