BAB II

LANDASAN TEORI

2.1 Jaringan Komputer

Menurut Kristanto menyatakan bahwa Jaringan komputer ialah sebuah sekelompok komputer yang saling terhubung satu sama lain, dengan memakai satu protocol komunikasi sehingga semua komputer dapat terhubung dan bisa berbagi informasi, program, sumber daya dan juga bisa saling terhubung perangkat keras lainnya secara bersamaan, seperti printer, harddisk dan lain sebagainya. [8]

2.1.1 LAN

Local Area Network (**LAN**) adalah sekumpulan komputer pribadi atau perangkat periferal yang saling terhubung oleh saluran transmisi data digital berkecepatan tinggi dalam satu atau lebih gedung di dekatnya. Istilah "jaringan area lokal" (**LAN**) juga ditemui. Tujuan utama semua jenis jaringan komputer adalah untuk mengatur akses bersama ke sumber daya komputer mana pun yang terhubung ke jaringan ini. Pertama-tama, ini adalah berbagi data dan program. Ini terjadi ketika data atau program yang terletak di salah satu komputer di jaringan (server file) dapat digunakan di komputer mana pun yang terhubung dengannya. Hal ini terjadi, misalnya, saat menggunakan program akuntansi jaringan, saat karyawan yang memiliki akses ke jaringan dapat membuat perubahan ke database tunggal. Untuk mengatur koneksi permanen antar komputer di jaringan lokal, mereka digabungkan ke dalam kelompok kerja.

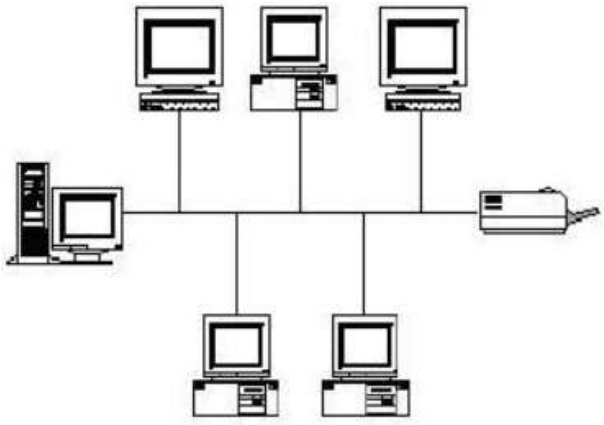
2.1.2 WAN

Jaringan area global (**WAN** – Wide Area Network) adalah jaringan yang menghubungkan komputer yang secara geografis jauh pada jarak yang jauh satu sama lain. Jaringan global menghubungkan jaringan lokal. **WAN** (Wide Area Netwrok) adalah jaringan global yang mencakup wilayah geografis yang luas, termasuk jaringan lokal dan jaringan telekomunikasi lain, perangkat. Saat ini, karena batas geografis jaringan meluas untuk menghubungkan pengguna dari berbagai kota dan negara bagian, **LAN** berubah menjadi jaringan area luas (**WAN**), dan jumlah komputer di jaringan sudah dapat bervariasi dari puluhan hingga beberapa ribu.

2.1.3 Topologi Jaringan

1. **Bus**

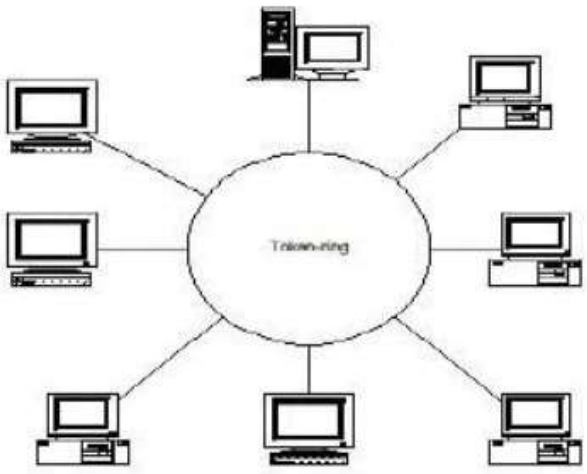
Semua komputer tampaknya dibangun dalam satu baris, yaitu. dari satu kabel ada keran ke masing-masing komputer di jaringan, dan ujung kabel terbuka. Paling sering, skema ini digunakan untuk menghubungkan beberapa komputer yang dipasang di ruangan yang sama, di mana kabel koaksial tipis atau tebal digunakan. Kelemahan dari topologi ini adalah Ketika ada putusnya kabel kehilangan komunikasi antara semua komputer.



