Pembelajaran 3. Teknik Komputer dan Jaringan

A. Kompetensi

Penjabaran model kompetensi yang selanjutnya dikembangkan pada kompetensi guru bidang studi yang lebih spesifik pada pembelajaran 3. Teknologi Komputer dan Jaringan, ada beberapa kompetensi guru bidang studi yang akan dicapai pada pembelajaran ini, kompetensi yang akan dicapai pada pembelajaran ini adalah guru P3K mampu menggunakan teknologi informasi dan komunikasi dalam disiplin atau materi pembelajaran lain dan sebagai media komunikasi.

B. Indikator Pencapaian Kompetensi

Dalam rangka mencapai komptensi guru bidang studi, maka dikembangkanlah indikator - indikator yang sesuai dengan tuntutan kompetensi guru bidang studi. Indikator pencapaian komptensi yang akan dicapai dalam pembelajaran 3. Teknologi Komputer dan Jaringan adalah sebagai berikut.

1. Menggambarkan sistem jaringan dasar
2. Menggambarkan Teknologi Jaringan Berbasis Luas (WAN)
3. Menggambarkan Media Jaringan (Nirkabel dan Fiber Optik)
4. Melaksanakan manajemen bandwidth dalam sebuah jaringan komputer
5. Menerapkan konsep sistem keamanan jaringan

C. Uraian Materi

1. Sistem Jaringan Dasar

a. Pengertian Jaringan

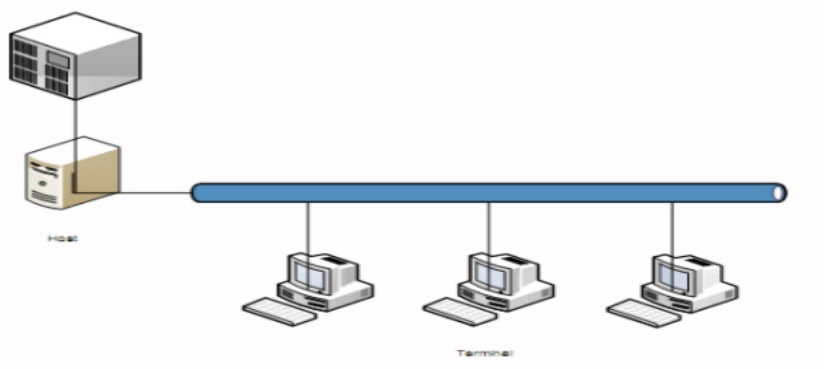
Istilah jaringan komputer sudah tidak asing lagi kita dengar, jaringan komputer adalah sebuah sistem jaringan telekomunikasi yang terdiri dari dua perangkat atau lebih saling terhubung satu sama lain melalui media transmisi. Adanya jaringan komputer memungkinkan perangkat untuk saling bertukar data atau informasi, media penyimpanan dan berbagi resource seperti data berupa file teks,

audio atau video. Implementasi sistem jaringan yang sering kita temui adalah mencetak data pada printer yang sama dan menggunakan hardware/software yang terhubung dalam satu jaringan yang sama.

b. Sejarah Jaringan Komputer

Jaringan komputer lahir pada tahun 1940-an di Amerika dari sebuah proyek pengembangan komputer MODEL I di laboratorium Bell dan group riset Harvard University yang dipimpin profesor H. Aiken. Pada mulanya proyek tersebut hanyalah ingin memanfaatkan sebuah perangkat komputer yang harus dipakai bersama. Untuk mengerjakan beberapa proses tanpa banyak membuang waktu kosong dibuatlah proses beruntun (Batch Processing), sehingga beberapa program bisa dijalankan dalam sebuah komputer dengan dengan kaidah antrian.

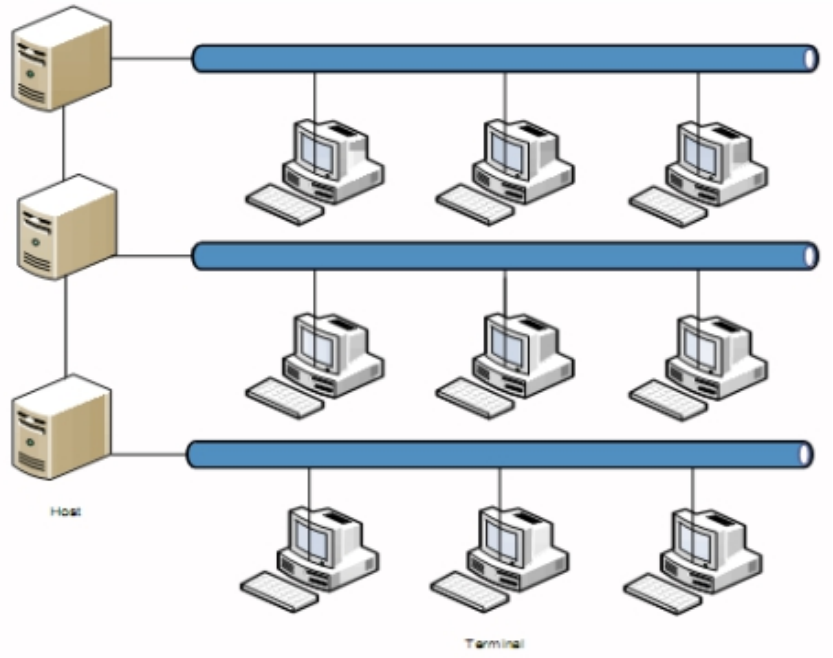
Ditahun 1950-an ketika jenis komputer mulai membesar sampai terciptanya super komputer, maka sebuah komputer mesti melayani beberapa terminal. Untuk itu ditemukan konsep distribusi proses berdasarkan waktu yang dikenal dengan nama TSS (Time Sharing System), maka untuk pertama kali bentuk jaringan (network) komputer diaplikasikan. Pada sistem TSS beberapa terminal terhubung secara seri ke sebuah host komputer. Dalam proses TSS mulai nampak perpaduan teknologi komputer dan teknologi telekomunikasi yang pada awalnya berkembang sendiri-sendiri.



Gambar 32. Time Sharing System

Memasuki tahun 1970-an, setelah beban pekerjaan bertambah banyak dan harga perangkat komputer besar mulai terasa sangat mahal, maka mulailah digunakan konsep proses distribusi (Distributed Processing). Dalam proses ini

beberapa host komputer mengerjakan sebuah pekerjaan besar secara paralel untuk melayani beberapa terminal yang tersambung secara seri disetiap host komputer. Dalam proses distribusi sudah mutlak diperlukan perpaduan yang mendalam antara teknologi komputer dan telekomunikasi, karena selain proses yang harus didistribusikan, semua host komputer wajib melayani terminal-terminalnya dalam satu perintah dari komputer pusat.



Gambar 33. Distributed Processing

c. Manfaat Jaringan Komputer

Adapun beberapa manfaat jaringan komputer adalah sebagai berikut:

1) Resource sharing
   a) Data sharing yaitu dengan adanya jaringan komputer kita bisa dengan mudah berbagi data seperti dokumen, gambar, video, dan lain-lain dengan kolega yang ada di lokasi yang jauh bahkan di negara yang berbeda.
   b) Hardware Sharing, jika dulunya satu komputer satu printer, dengan jaringan komputer, satu printer bisa digunakan oleh beberapa komputer sekaligus. Tidak hanya printer, kita bisa sharing storage dan banyak hardware lainnya.

c) Internet Access Sharing, jaringan komputer kecil memungkinkan beberapa komputer berbagi satu koneksi internet.

2) Connectivity dan Communication

Individu dalam sebuah gedung atau workgroup dapat dikoneksikan dalam jaringan LAN. Beberapa LAN dengan lokasi yang berjauhan terkoneksi kedalam jaringan WAN.

3) Data Security and Management

Data penting akan lebih aman dan lebih mudah ketika data tersebut disimpan secara terpusat dengan menggunakan Shared Server.

4) Performance Enhancement dan Balancing

Dalam kondisi tertentu sebuah jaringan dapat digunakan untuk meningkatkan kinerja dari beberapa aplikasi dengan cara mendistribusikan tugas komputasi pada beberapa komputer pada jaringan.

5) Entertainment

Jaringan komputer terutama internet, biasanya menyediakan banyak jenis hiburan dan permainan. Seperti multi-player game yang bisa dimainkan oleh beberapa user dalam waktu yang bersamaan, atau sekedar menonton video.

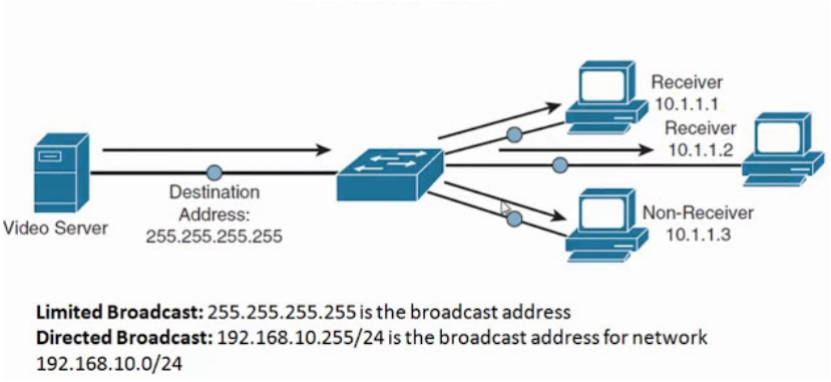
d. Jenis-jenis Jaringan Komputer

1) Berdasarkan jenis transmisi

Jaringan komputer dibagi berdasarkan transmisi dan jarak, terdapat dua jenis jaringan berdasarkan teknologi transmisi, yaitu jaringan broadcast dan jaringan point-to-point.

a) Jaringan broadcast memiliki saluran komunikasi tunggal yang dipakai bersama-sama oleh semua device yang terkoneksi ke jaringan. Pesan-pesan berukuran kecil, disebut paket, yang dikirimkan oleh suatu mesin akan diterima oleh mesin-mesin lainnya. Field alamat pada sebuah paket berisi keterangan tentang kepada siapa paket tersebut ditujukan. Saat menerima paket, mesin akan mencek field alamat. Bila paket tersebut ditujukan untuk dirinya, maka mesin akan memproses paket itu, bila paket

ditujukan untuk mesin lainnya, mesin terserbut akan mengabaikannya.



Gambar 34. jaringan broadcast

b) Jaringan Point-to-Point (unicast) terdiri dari beberapa koneksi pasangan individu, dari satu device ke satu device lain. Untuk mengirim paket dari sumber ke suatu tujuan, sebuah paket pada jaringan jenis ini mungkin harus melalui satu atau lebih mesin-mesin perantara. Seringkali harus melalui banyak route yang mungkin berbeda jaraknya. Karena itu algoritma route memegang peranan penting pada jaringan point-to-point.

Gambar 35. Jaringan point to point

2) Berdasarkan geografis

a) PAN

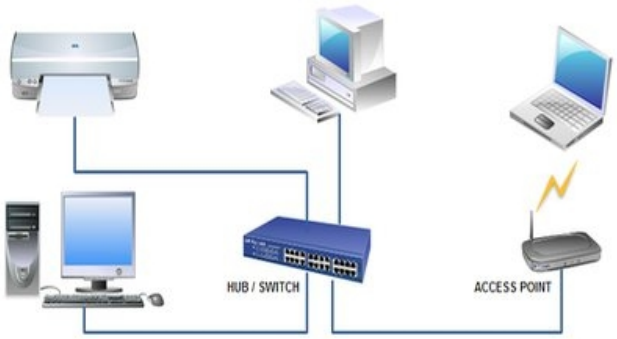
Untuk menghubungkan komputer atau perangkat lain seperti handphone, PDA, keyboard, tetikus, headset wireless, camera dan

peralatan lain yang jaraknya cukup dekat (4-6 meter), maka kita telah membentuk suatu Personal Area Network (PAN).

Gambar 36. PAN

b) LAN (*Local Area Network*)

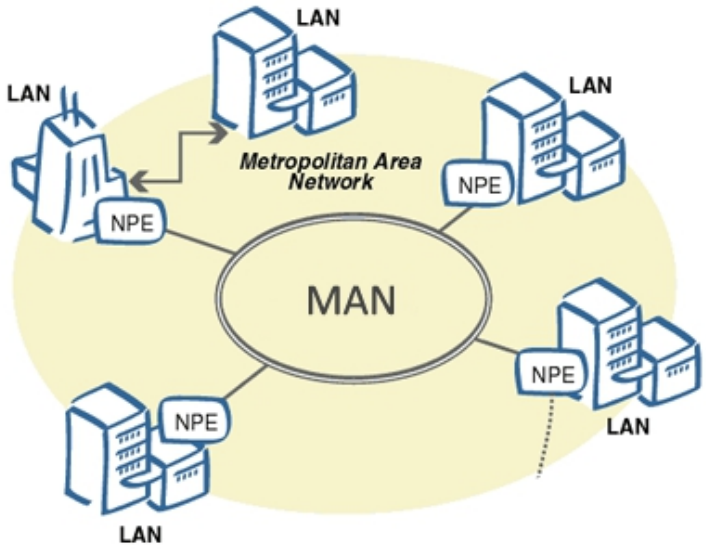
Local Area Network atau LAN, merupakan suatu jenis jaringan komputer dengan mencakup wilayah lokal. Dengan menggunakan berbagai perangkat jaringan yang cukup sederhana dan populer, seperti menggunakan kabel UTP (Unshielded Twisted-Pair), Hub, Switch, Router, dan lain sebagainya.



