BAB II

TINJAUAN PUSTAKA

2.1 Jaringan

2.1.1 Pengertian Jaringan Komputer

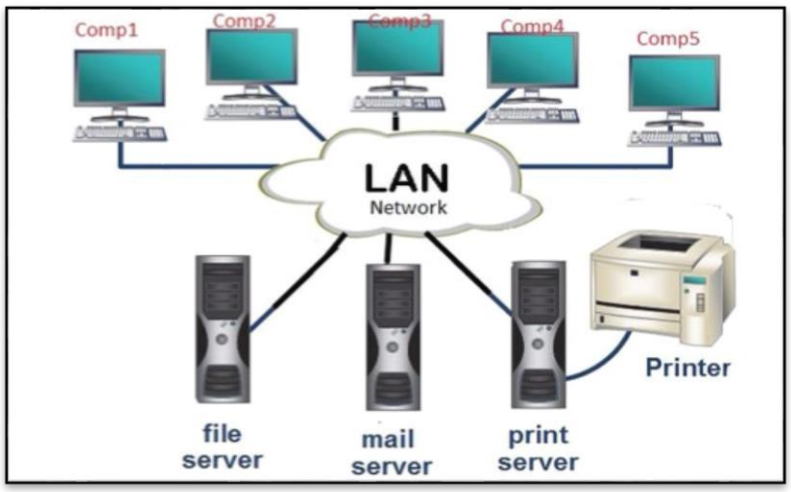
Jaringan komputer adalah kumpulan komputer dan alat-alat lain yang saling terhubung bersama menggunakan media komunikasi tertentu. Tujuan dari jaringan komputer ialah agar setiap bagian dari jaringan komputer dapat saling berkomunikasi dan berbagi atau Sharing informasi.

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)

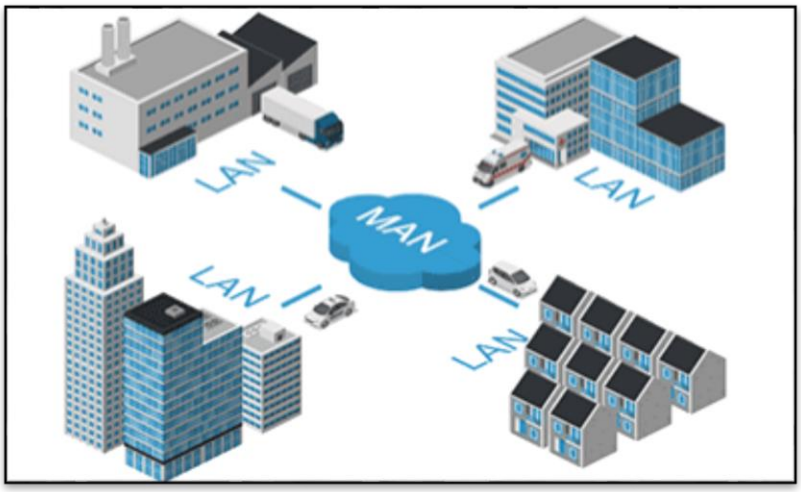
LAN adalah jaringan yang dibatasi oleh area yang relatif kecil, umumnya dibatasi oleh area lingkungan seperti sebuah perkantoran di sebuah gedung atau sebuah sekolah dan tidak jauh dari sekitar 1 km persegi (Madcoms, 2016).



Gambar 2.1 Model LAN

b. *Metropolitan Area Network* (MAN)

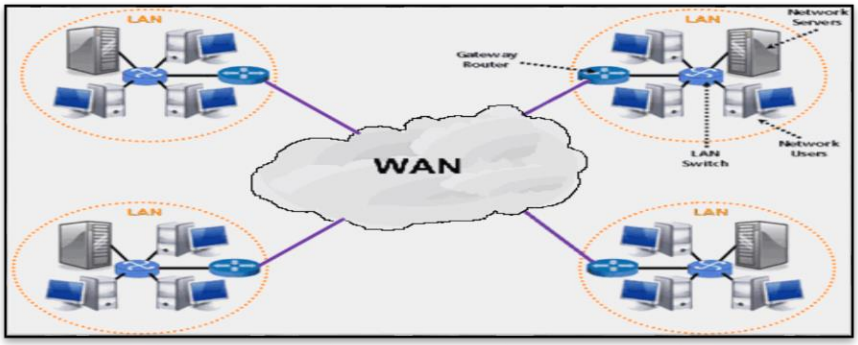
MAN meliputi area yang lebih besar dari LAN, misalnya antar wilayah dalam satu provinsi. Dalam hal ini jaringan menghubungkan beberapa buah jaringan-jaringan kecil ke dalam lingkungan area yang lebih besar, sebagai contoh yaitu jaringan bank dimana beberapa kantor cabang sebuah bank di dalam sebuah kota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

