# BAB II

# TINJAUAN PUSTAKA

## 2.1 Jaringan

### 2.1.1 Pengertian Jaringan Komputer

Jaringan komputer adalah terhubungnya dua komputer atau lebih dengan kabel penghubung (pada beberapa kasus, tanpa kabel atau *wireless* sebagai penghubung), sehingga antar komputer dapat saling tukar informasi (Sopandi, 2008).

Tujuan penggunaan jaringan komputer adalah :

a. Untuk berbagi sumber daya, sepert berbagi *printer*, CPU, memori, hardisk, dan lain-lain.
b. Untuk komunikasi, seperti e-mail, *instant messaging* , *chatting*, dan lain-lain.
c. Untuk mengakses informasi, seperti *web browsing*, *file server*, dan lain-lain.

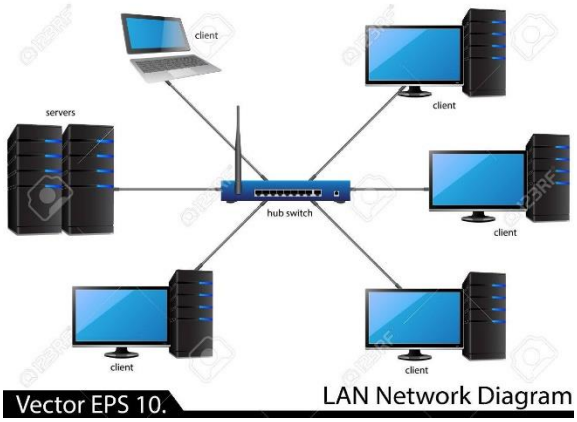
Untuk mencapai tujuan yang sama maka setiap bagian dalam suatu jaringan akan meminta dan memberikan layanan. Jadi, dalam jaringan terlibat dua pihak, yaitu pihak yang meminta layanan disebut klien (*client*) dan pihak yang memberikan layanan disebut pelayan (*server*). Arsitektur jaringan ini disebut dengan sistem *client-server* dan digunakan oleh seluruh jaringan (Hasan, 2016).

### 2.1.2 Klasifikasi Jaringan

Jaringan diklasifikasikan berdasarkan jarak dan lokasi, yaitu *Local Area Network* (LAN), *Metropolitan Area Network* (MAN), *Wide Area Network* (WAN), dan jaringan tanpa kabel (*Wireless*), yang dijelaskan sebagai berikut:

a. *Local Area Network* (LAN)

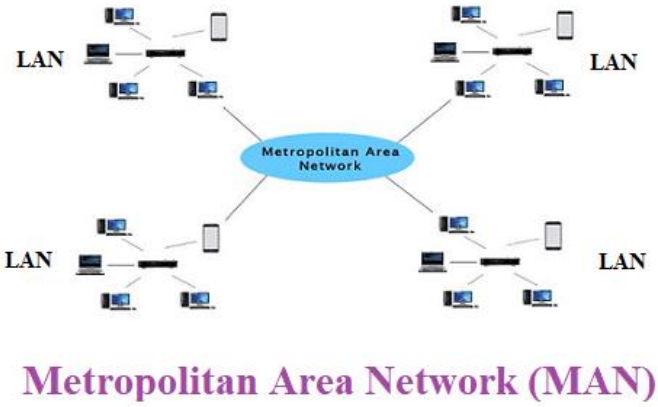
LAN adalah jaringan yang dibatasi oleh area yang relatif kecil, umumnya dibatasi oleh area lingkungan seperti sebuah perkantoran di sebuah gedung atau sebuah sekolah dan tidak jauh dari sekitar 1 km persegi (Madcoms, 2016).