Gambar 2Topologi Bus

2. **Ring**

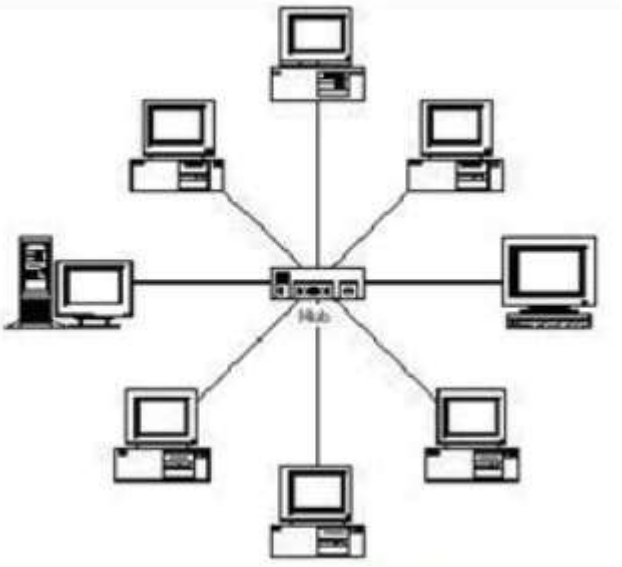
Semua komputer, seperti dalam kasus sebelumnya, dihubungkan menggunakan satu kabel, yang ujung-ujungnya saling berhubungan. Skema ini terutama digunakan untuk membuat jaringan Ring. Sekarang setiap putusnya kabel tidak lagi menyebabkan hilangnya komunikasi antar computer.



Gambar 3 Topologi Ring

3. **Star**

Setiap komputer di jaringan tersebut terhubung dengan kabel terpisah ke satu computer , yang berperan sebagai data server. Skema yang paling umum - jaringan area lokal dibuat atas dasar menggunakan hub. Putusnya kabel menyebabkan hilangnya kontak dengan hanya satu komputer atau segmen jaringan, tetapi untuk membuat jaringan sesuai dengan topologi ini, diperlukan distributor khusus (koneksi komputer sepenuhnya paralel satu sama lain).



Gambar 4 Topologi Star

2.1.4 Jaringan Internet

Internet adalah penyatuan semua jaringan kecil menjadi satu jaringan global melalui kabel khusus. Setelah beberapa waktu, orang mulai menghubungkan komputer terdekat dengan kabel khusus - yaitu, mereka membuat jaringan lokal . Itu belum tentu bisa disebut sebagai Internet, tetapi itu awal dari sebuah jaringan global. Informasi apa pun dapat ditransfer dalam koneksi lokal. Seiring waktu, semakin banyak komputer digabungkan hingga semua komputer dalam satu pulau, negara, atau benua menciptakan satu jaringan besar. Jaringan tersebut sudah bisa disebut dengan Internet, tetapi **World Wide Web** atau singkatan dari **WWW** sesuatu yang lebih global. Prinsip konstruksinya mirip dengan jaringan lokal, hanya saja komputer di benua berbeda yang dihubungkan dengan kabel tebal yang diletakkan di sepanjang dasar laut atau samudera. Jika kabel penghubung utama dihancurkan dengan cara apa pun, jaringan akan kembali berubah menjadi skala besar, tetapi terlokalisasi. Cara kerja Internet melalui kabel-kabel ini: semua file yang

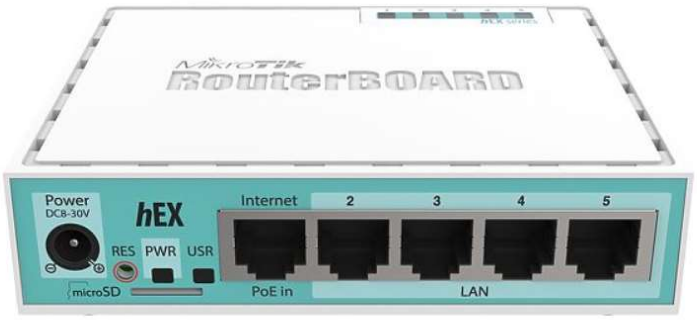
ditransmisikan dibagi menjadi beberapa paket dan dikirim ke penerima dengan kecepatan yang dimungkinkan oleh rencana tarif penyedia internet.

2.1.5 Komponen Jaringan

Berikut ini adalah komponen – komponen standar yang sering digunakan di dalam sebuah system jaringan computer.

1. **Router**

Perangkat yang digunakan untuk mengatur jaringan area lokal yang besar. Hal ini memungkinkan paket data untuk diarahkan secara ketat ke alamat IP tertentu (terdaftar sebelumnya), yang, misalnya, memungkinkan untuk menghindari intersepsi paket data dan mengecualikan "kebocoran" informasi. Komputer yang dikonfigurasi secara khusus dapat memainkan peran sebagai router.



Gambar 5 Router

2. **Switch**

Perangkat yang mengalihkan jalur komunikasi antara semua komputer, dan ini dilakukan secara real time, yang menghilangkan penurunan kinerja karena aliran data yang berlawanan. Ini juga memainkan peran repeater yang mencegah redaman sinyal.

