# BAB II

# LANDASAN TEORI

## 2.1. Tinjauan Jurnal

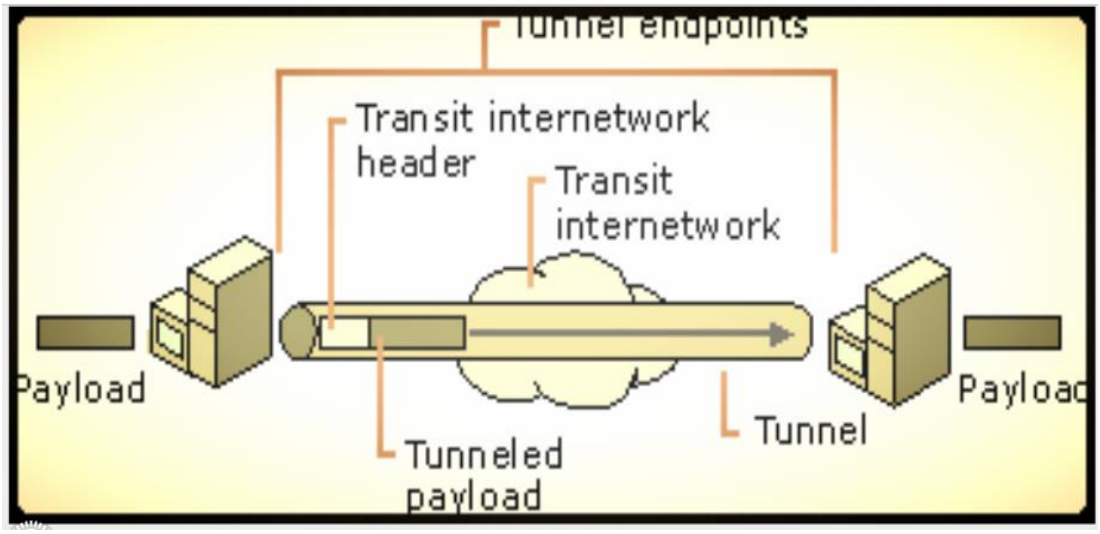
Menurut Trihadi;dkk (2008:26) "*Tunnels* yaitu merupakan hubungan *point-to-point* secara virtual yang melewati jaringan publik seperti internet".

> Sedangkan menurut Cahyadi (2010:52) menjelaskan bahwa:
> *Ethernet over IP* (EoIP) Merupakan protocol pada Mikrotik RouterOS yang berfungsi untuk membangun sebuah Network Tunnel antar MikroTik router di atas sebuah koneksi TCP/IP.EoIP merupakan protokol proprietary MikroTik (support juga di linux tetapi harus di-compile manual). Maka untuk menggunakan fitur ini, router di kantor pusat dan router di kantor cabang harus sama - sama menggunakan router MikroTik. EoIP menggunakan Protocol GRE (RFC1701).

Fitur tunneling dengan EoIP dapat dimanfaatkan untuk membuat bridging antar perangkat Mikrotik Router OS untuk menghubungkan dua atau lebih kantor suatu organisasi/lembaga melalui jaringan (publik *network / internet*), sehingga seolah-olah kantor-kantor tersebut terhubung dalam satu segmen jaringan intranet. Dalam aspek keamanan, walau EoIP tidak memberlakukan enkripsi seperti VPN-IP, namun administrator dapat mengaktifkan fungsi *firewall / filtering* dan monitoring pada interface-interface EoIP.

*Ethernet over IP* (EoIP) hanya bisa digunakan pada router Mikrotik dan tidak dapat dijalankan pada router lainnya. Syarat utama yang harus ada di EoIP Tunnel adalah mempunyai IP Publik statis dan membuat Tunnel ID yang samauntuk identitas EoIP Tunnel tersebut. Mikrotik mampu membuat tunnel menggunakan EoIP maksimum sebanyak 65535.

Cara kerja EoIP tunneling dengan membungkus dan mengenkapsulasi data dalam header tambahan. Header tambahan tersebut berisi tentang informasi routing sehingga data frame yang dikirim dapat sampai ketujuan.




Gambar II.1. Cara Kerja EoIP Tunnel

## 2.2. Konsep Dasar Jaringan

Dengan semakin berkembangnya kebutuhan pengolahan data dan informasi, di dalam sebuah perusahaan dibutuhkan beberapa komputer yang digunakan oleh banyak orang yang bekerja dalam sebuah tim. Untuk saling bertukar data dan informasi, maka komputer-komputer yang digunakan akan terhubung antara satu dengan yang lainnya. Kumpulan komputer yang saling terhubung disebut sebagai jaringan komputer.