**Gambar 2.1** Model LAN

b. *Metropolitan Area Network* (MAN)

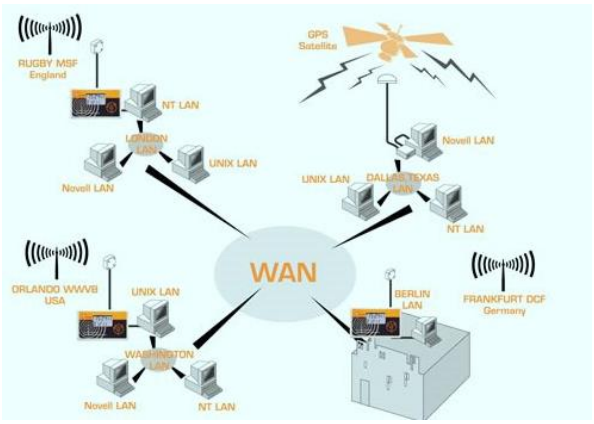
MAN meliputi area yang lebih besar dari LAN, misalnya antar wilayah dalam satu provinsi. Dalam hal ini jaringan menghubungkan beberapa buah jaringan-jaringan kecil ke dalam lingkungan area yang lebih besar, sebagai contoh yaitu jaringan bank dimana beberapa kantor cabang sebuah bank di dalam sebuah kota besar dihubungkan antara satu dengan lainnya (Madcoms, 2016).




**Gambar 2.2** Model MAN

c. *Wide Area Network* (WAN)

WAN adalah jaringan yang lingkupnya sudah menggunakan media satelit atau kabel bawah laut, sebagai contoh keseluruhan jaringan bank yang ada di Indonesia atau yang ada di negara - negara lain (Madcoms, 2016).




**Gambar 2.3** Model WAN

d. *Wireless Local Area Network* (WLAN)

WLAN adalah jaringan komputer yang menggunakan gelombang sinyal radio sebagai transmisi data. Data ditransfer dari satu perangkat ke perangkat yang lain tanpa menggunakan kabel sebagai perantara ( Madcoms, 2016 ).


**Gambar 2.4** Model WLAN

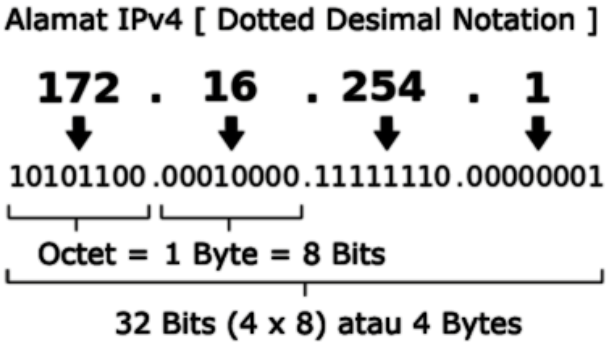
### 2.1.3 *IP Address*

*IP Address* merupakan singkatan dari "*Internet Protocol Address*". Ini digunakan sebagai alamat lokasi jaringan dan sebagai alat identifikasi *host* atau antarmuka pada jaringan yang dilabelkan pada alat komputer, *printer*, dan *router*. Semua ini bertujuan untuk mengenali komputer yang mencoba mengirimkan data kepadanya.

Ada 2 jenis *IP Address*, yaitu *"IP Address Public"* yang biasa digunakan pada jaringan *global internet*, kemudian *"IP Address Private"* yang biasa merupakan alamat IP untuk digunakan pada komputer dan perangkatnya dengan jaringan yang berskala lokal (LAN).

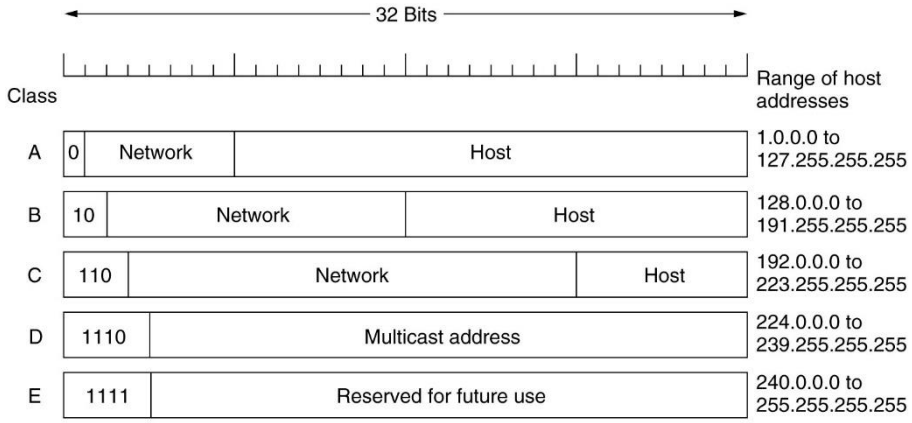
Ada beberapa alamat khusus yang baik untuk diketahui sebelumnya. Pertama adalah *"Network Address",* yang akan menunjukkan alamat suatu jaringan, namun yang paling kecil menurut *IP Address*. Selanjutnya *"Broadcast Address",* ini digunakan dalam jaringan yang paling kecil menurut IP Address untuk mengirimkan paket ke seluruh *host.* Terakhir merupakan *"Loopback",* yang merupakan alamat lokal yang dimiliki setiap komputer, dan bernilai 127.0.0.1.