Gambar 6 Switch

3. Bridge

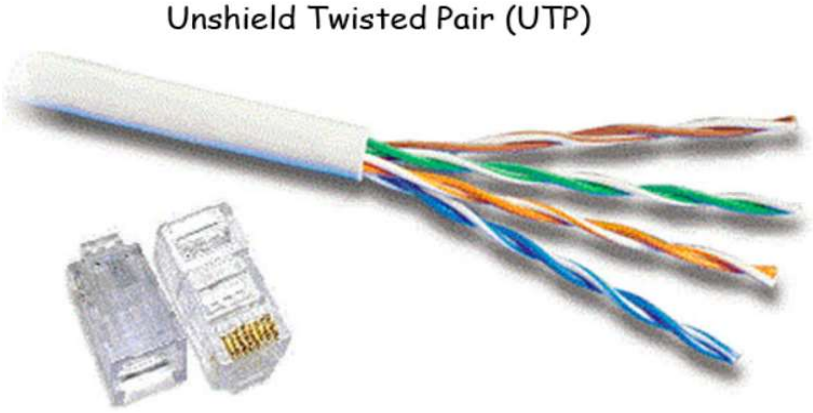
Bridge merupakan perangkat yang dapat menghubungkan jaringan komputer LAN (Local Area Connection) dengan jaringan lokal yang lain.

Gambar 7 Bridge

2.1.6 Media Transmisi

a. Twisted Pair

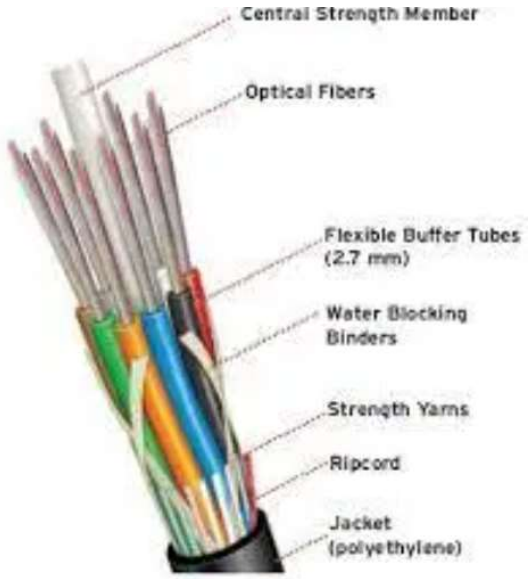
Kabel ini terdiri dari empat pasang konduktor yang terjalin dengan cara khusus (total delapan konduktor). Perbedaan terbesar antara LAN twisted-pair adalah kecepatan transfer datanya yang lebih tinggi (hingga 100 Mbps). Dalam kasus yang paling sederhana, "twisted pair" adalah kabel telepon dua kawat tanpa pelindung, namun kualitas koneksinya buruk.



Gambar 8 UTP

b. Serat Optik (Fiber Optic)

Digunakan untuk transmisi data jarak jauh dan dengan kecepatan tinggi (hingga 1 Gbit / s). Di rumah, kabel jenis ini tidak digunakan terutama karena harganya yang tinggi.



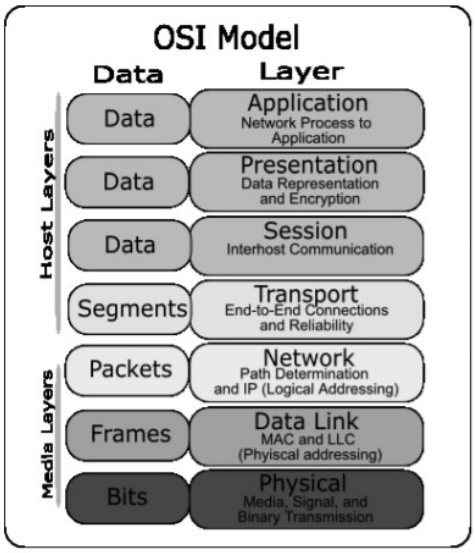
Gambar 9 Fiber Optic

c. Tanpa Kabel (Wireless)

Wi-fi merupakan singkatan dari *Wireless Fidelty* , Wi-fi suatu jaringan nirkabel yang menggunakan frekuensi radio untuk komunikasi antara perangkat , dan untuk komunikasi menggunakan *transiver* radio dua arah yang tipikalnya bekerja di *bandwith* 5 Ghz (802.11ac) atau 2.4 Ghz dan 5Ghz (802.11ax).

2.2.1 Lapisan Model Layer OSI

Model OSI terdiri dari 7 lapisan. Setiap tingkat disarikan dari yang lain dan tidak tahu apa-apa tentang keberadaan mereka. Model OSI dapat dibandingkan dengan mobil: mesin melakukan tugasnya dengan menghasilkan torsi dan mengirimkannya ke kotak roda gigi. Mesin sama sekali tidak memiliki perbedaan apa yang terjadi selanjutnya dengan torsi ini. Dia akan memutar roda, ulat atau baling-baling.



Gambar 10 Osi Layer

1. Application layer

Tingkat yang paling banyak dan beragam. Semua protokol tingkat tinggi dijalankan di atasnya. Seperti POP, SMTP, RDP, HTTP, dll. Protokol di sini tidak harus memikirkan tentang menjamin pengiriman informasi - ini dilakukan oleh tingkat yang lebih rendah.