2.2 Keamanan Jaringan

2.2.1 Pengertian Keamanan Jaringan

Keamanan jaringan ialah proses pencegahan yang dilakukan terhadap penyerang yang terhubung ke dalam jaringan komputer melalui akses yang tidak sah, atau penggunaan secara ilegal dari komputer dan jaringan

2.2.2 Aspek Dasar Keamanan Jaringan Komputer

Keamanan jaringan komputer sendiri secara garis besar memiliki tujuan sebagai berikut :

a. *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.

b. *Integrity*

Jaringan komputer yang dapat diandalkan juga berdasar pada fakta bahwa data yang tersedia apa yang sudah seharusnya. Jaringan komputer mau tidak mau harus terlindungi dari serangan *(attacks)* yang dapat merubah data selama dalam proses persinggahan *(transmit). Man-in-the-middle* merupakan jenis serangan yang dapat merubah integritas dari sebuah data yang mana penyerang *(attacker)* dapat membajak *session* atau memanipulasi data yang terkirim

Didalam jaringan komputer yang aman, partisipan dari sebuah transaksi data harus yakin bahwa orang yang terlibat dalam komunikasi data dapat diandalkan dan dapat dipercaya. Keamanan dari sebuah komunikasi data sangat diperlukan pada sebuah tingkatan yang dipastikan data tidak berubah selama proses pengiriman dan penerimaan pada Saat komunikasi data.

c. *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.

d. *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.*

e. *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.

2.2.3 Bentuk Ancaman Jaringan Komputer

Bentuk ancaman im ditujukan terhadap sumber daya fisik danlogik yang mendukung jarmgan yang ada, bentuk ancarnan tersebut diantaranya sebagai berikut :

1. ***Sniffer***, ancaman terhadap peralatan yang dapat memonitor proses yang sedang berlangsung.
2. ***Spoofing***, Penggunaan komputer untuk meniru (dengan cara menimpa identitas atau alamat IP).
3. ***Phreaking***, ancaman perilaku menjadikan sistem pengamanan telepon melemah.
4. ***Remote Attack***, segala bentuk serangan terhadap suatu mesin dimana penyerangnya tidak memiliki kendali terhadap mesin tersebut karena dilakukan dari jarak jaruh di luar sistem jarmgan atau media transmisi.
5. ***Hole***, kondisi dari atau *hardware* yang bisa diakses oleh pemakai yang tidak mermliki otoritas atau meningkatnya tingkat pengaksesan tanpa melalui proses autorisasi.
6. ***Hacker***, ialah seorang yang diam-diam mempelajari sistem yang biasanya sukar dimengerti untuk kemudian mengelolanya dan men-*share* hasil ujicoba yang dilakukannya, hacker tidak merusak sistem.
7. ***Cracker***, ialah orang yang secara diam-diam mempelajari sistem dengan maksud jahat, muncul karena sifat dasar manusia yang selalu ingin membangun (salah satunya merusak).

2.2.4 Metode Penyerangan Jaringan Komputer

Penyerangan terhadap jaringan komputer dilakukan dengan berbagai metode, diantaranya serangan dilakukan dengan metode sebagai berikut :

1. ***Eavesdropping***, mendapatkan duplikasi pesan tanpa ijin.

2. ***Masquerading***, mengirim atau menerima pesan menggunakan identitas lain tanpa ijin.
3. ***Message Tampering***, mencegat atau menangkap pesan dan mengubah isinya sebelum dilanjutkan ke penerima sebenarnya. *Man-in-the-middle attack* adalah bentuk *message tampering* dengan mencegat pesan pertama pada pertukaran kunci enkripsi pada pembentukan suatu saluran yang aman. Penyerangan menyisipkan kunci lain yang memungkinkan dia untuk mendeskrip pesan berikutnya sebelum dienkrip oleh penerima.
4. ***Replaying,*** menyimpan pesan yang ditangkap untuk pemakaian berikutnya.
5. ***Denial of Service,*** membanjiri saluran atau sesumber lain dengan pesan yang bertujuan untuk menggagalkan pengaksesan pemakai lain.