Menurut Arifin (2011:9) menyimpulkan bahwa ”Jaringan komputer merupakan kumpulan dari beberapa komputer yang dihubungkan satu dengan lainnya dengan menggunakan protokol komunikasi. Jaringan ini memerlukan media transmisi tertentu untuk dapat saling berbagi informasi, program, dan penggunaan bersama perangkat keras”.

Menurut Sofana (2013:4-5), Berdasarkan skala atau area, Jaringan komputer dapat terbagi menjadi 4, yaitu:

**1. *Local Area Network* (LAN)**

*Local Area Network* (LAN) adalah jaringan lokal yang dibuat pada area terbatas. Misalnya dalam satu gedung atau dalam satu ruangan. Kadang kala jaringan lokal disebut juga jaringan personal atau privat. LAN biasa digunakan pada sebuah jaringan kecil yang menggunakan *resource* secara bersama, seperti penggunaan *printer* secara bersama, penggunaan media penyimpanan secara bersama, dan sebagainya.

**2. *Metropolitan Area Network* (MAN)**

*Metropolitan Area Network* (MAN) menggunakan metode yang sama dengan LAN namun daerah cakupannya lebih luas. Daerah cakupan MAN bisa satu RW, beberapa kantor yang berada dalam komplek yang sama, satu atau beberapa desa, satu atau beberapa kota. Dapat dikatakan MAN merupakan pengembangan dari LAN.

**3. *Wide Area Network* (WAN)**

*Wide Area Network* (WAN) cakupannya lebih luas daripada MAN. Cakupan WAN meliputi satu kawasan, satu negara, satu pulau, bahkan satu dunia. Metode yang digunakan WAN hampir sama dengan LAN dan MAN. Umumnya WAN dihubungkan dengan jaringan telepon digital. Namun media transmisi lain pun dapat digunakan.

**4. *Internet***

*Internet* adalah interkoneksi jaringan komputer skala besar (mirip WAN), yang dihubungkan menggunakan protokol khusus. Jadi sebenarnya *Internet*

merupakan bagian dari WAN. Cakupan *Internet* adalah satu dunia bahkan tidak menutup kemungkinan antar planet. Koneksi antar jaringan komputer dapat dilakukan berkat dukungan protokol yang khas, yaitu TCP/IP (*Transmission Control Protocol/Internet Protocol*).

Tabel di bawah dapat digunakan untuk sekadar memberikan gambaran berapa kira-kira luas area LAN, MAN, WAN dan *Internet*.

Tabel II.1 Jaringan Komputer Berdasarkan Area

| **Jarak/cakupan (meter)** | **Contoh** | **Jenis** |
|---|---|---|
| 10-100 | Ruangan | LAN |
| 100-1.000 | Gedung | LAN |
| 1000-10.000 | Kampus | LAN |
| 10.000-100.000 | Kota | MAN |
| 100.000-1.000.000 | Negara | WAN |
| 1.000.000-10.000.000 | Benua | WAN |

Sumber: Sofana (2013:5)

Menurut Sofana (2013:7), Berdasarkan pola operasi atau fungsinya, jaringan komputer dapat dibagi menjadi 2 jenis, yaitu:

***1. Client Server***

*Client Server* adalah jaringan komputer yang mengharuskan salah satu (atau lebih) komputer difungsikan sebagai *server* atau *central*. *Server* melayani komputer lain yang disebut *client*. Layanan yang diberikan bisa berupa akses *Web, e-mail, file,* atau yang lain. *Client Server* banyak dijumpai pada jaringan Internet. Namun LAN atau jaringan lain pun bisa mengimplementasikan *client server*. Hal ini sangat bergantung pada kebutuhan masing-masing.

### *2. Peer to Peer*

*Peer to Peer* adalah jaringan komputer dimana setiap komputer bisa menjadi *server* sekaligus *client*. Jadi tidak ada komputer yang "lebih utama" dibandingkan komputer lain. Setiap komputer dapat menerima dan memberikan *access* dari/ke komputer lain. *Peer to Peer* banyak diimplementasikan pada LAN. Walaupun dapat juga diimplementasikan MAN, WAN, atau Internet. Namun kurang lazim. Salah satu alasannya adalah masalah manajemen dan *security*. Cukup sulit menjamin *security* pada jaringan *peer to peer* manakala pengguna komputer sudah sangat banyak.

