

BAB II

TINJAUAN PUSTAKA

2.1 Jaringan Komputer

Jaringan Komputer adalah suatu himpunan interkoneksi sejumlah komputer, dalam bahasa populer dapat dijelaskan bahwa jaringan komputer adalah kumpulan beberapa komputer, dan perangkat lain seperti *router*, *switch* dan sebagainya [1].

Jaringan Komputer adalah himpunan “interkoneksi” antara 2 komputer *autonomous* atau lebih yang terhubung dengan media transmisi kabel atau tanpa kabel *wireless*. Bila sebuah komputer dapat membuat komputer lainnya *restart*, *shutdown*, atau melakukan kontrol lainnya, maka komputer-komputer tersebut bukan *autonomous* tidak melakukan kontrol terhadap komputer lain dengan akses penuh [2].

Jaringan Komputer adalah kumpulan komputer yang saling terhubung dan memungkinkan antar komputer untuk saling bertukar data [3].

Jaringan dapat diartikan interkoneksi dari beberapa komputer. Komputer-komputer ini dapat dihubungkan secara bersama-sama untuk kepentingan yang berbeda dan menggunakan berbagai jenis kabel yang terpisah. Sehingga mengarah ke pengurangan pemakaian waktu dan meningkatnya produktifitas [4].

Dari berbagai definisi diatas dapat ditarik kesimpulan bahwa Jaringan Komputer adalah sekumpulan dari beberapa komputer yang tersambung dan saling

terhubung sehingga dapat saling berbagi informasi dan berkomunikasi antara satu perangkat dengan perangkat lainnya.

2.1.1 Jenis Jaringan Komputer

Jenis jaringan komputer dibagi menjadi 5 bagian diantaranya yaitu ;

1. *Local Area Network* (LAN)

Local Area Network adalah jaringan lokal yang di buat pada area terbatas. Misalkan dalam satu gedung atau satu ruangan. Kadangkala jaringan lokal di sebut juga jaringan personal atau privat. Lan bisa di gunakan pada sekala kecil yang menggunakan *resource* secara bersama, seperti penggunaan *printer* bersama, penggunaan media penyimpanan secara bersama, dan sebagainya.

2. *Metropolitan Area Network* (MAN)

Metropolitan area network menggunakan metode yang sama dengan LAN namun daerah cangkupnya lebih luas. Daerah cangkupan MAN bisa satu RW, beberapa kantor yang berada dalam satu komplek yang sama, satu/beberapa desa, satu/beberapa kota. Dapat dikatankan MAN pengembangan dari LAN.

3. *Wide Area Network* (WAN)

Wide area network cangkupnya lebih luas dari pada MAN. Cangkupan MAN meliputi satu kawasan, satu Negara, satu pulau, bahkan satu dunia, metode yang digunakan WAN sama seperti yang di gunakan LAN dan MAN. Umumnya WAN di hubungkan dengan jaringan telepon digita. Namun media transmisi lain pun dapat digunakan.

4. *Personal Area Network (PAN)*

Personal Area Network (PAN) adalah sebuah jaringan yang berfungsi untuk berkomunikasi antara komputer dengan perangkat-perangkat lainnya seperti handphone, speaker, printer, scanner dan masih banyak lagi. PAN dikendalikan menggunakan otoritas pribadi, PAN memakai teknologi *Wireless Application Protocol (WAP)* dan Bluetooth. Port yang digunakan untuk jaringan PAN antara lain adalah USB dan *Firewire*.

5. *Wireless Personal Area Network (WPAN)*

Wireless Personal Area Network (WPAN) merupakan jaringan area pribadi yang eksklusif dan berpusat di sekitar perangkat yang terhubung menggunakan media nirkabel. Umumnya, jangkauan dari jaringan ini lebih kurang 10 meter.