2. Presentation layer

Lapisan ini bertanggung jawab untuk mengubah protokol dan encoding / decoding data. Permintaan Aplikasi, diperoleh dengan tingkat aplikasi, itu berubah menjadi format untuk transmisi di jaringan, dan diterima dari data jaringan diubah dalam format, aplikasi intuitif. Pada level ini, dapat dilakukan kompresi / dekompresi dan encoding / decoding data, serta meneruskan permintaan ke sumber daya jaringan lain, jika tidak dapat diproses secara local.

3. Session layer

Session layer bertanggung jawab untuk menjaga komunikasi sesi, memungkinkan aplikasi untuk berkomunikasi di antara mereka sendiri untuk waktu yang lama. Lapisan mengontrol pembuatan / penghentian sesi, pertukaran informasi, sinkronisasi tugas, menentukan hak untuk mentransfer data dan mempertahankan sesi selama periode tidak aktifnya aplikasi ... Sinkronisasi transmisi disediakan dengan menempatkan aliran data titik kontrol, memulai dari mana memulai kembali proses saat menangani interaksi.

4. TransPort layer

Dirancang untuk mengirimkan data tanpa kesalahan, kehilangan dan duplikasi dalam urutan tersebut, bagaimana data tersebut ditransfer. Jika ini tidak penting, data apa yang dikirim, bagaimana dan di mana, itu, dia memberikan mekanisme transmisi sendiri. Blok data yang ia bagi menjadi beberapa fragmen, yang ukurannya bergantung pada protokol, menggabungkan yang pendek menjadi satu, dan memecah yang panjang. Contoh protokol: UDP.

5. Network layer

Dirancang untuk menentukan jalur transmisi data. Bertanggung jawab untuk menerjemahkan alamat dan nama logis menjadi alamat fisik, menentukan rute terpendek, peralihan dan perutean, melacak masalah dan kemacetan di jaringan. Pada level ini, perangkat jaringan seperti itu, sebagai router.

6. Data-Link layer

Dirancang untuk menyediakan jaringan interaksi pada tingkat fisik dan pengendalian kesalahan, yang mungkin terjadi. Ini mengemas data yang diterima dari lapisan fisik ke dalam bingkai, memeriksa integritas, jika perlu, memperbaiki kesalahan (mengirim permintaan kedua untuk bingkai yang rusak) dan mengirim ke lapisan jaringan. Lapisan tautan dapat berinteraksi dengan satu atau lebih lapisan fisik, mengontrol dan mengelola interaksi ini. Spesifikasi IEEE 802 membagi lapisan ini menjadi 2 sub-lapisan - MAC (Media Acces Control) mengatur akses ke media fisik bersama, LLC (Logical Link the Control) menyediakan tingkat jaringan layanan.

7. Physical layer

Tingkat terendah dimaksudkan langsung untuk mengirim aliran data. Menerapkan transfer sinyal listrik atau optik dalam kabel atau dalam siaran radio dan, masing-masing, penerimaan dan konversinya menjadi bit data sesuai dengan metode pengkodean sinyal digital. Dengan kata lain, menyediakan antarmuka antara media jaringan dan perangkat jaringan.

2.2.2 Pengalamatan Jaringan TCP/IP

Setiap komputer di jaringan TCP / IP memiliki tiga tingkat alamat:

1. Alamat IP lokal dari sebuah node, ditentukan oleh teknologi dimana jaringan terpisah dibangun, dimana node tersebut berada. Untuk host di jaringan lokal, ini adalah alamat MAC dari adaptor jaringan, misalnya, 21-E3-B6-12-5C-08. MAC atau alamat ini diberikan oleh produsen pembuat peralatan dan merupakan kode alamat unik karena dikelola secara terpusat. Untuk semua teknologi jaringan lokal yang ada, alamat MAC memiliki format 6 byte atau 3 byte teratas adalah pengenal perusahaan pabrikan, dan 3 byte bawah ditetapkan dengan cara unik oleh pabrikan itu sendiri. Untuk host di jaringan area luas seperti X.25 atau relai bingkai, alamat lokal ditetapkan oleh administrator WAN.

2. Alamat IP 4 byte, misalnya 109.26.17.110. Alamat ini digunakan di tingkat jaringan. Nomor jaringan dapat dipilih secara sewenang-wenang oleh administrator, atau ditetapkan atas rekomendasi unit khusus Internet (Network Information Center, NIC), jika jaringan akan berfungsi sebagai bagian integral dari Internet. Biasanya, ISP memperoleh rentang alamat dari NIC dan kemudian mendistribusikannya ke pelanggan.