2.3 Firewall

2.3.1 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.

2.3.2 Fungsi Firewall

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:

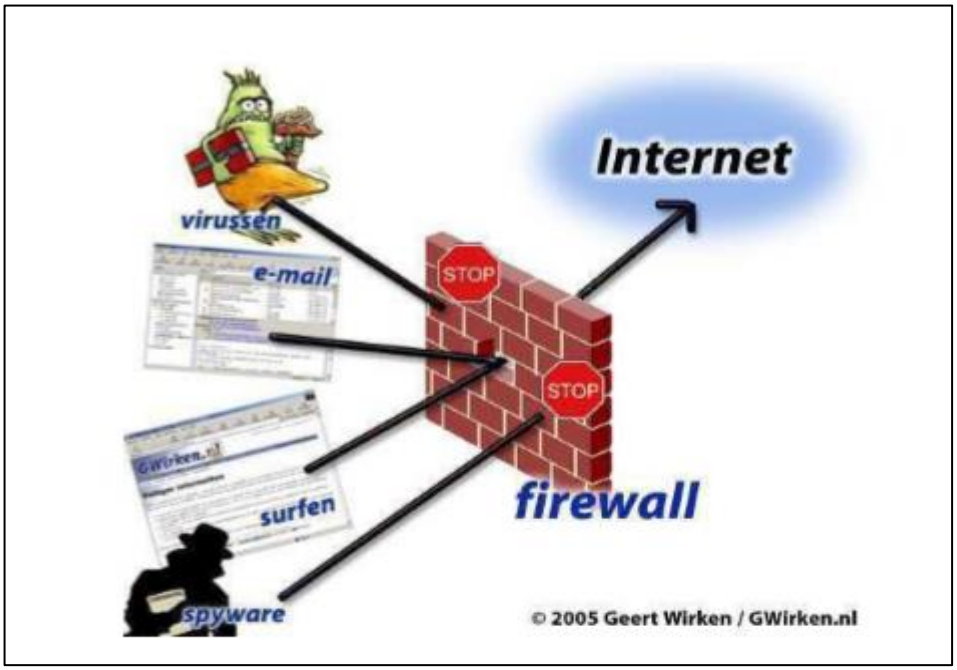
a. Alamat IP dari komputer sumber
b. Port TCP/UDP sumber dari sumber
c. Alamat IP dari komputer tujuan
d. Port TCP/UDP tujuan data pada komputer tujuan
e. Informasi dari header yang disimpan dalam paket data

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.



Gambar 2.5 *Firewall* mencegah *virus* dan ancaman lain masuk ke jaringan

2.4 Port

2.4.1 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. *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.

2.5 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.

2.6 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.

2.7 Mikrotik Router

2.7.1 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) .

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.

2.7.2 Jenis - Jenis Mikrotik

Berdasarkan fungsi dan bentuknya, mikrotik dibedakan menjadi 2 jenis, yaitu :

a. Mikrotik *Router* OS adalah sebuah *software* yang berfungsi mengubah PC (komputer) menjadi sebuah *router*. Mikrotik *Router* OS layaknya IOS cisco yang diinstall di dalam *Router* Cisco, hanya saja IOS cisco tidak bisa di install di dalam komputer kecuali menggunakarl *emulator* seperti GNS3. Pada dasarnya *Router* OS merupakan sistem operasi Mikrotik *RouterBOARD* yang berbasis Kernel Linux v2.6. Mikrotik *router* OS yang berbentuk perangkat lunak (*software*), yang dapat di-*download* di www.mikrotik.com.
b. *Built-in Hardware* Mikrotik atau yang berbentuk perangkat keras (*hardware*), yang dikemas dalam bentuk *routerboard* yang didalamnya sudah terinstall mikrotik *router* OS.