2.1.2 Kelebihan Jaringan Komputer

1. Meningkatkan komunikasi dan ketersediaan.
2. Memungkinkan untuk berbagi sumber daya yang lebih nyaman.
3. Membuat berbagi file lebih mudah.
4. Sangat fleksibel.
5. Sistem yang murah.
6. Meningkatkan efisiensi biaya.
7. Meningkatkan kapasitas penyimpanan.

2.1.3 Kekurangan Jaringan Komputer

1. Mengalami ketergantungan.
2. Kurang dalam keamanan.
3. Kurang memiliki ketahanan.
4. Memungkinkan lebih banyak virus komputer dan malware,
5. Mempromosikan tindakan negative.
6. Membutuhkan penanganan yang efisien.
7. Membutuhkan pengaturan yang mahal.

2.2 Topologi Jaringan

“*Topologi* dapat di artikan sebagai layout atau arsitektur atau diagram jaringan computer”. *Topologi* merupakan aturan bagaimana menghubungkan komputer secara fisik.

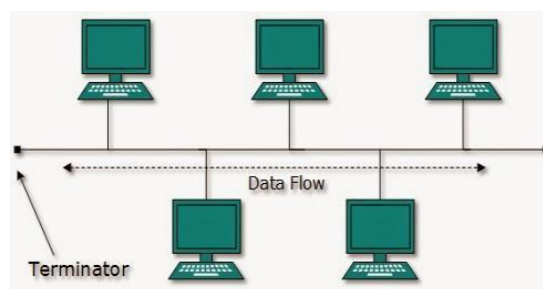
Topologi berkaitan dengan cara komponen-komponen jaringan seperti: (*server workstation, router, switch*) saling berkomunikasi melalui media tranmisi data [1].

Dari definisi diatas dapat ditarik sebuah kesimpulan bahwa *Topologi* berasal dari bahasa Yunani yaitu *topos* yang berarti "tempat", dan *logos*, yang berarti "ilmu". *Topologi* adalah cabang dari matematika yang menyangkut tata ruang yang tidak berubah dalam deformasi dwikontinu, yakni ruang yang dapat ditekuk, dilipat, disusutkan, direntangkan, dan dipilih, tetapi tidak diperbolehkan dipotong, disobek, ditusuk atau direkatkan.

Ia muncul melalui pengembangan konsep dari geometri dan teori himpunan, seperti ruang, dimensi, bentuk, transformasi. Ketika kita memilih satu *topologi* maka kita perlu mengikuti spesifikasi yang diberlakukan atas *topologi* tersebut. Ada beberapa *topologi* utama yang sering di gunakan yaitu: *Topologi Bus*, *Topologi Ring*, *Topologi Star*, *Topologi Tree*, *Topologi Mesh*.

1. *Topologi Bus*

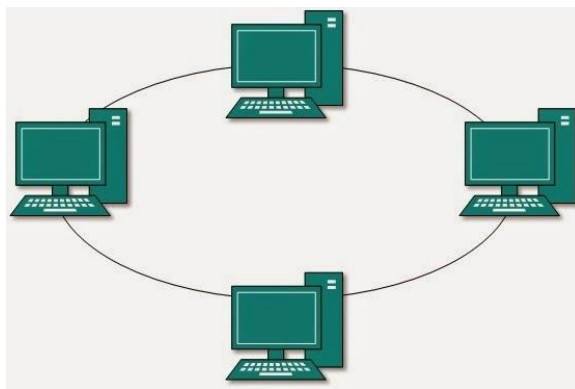
Topologi Bus, merupakan topologi yang menghubungkan beberapa komputer ke sebuah kabel dengan terminal. *Topologi Bus* menggunakan jenis kabel coaxial dengan beberapa konektor BNC. *Topologi Bus* menyediakan 1 jalur yang digunakan untuk komunikasi antar perangkat sehingga setiap perangkat harus bergantian dalam menggunakan jalur yang ada. Dalam berkomunikasi antar perangkat, hanya ada 2 perangkat yang dapat saling berkomunikasi. Kecepatan transfer rata-rata data antar perangkat sangat lambat karena harus bergantian dalam menggunakan jalur [5].