Tabel 1 **Tabel Metode TCP/IP**

Metode Pengalamatan Arsitektur TCP/IP	
Arsitektur TCP/IP	Metode Pengalamatan
Process/Application	Nama Host (Host Name)
Host-to-Host	Nomor Port (Port Number)
Internet	Alamat IP (IP Address)
Network Acces	Hardware Address (MAC Address)

Diantara keempat metode pengalamatan di atas, metode pengalamatan TCP/IP yang sering digunakan yaitu IP Address. Setiap device yang terhubung ke jaringan TCP/IP membutuhkan paling sedikit satu IP Address yang bersifat unik. Sebuah alamat IP Address terdiri dari dua bagian, yaitu;

a. Netword ID

Network ID merupakan identitas alamat dari sebuah jalur. Semua device yang terhubung pada jalur fisik yang sama harus memiliki Network ID yang sama.

b. Host ID

Host ID adalah identitas bagi host server, interface router terhubung ke jaringan TCP/IP. alamat IP terbagi dalam dua jenis.

1) IP Private

IP Address yang digunakan pada jaringan privat tidak digunakan pada jaringan publik. IP Address yang termasuk dalam kelas tersebut.

***Tabel 2* IP Private**

Class	IP Address	Subnet		
A	1-126	1-255	1-255	1-255
B	127-191	1-255	1-255	1-255
C	191-254	1-255	1-255	1-255

2) IP Public

IP Address yang biasa digunakan pada jalur publik dan penggunaanya harus melalui proses registrasi dahulu. Alamat IP terbagi ke dalam lima kelas, yaitu A, B, C, D, dan E.

***Tabel 3* IP Public**

Class	IP Address	Subnet		
A	1-126	1-255	1-255	1-255
B	127-191	1-255	1-255	1-255
C	192-223	1-255	1-255	1-255
D	224-239	1-255	1-255	1-255
E	240-255	1-255	1-255	1-255

2.2.3 Port Jaringan Di Komputer

Port fisik dapat dilihat dan dirasakan secara fisik. *Port* fisik memungkinkan untuk menghubungkan komponen perangkat keras internal atau perangkat eksternal ke prosesor utama komputer.

port logic berbeda dengan *port* fisik , *port* logic merupakan jenis *port* yang tidak dapat di sentuh atau tidak dapat dilihat secara fisik, fungsi *port* logic hampir sama system kerja di *port* fisik yaitu dapat menukarkan data atau informasi melalui protocol atau melalui media yang lain.

2.2.4 Port yang digunakan pada Jaringan Komputer

Port jaringan komputer adalah nomor yang mengidentifikasi tujuan aliran data jaringan dalam satu komputer. Semua host (komputer) berkomunikasi satu sama lain menggunakan alamat IP digital unik, yang diwakili oleh sistem biner.
Port memungkinkan untuk menentukan aplikasi jaringan yang berjalan di komputer, banyak di antaranya dapat berjalan secara bersamaan. Program jaringan utama dapat berupa:

1. WEB adalah server yang menyediakan penyiaran data dari situs web
2. FTP adalah server yang menyediakan transfer informasi.

Tujuan utama port adalah untuk menerima dan mengirimkan data jenis tertentu, serta untuk menghilangkan kesalahan ambiguitas saat mencoba membuat koneksi dengan host dengan alamat IP. Untuk menyediakan terjemahan data dari server web, harus menentukan alamat IP host dan nomor port yang menentukan program server web.

a. Port Fisik pada Jaringan Komputer

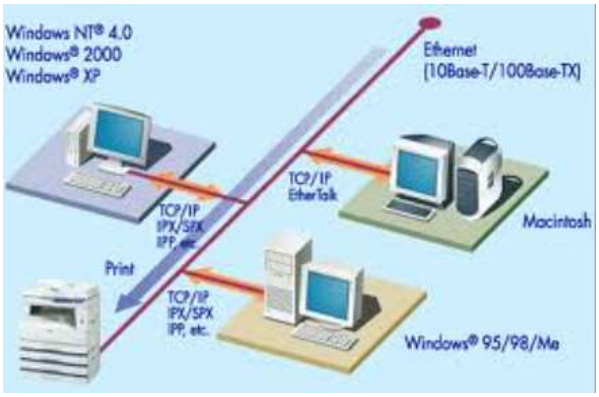
Setiap computer mempunyai port fisik, port yang digunakan pada jaringan computer adalah *port Ethernet* atau biasa disebut sebagai *LAN Card* . *Port* fisik ini bertugas menghubungkan kabel agar dapat terhubung dengan jaringan , ataupun terhubung dengan perangkat jaringan yang lain.

b. *Port* logic pada jaringan computer

Dalam computer ada banyak *Port* logic yang digunakan dalam sebuah jaringan , baik itu jaringan LAN , WAN , Internet , jaringan yang menggunakan protocol tertentu dan sebagainya. Sebuah *Port* Logic pada jaringan computer terdiri dari banyak sekali jenis dan fungsinya . *Port* yang paling sering digunakan di computer yaitu *port* 80 (HTTP)