Gambar 37. LAN

c) MAN (*Metropolitan Area Network)*

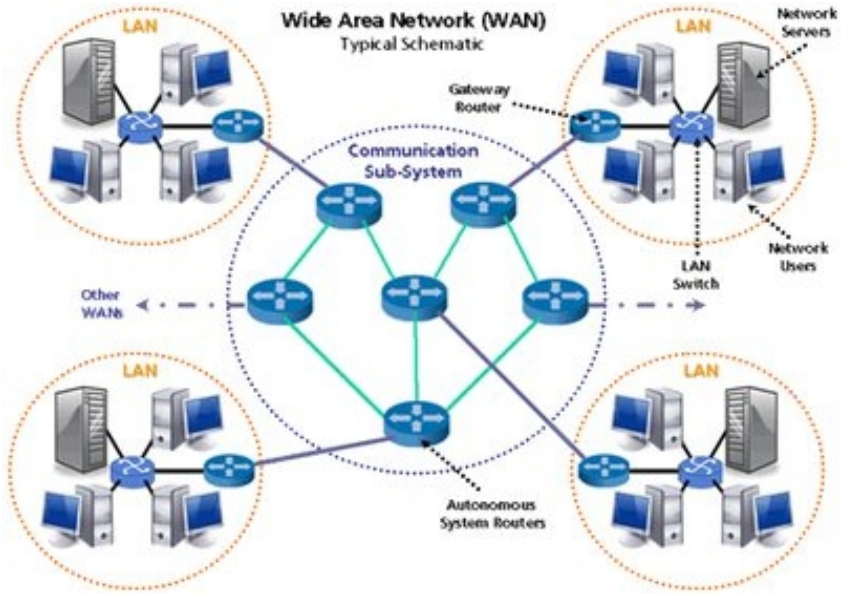
Metropolitan Area Network (MAN), merupakan jenis jaringan komputer yang lebih luas dan lebih canggih dari jenis jaringan komputer LAN. Jenis jaringan komputer MAN ini biasa digunakan untuk menghubungkan jaringan komputer dari suatu kota ke kota lainnya. Untuk dapat membuat suatu jaringan MAN, biasanya diperlukan adanya operator telekomunikasi untuk menghubungkan antar jaringan komputer.



Gambar 38. MAN

d) WAN (*Wide Area Network*)

Teknologi jaringanWAN biasa digunakan untuk menghubungkan suatu jaringan dengan negara lain atau dari satu benua ke benua yang lainnya. Jaringan WAN bisa terdiri dari berbagai jenis jaringan komputer LAN dan WAN karena luasnya wilayah cakupan dari jenis jaringan komputer WAN. Jaringan WAN, biasanya menggunakan kabel fiber optik serta menanamkannya di dalam tanah maupun melewati jalur bawah laut.



Gambar 39. WAN

e) Internet

Internet merupakan jaringan komputer yang global atau mendunia, karena internet merupakan jaringan-jaringan komputer yang terhubung secara mendunia, sehingga komunikasi dan transfer data atau file menjadi lebih mudah. Internet bisa dikatakan perpaduan antara berbagai jenis jaringan komputer beserta topologi dan tipe jaringan yang saling berhubungan satu sama lain.

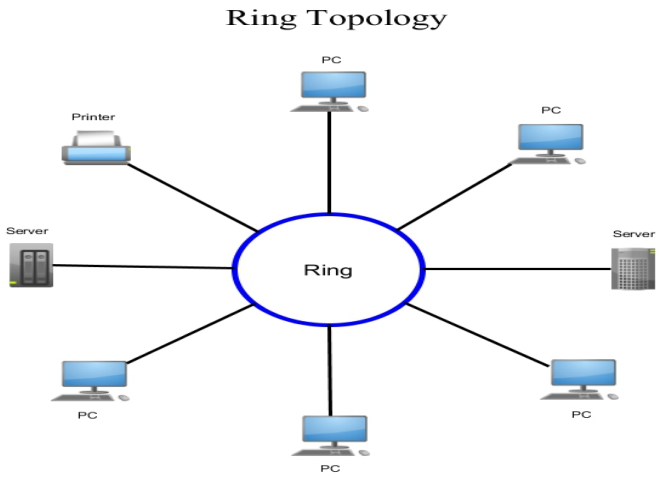
e. Topologi Jaringan

Topologi jaringan adalah hal yang menjelaskan hubungan geometris antara unsur-unsur dasar penyusun jaringan, yaitu node, link, dan station. Adapun topologi terbagi manjadi beberapa bagian, antara lain:

1) Topologi ring

Proses pengiriman informasi atau data dari node satu ke node yang lainnya tidak jarang melewati sebuah node diantara keduanya, maka dari itu proses pengiriman informasi dalam topologi ini dibantu oleh token. Token disini berfungsi untuk memeriksa apakah node yang dilewati memerlukan informasi yang dibawa oleh token. Sebelum adanya jaringan FDDI, proses pengiriman data pada topologi ring terbatas pada satu arah.

Token berisi informasi bersamaan dengan data yang berasal dari komputer sumber, token kemudian melewati titik/node dan akan memeriksa apakah informasi data tersebut digunakan oleh titik/node yang bersangkutan, jika ya maka token akan memberikan data yang diminta oleh node untuk kemudian kembali berjalan ke titik/node berikutnya dalam jaringan. Jika tidak maka token melewati titik/node sambil membawa data menuju ke titik/node berikutnya. proses ini akan terus berlangsung hingga sinyal data mencapai tujuannya.



Gambar 40. Topologi ring

Kelebihan topologi Ring:

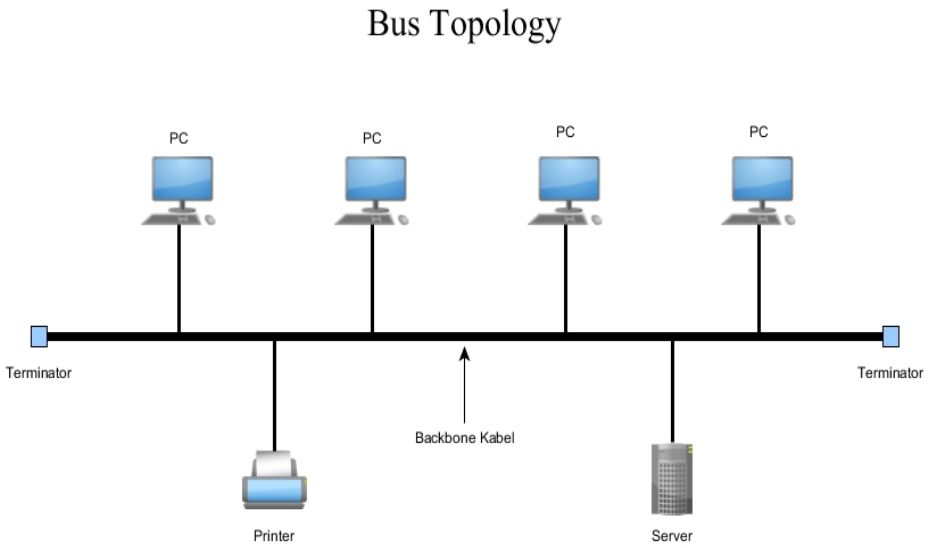
1) Cenderung mudah dirancang karena tidak banyak peralatan tambahan.
2) Akses data lebih baik daripada topologi bus, termasuk untuk data yang besar.
3) Mudah dalam proses konfigurasi.
4) Karena proses pengiriman data yang melalui satu jalur maka collision bisa lebih dihindari.
5) Konfigurasi Point to Point pada Topologi ring menyebabkan proses
6) Pendeteksian kesalahan lebih mudah dilakukan.
7) Hemat Kabel.

Kekurangan Topologi Ring:

1) Jika ada salah satu node yang mengalami gangguan maka seluruh jaringan akan ikut terganggu, namun ini dapat diatasi dengan menggunakan dua jalur cincin. Artinya diperlukan sebuah perangkat yang bertugas sebagai pusat jaringan.
2) Proses pengembangan lebih sulit dikarenakan proses penambahan, pengurangan, maupun pemindahan perangkat akan mempengaruhi jaringan secara keeluruhan.
3) Diperlukan penanganan dan pengelolaan khusus

2) Topologi bus

Topologi jaringan komputer bus tersusun rapi seperti antrian dan menggunakan satu kabel coaxial dan setiap komputer terhubung ke kabel menggunakan konektor BNC, dan kedua ujung dari kabel coaxial harus diakhiri oleh terminator.



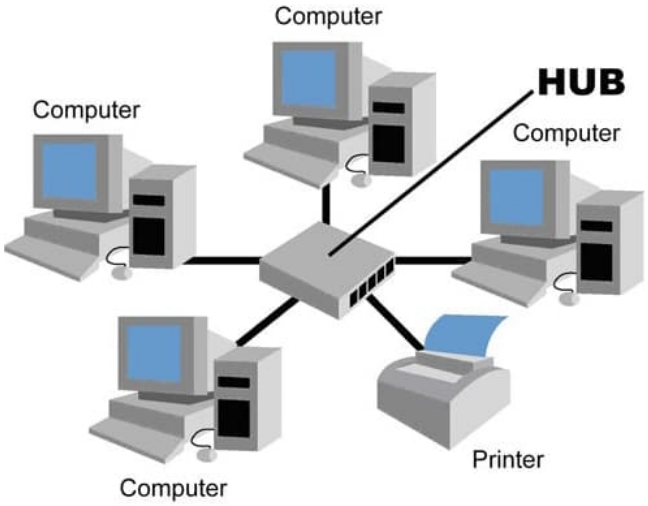
Gambar 41. Topologi BUS

Kelebihan dan kekurangan Topologi bus:

- Kelebihan dari bus hampir sama dengan ring, yaitu kabel yang digunakan tidak banyak dan menghemat biaya pemasangan.
- Kekurangan topologi bus adalah jika terjadi gangguan atau masalah pada satu komputer bisa menggangu jaringan di komputer lain, dan untuk topologi ini sangat sulit mendeteksi gangguan, sering terjadinya antrian data, dan jika jaraknya terlalu jauh harus menggunakan repeater.

3) Topologi Star

Topologi ini membentuk seperti bintang karena semua komputer di hubungkan ke sebuah hub atau switch dengan kabel UTP, sehingga hub/switch pusat dari jaringan dan bertugas untuk mengontrol lalu lintas data, jadi jika komputer 1 ingin mengirim data ke komputer 4, data dikirim ke switch dan langsung di kirimkan ke komputer tujuan tanpa melewati komputer lain. Topologi jaringan komputer inilah yang paling banyak digunakan karena kelebihannya lebih banyak.



Gambar 42. Topologi star

Kelebihan Topologi Star, yaitu:

1) Mudah mendeteksi komputer mana yang mengalami gangguan
2) Mudah untuk melakukan penambahan atau pengurangan komputer tanpa mengganggu yang lain
3) Tingkat keamanan sebuah data lebih tinggi.

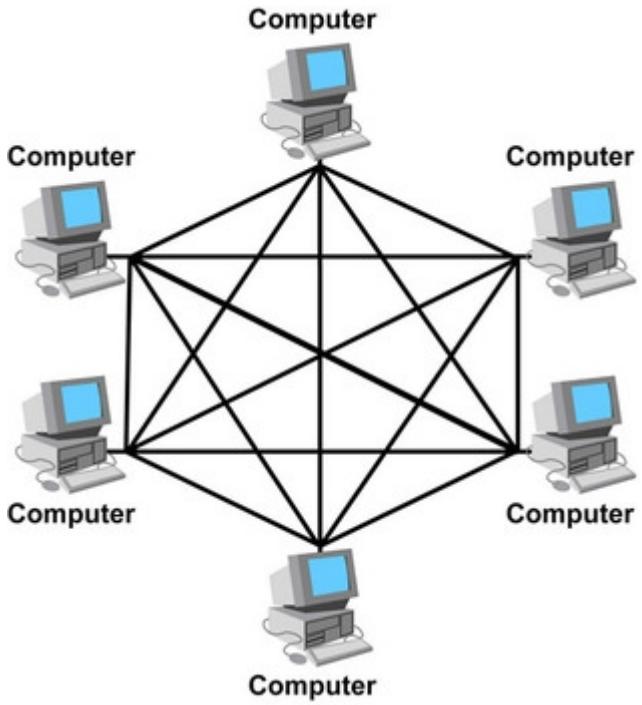
Kekurangan Topologi Star, yaitu:

1) Memerlukan biaya yang tinggi untuk pemasangan, karena membutuhkan kabel yang banyak serta switch/hub.

2) Kestabilan jaringan sangat tergantung pada terminal pusat, sehingga jika switch/hub mengalami gangguan, maka seluruh jaringan akan terganggu.

4) Topologi Mesh

Topologi bentuk ini setiap komputer akan terhubung dengan komputer lain dalam jaringannya menggunakan kabel tunggal, jadi proses pengirimandata akan langsung mencapai komputer tujuan tanpa melalui komputer lain ataupun switch atau hub. Pengertian lain dari Topologi mesh adalah sebuah bentuk topologi jaringan dimana setiap node terhubung langsung dengan node lain pada jaringan. Hingga membentuk rangkaian menyerupai jala / jaring. Karena setiap node terhubung secara langsung dengan node yang lain maka ketika akan berkomunikasi setiap node tidak memerlukan perantara atau biasa disebut dedicated links.