Gambar 1. *Topologi Bus*

2. *Topologi Ring*

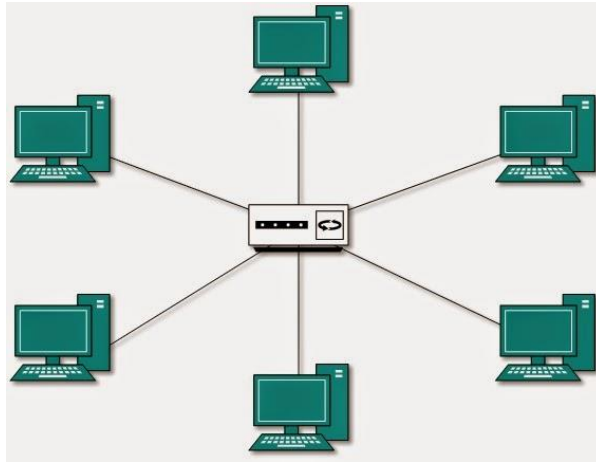
Topologi Ring, merupakan topologi yang menghubungkan beberapa komputer dengan membentuk lingkaran. Komputer yang terhubung dalam sebuah jaringan akan terkoneksi pada 2 komputer lain [5].



Gambar 2. *Topologi Ring*

3. *Topologi Star*

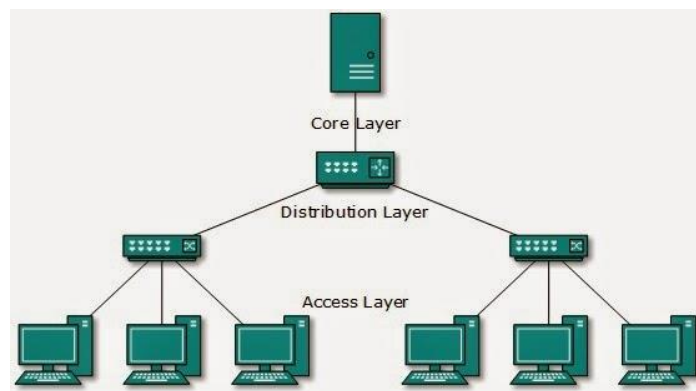
Topologi Star, merupakan topologi yang menghubungkan beberapa komputer dengan menggunakan perangkat yaitu Hub atau Switch. Perangkat ini berfungsi sebagai pengontrol dari semua computer yang terhubung dalam jaringan [5].



Gambar 3. *Topologi Star*

4. *Topologi Tree*

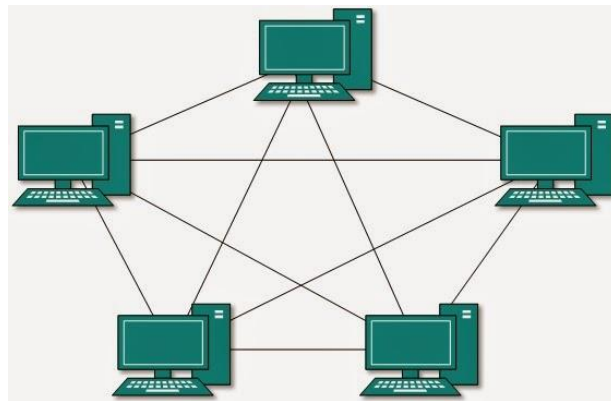
Topologi Tree, merupakan topologi yang biasa digunakan pada jaringan di dalam ruangan kantor yang bertingkat. Topologi ini biasanya digunakan untuk interkoneksi antarsentral dengan hirarki yang berbeda. Pada topologi ini terdapat beberapa tingkat simpul (*node*). Pusat atau simpul yang lebih tingkatannya, dapat mengatur simpul lain yang lebih rendah tingkatannya.