Menurut Wardoyo dkk (2014) (dalam Hartono, 2019) menjelaskan, Berdasarkan *format* dari *IP Address* versi 4 (IPv4) ini, terdiri dari bilangan biner 32 bit, dan terbagi menjadi 4 kelompok. Setiap kelompok terdiri dari bilangan biner 8 bit, dan tanda pemisah tersebut disebut dengan "oktet"




**Gambar 2.5** *Format* Penulisan IP *Address* versi 4 (IPv4)

Dalam *IP Address*, terdapat dua cara pembagian, yaitu: *"Classfull Addressing",* yang dibagi berdasarkan kelas-kelas *IP Address (Class A-E)*, dan *"Classless Addressing"*, yang berupa pengalamatan tanpa kelas, dengan cara mengalokasikan IP Address dalam notasi *"Classless Inter Domain Routing" (CIDR).*




**Gambar 2.6** Macam Kelas IP *Address*

Kelas A

Format : 0nnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh

Bit Pertama : 0

Panjang NetID : 8 bit

Panjang HostID : 24 Bit

Byte Pertama : 0-127

Jumlah : 126 Kelas A (0 dan 127 dicadangkan)

Range IP : 1.xxx.xxx.xxx sampai 126.xxx.xxx.xxx

Jumlah IP : 16.777.214 IP Address disetiap kelas A

Deskripsi : Diberikan untuk jaringan dengan jumlah host yang besar

Kelas B

Format : 10nnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh

Bit Pertama : 10

Panjang NetID : 16 Bit

Panjang HostID : 16 Bit

Byte Pertama : 128-191

Jumlah : 16.384 Kelas B

Range IP : 128.0.xxx.xxx sampai 191.155.xxx.xxx

Jumlah IP : 65.532 IP Address di setiap kelas B

Deskripsi : Dialokasikan untuk jaringan besar dan sedang

Kelas C

| | |
|---|---|
| Format | : 110nnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh |
| Bit Pertama | : 110 |
| Panjang NetID | : 24 Bit |
| Panjang HostID | : 8 Bit |
| Byte Pertama | : 192-223 |
| Jumlah | : 2.097.152 Kelas C |
| Range IP | : 192.xxx.xxx.xxx sampai 223.255.255.xxx |
| Jumlah IP | : 254 IP Address disetiap kelas C |
| Deskripsi | : Diberikan untuk jaringan berukuran kecil |

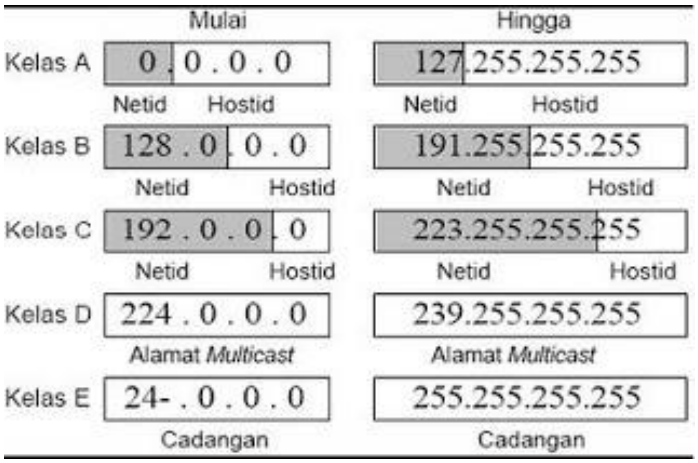
Kelas D

| | |
|---|---|
| Format | : 1110nnn.hhhhhhhh.hhhhhhhh.hhhhhhhh |
| Bit Pertama | : 1110 |
| Bit Multicast | : 28 Bit |
| Byte Inisial | : 224-247 |
| Deskripsi | : Kelas D digunakan untuk keperluan IP Multicast |