Gambar 43. Topologi mesh

Kelebihan Topologi Mesh, yaitu:

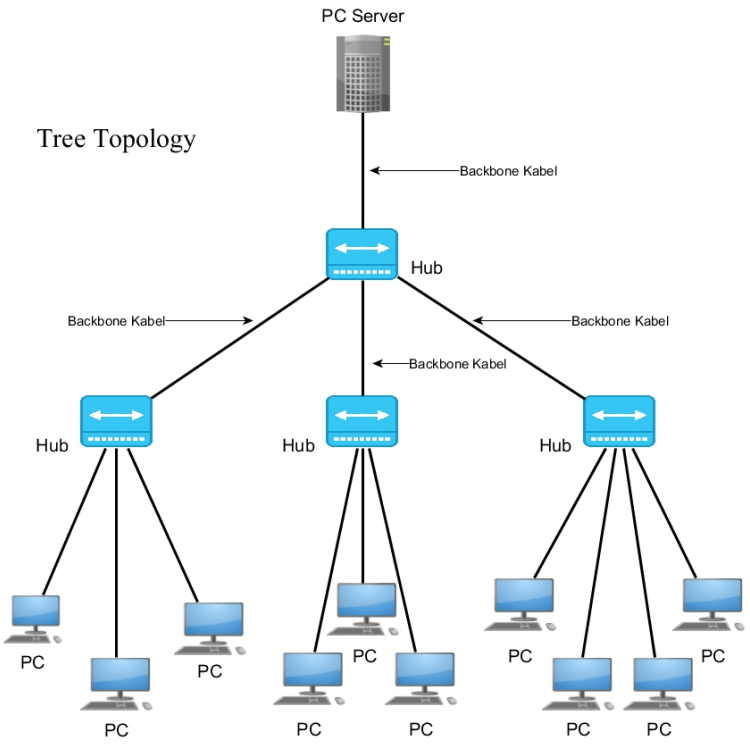
1) Proses pengiriman lebih cepat dan tanpa melalui komputer lain,
2) Jika salah satu komputer mengalami kerusakan tidak akan menggangu komputer lain.

Kekurangan Topologi Mesh, yaitu:

Kekurangan dari topologi ini sudah jelas, akan memakan sangat banyak biaya karena membutuhkan jumlah kabel yang sangat banyak dan setiap komputer harus memiliki Port I/ O.

5) Topologi *Tree*

Topologi jaringan komputer tree merupakan gabungan dari beberapa topologi star yang dihubungan dengan topologi bus, jadi setiap topologi star akan terhubung ke topologi star lainnya menggunakan topologi bus.



Gambar 44. Topologi tree

Karakteristik Topologi Tree, yaitu:

1) Komunikasi antara kelompok dilakukan melalui sebuah HUB.
2) Adanya HUB Pusat, sebagai pusat data maupun kendali jaringan.
3) Adanya pengelompokan tingkat dalam kelompok jaringan yang berbentuk topologi star
4) Adanya Kabel Utama / Backbone sebagai penghubung Jaringan.

Kelebihan Topologi Tree, yaitu:

1) Kelompok jaringan yang berada dibawah HUB Pusat dapat melakukan pengembangan atau penambahan client dengan mudah, Scalable.
2) Komunikasi terjadi secara point to point.
3) Mengatasi keterbatasan dari topologi jaringan star yang memiliki keterbatasan pada titik koneksi HUB dan keterbatasan lalu lintas yang diinduksi pada Topologi Bus.
4) Karena di lakukan pengelompokkan maka pendeteksian masalah jadi lebih mudah.
5) Jika salah satu client mati maka yang lain tidak akan terpengaruh (sifat topologi star).

Kekurangan Topologi tree, yaitu:

1) Kinerja jaringan secara keseluruhan bergantung pada HUB Pusat, apabila HUB rusak maka jaringan akan terganggu. (sifat topologi star).
2) Komunikasi yang tidak bisa dilakukan secara langsung antar komputer, melainkan harus melalui HUB terlebih dahulu.
3) Karena melalui sebuah kabel utama maka lalu lintas data sangat padat.
4) Meskipun dari segi pendeteksian masalah

f. Komunikasi dalam Jaringan (Daring)

Pengguna sarana telekomunikasi saat ini menjadi sangat dominan dalam kehidupan sehari-hari maupun dalam dunia bisnis. Perusahaan tanpa memiliki fasilitas telekomunikasi akan mengalami kesulitan dalam mengirimkan data dari satu lokasi ke lokasi lain. Kesulitan dalam mengirimkan data ini akan mengakibatkan kesulitan dalam mengolah data menjadi informasi sehingga pada akhirnya akan menyulitkan pula bagi manajemen suatu perusahaan dalam mengambil keputusan. Jaringan telekomunikasi saat ini menghubungkan beberapa daratan dan lautan untuk memindahkan data dalam jumlah besar. Esensi dari telekomunikasi adalah pengurangan waktu dan ruang. Dengan satelit komunikasi dua lokasi yang sangat jauh berbeda dapat dihubungkan dalam sekejap. Suatu perusahaan yang ingin mengirimkan data ke cabangnya yang berjarak 1000 mil atau lebih perlakuannya tidak jauh berbeda dengan mengirimkan data sejauh 100 mil.

1) Layer pada Jaringan

Layer OSI

Selanjutnya pada jaringan komputer terdapat tujuh lapisan OSI (*Open System Interconnection*), yaitu sebagai berikut.

a) *Physical layer* (lapisan fisik): Memindahkan, mengirimkan dan menerima bit antar devices, berkomunikasi langsung dengan jenis media transmisi, menentukan kebutuhan listrik, mekanis, prosedural dan fungsional, mempertahankan dan menonaktifkan hubungan fisik antarsistem. Contoh Protocol/Layanan : EIA/TIA-232, V.35
b) *Data-link layer* (lapisan keterkaitan data): Grouping data secara logikal (Framing), menggabungkan paket menjadi byte dan byte menjadi frame, menyediakan akses ke media menggunakan alamat MAC. Contoh Protocol/Layanan : IEEE 802.3/ 802.2/ HDLC
c) *Network layer* (lapisan jaringan): Menentukan alamat jaringan secara logic, Menentukan rute yang harus diambil selama perjalanan, Menjaga antrian trafik di jaringan, Error Checking,

Error Recovery, Data pada bagian ini disebut paket. Contoh Protocol/Layanan : Protokol IP, IPX

d) *Transport layer* (lapisan transpor): Melakukan segmentasi dan menyatukan kembali data yang tersegmentasi (reassembling) dari upper layer, Flow Control, memastikan host pengirim tidak mengirimkan data lebih cepat dari yang dapat diolah oleh host penerima, Error Checking, untuk mendeteksi transmisi yang error, Error Recovery, memintra pengiriman kembali data yang rusak/error. Contoh Protocol/Layanan: Protokol TCP, UDP.

TCP

TCP (*Transmission Control Protocol*) adalah salah satu jenis protokol yang memungkinkan sekumpulan komputer untuk berkomunikasi dan bertukar data didalam suatu jaringan.

TCP mempunyai karakteristik sebagai protokol yang berorientasi koneksi (Connection oriented). Protokol TCP menggunakan jalur data full duplex yang berarti antara kedua host terdapat dua buah jalur, jalur masuk dan jalur keluar sehingga data dapat dikirimkan secara simultan. Contoh aplikasi Telnet, FTP (File Transfer Protocol) dan SMTP (Simple Mail Transfer Protocol).

UDP

UDP (User Datagram Protocol) adalah transport layer connectionless yang memungkinkan sebuah perangkat lunak pada komputer bisa mengirimkan pesan ke komputer lain melalui jaringan tanpa perlu ada komunikasi awal. Aplikasi untuk UDP antara lain SunRPC, SNMP, DNS, dan TFTP. Proses transmisi data UDP dilakukan dalam bentuk datagram yang memungkinkan data yang diterima bisa mengalami kerusakan dan tidak urut karena Pesan-pesan UDP akan dikirimkan sebagai datagram tanpa adanya nomor urut atau pesan acknowledgment.

e) *Session layer* (lapisan sesi): Mendefinisikan bagaimana koneksi dimulai, dipelihara dan diakhiri, Sinkronisasi antara pertukaran data antar computer. Contoh Protocol/Layanan: Protokol SCP (Session Control Protocol), NETBIOS

f) *Presentation layer* (lapisan presentasi): Mentranslasikan data yang hendak ditransmisikan oleh aplikasi ke dalam format yang dapat ditransmisikan oleh jaringan (mengatur bagaimana data dipresentasikan), Menangani pemrosesan seperti enkripsi, tipe data, format data, struktur data. Contoh Protocol/Layanan : JPEG, GIF, ASCII, EBCDIC

g) *Application layer* (lapisan aplikasi): Interface antara jaringan dan s/w aplikasi, Mengatur bagaimana aplikasi dapat mengakses jaringan, dan kemudian membuat pesan-pesan kesalahan. Contoh Protocol/Layanan : Telnet, HTTP, FTP, SMTP, POP3

Darpa Model :

Dikenal juga dengan TCP/IP Architecture Model atau Internet Model atau Dod

- Layer 4, Application Layer: Menyediakan akses/antarmuka terhadap jaringan TCP/IP, Menangani masalah representasi data, proses encoding, dan dialog control yang memungkinkan komunikasi antar aplikasi jaringan
- Layer 3, Host-to-host Layer / Transport Layer : Membuat komunikasi antar 2 host, menyediakan layanan pengiriman data dari sumber ke tujuan dengan cara membuat logical connection diantara keduanya, memecah data dan menyatukan kembali data yang diterima dari application layer ke dalam aliran data yang sama antara sumber dan pengirim data.
- Layer 2, Internet Layer: Melakukan routing dan pembuatan paket IP (datagram).
- Layer 1, Network Access Layer: Meletakkan frame-frame data yang akan dikirim ke media jaringan, mengatur semua hal yang diperlukan sebuah paket IP (Datagram IP)

2) IP Address dan Subnetting

a) IP address Versi 4 (IPV4)

IP address digunakan sebagai alamat dalam hubungan antar host di internet. IP address terdiri dari bilangan biner 32 bit yang dipisahkan oleh tanda titik setiap 8 bitnya. Tiap 8 bit ini disebut sebagai octet. IP Address dapat dipisahkan menjadi 2 bagian, yakni bagian network (net ID) dan bagian host (host ID). Net ID berperan dalam identifikasi suatu network dari network yang lain, sedangkan host ID berperan untuk identifikasi host dalam suatu network. Jadi, seluruh host yang tersambung dalam jaringan yang sama memiliki net ID yang sama. Sebagian dari bit-bit bagian awal dari IP Address merupakan network bit/network number, sedangkan sisanya untuk host.

IP address dibagi ke dalam lima kelas, yaitu kelas A, kelas B, kelas C, kelas D dan kelas E.

- Bit pertama IP Address kelas A adalah 0, dengan panjang net ID 8 bit dan panjang host ID 24 bit. Byte pertama IP address kelas A mempunyai range dari 0-127. Kelas A terdapat 127 network dengan tiap network dapat menampung sekitar 16 juta host (255x255x255). IP address kelas A diberikan untuk jaringan dengan jumlah host yang sangat besar.
- Dua bit IP address kelas B selalu diset 10 sehingga byte pertamanya selalu bernilai antara 128-191.Network ID adalah 16 bit pertama dan 16 bit sisanya adalah host ID sehingga kalau ada komputer mempunyai IP address 192.168.26.161, network ID = 192.168 dan host ID = 26.161. Pada. IP address kelas B ini mempunyai range IP dari 128.0.xxx.xxx sampai 191.155.xxx.xxx, yakni berjumlah 65.255 network dengan jumlah host tiap network 255 x 255 host atau sekitar 65 ribu host.

- IP address kelas C mulanya digunakan untuk jaringan berukuran kecil seperti LAN. Tiga bit pertama IP address kelas C selalu diset 111. Network ID terdiri 24 bit dan host ID 8 bit sisanya sehingga dapat terbentuk sekitar 2 juta network dengan masing-masing network memiliki 256 host.
- IP address kelas D digunakan untuk keperluan multicasting, 4 bit pertama IP address kelas D selalu diset 1110 sehingga byte pertamanya berkisar antara 224-247, sedangkan bit-bit berikutnya diatur sesuai keperluan multicast group yang menggunakan IP address ini. Dalam multicasting tidak dikenal istilah network ID dan host ID.
- IP address kelas E tidak diperuntukkan untuk keperluan umum. 4 bit pertama IP address kelas ini diset 1111 sehingga byte pertamanya berkisar antara 248-255.

Network Address. Address ini digunakan untuk mengenali suatu network pada jaringan Internet.

Broadcast Address. Address ini digunakan untuk mengirim/menerima informasi yang harus diketahui oleh seluruh host yang ada pada suatu network.

Aturan Dasar Pemilihan network ID dan host ID

Berikut adalah aturan-aturan dasar dalam menentukan network ID dan host ID yang digunakan:

- Network ID tidak boleh sama dengan 127
  Network ID 127 secara default digunakan sebagai alamat loopback yakni IP address yang digunakan oleh suatu komputer untuk menunjuk dirinya sendiri.
- Network ID dan host id tidak boleh sama dengan 255
  Network ID atau host ID 255 akan diartikan sebagai alamat broadcast. ID ini merupakan alamat yang mewakili seluruh jaringan.