Gambar 4. *Topologi Tree*

5. Topologi Mesh

Topologi Mesh merupakan topologi yang bisa dipakai untuk rute banyak di jaringan yang ingin digunakan. Jaringan di topologi ini menggunakan kabel tunggal sehingga pengiriman data lebih cepat tanpa memakai hub ataupun switch.

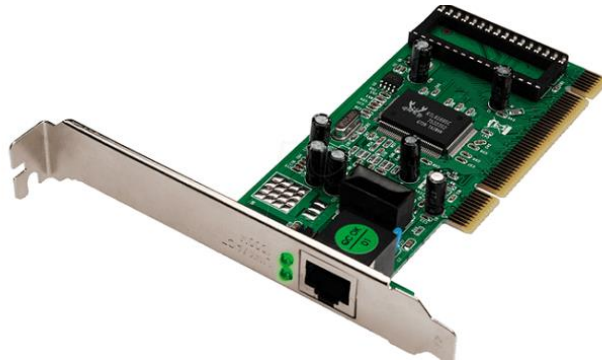


Gambar 5. Topologi Mesh

2.3 Perangkat Jaringan

1. Kartu Jaringan (*Ethernet/LAN Card*)

Kartu jaringan merupakan perangkat yang dipasang pada sebuah PC yang berfungsi untuk dapat berkomunikasi dengan computer melalui jaringan LAN. Setiap kartu jaringan memiliki *MAC Address* (Medium Access Control) yang bersifat unik, yang berarti tidak ada 2 buah kartu jaringan yang memiliki *MAC Address* yang sama [5].



Gambar 6. Kartu Jaringan (Ethernet /LAN Card)

2. Hub

Hub merupakan perangkat jaringan yang bekerja di OSI Layer 1 (Physical Layer). Hub berfungsi sebagai penerima sinyal dari sebuah komputer, kemudian mentransmisikan ke komputer lain. Dengan kata lain, Hub bekerja sebagai penyambung concentrator dan sebagai penguat sinyal pada kabel UTP [5].



Gambar 7. HUB

3. Switch

Switch merupakan perangkat jaringan yang bekerja pada OSI Layer 2 (Data Link Layer). Switch berfungsi hamper sama dengan Hub. Switch mengenal MAC Address yang digunakan untuk memilah data mana yang harus

di transmisikan. Switch menampung daftar MAC Address yang dihubungkan port-port yang digunakan untuk menentukan harus mengirim paket, sehingga akan mengurangi traffic pada jaringan [5].

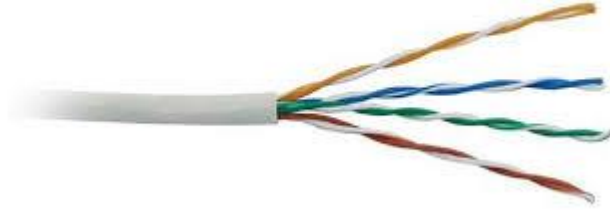


Gambar 8. Switch

4. Kabel Jaringan

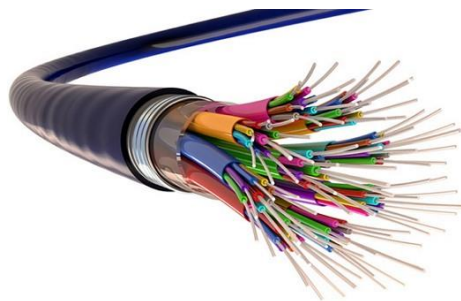
Kabel jaringan merupakan perangkat yang digunakan sebagai jalur yang menghubungkan Antara perangkat satu dengan perangkat yang lain [5]. Terdapat beberapa jenis kabel yang digunakan dalam jaringan komputer yaitu, diantaranya adalah :

- a. Kabel UTP (*Unshielded Twisted pair*) merupakan kabel yang sering dipakai dalam sebuah jaringan komputer. Kabel UTP digunakan sebagai media penghubung antar komputer dan peralatan jaringan yang lain (*Hub atau Switch*) .