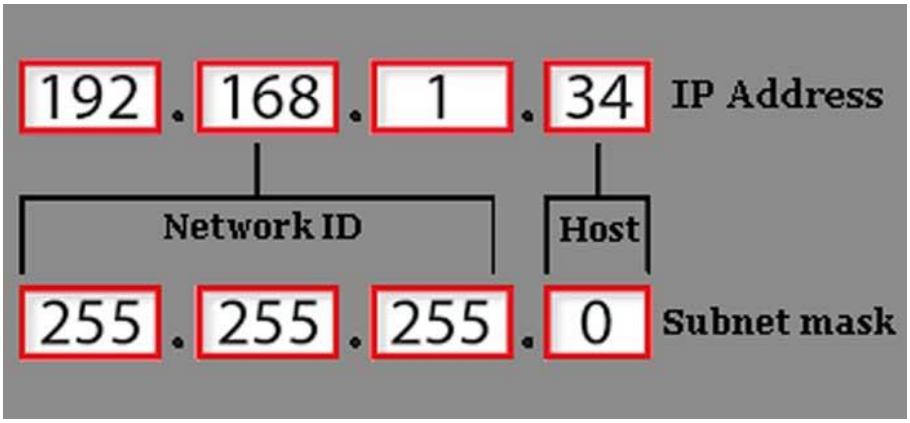
Kelas E

| | |
|---|---|
| Format | : 1111rrrr.rrrrrrrr.rrrrrrrr.rrrrrrrr |
| Bit Pertama | : 1111 |
| Bit Cadangan | : 28 Bit |
| Bit Inisial | : 248-255 |
| Deskripsi | : Kelas E dicadangkan untuk keperluan eksperimen |

Format IP *Address* juga terdiri dari pembagian kelas-kelas yang berdasarkan dua hal, yaitu: *"Network ID"*, yang digunakan untuk menunjukkan jaringan lokasi komputer berada, dan *"Host ID"* untuk menunjukkan host pada suatu jaringan, seperti *workstation, server, router, host TCP/IP*, dan lainnya.




**Gambar 2.7** *Format* Kelas IP *Address*




**Gambar 2.8** *Format* IP *Address*

Aturan dasar dalam menentukan *"Network ID"* adalah 127.0.0.1 tidak dapat digunakan. Ini dikarenakan merupakan *default* yang sudah diatur untuk menunjukkan dirinya sendiri *(loop-back). "Host ID"* juga tidak boleh diatur sebagai 1 (contohnya: 126.255.255.255), yang dapat diartikan sebagai *ID broadcast*, yang merupakan alamat mewakili seluruh anggota pada jaringan.

Menurut Lukman (2016) (dalam Hartono, 2019) menjelaskan bahwa *Network ID* dan *Host ID* tidak boleh menggunakan IP *Address* yang sama dengan 0 (contoh, 0.0.0.0). *Host ID* yang menggunakan 0, dapat diartikan sebagai alamat jaringan. Alamat jaringan digunakan untuk menunjukkan suatu jaringan, dan bukan host. Maka, *Host ID* harus unik dalam suatu jaringan, dan dalam dua host tidak boleh memiliki *Host ID* yang sama .

## 2.2 *Network Security* ( Keamanan Jaringan )

### 2.2.1 Pengertian Keamanan Jaringan

Keamanan informasi adalah bagaimana kita dapat mencegah penipuan atau mendeteksi adanya penipuan di sebuah sistem berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik (Rahardjo, 1998).

Keamanan jaringan menurut Mariusz Stawowski dalam jurnalnya "*The principles of network security design*", adalah Keamanan jaringan hal yang utama sebagai perlindungan sumber daya sistem terhadap ancaman yang berasal dari luar jaringan. Keamanan komputer digunakan untuk mengontrol resiko yang berhubungan dengan penggunaan komputer. Keamanan komputer yang dimaksud adalah keamanan sebuah komputer yang terhubung ke dalam sebuah jaringan (*Internet*).