- Network ID dan host ID tidak boleh sama dengan 0
  IP address dengan host ID 0 diartikan sebagai alamat network. Alamat network digunakan untuk menunjuk suatu jaringan bukan suatu host.
- Host ID harus unik dalam suatu network.
  Dalam suatu network tidak boleh ada dua host yang memiliki host ID yang sama

b) Subnetting

Subunetting adalah "memindahkan" garis pemisah antara bagian network dan bagian host dari suatu IP Address. Subnetmask digunakan untuk membaca bagaimana kita membagi jalan dan gang, atau membagi network dan hostnya. Address mana saja yang berfungsi sebagai SUBNET, mana yang HOST dan mana yang BROADCAST. Semua itu bisa kita ketahui dari SUBNET MASKnya. Jl Gatot Subroto tanpa gang dipahami menggunakan SUBNET MASK DEFAULT, atau dengan kata lain bisa disebut juga bahwa Network tersebut tidak memiliki subnet (Jalan tanpa Gang). SUBNET MASK DEFAULT ini untuk masing-masing Class IP Address adalah sbb:

CLASS	OKTET PERTAMA	SUBNET MAS DEFAULT	PRIVATE ADDRESS
A	1-127	255.0.0.0	10.0.0.0-10.255.255.255
B	128-191	255.255.0.0	172.16.0.0-172.31.255.255
C	192-223	255.255.255.0	192.168.0.0-192.168.255.255

Gambar 45. Subnet Mask Default

Subnet Mask	Nilai CIDR
255.128.0.0	/9
255.192.0.0	/10
255.224.0.0	/11
255.240.0.0	/12
255.248.0.0	/13
255.252.0.0	/14
255.254.0.0	/15
255.255.0.0	/16
255.255.128.0	/17
255.255.192.0	/18
255.255.224.0	/19

Subnet Mask	Nilai CIDR
255.255.240.0	/20
255.255.248.0	/21
255.255.252.0	/22
255.255.254.0	/23
255.255.255.0	/24
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29
255.255.255.252	/30

Gambar 46. Contoh perhitungan subnet
Sumber : https://youtu.be/Gqok2_VtwmM

Subnetting seperti apa yang terjadi dengan sebuah NETWORK ADDRESS 192.168.1.0/26 ?

Analisa: 192.168.1.0 adalah kelas C

Subnet Mask /26 = 255.255.255.192 diubah ke bentuk biner menjadi 11111111.11111111.11111111.11000000

- **Jumlah Subnet** = 2^x, dimana x adalah banyaknya binari 1 pada oktet terakhir subnet mask 11000000. Jadi Jumlah Subnet adalah $2^2 = 4$ subnet
- **Jumlah Host per Subnet** = $2^y - 2$, dimana y adalah adalah kebalikan dari x yaitu banyaknya binari 0 pada oktet terakhir subnet 11000000. Jadi jumlah host per subnet adalah $2^6 - 2 = 62$ host
- **Blok Subnet** = 256 – 192 (nilai oktet terakhir subnet mask(255.255.255.192)) = 64. Subnet berikutnya adalah 64 + 64 = 128, dan 128+64=192. Jadi subnet lengkapnya adalah **0, 64, 128, 192**.
- Bagaimana dengan alamat **host dan broadcast yang valid**? Sebagai catatan, host pertama adalah 1 angka setelah subnet, dan broadcast adalah 1 angka sebelum subnet berikutnya.

Subnet	192.168.1.**0**	192.168.1.**64**	192.168.1.**128**	192.168.1.**192**
Host Pertama	192.168.1.**1**	192.168.1.**65**	192.168.1.**129**	192.168.1.**193**
Host Terakhir	192.168.1.**62**	192.168.1.**126**	192.168.1.**190**	192.168.1.**254**
Broadcast	192.168.1.**63**	192.168.1.**127**	192.168.1.**191**	192.168.1.**255**

Gambar 47. Alamat Broadcast

3) Penerapan komunikasi daring

Berikut beberapa penerapan komunikasi daring yang sering kita temui dalam kehidupan sehari-hari.

a) Website

Sebuah sistem yang memunculkan informasi yang tersimpan baik dalam bentuk teks, gambar, audio, atau video dalam internet web sever, kedalam bentuk hypertext sehingga dapat diakses dan dilihat oleh pengguna internet.

b) E-mail

E-mail atau surat elektronik adalah sarana dalam mengirim pesan dalam format digital. E-mail merupakan sebuah bentuk berkomunikasi dengan cara surat menyurat.

c) Forum online

Forum merupakan salah satu program aplikasi internet yang digunakan sebagai sarana diskusi online antar anggota yang tergabung dalam suatu grup atau kelompok tertentu.

d) VoIP

Voice Over IP (VoIP) adalah percakapan secara online yang dilakukan dalam bentuk suara. Penggunanya dapat melalukan percakapan sepertihalnya orang menelepon menggunakan telepon. Bedanya, sarana yang digunakan bukanlah jaringan telepon, melaikan jaringan internet. Contoh aplikasi panggilan suara misalnya buddy talk, media ring talk, skype, dll.

e) Video conference

Video conference merupakan program aplikasi komunikasi online dimana pengunanya dapat saling bertatap muka satu sama lain, sehingga seakan-akan bertemu langsung dengan lawan bicara. Dalam video conference, pengguna dapat mengirimkan dan menerima pesan dalam bentuk gambar bergerak serta suara. Contoh aplikasi video conference misalnya skype. Aplikasi perpesanan seperti whatsapp, line, dan sebagainya, juga sekarang telah menambahkan fasilitas komunikasi melalui video call.

2. Konsep Teknologi Jaringan Berbasis Luas (WAN)

a. Jaringan berbasis luas (WAN)

WAN menjadi jaringan yang memiliki ruang lingkup yang sangat luas, dan bisa saling terhubung antar jaringan dari jarak jauh. WAN merupakan jaringan komputer yang mencakup area yang besar, sebagai contoh jaringan komputer antar wilayah, kota bahkan negara, atau dapat didefinisikan sebagai jaringan komputer yang membutuhkan router dan saluran komunikasi publik. WAN digunakan untuk menghubungkan jaringan area lokal yang satu dengan jaringan lokal yang lain, sehingga pengguna atau komputer di lokasi yang satu dapat berkomunikasi dengan pengguna dan komputer di lokasi yang lain.

WAN merupakan jaringan komunikasi data yang menghubungkan user- user yang ada di jaringan yang berada di suatu area geografis yang besar. Layanan WAN terfokus beroperasi pada layer physical dan data link pada model OSI layer. Jaringan WAN biasanya selalu menggunakan fasilitas transmisi yang disediakan oleh perusahaan telekomunikasi seperti perusahaan layanan telepon.

b. Perkembangan jaringan berbasis luas (WAN)

Sejarah pembentukan jaringan ini bermula pada tahun 1940-an di Amerika. Ada sebuah penelitian yang ingin memanfaatkan sebuah perangkat komputer secara bersama. Di tahun 1950-an ketika jenis komputer mulai membesar sampai terciptanya super komputer, karena mahalnya harga perangkat komputer maka

ada tuntutan sebuah komputer harus melayani beberapa terminal. Dari sinilah muncul konsep distribusi proses berdasarkan waktu yang dikenal dengan nama TSS (Time Sharing System), bentuk pertama kali jaringan (network) komputer diaplikasikan. Pada sistem TSS beberapa terminal terhubung secara seri ke sebuah host komputer.

Proses selanjutnya, konsep ini berkembang menjadi proses distribusi (distributed processing). Dalam proses ini beberapa host komputer mengerjakan sebuah pekerjaan besar secara paralel untuk melayani beberapa terminal yang tersambung secara seri di setiap host komputer. Harga-harga komputer kecil sudah mulai menurun dan konsep proses distribusi sudah matang, maka penggunaan komputer dan jaringannya sudah mulai beragam dari mulai menangani proses bersama maupun komunikasi antar komputer (peer to peer system) saja tanpa melalui komputer pusat. Oleh karena itu mulailah berkembang teknologi jaringan lokal yang dikenal dengan sebutan LAN (Local Area Network). Demikian pula ketika internet mulai diperkenalkan, maka sebagian besar LAN yang berdiri sendiri mulai berhubungan dan terbentuklah jaringan raksasa di tingkat dunia yang disebut dengan istilah WAN.

c. Kegunaan teknologi berbasi luas (WAN)

Kegunaan teknologi WAN menurut definisinya adalah sebagai berikut.

1) Mengoperasikan jaringan area dengan batas geografis yang sangat luas.
2) Memungkinkan akses melalui interfance serial yang beroperasi pada kecepatan yang rendah.
3) Memberikan koneksi full-time (selalu ON) atau part-time (dial-on-demand).
4) Menghubungkan perangkat-perangkat yang terpisah melewati area global yang luas.

Teknologi WAN mendefinisikan koneksi perangkat-perangkat yang terpisah oleh area yang luas menggunakan media transmisi, perangkat, dan protokol yang berbeda. Data transfer rate pada komunikasi WAN umumnya jauh lebih lambat dibanding kecepatan jaringan lokal LAN.

d. Koneksi jaringan berbasis luas (WAN)

Berikut jenis-jenis koneksi dalam jaringan berbasis luas (WAN).

1) Packet Switching
   Packet swicthing adalah jalur komunikasi yang berdasarkan pada transmisi data dalam paket-paket yang memungkinkan data dari berbagai alat pada network untuk berbagi kanal komunikasi yang sama secara serentak.
2) Leased Line
   Leased line disebut juga point-to-point atau dedicated connections (koneksi yang disediakan khusus untuk pelanggan di mana bandwith-nya khusus untuk pelanggan itu saja).
3) Circuit Switching
   Circuit switching adalah jalur komunikasi yang digunakan dengan network dial up seperti PPP dan ISDN yang harus melakukan set up pada koneksi terlebih dahulu sebelum melewatkan data, sama seperti melakukan panggilan telepon.

e. Keuntungan dan kelemahan jaringan berbasis luas (WAN)

Pada penggunaannya, kehadiran jenis jaringan ini tetap memiliki beberapa keunggulan dan kelemahan, yaitu sebagai berikut.

1) Keunggulan Jaringan Berbasis Luas
   Kelebihan dari jaringan berbasis luas antara lain sebagai berikut.
   a) Hal-hal yang mahal (seperti *printer* atau saluran telepon ke internet) dapat dibagi oleh semua komputer pada jaringan ini tanpa harus membeli perangkat yang berbeda untuk setiap komputernya.
   b) Semua orang yang ada di jaringan ini dapat menggunakan data yang sama. Hal ini untuk menghindari masalah di mana beberapa pengguna mungkin memiliki informasi lebih banyak daripada yang lain.
   c) Berbagi informasi/*file* melalui area yang lebih besar.
   d) Besar jaringan penutup.
   e) Bisa diakses dengan jangkauan area geografis yang luas sehingga berbisnis dengan jarak jauh dapat terhubung dengan jaringan ini.

f) Dapat berbagi *software* dan *resources* dengan koneksi *workstations*.
g) Pesan dapat dikirim dengan sangat cepat kepada orang lain pada jaringan ini (bisa berupa gambar, suara, atau data yang disertakan dengan suatu lampiran).

2) Kelemahan dari Jaringan Berbasis Luas

Kelemahan dari jaringan berbasis luas adalah sebagai berikut.

a) Keamanan merupakan masalah yang paling nyata ketika orang yang berbeda memiliki kemampuan untuk menggunakan informasi dari komputer lain. Perlindungan terhadap hacker dan virus menambah kompleksitas lebih dan membutuhkan biaya.
b) Setelah diatur, memelihara jaringan adalah pekerjaan penuh waktu (full time) yang membutuhkan jaringan pengawas dan teknisi untuk dipekerjakan.
c) Informasi tidak dapat memenuhi kebutuhan lokal atau kepentingan.
d) Rentan terhadap hacker atau ancaman dari luar lainnya.
e) Biaya operasional mahal dan umumnya lambat.
f) Memerlukan firewall yang baik untuk membatasi pengguna luar yang masuk dan dapat mengganggu jaringan ini.
g) Menyiapkan jaringan bisa menjadi pengalaman yang sangat mahal dan rumit.

f. Penggunaan alat dan perancangan jaringan berbasis luas (WAN)

1) Access point

Access point adalah perangkat jaringan yang berisi sebuah transceiver dan antena untuk transmisi dan menerima sinyal ke dan dari client remote. Dengan access points (AP) client wireless bisa dengan cepat dan mudah untuk terhubung kepada jaringan LAN kabel secara wireless. Ukuran kekuatan sinyal memengaruhi sistem pemancaran, makin besar kekuatan sinyal makin luas jangkauannya.

2) Router

Router memiliki tingkat kecerdasan yang tinggi dan mampu meneruskan data ke alamat-alamat tujuan yang berada pada jaringan yang berbeda.

3) Kabel UTP

Kabel UTP adalah perangkat yang berfungsi sebagai media transfer data dari perangkat *accespoint* dengan computer

4) Antena

Fungsi dari antena adalah untuk memperkuat dan mengarahkan sinyal wireless untuk melakukan koneksi point to point atau point to multipoint.

5) Kabel Pigtail

Fungsi kabel pigtail yaitu untuk menghubungkan antena grid dengan access point radio.

6) Switch

Switch bekerja pada lapisan data-link, oleh sebab itu sering disebut switch lapisan kedua (layer-2 switch). Pada switch, disediakan satu jalur tersendiri untuk setiap port.

7) Bridge

Untuk mengurangi kemacetan pada jaringan komputer, maka jaringan-jaringan tersebut dibagi menjadi beberapa segmen jaringan yang lebih kecil. Peralatan jaringan yang dapat membagi suatu jaringan menjadi dua segmen adalah bridge.

8) Repeater

Repeater adalah suatu peralatan jaringan yang berfungsi untuk memperkuat sinyal yang akan dikirim agar dapat diteruskan ke komputer lain pada jarak yang jauh.

9) Hub

Hub hanya berfungsi untuk memperkuat sinyal dan tidak memiliki kemampuan untuk menentukan tujuan akhir informasi yang dikirim. Perbedaannya dengan repeater, hub memiliki sejumlah port sehingga sering disebut juga multi-port repeater. Hub umumnya digunakan pada jaringan dengan topologi star.

g. Penggunaan dan Perancangan Jaringan Berbasis Luas (WAN)

Kemunculan jaringan berbasis luas ini sangat membantu bidang komunikasi di era modern ini. Jaringan ini banyak digunakan untuk saling menghubungkan jaringan-jaringan yang secara fisik tidak saling berdekatan terpisah antarkota, provinsi, atau bahkan terpisahkan benua melewati batas wilayah negara satu sama lain. Koneksi antar-remote jaringan ini umumnya dengan kecepatan yang sangat jauh lebih lambat dari koneksi jaringan lokal lewat kabel jaringan.