Gambar 9. Kabel UTP

- b. Kabel Fiber Optic merupakan kabel jaringan yang dapat mentransmisikan cahaya. Dibandingkan dengan jenis lainnya kabel Fiber Optic lebih mahal harganya. Kabel Fiber Optic memiliki jangkauan yang lebih jauh sampai dengan ratusan kilometer.



Gambar 10. Kabel Fiber Optic

5. Konektor

Konektor merupakan perangkat yang digunakan sebagai penghubung kabel. Konektor terpasang pada ujung-ujung kabel [5]. Jenis konektor yang digunakan harus disesuaikan dengan jenis kabel yang dipergunakan :

- a. Konektor RJ-45 (*Registered Jack*) merupakan konektor yang digunakan untuk jenis kabal UTP.



Gambar 11. Konektor Rj-45

- b. Konektor ST merupakan konektor yang digunakan untuk jenis kabal Fiber Optic. Bentuk konektor ST hamper mirip dengan konektor BNC. Konektor ini umum digunakan untuk single mode maupun multi mode.



Gambar 12. Konektor ST

6. Tang Crimping

Tang crimping merupakan peralatan yang digunakan untuk memasang konektor RJ-45 pada kabel UTP [5].



Gambar 13. Tang Crimping

7. Kabel Tester

Kabel Tester merupakan peralatan yang digunakan untuk menguji hasil pemasangan konektor pada kabel. Fungsinya untuk mengetahui apakah pemasangan konektor sudah benar atau belum [5].

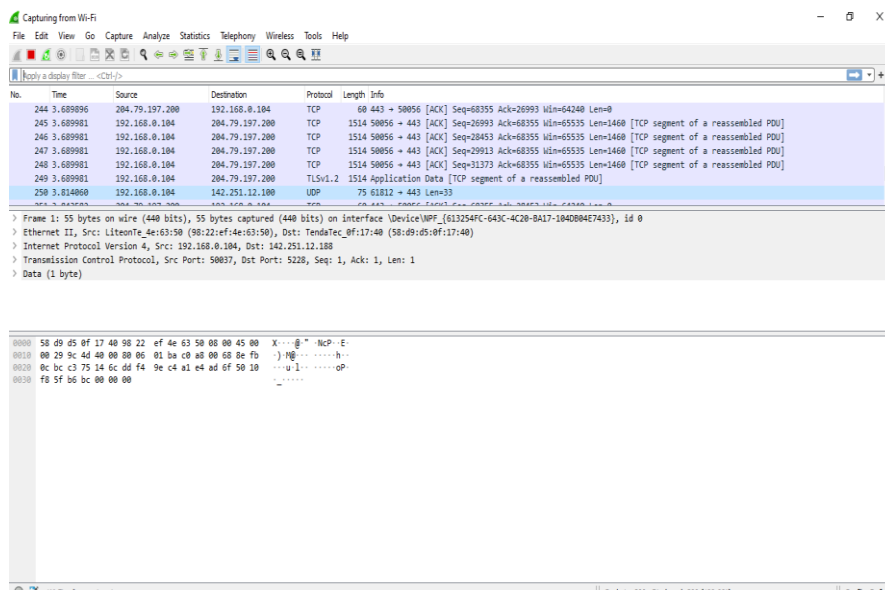


Gambar 14. Kabel Tester

8. Software Wireshark

Wireshark merupakan suatu aplikasi yang digunakan untuk menganalisa *packet* jaringan, sebuah *packet* jaringan *analyzer* yang digunakan untuk menangkap *packet* jaringan dan untuk menampilkan data *packet* sedetail mungkin. Untuk logika *analyzerpacket* jaringan dan aplikasi digunakan untuk melakukan *sniffing* atau mengamati *traffic* data yang ada dalam jaringan. Dengan menggunakan *wireshark*, seseorang dapat melihat dan menyimpan *traffic* data dalam sebuah jaringan, yang kemudian data yang berhasil dikumpulkan dapat dianalisa lebih lanjut.