Gambar 2.6 Mikrotik *Routerboard*

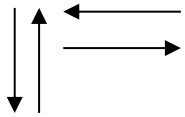
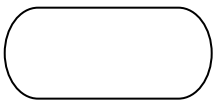
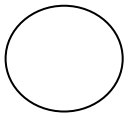
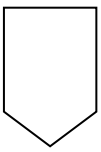
2.8 Flowchart

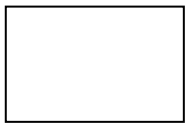
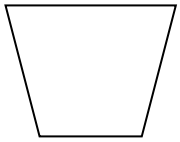
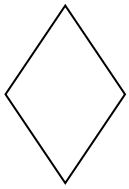
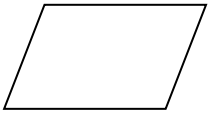
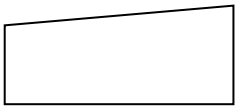
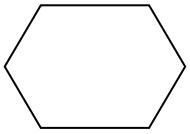
Flowchart merupakan penggambaran secara fisik dari langkah-langkah dan urutan prosedur program yang biasanya mempermudah penyelesaian masalah. Flowchart atau diagram alir merupakan sebuah diagram dengan simbol-simbol gratis yang menyatakan aliran algoritma atau proses yang menampilkan langkah-langkah yang disimbolkan dalam bentuk kotak, beserta urutannya dengan menghubungkan masing-masing langkah tersebut menggunakan tanda panah.

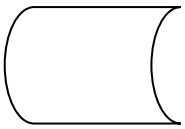
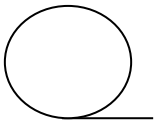
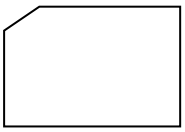
Berdasarkan pendapat yang dikemukakan diatas, dapat ditarik kesimpulan bahwa flowchart atau diagram alur adalah suatu alat yang banyak digunakan untuk membuat algoritma, yakni bagaimana rangkaian pelaksanaan suatu kegiatan. Suatu diagram alur memberikan gambaran dua dimensi berupa simbol-simbol grafis. Masing-masing simbol telah ditetapkan terlebih dahulu fungsi dan artinya.

Simbol-simbol flowchart beserta fungsinya dapat ditunjukkan pada tabel di bawah ini:

Tabel 2.3 Simbol – Simbol Flowcart

	**Flow Direction Symbol** Yaitu simbol yang digunakan untuk menghubungkan antara simbol yang satu dengan simbol yang lain. Simbol ini disebut juga connecting line.
	**Terminator Symbol** Yaitu simbol untuk permulaan (start) atau akhir (stop) dari suatu kegiatan.
	**Connector Symbol** Yaitu simbol untuk keluar – masuk atau penyambungan proses dalam lembar / halaman yang sama.
	**Connector Symbol** Yaitu simbol untuk keluar – masuk atau penyambungan proses dalam lembar / halaman yang berbeda.

	**Processing Symbol** Simbol yang menunjukkan pengolahan yang dilakukan oleh komputer.
	**Manual Operation Symbol** Simbol yang menunjukkan pengolahan yang tidak dilakukan oleh komputer.
	**Decision Symbol** Simbol pemilihan proses berdasarkan kondisi yang ada.
	**Input – Output Symbol** Simbol yang menyatakan proses input dan output tanpa tergantung dengan jenis peralatannya.
	**Manual Input Symbol** Simbol untuk pemasukan data secara manual on-line keyboard.
	**Preparation Symbol** Simbol untuk mempersiapkan penyimpanan yang akan digunakan sebagai tempat pengolahan di dalam storage.
	**Predifined Process Symbol** Simbol untuk pelaksanaan suatu bagian (sub-program) atau prosedur.

	**Display Symbol** Simbol yang menyatakan peralatan output yang digunakan yaitu layar, yaitu plotter, printer dan sebagainya.
	**Disk and On-line Storage Symbol** Simbol yang menyatakan input yang berasal dari disk atau disimpan ke disk.
	**Magnetic Tape Unit Symbol** Simbol yang menyatakan input berasal dari pita magnetik atau outpuy disimpan ke pita magnetik.
	**Punch Card Symbol** Simbol yang menyatakan bahwa input berasal dari kartu atau output ditulis ke kartu.
	**Document Symbol** Simbol yang menyatakan input berasal dari dokumen dalam bentuk kertas atau output dicetak ke kertas.