Penerapan dari teknologi jaringan ini bisa kita lihat pada beberapa peralatan yang ada di sekitar kita. Berikut beberapa layanan yang muncul dari adanya teknologi WAN.

1) ATM
2) X.25

3. Media Jaringan (Nirkabel dan Fiber Optik)

a. Jaringan nirkabel

Teknologi jaringan nirkabel (wireless) dapat diklasifikasikan berdasarkan beberapa kriteria, diantaranya adalah:

1) Berdasarkan jenis topologi jaringan

Topologi jaringan nirkabel hanya mempunyai dua topologi. Berdasarkan standar IEEE 802.11 yang menangani Wireless LAN (WLAN) dan Mesh (Wi-Fi certification), dua topologi jaringan nirkabel adalah topologi Ad-Hoc dan topologi infrastruktur (infrastructure).

a) Topologi Ad-hoc

Topologi Ad-Hoc merupakan jaringan nirkabel sederhana dimana komunikasi yang terjadi antara dua atau lebih komputer dilakukan secara langsung tanpa melalui perantara berupa wireless access point. Topologi Ad-Hoc dapat pula dikatakan sebagai koneksi peer-to-peer atau computer-to-computer karena koneksi jaringan dilakukan langsung antar komputer.

b) Topologi Infrastruktur

Topologi infrastruktur merupakan jaringan nirkabel dimana komunikasi yang terjadi antara dua atau lebih komputer menggunakan perantara berupa wireless access point. Access point bertidak seperti hub atau switch pada jaringan kabel (wired networking) dan menjadi sentral atau pusat jaringan nirkabel. Pada topologi infrastruktur, perangkat wireless (wireless adapter) komputer berkomunikasi melalui access point, tidak langsung ke perangkat wireless komputer yang lain. Selain sebagai

sentral atau pusat jaringan nirkabel pada topologi infrasturktur, access point juga dapat dihubungkan dengan koneksi jaringan kabel LAN. Topologi infrastruktur dikenal pula dengan nama BSS (Basic Service Set).

Jaringan nirkabel yang khusus menggunakan perangkat *Access point* (AP) ataupun *Base Transceiver Station* (BTS) dikelompokkan menjadi 2 jenis tolopogi yaitu:

(1) Point to point

Jaringan *point to point* adalah jaringan nirkabel yang menghubungkan antar BTS atau antar *access point*. Frekuensi yang digunakan adalah 2.5 GHz, 5 GHz, 10 GHz, 15 GHz dan seterusnya.

(2) Point to multipoint

Topologi jaringan *point to multipoint* adalah topologi jaringan nirkabel yang menghubungkan satu *Access point* (AP) atau BTS ke banyak titik (*node*) perangkat *wireles*s (WiFi). Topologi jaringan *nirkabel point to multi point* (P2MP) biasanya digunakan untuk jarak jangkauan yang relatif dekat.

Dewasa ini telah berkembang teknologi wireless terbaru yaitu teknologi WiMAX (*Worldwide Interoperability for Microwave Access*). Teknologi nirkabel ini memungkinkan BTS atau *access point* (AP) dapat berkomunikasi dengan berbagai *remote/client* yang berbeda *merk* atau *multivendor*, dengan kecepatan yang sangat tinggi. Teknologi WiMax menggunakan standar baru nirkabel IEEE 802.16 dengan kecepatan 11 *mega byte* (MB) per detik. Wi-Max bisa melayani akses internet nirkabel hingga jangkauan mencapai jarak puluhan kilometer. Topologi *Point-to-MultiPoint* (PMP) ini ditujukan untuk membentuk wireless *Metropolitan Area Network* (MAN). Gambar berikut menjelaskan keterkaitan antara kedua topologi jaringan nirkabel.

b. Prinsip Kerja Jaringan Nirkabel

Jaringan nirkabel juga disebut dengan wireless, dimana prinsip kerja jaringan ini menggunakan gelombang radio, seperti ponsel, televisi, dan radio. Bahkan, komunikasi melalui jaringan wireless sangat mirip dengan komunikasi radio dua arah. Wireless internet adalah layanan internet yang dapat diakses tanpa koneksi kabel fisik ke komputer menggunakan internet. Layanan internet *wireless* umumnya disediakan oleh penyedia layanan internet melalui *router wireless*, atau secara lokal melalui penggunaan *router wireless* yang terhubung ke kabel atau modem DSL di rumah atau di kantor. Penggunaan yang paling umum digunakan adalah untuk menghubungkan pengguna laptop yang melakukan perjalanan dari lokasi ke lokasi atau untuk jaringan *mobile* yang terhubung melalui satelit.

1) Cara kerja jaringan *wireless*

Jaringan wireless terdapat tiga buah komponen yang dibutuhkan untuk mengirim dan menerima data, yaitu sebagai berikut.

a) Sinyal radio (radio signal).
b) Format data (data format).
c) Struktur jaringan (*network structure*).

2) Sifat Jaringan Nirkabel

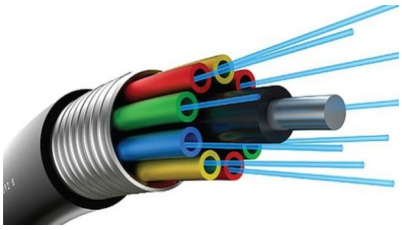
Ketika gelombang elektromagnetik mengenai atau menabrak atmosfer akan terjadi suatu interaksi tertentu. Bentuk interaksi tersebut dapat berupa pematulan (*Reflection*), penyerapan (*Absorption*), atau pemendaran (*Scattering*). Interaksi tersebut disebabkan adanya tempaan antara gelombang elektromagnetik yang terpancar dengan partikel-partikel yang terdapat di atmosfer bumi.

Berikut beberapa masalah pada jaringan nirkabel yang sering kita temui adalah:

1) Jaringan lambat
2) Lupa Password
3) Lupa Mengatur IP *Address*
4) Sinyal Lemah
5) *Wireless Network Adapter* Ter-*Disable*

c. Jaringan fiber optik

Fiber optik adalah suatu jenis kabel yang terbuat dari kaca atau plastik yang sangat halus, dan digunakan sebagai media transmisi karena dapat mentransmisikan sinyal cahaya dari suatu lokasi ke lokasi lainnya dengan kecepatan tinggi. Ukuran fiber optik ini sangat kecil dan halus (diameternya hanya 120 mikrometer), bahkan lebih kecil dari helaian rambut manusia. Komponen jaringan ini memiliki kecepatan transmisi yang tinggi dengan menggunakan pembiasan cahaya sebagai prinsip kerjanya. Sumber cahaya yang digunakan untuk proses transmisi adalah laser atau LED.

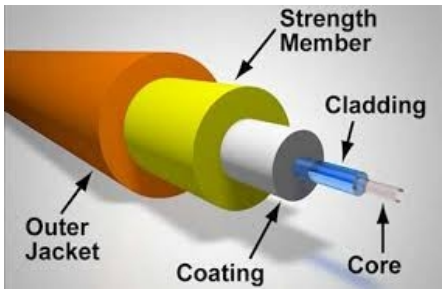


Gambar 48. Kabel fiber optik

Fiber optik atau serat optik menjadi salah satu komponen yang cukup populer dalam dunia telekomunikasi belakangan ini. Pasalnya, kabel jaringan tersebut memiliki kecepatan akses yang tinggi, sehingga banyak digunakan sebagai saluran komunikasi.

1) Kegunaan Kabel Fiber Optik

Fungsi dari kabel fiber optik adalah kecepatan akses yang tinggi serta kemampuan transfer data lebih cepat. Kecepatan pengiriman data bisa sampai kisaran Gigabit per detiknya. Bagian-bagian Kabel Fiber Optik



Gambar 49. Bagian-bagian kabel fiber optik

2) Prinsip Kerja Kabel Fiber Optik

Intinya di dalam kabel fiber optik menggunakan cara kerja dengan memanfaatkan cermin untuk menghasilkan total internal reflection atau bahasa umumnya adalah refleksi total pada bagian serat kaca.

Prinsip menggunakan gelombang cahaya pada kabel jaringan fiber optik membuatnya mampu membawa informasi lebih banyak dan menghantarkannya ke jarak yang jauh dibanding kabel jaringan lainnya yang masih menggunakan prinsip sinyal listrik. Hal ini disebabkan oleh bahan baku yang digunakannya mernpakan serat kaca murni yang dapat terus memancarkan cahaya sepanjang kabel yang ada. Cara kerja kabel fiber optik adalah dengan memanfaatkan cermin yang menghasilkan total internal reflection (refleksi total pada bagian dalam serat kaca).

3) Keunggulan dan Kelemahan Fiber Optik

Kabel jaringan fiber optik menjadi salah satu wujud teknologi canggih saat ini yang memiliki banyak keunggulan jika dibandingkan dengan kabel jaringan generasi sebelumnya (kabel coaxial ataupun kabel twisted pair). Namun, tetap saja setiap keunggulan disertai kelemahan. Berikut penjelasannya.

Keunggulan Fiber Optik

a) Bisa bertahan pada kondisi kelembapan udara dan cahaya (panas).
b) lebih efisien dibanding kabel jaringan lainnya
c) kabel jaringan fiber optik juga kuat terhadap interferensi elektromagnetik yang berasal dari sekitar kabel.
d) Kabel jaringan fiber optik dapat beroperasi dengan kecepatan yang sangat tinggi dalam membawa informasi atau data, bahkan lebih tinggi dibanding kabel jaringan coaxial ataupun kabel twisted pair. Kecepatan transfer data dapat mencapai 1000 Mbps.
e) Bandwith kabel jaringan fiber optik mampu membawa paket-paket dengan kapasitas besar (1 gigabit per detik).

f) Kabel jaringan fiber optik dapat mengirim sinyal lebih jauh dibanding kabel jaringan jenis lainnya, bahkan tanpa memerlukan perangkat penguat sinyal seperti repeater atau lainnya. Jika dibutuhkan, penguat sinyal tidak perlu dipasang setiap 5 km seperti kabel-kabel jaringan lainnya, melainkan cukup dipasang setiap 20 km saja.
g) Tidak menyebabkan terjadinya korsleting atau kebakaran. Khusus pada kabel fiber optik.
h) Tidak terjadinya penyadapan, hal ini tidak berlaku pada kabel jaringan fiber optik karena dapat meneruskan data tanpa ada distorsi atau gangguan.
i) Kabel jaringan fiber optik dapat dengan mudah di- upgrade bahkan tanpa perlu mengubah sistem kabel yang ada.
j) Kabel jaringan fiber optik terdiri dari berbagai macam jenis yang dapat menjadi opsi untuk menyesuaikan dengan lokasi instalasinya.
k) Kabel jaringan fiber optik mampu mengatasi masalah gangguan gelombang frekuensi bahan elektrik.
l) Diameter kabel jaringan fiber optik yang relatif kecil dan tipis, ditambah lagi dengan bobotnya yang ringan membuat proses instalasi kabel fiber optik relatif mudah karena bersifat fleksibel.

Kelemahan Fiber Optik

a) Dalam proses pengiriman sinyal, harus dilakukan perubahan sinyal listrik ke sinyal optik terlebih dahulu, maka kabel jaringan fiber optik menurut adanya sumber cahaya yang kuat untuk melakukan pensinyalan seperti alat pembangkit listrik eksternal.
b) Jika rusak, perbaikan instalasi kabel jaringan fiber optik yang kompleks memerlukan tenaga ahli di bidang ini.
c) tidak dapat diinstal dalam jalur yang berbelok secara tajam atau menyudut.
d) Harga kabel jaringan fiber optik masih terlalu mahal,
e) Kabel jaringan fiber optik bisa menyerap hidrogen sehingga dapat menyebabkan loss data.
f) Sangat mahal dalam instalasi sebuah jaringan komputer.

4. Manajemen Bandwidth

Bandwidth adalah suatu ukuran dari banyaknya informasi yang dapat mengalir dari suatu tempat ke tempat lain (dari source ke destination) dalam waktu tertentu biasanya dalam hitungan detik (Futri, 2017). Dengan kata lain bandwidth adalah kapasitas maksimum dari suatu jalur komunikasi yang dapat dipakai untuk mentransfer data dalam hitungan detik. Bandwidth dapat dipakai untuk mengukur, baik aliran data analog maupun aliran data digital. Satuan yang digunakan untuk bandwidth digital adalah bps (bit per second). Ini berarti jumlah bit yang dapat mengalir tiap detik melalui suatu media transmisi (kabel maupun nirkabel).

Throughput adalah bandwidth yang sebenarnya (aktual) yang diukur dengan satuan waktu tertentu dan pada kondisi jaringan tertentu yang digunakan untuk melakukan transfer file dengan ukuran tertentu. Bandwidth adalah batas maksimal, sedangkan throughput adalah data sebenarnya yang mengalir pada media transmisi (Kemendikbud, 2014).

Terdapat dua jenis bandwidth, yaitu bandwidth digital dan bandwidth analog. Bandwidth digital, yaitu jumlah atau volume data yang dapat dikirimkan melalui sebuah saluran komunikasi dalam satuan bits per second tanpa distorsi. Sedangkan bandwidth analog, yaitu perbedaan antara frekuensi terendah dengan frekuensi tertinggi dalam sebuah rentang frekuensi yang diukur dalam satuan Hertz (Hz) atau siklus per detik, yang menentukan berapa banyak informasi yang bisa ditransimisikan dalam satu saat.