Saat ini *wireshark* merupakan salah satu analisis terbaik tersedia dalam bentuk *packet open source*. Tampilan yang tersedia terbilang sangat bersahabat dan *user friendly* menggunakan tampilan grafis GUI (*Graphical User Interface*).



Gambar 15. Penggunaan *Wireshark*

2.4 TCP/IP

Dalam komunikasi antar dua network device atau lebih, diperlukan sebuah standar yang saling dimengerti antara satu dengan yang lain, dalam sebuah jaringan istilah ini disebut dengan protocol. TCP/IP sebenarnya mengacu pada sekumpulan set protocol yang terdiri dari dua protokol utama yaitu : *Transmission Control Protocol* dan *Internet Protocol*. TCP/IP memungkinkan terjadinya komunikasi antar komputer yang memiliki karakteristik dari segi *hardware* maupun *software* [5].

2.4.1 TCP (*Transmission Control Protocol*)

TCP merupakan bagian dari Protokol TCP/IP yang digunakan bersama dengan IP untuk mengirim data dalam bentuk unit-unit pesan antara komputer ke internet.

Protokol TCP bertanggung jawab untuk pengiriman data dari sumber ke tujuan dengan benar. TCP juga bertugas mendeteksi kesalahan atau hilangnya data dan melakukan pengiriman kembali sampai data yang benar diterima dengan lengkap [5].

2.4.2 IP (*Internet Protocol*)

IP adalah protokol pada TCP/IP yang mengatur bagaimana suatu data dapat dikenal dan dikirim dari satu komputer ke komputer lain hingga sampai ke tujuan dalam suatu jaringan komputer. IP memiliki karakteristik sebagai *connectionless protocol* [5].

2.5 Sistem Keamanan Jaringan

Keamanan jaringan menurut Mariusz Stawowski dalam jurnalnya "*The principles of network security design*", adalah Keamanan jaringan yang utama sebagai perlindungan sumber daya sistem terhadap ancaman yang berasal dari luar jaringan [6].

Sistem keamanan jaringan, jaringan komputer adalah koneksi dari dua atau lebih perangkat yang terhubung secara fisik dan logis sehingga mereka dapat bertukar data. Jika perangkat di jaringan dapat bertukar data dan berbagi sumber daya, jaringan komputer dapat diartikan terhubung [7].

Keamanan jaringan komputer adalah tugas untuk melindungi dan mengamankan jaringan komputer yang dibangun. Keamanan jaringan merupakan salah satu halter penting dalam membangun jaringan komputer. Satu hal yang perlu diingat adalah tidak ada jaringan yang anti sadap, atau tidak ada jaringan komputer yang sepenuhnya aman [7].

Dari berbagai definisi diatas dapat ditarik kesimpulan bahwa sistem Keamanan jaringan komputer adalah suatu sistem untuk mencegah dan mengidentifikasi penggunaan yang tidak sah dari jaringan komputer. Langkah-langkah pencegahan membantu menghentikan pengguna yang tidak sah yang disebut "penyusup" untuk mengakses setiap bagian dari sistem jaringan komputer. Tujuan keamanan jaringan komputer adalah untuk mengantisipasi resiko jaringan komputer berupa bentuk ancaman fisik maupun logik baik langsung ataupun tidak langsung mengganggu aktivitas yang sedang berlangsung dalam jaringan komputer

Satu hal yang perlu diingat bahwa tidak ada jaringan yang anti sadap atau tidak ada jaringan komputer yang benar-benar aman. Sifat dari jaringan adalah melakukan komunikasi. Setiap komunikasi dapat jatuh ke tangan orang lain dan disalahgunakan.