2.2.5 Protokol Jaringan

Protokol jaringan adalah sekumpulan aturan yang memungkinkan komunikasi dan pertukaran data antara dua atau lebih komputer yang terhubung ke jaringan. Aturan tersebut termasuk pedoman yang mencakup beberapa kriteriakriteria sebuah jaringan, ini termaksud cara mengakses internet , kecepatan pengiriman data dan lain-lain. Protokol jaringan dicontohkan sebagai alat komunikasi antar computer dalam jaringn. [9]



Gambar 11 Protocol Jaringan

1. Protokol Jaringan Ethernet

Ethernet adalah teknologi yang menghubungkan jaringan area lokal berkabel (LAN) dan memungkinkan perangkat untuk berkomunikasi satu sama lain menggunakan protokol yang merupakan bahasa jaringan yang umum. Jaringan area lokal ini adalah jaringan komputer dan perangkat elektronik lainnya yang menjangkau area kecil di kantor, rumah, ruangan, atau Gedung. Jaringan *Ethernet* biasanya digunakan untuk topologi *start* , *linear bus* , atau *tree* . Jaringan *Ethernet* merupakan protocol yang paling banyak digunakan . *Ethernet* tidak menyediakan layanan jabat tangan (handshake service) dan tanpa koneksi untuk media bersama yang menggunakan CSMA / CD (Carrier Sense Multiple Access / Collision Detection) sebagai metode akses media. Media bersama memerlukan header Frame Ethernet untuk menggunakan alamat Link Layer untuk mengidentifikasi node sumber dan node tujuan. Seperti kebanyakan protokol LAN, alamat ini disebut sebagai alamat MAC host. Alamat MAC Ethernet adalah 48 bit dan biasanya direpresentasikan dalam format heksadesimal.

2. Protokol Jaringaan Ethernet

Untuk meningkatkan pengiriman paket data yang lebih cepat, protocol *Ethernet* mengembangkan pengiriman paket data yang mampu mentransmisikan data pada 1000 Mbps melalui twisted pair atau kabel serat optik. Di antara jenis kabel Ethernet lainnya.

3. Protokol Jaringan Token Ring

Token Ring adalah protokol transfer data dalam jaringan area lokal dengan topologi ring dan "akses token". Terletak di lapisan data link model OSI. Stasiun dalam jaringan area lokal Token Ring secara logis diatur ke dalam topologi ring, dengan data yang dikirim secara berurutan dari satu stasiun di ring ke yang lain. Token Ring menggunakan blok data tiga byte khusus yang disebut token yang juga bergerak di sekitar ring. Memiliki token memberi pemiliknya hak untuk mengirimkan data.

4. TCP/IP (Transmission Control Protocol/Internet Protocol)

Transmission Control Protocol (TCP) adalah standar komunikasi yang memungkinkan aplikasi dan perangkat komputasi untuk bertukar pesan melalui jaringan. Ini dirancang untuk mengirim paket melalui Internet dan memastikan pengiriman data dan pesan yang berhasil melalui jaringan.

TCP adalah salah satu standar utama yang mendefinisikan aturan Internet dan termasuk dalam standar yang ditentukan oleh *Internet Engineering Task Force* (IETF). Ini adalah salah satu protokol yang paling umum digunakan dalam komunikasi jaringan digital dan menyediakan pengiriman data ujung ke ujung.

Protokol Internet (IP) adalah metode mentransfer data dari satu perangkat ke perangkat lain melalui Internet. Setiap perangkat memiliki alamat IP unik yang menentukannya, yang memungkinkannya untuk berkomunikasi dengan perangkat lain yang terhubung ke Internet.

Alamat *IP* bertanggung jawab untuk menentukan bagaimana aplikasi dan perangkat bertukar paket data satu sama lain. Ini adalah protokol komunikasi utama yang bertanggung jawab atas format dan aturan untuk pertukaran data dan pesan antar komputer dalam satu atau lebih jaringan yang terhubung ke Internet. Ini dicapai melalui suite Internet Protocol (TCP / IP), sekelompok protokol komunikasi yang dibagi menjadi empat tingkat abstraksi.

IP adalah protokol utama pada lapisan Internet TCP / IP. Tujuan utamanya adalah untuk mengirimkan paket data antara aplikasi atau perangkat sumber dan tujuan

menggunakan metode dan struktur yang menempatkan tag, seperti informasi alamat, dalam paket data.

5. UDP (User Datagram Protokol)

User Datagram Protocol (UDP) adalah untuk mentransfer data antar proses aplikasi tanpa jaminan pengiriman, sehingga paketnya bisa hilang, digandakan, atau sampai dalam urutan yang salah saat dikirim.

6. Domain Name System (DNS)

Domain Name System (DNS) adalah *distribute database system* digunakan untuk pencarian nama computer (name resolution) di jaringan Internet yang mengunakan *TCP/IP*.

7. HTTP (Hypertext Transfer Protocol)

HTTP (HyperText Transfer Protocol) adalah protokol aplikasi untuk mentransfer data dalam jaringan. Saat ini digunakan untuk memperoleh informasi dari situs web. Protokol HTTP didasarkan pada penggunaan teknologi "klien-server": klien yang mengirim permintaan koneksi, server yang menerima permintaan mengeksekusinya dan mengirimkan hasilnya ke klien.