Fungsi utama bandwidth, yaitu digunakan sebagai jalur pengiriman data dari suatu perangkat ke perangkat lain. Selain itu bandwidth juga digunakan sebagai pembatas kecepatan maupun jumlah data. Bandwidth sebagai jalur pengiriman data memungkinkan data antara perangkat satu dengan lainnya yang ada di suatu jaringan untuk saling berpindah atau ditransfer. Bandwidth digunakan sebagai pembatas kecepatan transfer atau pengiriman data, berarti kecepatan maksimal data dibatasi. Bandwidth digunakan sebagai pembatas jumlah data yang bisa dikirim, berarti jumlah maksimal data yang dibatasi.

Sebagai contoh, misalnya bandwidth internet di sebuah rumah diketahui adalah 4 Mbps, kemudian kita ingin mendownload file di internet berukuran 12 Mb, seharusnya file tersebut sudah sampai ke komputer kita hanya dengan waktu 3 detik (12/4). Akan tetapi yang terjadi secara aktual, file yang kita download tiba dalam waktu 6 detik. Jadi, bandwidth yang sebenarnya atau yang disebut throughtput adalah 12 Mb/6 detik = 2 Mbps.

Untuk lebih memahami tentang analisis kebutuhan bandwidth, berikut ini akan diberikan contoh analisis kebutuhan bandwidth dalam sebuah jaringan. Misalnya, akan dibangun sebuah warung internet (warnet) yang menyediakan layanan web atau browsing. Layanan web ini membutuhkan bandwidth minimal 512 kbps. Jika pada warnet tersebut kita sediakan 30 komputer, maka kebutuhan bandwidth adalah 512 kbps x 30 komputer = 15360 kbps atau sekitar 15 Mbps.

Manajemen bandwidth (bandwidth management) merupakan sebuah metode yang diterapkan untuk mengatur besarnya bandwidth yang akan digunakan oleh masing-masing pengguna di sebuah jaringan sehingga penggunaan bandwidth akan terdistribusi secara merata (Togohodoh, 2018). Manajemen bandwidth adalah pengalokasian yang tepat dari suatu bandwidth untuk mendukung kebutuhan atau keperluan aplikasi atau suatu layanan jaringan. Pengalokasian bandwidth yang tepat dapat menjadi salah satu metode dalam memberikan jaminan kualitas suatu layanan jaringan Quality of Service (QoS). Cara yang dapat dilakukan untuk melakukan pembagian bandwidth, diantaranya adalah dengan limit(membatasi bandwidth sesuai dengan kebutuhan dan jumlah pengguna), grouping (pembagian bandwidth berdasarkan suatu grup atau kelompok), burst (pembagian bandwidth dimana jika pengguna tidak terus menerus menggunakan bandwidth maka penggunaan bandwidth dapat ditingkatkan dari limit yang telah ditentukan) dan priority (pembagian bandwidth berdasarkan prioritas pengguna).

Quality of Service (QoS) merupakan mekanisme jaringan yang memungkinkan aplikasi-aplikasi atau layanan dapat beroperasi sesuai dengan yang diharapkan (Bunafit, 2005).

Quality of Service (QoS) didefinisikan sebagai suatu pengukuran tentang seberapa baik jaringan. QoS juga disebut suatu usaha untuk mendefinisikan karakteristik dan sifat dari suatu layanan atau jaringan. Pada jaringan berbasis IP, IP QoS mengacu pada performansi dari paket-paket IP yang melalui satu atau lebih jaringan.

QoS didesain untuk membantu end user menjadi lebih produktif dengan memastikan bahwa end user mendapatkan performansi yang handal dari aplikasi-aplikasi berbasis jaringan. QoS mengacu pada kemampuan jaringan untuk menyediakan layanan yang lebih baik pada traffic jaringan tertentu melalui teknologi yang berbeda-beda. Beberapa parameter performansi dari jaringan IP, yaitu delay, jitter, packet loss, dan throughput.

a. Delay

Delay didefinisikan sebagai total waktu tunda suatu paket yang diakibatkan oleh proses transmisi dari satu titik ke titik lain yang menjadi tujuannya. Delay di dalam jaringan dapat digolongkan menjadi 5 (lima), yaitu delay processing, delay packetization, delay serialization, delay jitter buffe, dan delay network.

b. Jitter

Jitter didefinisikan sebagai variasi dari delay atau variasi waktu kedatangan paket. Banyak hal yang dapat menyebabkan jitter, yaitu peningkatan traffic secara tiba-tiba sehingga menyebabkan penyempitan bandwith dan menimbulkan antrian. Selain itu, kecepatan terima dan kirim paket dari setiap node juga dapat menyebabkan jitter.

c. Packet Loss

Packet loss adalah perbandingan seluruh paket IP yang hilang dengan seluruh paket IP yang dikirimkan antara pada source dan destination. Salah satu penyebab paket loss adalah antrian yang melebihi kapasitas buffer pada setiap node. Beberapa penyebab terjadinya paket loss, yaitu sebagai berikut.

1) Congestion, disebabkan terjadinya antrian yang berlebihan dalam jaringan.
2) Node yang bekerja melebihi kapasitas buffer.
3) Memori yang terbatas pada node.

4) Policing atau kontrol terhadap jaringan untuk memastikan bahwa jumlah traffic yang mengalir sesuai dengan besarnya bandwidth. Jika besarnya traffic yang mengalir di dalam jaringan melebihi dari kapasitas bandwidth yang ada maka policing control akan membuang kelebihan traffic yang ada.

d. Throughput

Throughput adalah jumlah total kedatangan paket IP sukses yang diamati di tempat pengukuran pada destination selama interval waktu tertentu dibagi oleh durasi interval waktu tersebut (sama dengan jumlah pengiriman paket IP sukses per service-second).

Terdapat dua teknik manajemen bandwidth yang banyak digunakan di lapangan, yaitu, Hierarchical Token Bucket (HTB) dan Class-Based Queueing (CBQ). Hierarchical Token Bucket (HTB) adalah metode yang berfungsi untuk mengatur pembagian bandwidth. Pembagian dilakukan secara hirarki yang dibagi-bagi ke dalam kelas sehingga mempermudah pengaturan bandwidth.

Ada tiga tipe kelas dalam HTB, yaitu: root, inner, dan leaf. Root class berada paling atas, dan semua trafik harus melewati kelas ini. Inner class memiliki parent class dan child classes. Sedangkan leaf class adalah terminal class yang mempunyai parent class tetapi tidak mempunyai child class.

Pada antrian HTB mempunyai parameter yang menyusunnya dalam antrian, yaitu rate, ceil dan Random Early Detection (RED). Parameter rate menentukan bandwidth maksimum yang bisa digunakan oleh setiap class, jika bandwidth melebihi nilai “rate”, maka paket data akan dipotong atau dijatuhkan (drop). Parameter ceil diatur untuk menentukan peminjaman bandwidth antar class (kelas), peminjaman bandwidth dilakukan kelas paling bawah ke kelas di atasnya, teknik ini disebut link sharing. Random Early Detection atau bisa disebut Random Early Drop biasanya digunakan untuk gateway/router backbone dengan tingkat trafik yang sangat tinggi.

CBQ membagi pengguna traffic ke dalam hirarki class berdasarkan IP Address, protokol dan tipe aplikasi. Sebagai contoh hirarki class berdasarkan tipe aplikasi, pada perusahaan departemen keuangan tentunya tidak membutuhkan akses internet seperti pada departemen teknisi. Karena setiap perusahaan mempunyai peraturan, kebutuhan bisnis dan kebutuhan vital lain yang berbeda. Hal itulah yang akan mendasari pengelompokan hirarki class pada CBQ.

Class-based Queueing (CBQ) merupakan teknik klasifikasi paket data yang memungkinkan sharing bandwidth antar kelas (class) dan memiliki fasilitas pengguna interface. Konsep kerja CBQ dimulai saat classifier menentukan paket yang datang dan menempatkan ke kelas yang tepat. Kemudian general scheduler menentukan bandwidth yang diperuntukkan untuk suatu kelas, estimator memeriksa apakah kelas-kelas mendapatkan bandwidth sesuai dengan yang dialokasikan. Jika suatu kelas kekurangan maka dengan bantuan link-sharing scheduler kelas yang memiliki bandwidth yang tidak terpakai bisa dipinjamkan ke kelas yang membutuhkan tambahan bandwidth.

Manajemen bandwidth merupakan implementasi dari proses mengantrikan data, sehingga fungsi manajemen bandwidth pada RouterOS Mikrotik disebut dengan istilah queue. Secara garis besar, ada dua metode queue pada RouterOS Mikrotik yaitu Simple Queue dan Queue Tree (Citraweb Solusi Teknologi). Simple Queue merupakan metode manajemen bandwidth termudah yang ada di RouterOS Mikrotik untuk membatasi bandwidth berdasarkan alamat IP tertentu. Queue Tree digunakan untuk melakukan pembagian bandwidth berdasarkan protokol, port, kelompok alamat IP, dan lain-lain.

Simple Queue merupakan metode bandwidth management termudah yang ada di RouterOS Mikrotik untuk membatasi bandwidth berdasarkan alamat IP tertentu. Menu dan konfigurasi yang dilakukan untuk menerapkan Simple Queue cukup sederhana dan mudah dipahami.

Queue Tree digunakan untuk melakukan pembagian bandwidth berdasarkan protokol, port, kelompok alamat IP, dan lain-lain. Queue Tree merupakan fitur bandwidth management di RouterOS Mikrotik yang sangat fleksibel dan cukup kompleks.

Load balancing adalah teknik untuk mendistribusikan beban trafik pada dua atau lebih jalur koneksi secara seimbang, agar trafik dapat berjalan optimal, dan menghindari overload pada salah satu jalur koneksi (Sumarno & Hasmoro, 2013). load balancing dua jalur koneksi, maka besar bandwidth yang akan didapat menjadi dua kali lipat dari bandwidth sebelum menggunakan load balancing. Hal ini perlu diperjelas, bahwa load balancing tidak akan menambah besar bandwidth yang diperoleh, tetapi hanya bertugas untuk membagi trafik dari kedua bandwidth tersebut agar dapat terpakai secara seimbang.

Ada berbagai metode load balancing, antara lain yaitu: Static Route dengan Address List, Equal Cost Multi Path (ECMP), Nth dan Per Connection Classifier (PCC). Setiap metode load balancing tersebut memiliki kekurangan maupun kelebihan tersendiri, namun lebih dari hal itu yang paling terpenting dalam menentukan metode load balancing apa yang akan digunakan adalah harus terlebih dahulu mengerti karakteristik dari jaringan yang akan diimplementasikan.

Static route dengan Address list adalah metode load balancing yang mengelompokkan suatu range IP Address untuk dapat di atur untuk melewati salah satu gateway dengan menggunakan static routing.

Equal Cost Multi Path adalah pemilihan jalur keluar secara bergantian pada gateway. Contohnya jika ada dua gateway, dia akan melewati kedua gateway tersebut dengan beban yang sama (equal cost) pada masing-masing gateway.

Nth menggunakan algoritma round robin yang menentukan pembagian pemecahan connection yang akan di-mangle ke rute yang dibuat untuk load balancing.

Per Connection Classifier (PCC) merupakan metode yang menspesifikasikan suatu paket menuju gateway suatu koneksi tertentu. PCC mengelompokkan trafik koneksi yang keluar masuk router menjadi beberapa kelompok

5. Sistem Keamanan Jaringan

Keamanan jaringan (Network Security) adalah suatu cara atau suatu sistem yang digunakan untuk memberikan proteksi (perlindungan) dalam jaringan komputer.

Penyediaan keamanan jaringan adalah sebagai aksi penyeimbang antara open acces dengan security.

a. Resiko Keamanan Jaringan

Berdasarkan lubang keamanan, keamanan dapat diklasifikasikan menjadi empat, yaitu:

1) Keamanan yang bersifat fisik (*physical security*) termasuk akses orang ke gedung, peralatan, dan media yang digunakan.
2) Keamanan dari data dan media serta teknik komunikasi (*communications*).
3) Keamanan dalam operasi yaitu adanya prosedur yang digunakan untuk mengatur dan mengelola sistem keamanan, dan juga termasuk prosedur setelah serangan (*post attack recovery*).

Aspek tujuan keamanan jaringan adalah sebagai berikut :

1) *Privacy / Confidentiality, Privacy / Confidentiality* adalah menjaga informasi dari orang yang tidak berhak mengakses. *Privacy* lebih ke arah data-data yang sifatnya privat.
2) *Integrity, Integrity* adalah informasi tidak boleh diubah tanpa seijin pemilik informasi.
3) *Authentication, Authentication* adalah metode untuk menyatakan bahwa informasi betul-betul asli, atau orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud. *Availability*
4) *Availability* adalah berhubungan dengan ketersediaan informasi ketika dibutuhkan.
5) *Access Control. Access Control* adalah cara pengaturan akses kepada informasi. Berhubungan dengan masalah *authentication* dan juga *privacy*. Metodenya yaitu menggunakan kombinasi *user id/password* atau dengan menggunakan mekanisme lain.
6) *Non-repudiation. Non-repudiation* adalah aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi. Dukungan bagi *electronic commerce*.

b. Security Attack Models

Menurut W. Stallings (William Stallings, “Network and Internetwork Security,” Prentice Hall, 1995). serangan (attack) terdiri dari:

1) *Interruption* yaitu perangkat sistem menjadi rusak atau tidak tersedia. Serangan ditujukan kepada ketersediaan (*availability*) dari sistem. Contoh serangan adalah “*denial of service attack*”.
2) *Interception* yaitu pihak yang tidak berwenang berhasil mengakses aset atau informasi. Contoh dari serangan ini adalah penyadapan (*wiretapping*).
3) *Modification* yaitu pihak yang tidak berwenang tidak hanya berhasil mengakses, akan tetapi dapat juga mengubah (*tamper*) aset. Contoh dari serangan ini antara lain adalah mengubah isi dari *website* dengan pesan-pesan yang merugikan pemilik *website*.
4) *Fabrication* yaitu pihak yang tidak berwenang menyisipkan objek palsu ke dalam sistem. Contoh dari serangan jenis ini adalah memasukkan pesan-pesan palsu seperti *e-mail* palsu ke dalam jaringan komputer.