Target *network security* adalah bagaimana mencegah dan menghentikan berbagai *threats* (potensi serangan) agar tidak memasuki dan menyebar pada suatu *network* (Sofana 2010:310). Pada dasarnya banyak *threats* (potensi serangan) yang mengancam *network security*, seperti yang telah dipaparkan oleh Sofana dalam bukunya yang berjudul Cisco CCNA & Jaringan Komputer (2010: 310) berbagai *threats* yang mengancam *network security* dapat digolongkan menjadi beberapa golongan, diantaranya adalah : (1) *Viruses*, *Worms*, and *Trojan horses*; (2) *Spyware and adware*; (3) *Zero-day attacks (zero-hour) attacks*; (4) *Hacker attacks*; (5) *Denial of service attacks (DoS*); (6) *Data interception and theft*; (7) *Identity theft.*

### 2.2.2 Sistem Keamanan Jaringan Komputer

Sistem keamanan jaringan komputer adalah suatu sistem yang memiliki tugas untuk melakukan pencegahan dan identifikasi kepada pengguna yang tidak sah dalam jaringan komputer. Langkah pencegahan ini berfungsi untuk menghentikan penyusup untuk mengakses lewat sistem jaringan komputer. Tujuan dari dilakukan sistem keamanan jaringan komputer adalah untuk antisipasi dari ancaman dalam bentuk fisik maupun *logic* baik secara langsung atau tidak langsung yang mengganggu sistem keamanan jaringan.

### 2.2.3 Aspek Dasar Keamanan Jaringan Komputer

Garfinkel mengemukakan bahwa keamanan komputer (*computer security*) melingkupi empat aspek, yaitu *privacy*, *integrity*, *authentication* dan *availability*. Selain hal tersebut, ada dua aspek yang ada kaitannya dengan *electronic commerce*, yaitu *access control* dan *non-repudiation* (Rahardjo, 1998: 10-13).

1. *Privacy* atau *Confidentiality*

Merupakan suatu usaha untuk menjaga informasi dari orang yang tidak memiliki hak akses. *Privacy* lebih kearah data-data yang sifatnya privat sedangkan *confidentiality* berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu (misalnya sebagai bagian dari pendaftaran sebuah servis). Serangan terhadap aspek *privacy* misalnya adalah usaha untuk melakukan penyadapan. Usaha yang dapat dilakukan untuk meningkatkan *privacy* dan *confidentiality* adalah dengan menggunakan teknologi kriptografi.

2. *Integrity*

Aspek yang menekankan bahwa informasi atau data tidak boleh diubah tanpa seizin pemilik informasi. Adanya *virus*, *trojan horse* atau pemakai lain yang mengubah informasi tanpa ijin merupakan contoh masalah yang harus dihadapi. Sebuah *e-mail* dapat saja "ditangkap" (*intercept*) di tengah jalan, diubah isinya, kemudian diteruskan ke alamat yang dituju. Dengan kata lain, integritas dari informasi sudah tidak terjaga. Penggunaan enkripsi dan *digital signature* misalnya, dapat mengatasi masalah ini. Contoh serangan lain adalah *"man in the middle*

*attack"* dimana seseorang menempatkan diri ditengah pembicaraan dan menyamar sebagai orang lain.

3. *Authentication*

Aspek ini berhubungan dengan metode untuk menyatakan bahwa informasi betul-betul asli, orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud. Dalam hal ini pengguna harus menunjukkan bukti bahwa memang dia adalah pengguna yang sah, misalnya penggunakan *password*, keamanan *biometric* dan sejenisnya.

4. *Availability*

Aspek ini berhubungan dengan ketersediaan informasi ketika dibutuhkan. Sistem informasi yang diserang atau dijebol dapat menghambat atau meniadakan askes ke informasi. Contoh hambatan adalah serangan *"denial of service attack"* atau lebih dikenal dengan sebutan *DoS Attack*, dimana server dikirimi permintaan (biasanya palsu) yang bertubi-tubi sehingga tidak dapat melayani permintaan lain tau bahkan sampai *down, hang, crash.*

5. *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, password* atau dengan menggunakan mekanisme.

6. *Non Repudiation*

Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan suatu transaksi. Sebagai contoh, seseorang yang mengirimkan *email* untuk memesan barang tidak dapat menyangkal bahwa dia telah mengirimkan *email* tersebut. Aspek ini sangat penting dalam *electronic commerce*. Penggunaan *digital signature* dan teknologi kriptografi secara umum dapat menjaga aspek ini.