8. HTTPS

HTTPS (HyperText Transfer Protocol Secure) adalah ekstensi dari protokol HTTP yang mendukung enkripsi menggunakan protokol kriptografi SSL dan TLS.

9. SSL (Secure Socket Layer)

SSL (Secure Socket Layer) adalah *arguably Internet* paling banyak digunakan untuk enkripsi data. SSL digunakan tidak hanya keamanan keneksi *Web*. Tetapi untuk aplikasi yang memerlukan enkripsi jaringan.

2.2.6 Keamanan Jaringan Komputer

Aspek umum jaringan computer yang digunakan CIA Triad, Aspek tersebut yaitu confidentiality, integrity, dan availability. [5]

1. Confidentiality Kerahasiaan

Confidentialty atau Kerahasiaan dirancang untuk mencegah informasi rahasia menjangkau orang yang salah, sambil memastikan bahwa orang yang tepat benar-benar bisa mendapatkannya. akses harus dibatasi pada mereka yang berwenang untuk melihat data yang dipermasalahkan. Juga umum untuk mengklasifikasikan data menurut

jumlah dan jenis kerusakan yang dapat dilakukan jika jatuh ke tangan yang tidak disengaja.

2. Integrity

Aspek *Integrity* ini bahwa data atau informasi tidak boleh diubah tanpa seizin yang mempunyai data atau informasi. Data atau informasi yang diterima harus sesuai seperti data atau informasi yang dikirimkan. Jika terdapat perubahan antara data atau informasi yang dikirimkan yang diterima maka aspek dari *integrity* tidak terpenuhi . Adanya *Spoofing* atau pemakai lain yang mengubah data atau informasi tanpa izin merupakan salah satu contoh masalah harus dihadapi.

3. Availability

Aspek *availability* ini berbuhungan dengan ketersediaan informasi dan data. Informasi dan data yang berada dalam suatu system jaringan computer tersedia dan dapat dimanfaatkan oleh user yang berhak . Aspek *availability* ini berhubungan dengan ketersediaan data atau informasi ketika dibutuhkan

2.2.6.1 Aspek ancaman keamanan

Aspek ancaman keamanan jaringan computer dalam dunia *Cyber* yang sangat keras saat ini, ancaman keamanan jaringan computer sudah sangat memilikin resiko yang tinggi. [5]

1. Interruption

Interruption berupa ancaman terhadap *availability*. Informasi dan data yang ada dalam system jaringan computer dihapus dan dirusak, sehingga jika dibutuhkan, data atau informasi sudah hilang.

2. Interception

Interception berupa ancaman terhadap kerahasiaan. Data atau informasi yang ada disadap atau orang yang tidak berhak untuk mendapatkan akses ke computer dimana informasi atau data tersebut disimpan, Pada aspek ini, data atau informasi diambil sebelum atau sesudah data ditransimiskan ke tujuan.

3. Modifikasi

Aspek modifikasi adalah ancaman terhadap integritas. Seseorang yang tidak berhak berhasil menyadap lalu lintas jaringan data atau informasi yang sedang dikirim dan diubah sesuai keinginan dari penyadap tersebut. Aspek ini data atau informasi tidak langsung terkirim ke tujuan, namun terkirim ke penyadap atau pelaku dan mempunyai otoritas full apakah data atau informasi ingin diubah atau dihapus , bahkan pelaku bisa saja tidak mengirim data atau informasi tersebut ke tujuan.

4. Fabrication

Fabriaction merupakan ancaman terdahap *integrity*. Penyadap yang tidak berhak berhasil meniru dengan memalsukan suatau data atau informasi yang ada sehingga orang penerima data atau informasi tersebut, menyangka data atau informasi tersebut berasal dari orang yang dihendaki data atau informasi tersebut,

2.2.6.2 Ancaman serangan Sistem Komputer

Bentuk ancanman serangan pada suatu jaringan computer sendiri pada dasarnya memiliki tiga bentuk utama yaitu [6].

1. Pertama adalah ancaman serangan fisik. Ancaman serangan ini ditujukan pada fasilitas jaringan,computer dan perangkat elektronik

2. Kedua adalah ancaman serangan sintaktik. Ancaman serangan ini ditujukan terhadap celah keamannan(*vulnerability*) pada *software*, celah yang terdapat pada algoritma kriptografi.

3. Ancaman serangan semantic, serangan jenis ini memanfaatkan dari isi pesan yang dikirim.

2.2.6.3 Ancaman serangan Sistem Jaringan Komputer

Sniffer yang dapat memonitor proses yang sedang berlangsung sebagai berikut [6].

1. *Remote Attack* bentuk ancaman serangan terhadap suatu computer dimana penyerang memiliki kendali terdahap computer tersebut karena dilakukan dari jarak jauh diluar system jaringan atau media transmisi
2. *Spoofing* penggunaan computer untuk dapat meniru atau dengan cara menimpa identitas *IP Address*

2.2.6.4 Ancaman serangan Port Sistem Jaringan Komputer

Berikut ini adalah beberapa port yang digunakan untuk menyerang di system jaringam computer [7].