Jenis-jenis ancaman pada sistem keamanan jaringan yaitu sebagai berikut:

1) Memaksa masuk dan kamus *password*
   Jenis ancaman keamanan jaringan ini lebih umum disebut sebagai *Brute Force and Dictionary*, serangan ini dilakukan dengan upaya masuk ke dalam jaringan dengan menyerang *database password* atau menyerang *login prompt* yang sedang aktif.
2) *Denial of Services* (DoS)
   Serangan *Denial of Services* (DoS) ini adalah salah satu ancaman keamanan jaringan yang membuat suatu layanan jaringan menjadi terblokir, serangan yang membuat jaringan anda tidak bisa diakses atau serangan yang membuat system anda tidak bisa memproses atau merespon terhadap *traffic* yang legitimasi atau permintaan layanan terhadap *object* dan *resource* jaringan. Bentuk umum dari serangan *Denial of Services* ini adalah dengan cara mengirim paket data dalam

jumlah yang sangat besar terhadap suatu server dimana server tersebut tidak bisa memproses semuanya.

3) *Smurf Attack*

Serangan keamanan jaringan dalam bentuk *Smurf Attack* terjadi ketika sebuah server digunakan untuk membanjiri korban dengan data sampah yang tidak berguna. Serangan yang umum adalah dengan jalan mengirimkan *broadcast* kepada segmen jaringan sehingga semua *node* dalam jaringan akan menerima paket *broadcast* ini, sehingga setiap *node* akan merespon balik dengan satu atau lebih paket respon.

4) *Ping of death*

Serangan keamanan jaringan *Ping of Death*, adalah serangan *ping* yang *oversize*. Dengan menggunakan *tool* khusus, si penyerang dapat mengirimkan paket *ping oversized* yang banyak sekali kepada korbannya. Dalam banyak kasus sistem yang diserang mencoba memproses data tersebut, *error* terjadi yang menyebabkan *system crash*, *freeze* atau *reboot*. *Ping of Death* hampir sama dengan serangan *Buffer overflow*, tetapi karena sistem yang diserang sering jadi down, maka disebut *DoS attack*.

5) *Stream Attack*

Stream Attack terjadi saat banyak jumlah paket yang besar dikirim menuju ke port pada sistem korban menggunakan sumber nomor yang random.

6) *Spoofing*

Spoofing adalah Serangan dengan cara menjelma menjadi sesuatu yang lain. *Spoofing Attack* terdiri dari *IP Address* dan *node source* atau tujuan yang asli atau yang *valid* diganti dengan *IP Address* atau *node source* atau tujuan yang lain.

7) *Serangan Man-in-the-middle*

Serangan keamanan jaringan *Man-in-the-middle* (serangan pembajakan) terjadi saat *user* perusak dapat memposisikan diantara dua titik *link* komunikasi. Dengan jalan menyalin atau menyusup *traffic* antara dua *party*, hal ini pada dasarnya merupakan serangan penyusup. Para

penyerang memposisikan dirinya dalam garis komunikasi dimana dia bertindak sebagai *proxy* atau mekanisme *store-and-forwad* (simpan dan lepaskan). Para penyerang ini tidak tampak pada kedua sisi *link* komunikasi ini dan bisa mengubah isi dan arah *traffic*. Dengan cara ini para penyerang bisa menangkap *logon credensial* atau *data sensitive* ataupun mampu mengubah isi pesan dari kedua titik komunikasi ini.

8) *Spamming*

Spam sering kita definisikan sebagai *email* sampah yang tak diundang, *newsgroup*, atau pesan diskusi forum. Spam bisa merupakan iklan dari *vendor* atau bisa berisi kuda *Trojan. Spam* pada umumnya bukan merupakan serangan keamanan jaringan akan tetapi hampir mirip DoS.

9) *Sniffer*

Adalah Suatu serangan keamanan jaringan dalam bentuk *Sniffer* (atau dikenal sebagai *snooping attack*) merupakan kegiatan user perusak yang ingin mendapatkan informasi tentang jaringan atau *traffic* lewat jaringan tersebut. suatu *Sniffer* sering merupakan program penangkap paket yang bisa menduplikasikan isi paket yang lewat media jaringan ke dalam file. Serangan *Sniffer* sering difokuskan pada koneksi awal antara client dan server untuk mendapatkan *logon credensial*, kunci rahasia, *password* dan lainnya.

10) *Crackers*

Ancaman keamanan jaringan *Crackers* adalah user perusak yang bermaksud menyerang suatu system atau seseorang. *Cracker* bisasanya termotivasi oleh ego, *power*, atau ingin mendapatkan pengakuan. Akibat dari kegiatan *hacker* bisa berupa pencurian (data, ide, dll), *disable system*, kompromi keamanan, *opini negative public*, kehilangan pasar saham, mengurangi keuntungan, dan kehilangan produktifitas. Contoh akibat dari jebolnya sistem keamanan, antara lain ditahun 1988, Keamanan *system mail sendmail* dieksploitasi oleh Robert Tapan Morris sehingga melumpuhkan sistem Internet. Kegiatan ini dapat diklasifikasikan sebagai "*denial of service attack*".

c. Lapisan Keamanan

Pada lapisan keamanan ini, terdapat beberapa cara yang dapat Anda lakukan untuk mengamankan diri dari kejahatan yang ada pada sistem keamanan jaringan adalah sebagai berikut:

1) Keamanan Fisik. Keamanan fisik ini berarti keamanan yang nampak seperti komputer, laptop, dan sebagainya,
2) Keamanan lokal berarti keamanan yang berkaitan dengan user dan hak-haknya.
3) Keamanan file dan system file . Keamanan *file* dan *system file* adalah keamanan yang berkaitan dengan *file data* yang ada pada OS Windows ataupun LINUX.
4) Keamanan password dan enkripsi. Keamanan *password* dan *enkripsi* adalah keamanan yang berkaitan dengan penggunaan *password* pada *system* ataupun terhadap *file*.
5) Keamanan Kernel, Keamanan kernel adalah keamanan yang berkaitan dengan penggunaan *operating system* yang terbaru.
6) Keamanan Jaringan. Keamanan jaringan adalah keamanan yang berkaitan dengan penggunaan jaringan saat melakukan suatu aktivitas.

d. Definisi Firewall

Istilah "*firewall*" sendiri sebenarnya juga dikenal dalam disiplin lain, dan dalam kenyataannya, istilah ini tidak hanya bersangkutan dengan *terminology* jaringan. *Firewall* didefinisikan sebagai sebuah komponen atau kumpulan komponen yang membatasi akses antara sebuah jaringan yang diproteksi dan internet, atau antara kumpulan kumpulan jaringan lainnya. Definisi lain mengatakan bahwa, *firewall* adalah sebuah computer yang memproteksi jaringan dari jaringan yang tidak dipercaya yang memisahkan antara jaringan local dengan jaringan publik, dengan melakukan metode *filtering* paket data yang masuk dan keluar.

e. Jenis-jenis *Firewall*

Melihat betapa dibutuhkannya *firewall*, ragamnya pun bervariasi sesuai dengan kebutuhan pengguna. Diantaranya, terdapat 7 jenis *firewall* yang perlu anda

ketahui sebagai aktivis dunia maya. Ketujuh jenis tersebut kami uraikan secara jelas seperti berikut.

1) *Packet Filter. Firewall* yang satu ini merupakan sebuah komputer yang dibekali dengan dua buah *Network Interface Card* (NIC) yang mana fungsinya menyaring berbagai paket yang masuk.
2) *Circuit Level Gateway.* Jenis ini umumnya berupa komponen suatu *proxy server*. *Firewall* ini tepatnya bekerja pada lapisan sesi (*session layer*).
3) *Application Level.* Penggunaan *firewall* ini akan mengakibatkan tidak dibolehkannya paket untuk masuk melewati *firewall* tersebut secara langsung.
4) *Network Address Translation* (NAT). *firewall* yang satu ini menyediakan proteksi secara otomatis terhadap sistem dibalik *firewall*. NAT ini hanya mengizinkan koneksi dari komputer yang letaknya dibalik *firewall*. NAT *firewall* yaitu melakukan *multiplexing* pada lalu lintas jaringan internal lalu menyampaikannya ke jaringan semacam WAN, MAN ataupun jaringan internet yang memang lebih luas jaringannya.
5) *Stateful Firewall. Firewall* jenis ini dapat melakukan *filtering* pada lalu lintas atas dasar karakteristik paket, sebagaimana halnya *filtering* berjenis *packet filtering* serta memiliki pengecekan pada sesi koneksi guna meyakinkan kalau sesi koneksi tersebut diizinkan.
6) *Virtual Firewall. virtual firewall* dimana nama virtual tersebut adalah sebutan yang dialamatkan pada *firewall* logis tertentu yang berada dalam suat perangkat fisik (seperti komputer maupun perangkat *firewall* yang lain).
7) *Transparent Firewall.* Jenis ini bisa juga disebut dengan *bridging firewall* merupakan sebuah turunan atas *satateful firewall*. *Transparent firewall* melakukan apa saja yang dapat dilakukan oleh firewall jenis *packet filtering*, sebagaimana halnya *stateful firewall* serta tak nampak oleh pengguna.

f. Tujuan Penggunaan *Firewall*

Terdapat beberapa tujuan penggunaan *firewall*, antara lain:

1) *Firewall* biasanya digunakan untuk mencegah atau mengendalikan aliran data tertentu.
2) Untuk *melindungi* dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan/kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkupnya.
3) Penggunaan *firewall* yang dapat mencegah upaya berbagai *Trojan horses, virus, phishing, spyware* untuk memasuki sistem yang dituju dengan cara mencegah hubungan dari luar, kecuali yang diperuntukan bagi komputer dan *port* tertentu seperti gambar berikut.
4) *Firewall* akan memfilter serta mengaudit *traffic* yang melintasi perbatasan antara jaringan luar maupun dalam.

g. Fungsi Firewall

Firewall sendiri memiliki beberapa fungsi untuk melindungi jaringan komputer yang dapat dijabarkan dalam beberapa poin berikut:

1) Sebagai pos keamanan jaringan. *firewall* akan berusaha menyaring agar lalu lintas sesuai dengan keamanan yang telah ditentukan.
2) Mencegah informasi berharga bocor tanpa sepengatahuan *firewall* banyak dipasang untuk *file transfer protocol* (ftp), sehingga setiap lalu lintas data dikendalikan oleh *firewall*.
3) Mencatat aktivitas pengguna. *Firewall* mampu mengakses data *log* sekaligus menyediakan statistik mengenai penggunaan jaringan.
4) Memodifikasi paket data yang datang. Dikenal juga dengan istilah NAT (*network address translation*). NAT digunakan untuk menyembunyikan sebuah *IP Adress*, sehingga membuat para pengguna dapat mengakses internet tanpa *IP Adress* publik, yang sering juga disebut dengan istilah IP *masquerading*.
5) Mencegah modifikasi data pihak lain. Firewall mencegah modifikasi data-data tersebut sehingga tetap berada dalam keadaan aman.

h. Cara Kerja *Firewall*

Pada dasarnya, *firewall* bekerja dengan cara membatasi komputer pribadi dengan internet. *Firewall* bekerja layaknya penjaga keamanan di depan gerbang rumah dan mengidentifikasi pengunjung yang datang, sekaligus menyaring

penyusup yang berusaha memasuki komputer pribadi. *Firewall* bekerja seperti garda pertahanan terdepan untuk menahan segala usaha *hacking* yang masuk ke dalam komputer. Teknologi *firewall* pun kian hari kian berkembang. Sebelumnya, *firewall* bekerja menyaring lalu lintas komputer dengan menggunakan alamat IP, nomor *port*, serta protokol. Seiring dengan perkembangannya, kini *firewall* mampu menyaring data yang masuk dengan mengidentifikasi terlebih dahulu pesan konten yang dibawanya.