## 2.3 *Blocking Port*

*Blocking port* adalah konsep yang dalam kinerjanya menutup jalan port yang rentan oleh masuknya virus kedalam jaringan. Dalam pengimplementasiannya, *Setting blocking port* menggunakan mikrotik dengan memanfaatkan fitur *firewall*. Fitur ini berfungsi untuk *filtering* koneksi pada jaringan.

Jika *firewall* sudah tersetting secara otomatis seluruh port yang sudah diblock / *filter* tidak dapat di kunjungi oleh *client. Port* yang tidak terfilter oleh mikrotik, saat *client request* ke server layanan akan dibalas oleh server sesuai dengan permintaan dari *client. Blocking port* ini sangatlah efisien digunakan, karena dapat meminimalisir virus dari *port* yang tidak terpercaya masuk dalam sebuah jaringan (Pratiwi dan Akbi, 2018).

## 2.4 *Firewall*

### 2.4.1 Pengertian *Firewall*

*Firewall* atau dinding api adalah sistem perangkat lunak yang mengizinkan lalu lintas jaringan yang dianggap aman untuk dapat melaluinya dan mencegah lalu lintas jaringan yang dianggap tidak aman. Pada dasarnya sebuah *firewall* dipasang pada sebuah *router* yang berjalan pada *gateway* antara jaringan lokal dengan jaringan Internet (Komputer, 2014).

### 2.4.2 Fungsi *Firewall*

Menurut Wahana Komputer (2014:72), *Firewall* berperan dalam melindungi jaringan dari serangan yang berasal dari jaringan luar. *Firewall* mengimplementasikan paket *filtering*. Dengan demikian, *firewall* menyediakan fungsi keamanan yang digunakan untuk mengelola aliran data ke , dari, dan melalui *router*. Berikut fungsi – fungsi *firewall* secara umum:

1. Mengontrol dan mengawasi paket data yang mengalir di jaringan.

   *Firewall* harus dapat mengatur, memfilter dan mengontrol lalu lintas data yang diizin untuk mengakses jaringan privat yang dilindungi *firewall. Firewall* harus dapat melakukan pemeriksaan terhadap paket data yang akan melewati jaringan *private*.

Beberapa kriteria yang dilakukan firewall apakah memperbolehkan paket data lewati atau tidak, antara lain:

a. Alamat IP dari komputer sumber
b. *Port* TCP/UDP sumber dari sumber
c. Alamat IP dari komputer tujuan
d. *Port* TCP/UDP tujuan data pada komputer tujuan
e. Informasi dari *header* yang disimpan dalam paket data

2. Melakukan autentifikasi terhadap akses.
3. Aplikasi *Proxy*

*Firewall* mampu memeriksa lebih dari sekedar *header* dari paket data, kemampuan ini menuntut *firewall* untuk mampu mendeteksi protokol aplikasi tertentu yang spesifikasi.

4. Mencatat semua kejadian di jaringan

Mencatat setiap transaksi kejadian yang terjadi di *firewall*. Ini memungkinkan membantu sebagai pendeteksian dini akan kemungkinan penjebolan jaringan.

## 2.5 *Router*

### 2.5.1 Pengertian *Router*

*Router* adalah perangkat yang melewatkan paket IP dari suatu jaringan ke jaringan yang lain menggunakan metode *addressing* dan *protocol* tertentu. *Router-router* yang terhubung dalam jaringan tergabung dalam suatu algoritma *routing* untuk menentukan jalur terbaik yang dilalui paket IP (Herlambang dkk, 2008).

Proses *routing* dilakukan secara *hop by hop*. IP tidak mengetahui seluruh jalur menuju tujuan setiap paket. IP hanya *routing* menyediakan IP *address* dari *router* berikutnya yang lebih dekat ke *host* tujuan. Fungsi *router* sebagai berikut :

a. Membaca alamat logika / *IP address source* dan *destination* untuk menentukan *routing* dari suatu LAN ke LAN lainnya.
b. Menyimpan *routing table* untuk menentukan rute terbaik antara LAN ke WAN.
c. Perangkat layer ke-3 dalam *Open Systems Interconnection (OSI) Layer*.

d. Dapat berupa "*box*" atau sebuah OS yang menjalankan sebuah daemon *routing*.
e. *Interfaces Ethernet*, Serial.