## 2.3. Manajemen Jaringan

Manajemen Jaringan adalah sebuah fungsi pengawasan terhadap kinerja jaringan dan pengambilan tindakan untuk mengendalikan aliran trafik agar kapasitas pengoperasian pada sebuah jaringan dapat di lakukan secara maksimal**.** Model manajemen jaringan OSI mengkategorikan lima bagian fungsi, dikenal sebagai model FCAPS.

### 2.3.1. *Fault Management* (Kesalahan Manajemen)

*Fault Management* adalah kegiatan yang dilakukan untuk memelihara pelayanan jaringan secara dinamis.

Mekanisme:

a) Mendeteksi dan mengidentifikasi kesalahan yang timbul (*trace faults and maintain error logs*)
b) Mengisolasi sebab dari kesalahan
c) Mendiagnosa kesalahan (*diagnostic tests*)

d) Mengkoreksi kesalahan (*correct faults*)

### *2.3.2. Configuration Management*

Manajemen konfigurasi adalah Kegiatan yang menyediakan fungsi untuk memonitor dan mengenali unsur jaringan (*Network Element* – NE), mengambil dan memberikan data dari atau ke NE.sehingga perangkat jaringan dapat dikelola dengan baik. Manajemen Konfigurasi meliputi :

a) Perencanaan Jaringan dan Rekayasa
b) Instalasi
c) Pengendalian dan Status
d) Penyediaan (*Provisioning*)
e) Menyimpan imformasi konfigurasi (dokumentasi)
f) Perencanaan dan Negosisi Layanan

### *2.3.3. Accounting Management*

Menyediakan fungsi yang memungkinkan untuk dilakukannya pengukuran layanan jaringan serta penentuan biaya penggunaannya.

Fungsinya meliputi:

a) Pengukuran pemakaian
b) Pentarifan
c) Penagihan
d) Keuangan
e) Pengendalian perusahaan.

### *2.3.4. Performance Management*

Performance Management adalah kegiatan yang dilakukan untuk menilai indikator unjuk kerja dari operasi jaringan secara berkesinambungan. Dengan adanya manajemen performance diharapkan

*a)* Tingkat pelayanan dapat dipertahankan – *Optimize QoS (Quality of service)*

b) Kondisi jaringan dapat dikenali

c) Kemungkinan gangguan dapat diprediksi

d) Dapat membuat laporan yang lengkap untuk kegiatan pengambilan keputusan dan perencanaan

### *2.3.5. Security Management*

*Security Management* adalah kegiatan yang dilakukan untuk mengamankan jaringan yang ada

a) Membatasi akses pengguna terhadap perangkat jaringan (autentifikasi dan otorisasi)

b) Mencegah kebocoran keamanan (enkripsi)

c) Pengaturan *Firewall*

*d) Security Logs*

## 2.4. Konsep Penunjang Usulan

### 2.4.1. VPN (*Virtual Private Network*)

Menurut Sofana (2013:536) “VPN merupakan sebuah model jaringan yang dapat menghubungkan beberapa LAN yang lokasinya berjauhan. Media

yang digunakan untuk menghubungkan antar lokasi adalah media jaringan publik".

Menurut IETF, *Internet Engineering Task Force* VPN merupakan suatu bentuk *private internet* yang melalui *public network* (*internet*), dengan menekankan pada keamanan data dan akses global melalui *internet*. Hubungan ini dibangun melalui suatu *tunnel* (terowongan) virtual antara dua *node*.

Teknonologi VPN menyediakan tiga fungsi utama untuk penggunaanya, yaitu *Confidentially* (Kerahasiaan), *Data Integrity* (Keutuhan Data/Keaslian Data) dan *Origin Authentication* (Autentikasi Sumber).

**1. *Confidentially* (Kerahasiaan)**

Teknologi VPN memiliki sistem kerja mengenkripsi semua data yang lewat melaluinya. Dengan adanya teknologi enkripsi ini, maka kerahasiaan data menjadi lebih terjaga. Walaupun ada pihak yang dapat menyadap data yang melewati *internet* bahkan jalur VPN itu sendiri, namun belum tentu dapat membaca data tersebut, karena data tersebut telah teracak. Dengan menerapkan sistem enkripsi ini, tidak ada satupun orang yang dapat mengakses dan membaca isi jaringan data dengan mudah.