2.5.1 Aspek Keamanan Jaringan

a. Confidentiality

Confidentiality merupakan pencegahan bagi mereka yang tidak berkepentingan dapat mencapai informasi. Secara umum dapat disebutkan bahwa kerahasiaan mengandung makna bahwa informasi yang tepat terakses oleh mereka yang berhak dan bukan orang lain, sama analoginya dengan e-mail maupun data-data perdagangan dari perusahaan.

b. Integrity

Integrity merupakan pencegahan bagi mereka yang tidak berkepentingan dapat mencapai informasi. Secara umum dapat disebutkan bahwa kerahasiaan mengandung makna bahwa informasi yang tepat terakses oleh mereka yang berhak dan bukan orang lain, sama analoginya dengan E-mail maupun data-data perdagangan dari perusahaan adalah pencegahan terhadap kemungkinan amandemen atau penghapusan informasi oleh mereka yang tidak berhak. Secara umum maka integritas ini berarti bahwa informasi yang tepat, memang tepat dimana-mana dalam sistem atau mengikuti istilah *messaging* tidak terjadi cacat maupun terhapus dalam perjalanannya dari penyaji kepada para penerima yang berhak.

c. Availability

Availability merupakan upaya pencegahan ditahannya informasi atau sumber daya terkait oleh mereka yang tidak berhak. Secara umum maka makna yang dikandung adalah bahwa informasi yang tepat dapat diakses bila dibutuhkan oleh siapapun yang memiliki legitimasi untuk tujuan ini.

Berkaitan dengan *messaging system* maka pesan itu harus dapat dibaca oleh siapapun yang dialamatkan atau yang diarahkan, sewaktu mereka ingin membacanya.

d. Authentication

Authentication merupakan suatu langkah untuk menentukan atau mengonfirmasi bahwa seseorang atau sesuatu adalah autentik atau asli. Melakukan autentikasi terhadap sebuah objek adalah melakukan konfirmasi terhadap kebenarannya. Sedangkan melakukan autentikasi terhadap seseorang biasanya adalah untuk memverifikasi identitasnya. Pada suatu sistem komputer, autentikasi biasanya terjadi pada saat login atau permintaan akses.

e. Access Control

Access Control merupakan sebuah metode untuk mentransmisikan sinyal yang dimiliki oleh node-node yang terhubung ke jaringan tanpa terjadi konflik hak akses. *Accountability* Aspek ini berhubungan dengan ketersediaan informasi ketika dibutuhkan. Sistem informasi yang diserang dapat menghambat atau meniadakan akses ke informasi. Proses *Access Control* ditujukan untuk memastikan bahwa hanya orang-orang yang berwenang dan

punya alasan yang absah, terkait dengan operasi dan bisnis, mendapatkan ijin, dan memahami dan memenuhi persyaratan yang ditentukan untuk masuklah yang dapat memasuki dan/atau bekerja di dalam fasilitas. Hal ini dimaksudkan agar keselamatan dan keamanan fasilitas, dan orang-orang yang berada di dalamnya dapat terjaga

2.5.2 Ancaman Keamanan Jaringan

Serangan terhadap keamanan sistem informasi *security attack* dewasa ini seringkali terjadi. Kejahatan komputer atau *cyber crime* pada dunia maya sering kali dilakukan oleh sekelompok orang yang ingin menembus suatu keamanan sebuah sistem. Aktivitas ini bertujuan untuk mencari, mendapatkan, mengubah, dan bahkan menghapus informasi yang ada pada sistem tersebut jika memang benar-benar dibutuhkan. Ada beberapa kemungkinan tipe dari serangan yang dilakukan oleh penyerang yaitu :

- a. *Interception* yaitu pihak yang tidak mempunyai wewenang telah berhasil mendapatkan hak akses informasi.
- b. *Interruption* yaitu penyerang telah dapat menguasai sistem, tetapi tidak keseluruhan. Admin asli masih bisa login.
- c. *Fabrication* yaitu penyerang telah menyisipkan objek palsu ke dalam sistem target.
- d. *Modification* yaitu penyerang telah merusak sistem dan telah mengubah secara keseluruhan.