## 2.6 Mikrotik *Router*

### 2.6.1 Pengertian Mikrotik

Mikrotik adalah sistem operasi independen berbasis Linux, khusus untuk komputer yang berfungsi sebagai *router*. Mikrotik sangat baik untuk keperluan administrasi jaringan komputer seperti merancang dan membangun sebuah sistem jaringan berskala kecil hingga yang kompleks. Mikrotik digunakan sejak tahun 1995 yang awalnya ditujukan untuk perusahaan jasa layanan *internet (Internet Service Provider* / ISP) (Husaini, 2008) .

Saat ini mikrotik memberi layanan kepada banyak ISP untuk layanan akses internet di seluruh dunia. Mikrotik pada hardware berbasis PC dikenal dengan kestabilan, kualitas kontrol, dan fleksibilitas untuk berbagai jenis paket data dan penanganan proses rute (*routing*). Mikrotik yang dijadikan *router* berbasis komputer banyak bermanfaat untuk ISP yang ingin menjalankan beberapa aplikasi. Selain *routing,* mikrotik dapat digunakan sebagai manajemen kapasitas akses, seperti *bandwidth, firewall, wireless access point* (WiFi*), backhaul link, system hotspot, Virtual Private Network Server,* dan lainnya (Husaini, 2008).

### 2.6.2 Jenis - Jenis Mikrotik

Menurut Husaini (2008), Berdasarkan fungsi dan bentuk mikrotik dibedakan menjadi 2 jenis, yaitu :

a. Mikrotik *router* OS yang berbentuk perangkat lunak (*software*), yang dapat di-download di www.mikrotik.com dan dapat diinstal pada komputer PC.
b. *Built-in Hardware* Mikrotik atau yang berbentuk perangkat keras (*hardware*), yang dikemas dalam bentuk *routerboard* yang didalamnya sudah terinstall mikrotik *router* OS.


**Gambar 2.9** Mikrotik *Routerboard*

## 2.7 *Malware*

### 2.7.1 Pengertian *Malware*

*Malware (malicious software)* adalah perangkat lunak yang dapat mengganggu proses atau kinerja dalam sistem operasi komputer seperti mencuri informasi data sensitif dan melakukan remote pada komputer target tanpa seizin pemilik. *Malware* ada dalam berbagai bentuk seperti *script, code, active content*, dan perangkat lunak (Ryansyah dan Maulana, 2018).

### 2.7.2 Macam – Macam *Malware*

Menurut Yudhanto (dalam Sumardi dan Triyono, 2013: 17-18) menjelaskan macam-macam *malware*, fungsi dan cara kerjanya yaitu sebagai berikut :

a. *Virus* adalah suatu program komputer yang dapat menyebar pada komputer atau jaringan dengan cara membuat *copy* dari dirinya sendiri tanpa sepengetahuan dari pengguna komputer tersebut;
b. *Worm* atau dalam bahasa Indonesia disebut dengan cacing. Seperti sifat cacing, *worm* dapat menyebar ke beberapa komputer melalui *port* tertentu. *Worm* mampu membuat *copy* dari dirinya sendiri dan menggunakan jaringan komunikasi antar komputer untuk menyebarkan dirinya. *Worm* di desain untuk merusak sistem komputer tertentu yang sudah menjadi target dari jarak jauh (*remote*). Perbedaan *worm* dan *virus* adalah *virus* menginfeksi target *code*, tetapi *worm* tidak. *Worm* hanya menetap di memori;

c. *Trojan* adalah program yang bersifat menghancurkan dan dapat mengelabuhi targetnya. Seperti halnya dengan *virus*, *trojan* juga memiliki kemampuan untuk menggandakan diri seperti *virus.* Selain itu *trojan* juga dapat mengendalikan program tertentu dan dapat mengelabuhi sistem dengan menyerupai aplikasi biasa.