**2. *Data* Intergrity (Keutuhan Data/Keaslian Data)**

Ketika melewati jaringan *internet*, sebenarnya data telah bejalan sangat jauh melintasi berbagai negara. Pada saat perjalanan tersebut, berbagai gangguan dapat terjadi terhadap isinya, baik hilang, rusak, ataupun dimanipulasi oleh orang yang tidak seharusnya. Teknologi VPN akan menjaga keaslian data dengan memastikan data yang sampai masih tetap sama seperti ketika dikirimkan.

### 3. *Origin Authentication* (Autentikasi Sumber)

Teknologi VPN memiliki kemampuan untuk melakukan autentikasi terhadap sumber-sumber pengirim data yang akan diterimanya. VPN akan melakukan pemeriksaan terhadap semua data yang masuk dan mengambil informasi dari sumber datanya. Kemudian alamat sumber data tersebut akan disetujui apabila proses autentikasinya berhasil. Dengan demikian, VPN menjamin semua data yang dikirim dan diterima berasal dari sumber yang seharusnya. Tidak ada data yang dipalsukan atau dikirim oleh pihak-pihak lain.

Tipe-tipe VPN secara garis besar, yaitu *Remote Access* VPN dan *Site to site* VPN.

### 1. *Remote Access* VPN

*Remote Access* juga dikenal sebagai *Virtual Private Dial-Up Network* (VPDN), merupakan koneksi *user-to-LAN* yang digunakan sebuah perusahaan untuk para pekerjanya yang membutuhkan koneksi ke jaringan mereka dari berbagai lokasi *remote*. *Remote Access* VPN memungkinkan pekerja untuk mengakses data-data dan segala sumber daya dimanapun mereka berada.

### 2. Site to Site VPN

Site to site VPN memungkinkan suatu *private network* diperluas melintasi jaringan *internet* atau layanan *public network* lainnya dengan cara yang aman. *Site to site* VPN merupakan suatu alternatif dari infrastruktur WAN yang bisa menghubungkan kantor-kantor cabang, kantor pusat, maupun *partner* bisnis ke dalam seluruh jaringan yang ada dalam perusahaan.

*Site to site* VPN dibedakan menjadi 2 bagian yaitu:

a. *Internet* VPN

Biasa digunakan untuk menghubungkan antara kantor pusat dan kantor cabang yang letaknya berjauhan melalui suatu *public* infrastruktur.

b. *Extranet* VPN

Biasanya digunakan untuk menghubungkan suatu perusahaan dengan perusahaan lain misalnya penjual, partnet bisnis, dll. Dengan adanya *extranet* VPN perusahaan-perusahaan yang terlibat dapat berkomunikasi serta bertukar informasi secara cepat, mudah, tapi dalam sistem keamanan yang terjamin.

Beberapa fitur keamanan yang ada dalam VPN, yaitu Enkripsi dan Tunneling.

**1. Enkripsi**

Merupakan salah satu metode yang digunakan untuk mengubah data asli menjadi bentuk sandi (*chipper text*) yang mana sandi-sandi tersebut hanya dapat dimengerti oleh pihak pengirim dan penerima data, sehingga data tersebut tidak dapat dibaca oleh orang luar yang tidak memiliki hak akses terhadap data tersebut.

***2. Tunneling***

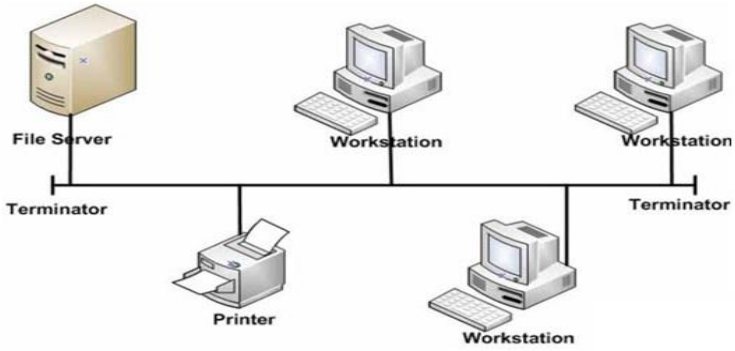
Teknologi *tunneling* merupakan teknologi yang bertugas untuk menangani dan menyediakan koneksi *point to point* dati sumber ke tujuannya. Disebut *tunnel* karena koneksi *point to point* tersebut sebenarnya terbentuk melewati jaringan umum, namun seolah-olah koneksi tersebut menjadi bersifat *private* karena tidak mempedulikan paket-paket data milik orang lain yang sama-sama menggunakan jalur tersebut.