2.5.3 Serangan Keamanan Jaringan

a. *Cisco Discovery Protocol (CDP)*

Cisco Discovery Protocol (CDP) adalah tool yang berguna untuk mengatasi *incomplete* atau *inaccurate network*. CDP merupakan media dan protocol independent yang hanya menampilkan informasi tentang koneksi router tetangga terdekat.

CDP digunakan untuk mendapatkan informasi tentang cisco tetangga, seperti informasi tentang tipe *device* yang terhubung, interface yang terhubung, *interface* yang digunakan untuk koneksi dan jumlah model *device*. CDP adalah media dan protokol yang independen dan jalan di atas *Subnetwork Access Protocol (SNAP)*.

b. *Telecommunications Network Protocol (Telnet)*

Telecommunications Network Protocol (Telnet) merupakan remote login yang terjadi pada jaringan internet disebabkan karena adanya *service* dari *protocol Telnet*. Dengan adanya Telnet dapat memungkinkan pengguna dapat mengakses komputer lain secara remote melalui jaringan internet.

Telnet digunakan untuk melakukan login ke komputer lain yang ada di jaringan internet dan dapat melakukan akses pada pelayanan umum, termasuk pada berbagai macam database. Penggunaanya dapat duduk saja di depan komputer yang terhubung ke jaringan internet. Dengan kata lain dapat terkoneksi ke komputer lain dalam satu gedung, satu ruangan atau bahkan

pada komputer di seluruh penjuru dunia. Setelah terhubung atau terkoneksi, input yang diberikan pada keyboard dapat secara langsung mengontrol ke remote komputer tadi, dapat diakses pelayanan apa saja yang telah disediakan oleh remote machine dan hasilnya akan ditampilkan pada terminal lokal. Dengan menggunakan Telnet, pengguna dapat mengakses berbagai layanan misalnya seperti melihat katalog perpustakaan dan masih banyak lagi layanan yang lainnya. Pada penggunaannya Telnet memakai 2 program yaitu pada *client* dan *server*. Program pada *client* digunakan untuk meminta layanan pada server, sedangkan program yang terdapat pada *server* akan memberikan layanan yang diminta oleh *client*.

c. *Mac Addresss Table Floodin Attack*

Mac Addresss Table Floodin Attack adalah tipe serangan ini seseorang dapat mengirimkan paket dengan konstruksi header yang berbeda antar satu paket dengan paket lainnya. Dengan mekanisme serangan tersebut secara otomatis switch akan mengirimkan pesan *OFPT PACKET IN* ke kontroler. Hal ini dapat menyebabkan kontroler menggunakan seluruh sumber daya yang dimiliki untuk memproses paket yang masuk sehingga dapat menyebabkan kontroler menjadi crash dan jaringan tidak dapat diakses.

d. *Virtual Local Area Network (VLAN)*

Virtual Local Area Network VLAN merupakan sekumpulan dari *device* pada sebuah jaringan LAN yang dikonfigurasi menggunakan *management software*, sehingga bisa berkomunikasi jika device tersebut

terhubung pada kabel yang sama dan dialokasikan pada jumlah segment LAN yang berbeda karena VLAN berdasarkan pada *logical connection* dari pada *physical connection* dan VLAN sangat fleksibel. Dalam hal ini berarti transmisi dihasilkan oleh sebuah *station* pada VLAN dan diterima oleh *station-station* yang belum ditentukan oleh kriteria tertentu dalam domain.

e. *Dynamic Host Configuration Protocol (DHCP)*

Dynamic Host Configuration Protocol (DHCP) adalah protokol yang berbasis arsitektur *client/server* yang dipakai untuk memudahkan pengalokasian alamat IP dalam satu jaringan. Sebuah jaringan lokal yang tidak menggunakan DHCP harus memberikan alamat IP kepada semua komputer secara manual. Jika DHCP dipasang di jaringan lokal, maka semua komputer yang tersambung di jaringan akan mendapatkan alamat IP secara otomatis dari server DHCP. Selain alamat IP, banyak parameter jaringan yang dapat diberikan oleh DHCP, seperti *default gateway* dan DNS server