1. *DDOS* (*Distributed Denial of Services*) adalah sebuah ancaman serangan yang bertujuan untuk menghabiskan sumber daya sebuah *device* jaringan computer sehingga jaringan computer menjadi terganggu
2. *IP Spoofing* dan *DNS Forgery* sebuah ancaman serangan yang bertujuan untuk menipu seseorang. Dengan cara mengubah sebuah paket data, sehingga dapat menipu *host* penerima paket data.

3. *Packet Sniffing* sebua ancaman dengan cara melihat seluruh paket data yang lewat pada sebuah media komunikasi, baik itu dari media kabel maupun radio. Setelah paket data didapat, kemudian disusun ulang sehingga paket data yang dikirimkan oleh sebuah pihak dapat dicuri oleh pihak yang tidak berwenang

2.2.6.5 Sistem Keamanan Jaringan Komputer

Berikut ini adalah sistem keamanan yang digunakan untuk dalam hal keamanan jaringan computer [4]

1. *DNS-over-HTTPS* adalah untuk mengenkripsi permintaan DNS. Domain Name System (DNS) memainkan peran yang sangat penting ketika mencari situs yang diinginkan di Internet. Di baris input di browser, saat menentukan nama domain, permintaan DNS yang dihasilkan dari browser dikirim ke server dengan alamat IP yang ditentukan dalam catatan A / ABCD untuk domain ini. Permintaan dan tanggapan DNS dibuat dan disediakan dalam teks yang jelas tanpa enkripsi. Ini adalah masalah utama, karena penipu dapat mencegat dan menggunakan informasi untuk tujuan egois mereka sendiri. Oleh karena itu, banyak waktu dan upaya yang dikerahkan untuk memecahkan masalah keamanan data ini.
2. *Arp for Lease* adalah fitur yang di punya oleh Mikrotik, fungsi *Arp Lease* sebagai keamanan agar client dapat koneksi hanya dari alokasi *IP* secara *DHCP* , jika client mengubah *IP* secara *static* maka client tidak bisa terhubung dengan router.
3. *Port Scanning* adalah sebuah aplikasi memeriksa *Port* yang terbuka yang adanya aplikasi jaringan computer yang terima koneksi. *Port Scanning* ini dapat menjadi pintu penyerangan ke dalam sistem jaringan.

2.2.7 Sistem Operasi

1.Windows

Microsoft Windows adalah sebuah system operasi yang dikembangkan oleh *Microsoft* dengan menggunakan antarmuka pengguna grafis, ini memiliki beberapa versi , yang paling popular XP, 7, 8, 10. Saat menyalakan computer ,dapat melihat gambar dan segala macam ikon, tombol, dan sebagainya. Semua yang dapat lihat dan gunakan ini hanya mungkin berkat sistem operasinya. Jika tidak ada, maka ketika dihidupkan hanya akan ada layar hitam dengan huruf dan angka bahasa Inggris.

2. Linux

Linux adalah sistem operasi dengan kernel gratis . Ini terdiri dari kernel sistem dan satu set program kecil yang berinteraksi dengan kernel ini. Pengembangan inti dimulai pada tahun 1991 oleh Linus Torvalds, seorang mahasiswa dari Finlandia. Versi pertama 0,01 disajikan olehnya pada 17 September 1991. Merek dagang Linux telah didaftarkan

oleh pengembang, tetapi nama itu sendiri dipilih melalui pemungutan suara pengguna. *Linux* awalnya bagian dari *UNIX* untuk arsitektur *IBM.*

2.2.8 Aplikasi

Berikut ini adalah aplikasi – aplikasi yang digunakan dalam analisis dan implementasi keamanan jaringan menggunakan *DNS over HTTPS (DoH)*

1. Ettercap

Ettercap adalah aplikasi untuk menganalisis lalu lintas jaringan yang melewati antarmuka komputer, tetapi dengan fungsionalitas tambahan. Program ini memungkinkan melakukan serangan *man-in-the-middle* untuk memaksa komputer lain mengirim paket bukan ke router, tetapi kepada penyerang.

2. ARP Guard

Software aplikasi ini dirancang untuk mencengah kecurian data pribadi di Wi-Fi terbuka. Program ini memiliki dua mode perlindungan. Bekerja dalam mode pertama, aplikasi akan memperingatkan tentang bahaya jika serangan terdeteksi. Dalam mode kedua, program membuat perangkat yang dilindungi kebal terhadap serangan ARP Spoofing. Tidak ada peringatan, tidak ada shutdown Wi-Fi, atau tindakan pencegahan lainnya yang diperlukan. Seorang penyerang tidak bisa merutekan lalu lintas melalui dirinya sendiri. Dalam hal ini, perangkat akan mendapatkan kekebalan, termasuk terhadap metode Man-In-The-Middle