## 2.8 *Port*

### 2.8.1 Pengertian *Port*

*Port* adalah tempat di mana informasi masuk dan keluar dari komputer, *port scanning* mengidentifikasi pintu terbuka ke komputer. Port memiliki penggunaan yang sah dalam mengelola jaringan, tetapi *port scanning* juga bisa berbahaya jika seseorang sedang mencari titik akses yang lemah untuk masuk ke komputer anda.

*Port* dapat mengidentifikasikan aplikasi dan layanan yang menggunakan koneksi di dalam jaringan TCP/IP. Sehingga, *port* juga mengidentifikasikan sebuah proses tertentu dimana sebuah *server* dapat memberikan sebuah layanan kepada klien atau bagaimana sebuah klien dapat mengakses sebuah layanan yang ada dalam *server*. *Port* dapat diklasifikasikan ke dalam *Port* TCP dan *Port* UDP. Total maksimum jumlah *port* untuk setiap protokol *transport* yang digunakan adalah 65536 buah ( Sumardi dan Triyono, 2013).

*Port* TCP dan UDP dibagi menjadi tiga macam, yaitu:

1. *Well-known Port*: pada awalnya berkisar antara 0 hingga 255 tapi kemudian diperlebar untuk mendukung antara 0 hingga 1023. *Port number* yang termasuk ke dalam *well-known port* selalu merepresentasikan layanan jaringan yang sama, dan ditetapkan oleh *Internet Assigned Number Authority* (IANA);
2. *Registered Port*: *Port-port* yang digunakanoleh vendor-vendor komputer atau jaringan yang berbeda untuk mendukung aplikasi dan sistem operasi masing-masing. *Registered port* diketahui dan didaftarkan oleh IANA tapi tidak dialokasikan secara permanen, sehingga vendor lainnya dapat menggunakan port number yang sama. *Range Registered Port* berkisar dari

1024 hingga 49151 dan beberapa *port* diantaranya adalah *Dynamically Assigned Port*;

3. *Dynamically Assigned Port*: merupakan *port-port* yang ditetapkan oleh sistem operasi atau aplikasi yang digunakan untuk melayani *request* dari pengguna sesuai dengan kebutuhan. *Dynamically Assigned Port* berkisar dari 1024 hingga 65536 dan dapat digunakan atau dilepaskan sesuai kebutuhan.

## 2.9 *Port Scanning*

### 2.9.1 Pengertian *Port Scanning*

*Port scanning* adalah suatu kegiatan atau aktifitas atau proses untuk mencari dan melihat serta meneliti *port* pada suatu komputer atau peralatan lainnya. Tujuannya adalah meneliti kemungkinan kelemahan dari suatu sistem yang terpasang pada komputer melalui *port* yang terbuka.

*Port scanning* juga dianggap sebagai bentuk yang lebih bertarget dari pengumpulan informasi yang mencoba untuk profil layanan yang dijalankan pada target potensial. *Port Scanning* adalah salah satu teknik popular yang digunakan para penyerang untuk mencari celah sehingga mereka dapat masuk ke suatu layanan. Semua sistem yang terhubung ke jaringan LAN ataupun internet melalui *modem* menjalankan layanan dengan *port* yang sudah dikenal dan tidak dikenal. *Port scanning* terdiri dari penyelidikan sejumlah jaringan untuk mencari *port* yang terbuka (Habsoro dkk, 2015:139).

## 2.10 *Network Mapper* (NMAP)

### 2.10.1 Pengertian NMAP

Nmap (*Network Mapper*) adalah sebuah *tool open source* untuk eksplorasi dan audit keamanan jaringan. Nmap menggunakan paket *IP raw* untuk mendeteksi *host* yang terhubung dengan jaringan dilengkapi dengan layanan (nama aplikasi dan versi) yang diberikan, sistem operasi (dan versi), apa jenis *firewall/filter* paket yang digunakan, dan sejumlah karakteristik lainnya.

*Output* Nmap adalah sebuah daftar target *host* yang diperiksa dan informasi tambahan sesuai dengan opsi yang digunakan, informasi yang didapat dari *output* NMAP yaitu :

1. Nomor *port*
2. Nama layanan
3. *Status port* : terbuka (*open*), difilter (*filtered*), tertutup (*closed*), atau tidak difilter (*unfiltered*).
4. Nama *reverse* DNS
5. Prakiraan sistem operasi
6. Jenis *device*
7. Alamat *MAC*