### 2.4.2. Topologi

Topologi jaringan adalah suatu aturan atau cara untuk menghubungkan komputer yang satu dengan komputer yang lainnya sehingga membentuk suatu jaringan. Topologi jaringan juga dapat didefinisikan sebagai gambaran secara fisik dari pola hubungan antara komponen jaringan, yang meliputi *Server*, *Workstation*, Hub, dan pengkabelannya.

**1) Topologi Bus**

> Daryanto (2010:30) dalam tulisannya menyimpulkan bahwa: Topologi bus diimplementasikan dengan menggunakan media fisik berupa kabel koaksial. Topologi ini umumnya digunakan untuk jaringan komputer yang terhubung secara sederhana sehingga komputer-komputer yang terlibat di dalamnya bisa berkomunikasi satu sama lainnya. Realisasi dari topologi bus ini adalah sebuah jalur utama yang menjadi penghubung antar komputer.




Sumber: http://feriantono.com

Gambar II.2. Topologi Bus

Keunggulan Topologi Bus:

a. Penggunaan kabel sedikit, sehingga terlihat sederhana dan hemat biaya.
b. Pengembangan menjadi mudah.

Kelemahan Topologi Bus:

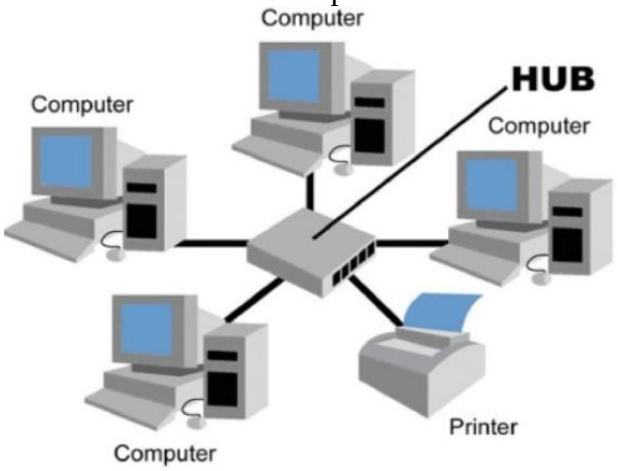
a. Jaringan akan terganggu bila salah satu komputer rusak.
b. Jika tingkat lalu-lintas data tinggi dapat menyebabkan kemacetan.

c. Membutuhkan *Repeater* untuk jarak jaringan yang terlalu jauh (jika menggunakan kabel *coaxial*).

d. Bila terjadi gangguan yang terlalu serius, maka proses pengiriman data menjadi lambat karena lalu lintas jaringan penuh dan padat akibat tidak ada pengontrol *User*.

**2) Topologi Star**

Daryanto (2010:32) dalam tulisannya menyimpulkan bahwa: Topologi model ini didesain dimana setiap node (*fileserver*, *workstation*, dan perangkat lainnya) terkoneksi ke jaringan melewati sebuah hub atau *concentrator*. Data yang terkirim ke jaringan akan melewati *Hub/concentrator* sebelum melanjutkan ke tempat tujuannya. *Hub* ataupun concentrator akan mengatur dan mengontrol keseluruhan fungsi jaringan. Dia juga bertindak sebagai *repeater*/penguat aliran data. Konfigurasi pada jaringan model ini menggunakan kabel *Twisted pair*, dan dapat digunakan bersama kabel koaksial atau fiber optik.




Sumber: http://www.aldo-expert.com

Gambar II.3. Topologi Star

Keunggulan Topologi Star:

a. Fleksibel dalam hal pemasangan jaringan baru, tanpa mempengaruhi jaringan yang sudah ada sebelumnya.

b. Bila salah satu kabel koneksi *User* putus, maka hanya komputer *User* yang bersangkutan saja yang tidak berfungsi dan tidak mempengaruhi *User* yang lain (keseluruhan hubungan jaringan masih tetap bekerja).