D. Rangkuman

1. Rangkuman Sistem Jaringan Dasar
   a. Manfaat jaringan komputer, antara lain:
      1) Jaringan komputer dapat mengakses file yang dimiliki sekaligus file orang lain yang telah disebarluaskan melalui suatu jaringan, semisal jaringan internet.
      2) Melalui jaringan komputer dapat melakukan proses pengiriman data secara cepat dan efisien.
   b. Jenis Jaringan komputer secara umum terbagi atas 5 macam, yaitu LAN (Local Area Network), MAN (Metropolitan Area Network), WAN (Wide Area Network), Internet, dan Wireless (jaringan tanpa kabel). Komunikasi daring memiliki beberapa keunggulan jika dibandingkan dengan komunikasi konvensional, antara lain sebagai berikut.
      1) Dapat dilakukan kapan saja di mana saja. Dengan komunikasi daring, setiap pengguna dapat melakukan komunikasi di mana saja dan kapan saja, dengan syarat terkoneksi dengan jaringan internet dan memiliki sarana yang mencukupi.
      2) Efisiensi biaya. Berbeda dengan komunikasi konvensional, komunikasi daring tidak memerlukan pihak yang berkomunikasi untuk bertemu tatap muka, dengan komunikasi daring Anda dapat menghemat biaya transportasi.
2. Rangkuman Konsep Teknologi Jaringan Berbasis Luas (WAN)
   a. Jaringan WAN adalah jaringan komunikasi data yang menghubungkan user-user di jaringan yang berada di suatu area geografis yang besar.

b. WAN digunakan untuk menghubungkan jaringan lokal yang satu dengan jaringan lokal yang lain, sehingga pengguna atau komputer di lokasi yang satu dapat berkomunikasi dengan pengguna dan komputer di lokasi yang lain.
c. Jenis-jenis koneksi dalam jaringan berbasis luas (WAN) adalah sebagai berikut.
    1) Packet swicthing adalah sebuah jalur komunikasi yang berdasarkan pada transmisi data dalam paket-paket yang memungkinkan data dari berbagai alat pada network untuk berbagi kanal komunikasi yang sama secara serentak.
    2) Leased Line disebut juga point-to-point atau dedicated connections (koneksi yang disediakan khusus untuk pelanggan di mana bandwidth-nya khusus untuk pelanggan itu saja).
    3) Circuit switching adalah sebuah jalur komunikasi yang digunakan dengan network dial up seperti PPP dan ISDN yang harus melakukan set-up pada koneksi terlebih dahulu sebelum melewatkan data, sama seperti melakukan panggilan telepon.
d. Komponen teknologi WAN di antaranya sebagai berikut.
    1) Switch juga bekerja pada lapisan data-link, oleh sebab itu sering disebut switch lapisan kedua (Layer-2 switch).
    2) Bridge adalah peralatan jaringan yang dapat membagi suatu jaringan menjadi dua segmen.
    3) Repeater ada lah suatu peralatan jaringan yang berfungsi untuk memperkuat sinyal yang akan dikirim agar dapat diteruskan ke komputer lain pada jarak yang jauh.
    4) Hub yang fungsinya untuk memperkuat sinyal dan tidak memiliki kecerdasan untuk menentukan tujuan akhir informasi yang dikirim.
    5) Router yang bekerja pada lapisan network atau lapisan ketiga model OSI dan meneruskan paket data berdasarkan alamat logika seperti IP address.
    6) Routing switch atau sering disebut switch lapisan ketiga (layer-3 switch) adalah gabungan antara switch dan router.
    7) Multiplexer yang digunakan untuk mentransfer beberapa data secara simultan (terus-menerus), seperti video, sound, text, dan lain-lain.

8) Communication server adalah server khusus "dial in/out" bagi pengguna untuk dapat melakukan dial dari lokasi remote sehingga dapat terhubung ke LAN.
9) Switch X.25 dan Frame Relay yang menghubungkan data local/private.
10) Melalui jaringan data menggunakan sinyal digital. Unit ini sama dengan switch ATM.
11) Media transmisi yang berupa kabel yang digunakan pada jaringan komputer.
12) Switch ATM yang menyediakan transfer data berkecepatan tinggi.

3. Rangkuman Media Jaringan (Nirkabel dan Fiber Optik)
   a. Jaringan nirkabel merupakan salah satu teknologi atau model komunikasi data yang berkaitan dengan komunikasi antar sistem komuputer tanpa menggunakan kabel. Jaringan nirkabel ini sering dipakai untuk jaringan komputer, baik pada jarak yang dekat (beberapa meter, memakai alat/pemancar bluetooth) maupun pada jarak jauh (lewat satelit). Fiber optik adalah suatu jenis kabel yang terbuat dari kaca atau plastik yang sangat halus, dan digunakan sebagai media transmisi karena dapat mentransmisikan sinyal cahaya dari suatu lokasi ke lokasi lainnya dengan kecepatan tinggi.
   b. Teknologi jaringan nirkabel (wireless) dapat diklasifikasikan berdasarkan beberapa kriteria, yaitu berdasarkan topologi jaringan, topologi Ad-hoc, dan topologi infrastruktur.
   c. Pembuatan kabel jaringan fiber optik terbilang sangat rumit, karena dilakukan dengan cara menarik bahan dasar berupa kaca yang telah dicairkan hingga kental dan akhirnya diperoleh serabut atau serat kaca dengan penampang tertentu.
   d. Kabel jaringan fiber optik terdiri atas beberapa jenis, yaitu Single Mode, dan Multimode.
   e. Tipe-tipe kabel fiber optik adalah Single mode, Grade index multimode, dan Step-index multimode.

4. Rangkuman Manajemen Bandwidth

Bandwidth adalah suatu ukuran dari banyaknya informasi yang dapat mengalir dari suatu tempat ke tempat lain (dari source ke destination) dalam waktu tertentu biasanya dalam hitungan detik (Futri, 2017). Dengan kata lain bandwidth adalah kapasitas maksimum dari suatu jalur komunikasi yang dapat dipakai untuk mentransfer data dalam hitungan detik. Bandwidth dapat dipakai untuk mengukur, baik aliran data analog maupun aliran data digital. Satuan yang digunakan untuk bandwidth digital adalah bps (bit per second). Ini berarti jumlah bit yang dapat mengalir tiap detik melalui suatu media transmisi (kabel maupun nirkabel).

Throughput adalah bandwidth yang sebenarnya (aktual) yang diukur dengan satuan waktu tertentu dan pada kondisi jaringan tertentu yang digunakan untuk melakukan transfer file dengan ukuran tertentu. Bandwidth adalah batas maksimal, sedangkan throughput adalah data sebenarnya yang mengalir pada media transmisi (Kemendikbud, 2014).

Terdapat dua jenis bandwidth, yaitu bandwidth digital dan bandwidth analog. Bandwidth digital, yaitu jumlah atau volume data yang dapat dikirimkan melalui sebuah saluran komunikasi dalam satuan bits per second tanpa distorsi. Sedangkan bandwidth analog, yaitu perbedaan antara frekuensi terendah dengan frekuensi tertinggi dalam sebuah rentang frekuensi yang diukur dalam satuan Hertz (Hz) atau siklus per detik, yang menentukan berapa banyak informasi yang bisa ditransimisikan dalam satu saat.

Manajemen bandwidth adalah pengalokasian yang tepat dari suatu bandwidth untuk mendukung kebutuhan atau keperluan aplikasi atau suatu layanan jaringan. Pengalokasian bandwidth yang tepat dapat menjadi salah satu metode dalam memberikan jaminan kualitas suatu layanan jaringan Quality of Service (QoS).

Quality of Service (QoS) merupakan mekanisme jaringan yang memungkinkan aplikasi-aplikasi atau layanan dapat beroperasi sesuai dengan yang diharapkan (Bunafit, 2005).

Terdapat dua teknik manajemen bandwidth yang banyak digunakan di lapangan, yaitu, Hierarchical Token Bucket (HTB) dan Class-Based

Queueing (CBQ). Hierarchical Token Bucket (HTB) adalah metode yang berfungsi untuk mengatur pembagian bandwidth. Pembagian dilakukan secara hirarki yang dibagi-bagi ke dalam kelas sehingga mempermudah pengaturan bandwidth. CBQ membagi pengguna traffic ke dalam hirarki class berdasarkan IP Address, protokol dan tipe aplikasi.

Manajemen bandwidth merupakan implementasi dari proses mengantrikan data, sehingga fungsi manajemen bandwidth pada RouterOS Mikrotik disebut dengan istilah queue. Secara garis besar, ada dua metode queue pada RouterOS Mikrotik yaitu Simple Queue dan Queue Tree (Citraweb Solusi Teknologi). Simple Queue merupakan metode manajemen bandwidth termudah yang ada di RouterOS Mikrotik untuk membatasi bandwidth berdasarkan alamat IP tertentu. Queue Tree digunakan untuk melakukan pembagian bandwidth berdasarkan protokol, port, kelompok alamat IP, dan lain-lain.

Load balancing adalah teknik untuk mendistribusikan beban trafik pada dua atau lebih jalur koneksi secara seimbang, agar trafik dapat berjalan optimal, dan menghindari overload pada salah satu jalur koneksi (Sumarno & Hasmoro, 2013). load balancing dua jalur koneksi, maka besar bandwidth yang akan didapat menjadi dua kali lipat dari bandwidth sebelum menggunakan load balancing. Hal ini perlu diperjelas, bahwa load balancing tidak akan menambah besar bandwidth yang diperoleh, tetapi hanya bertugas untuk membagi trafik dari kedua bandwidth tersebut agar dapat terpakai secara seimbang.

Ada berbagai metode load balancing, antara lain yaitu: Static Route dengan Address List, Equal Cost Multi Path (ECMP), Nth dan Per Connection Classifier (PCC). Setiap metode load balancing tersebut memiliki kekurangan maupun kelebihan tersendiri, namun lebih dari hal itu yang paling terpenting dalam menentukan metode load balancing apa yang akan digunakan adalah harus terlebih dahulu mengerti karakteristik dari jaringan yang akan diimplementasikan.

5. Rangkuman Keamanan Jaringan

Keamanan jaringan (Network Security) adalah suatu cara atau suatu sistem yang digunakan untuk memberikan proteksi (perlindungan) dalam jaringan komputer. Dalam jaringan komputer sangat penting dilakukan untuk memonitor akses jaringan dan mencegah penyalahgunaan sumber daya jaringan yang tidak sah.

a. Resiko Keamanan Jaringan
   1) Keamanan yang bersifat fisik (physical security) termasuk akses orang ke gedung, peralatan, dan media yang digunakan diantaranya wiretapping, denial of service dan syn flood attack.
   2) Keamanan yang berhubungan dengan orang (personal), diantaranya username dan password, profil pemakai dan pengelola,
   3) Keamanan dari data dan media serta teknik komunikasi
   4) Keamanan dalam operasi

b. Tujuan keamanan jaringan terdiri atas ,
   1) *Privacy* / *Confidentiality* adalah menjaga informasi dari orang yang tidak berhak mengakses,
   2) Integrity adalah informasi tidak boleh diubah tanpa seijin pemilik informasi.
   3) Authentication adalah metode untuk menyatakan bahwa informasi betul-betul asli, atau orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud,
   4) Availability adalah berhubungan dengan ketersediaan informasi ketika dibutuhkan,
   5) *Access Control* adalah cara pengaturan akses kepada informasi dan
   6) Non-repudiation adalah aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi.

c. Jenis-Jenis Ancaman Pada Sistem Keamanan Jaringan
   1) Memaksa masuk dan kamus password , Brute Force and Dictionary, serangan ini dilakukan dengan upaya masuk ke dalam jaringan dengan menyerang database password atau menyerang login prompt yang sedang aktif.

2) Denial of Services (DoS) adalah salah satu ancaman keamanan jaringan yang membuat suatu layanan jaringan menjadi terblokir
3) Smurf Attack terjadi ketika sebuah server digunakan untuk membanjiri korban dengan data sampah yang tidak berguna.
4) Ping of Death, adalah serangan ping yang oversize.
5) Stream Attack terjadi saat banyak jumlah paket yang besar dikirim menuju ke port pada sistem korban menggunakan sumber nomor yang random
6) Spoofing adalah Serangan dengan cara menjelma menjadi sesuatu yang lain.
7) Man-in-the-middle (serangan pembajakan) terjadi saat user perusak dapat memposisikan diantara dua titik link komunikasi.
8) Spam sering kita definisikan sebagai email sampah yang tak diundang, newsgroup, atau pesan diskusi forum. Spam bisa merupakan iklan dari vendor atau bisa berisi kuda Trojan.
9) Sniffer (atau dikenal sebagai snooping attack) merupakan kegiatan user perusak yang ingin mendapatkan informasi tentang jaringan atau traffic lewat jaringan tersebut.
10) Crackers adalah user perusak yang bermaksud menyerang suatu system atau seseorang.

d. Beberapa cara yang dapat Anda lakukan untuk mengamankan diri dari kejahatan yang ada pada sistem keamanan jaringan adalah sebagai berikut
   1) Keamanan fisik ini berarti keamanan yang nampak seperti komputer, laptop, dan sebagainya.
   2) Keamanan lokal berarti keamanan yang berkaitan dengan user dan hak-haknya.
   3) Keamanan file dan system file adalah keamanan yang berkaitan dengan file data yang ada pada OS Windows ataupun LINUX.
   4) Keamanan password dan enkripsi adalah keamanan yang berkaitan dengan penggunaan password pada system ataupun terhadap file.
   5) Keamanan kernel adalah keamanan yang berkaitan dengan penggunaan operating system yang terbaru.

6) Keamanan jaringan adalah keamanan yang berkaitan dengan penggunaan jaringan saat melakukan suatu aktivitas

e. Firewall

Firewall didefinisikan sebagai sebuah komponen atau kumpulan komponen yang membatasi akses antara sebuah jaringan yang diproteksi dan internet, atau antara kumpulan kumpulan jaringan lainnya. Definisi lain mengatakan bahwa, firewall adalah sebuah computer yang memproteksi jaringan dari jaringan yang tidak dipercaya yang memisahkan antara jaringan local dengan jaringan publik, dengan melakukan metode filtering paket data yang masuk dan keluar.

f. Fungsi Firewall

Firewall sendiri memiliki beberapa fungsi untuk melindungi jaringan komputer yang dapat dijabarkan dalam beberapa poin berikut:

1) Sebagai pos keamanan jaringan.
2) Mencegah informasi berharga bocor tanpa sepengatahuan.
3) Mencatat aktivitas pengguna.
4) Memodifikasi paket data yang datang.
5) Mencegah modifikasi data pihak lain.

g. Cara Kerja Firewall

Pada dasarnya, firewall bekerja dengan cara membatasi komputer pribadi dengan internet. Firewall bekerja layaknya penjaga keamanan di depan gerbang rumah dan mengidentifikasi pengunjung yang datang, sekaligus menyaring penyusup yang berusaha memasuki komputer pribadi. Firewall bekerja seperti garda pertahanan terdepan untuk menahan segala usaha hacking yang masuk ke dalam komputer. Firewall mampu menyaring data yang masuk dengan mengidentifikasi terlebih dahulu pesan konten yang dibawanya.