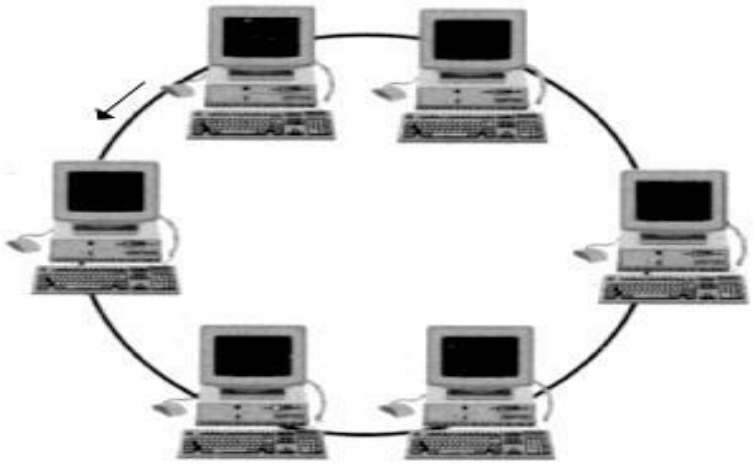
Kelemahan Topologi Star:

a. Boros dalam pemakaian kabel, jika dihubungkan dengan jaringan yang lebih besar dan luas.

b. Bila pengiriman data secara bersamaan waktunya, dapat terjadi bentrokan data.

**3) Topologi Ring**

Athaillah (2013:10) menyimpulkan bahwa: Topologi ini adalah jaringan komputer yang dibentuk seperti lingkaran atau dalam bahasa Inggris disebut Ring, dimana komputer dalam topologi jaringan ini terhubung masing-masing di dua titik dari komputer lainnya. Pada tipe Topologi Ring ini masing-masing node atau komputer dapat menjadi Repeater yang memperkuat sinyaldi sepanjang sirkulasi.



Sumber: http:// rudinazar.com

Gambar II.4. Topologi Ring

Keuntungan dari topologi jaringan ini antara lain adalah tingkat kerumitan jaringan rendah (sederhana). Topologi ini sering digunakan untuk jaringan yang luas pada satu kota dengan menggunakan media transmisi kabel fiber,

misalnya untuk menghubungkan beberapa ISP pusat dan cabang dalam satu kota.

Keunggulan Topologi Ring:

a. Hemat kabel.
b. Untuk membangun jaringan dengan topologi ini lebih murah bila dibandingkan dengan topologi Star.

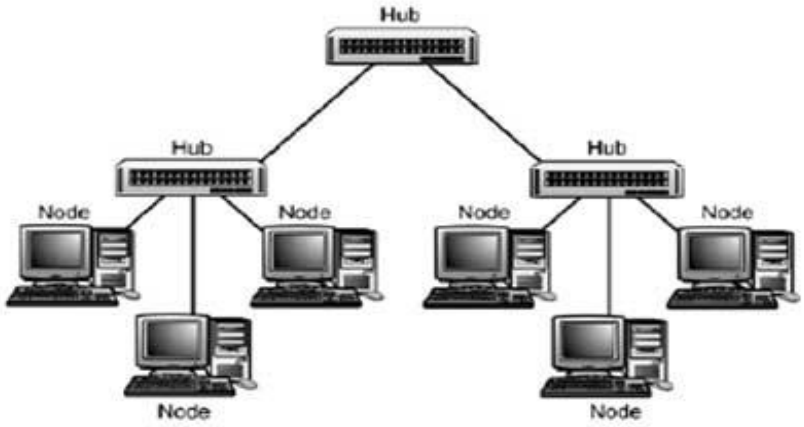
Kelemahan Topologi Ring:

a. Sangat peka terhadap kesalahan jaringan.
b. Sukar untuk mengembangkan jaringan, sehingga jaringan tersebut menjadi kaku.
c. Biaya pemasangan lebih besar.

**4) Topologi Tree**

Athaillah (2013:15) dalam bukunyamendefinisikan bahwa ”Topologi Tree atau Topologi pohon adalah penggabungan dari dua Topologi sebelumnya, yaitu Topologi Bus dan Topologi Star atau bintang”.

Bentuk dari topologi ini adalah sekelompok node yang terhubung satu sama lainnya dengan menggunakan Topologi Star, kemudian kelompok node dalam jaringan Topologi Star tersebut terhubung ke kelompok jaringan yang lain dengan menggunakan Topologi Bus. Topologi model ini biasanya digunakan pada jaringan komputer yang sangat luas, salah satunya adalah jaringan internet.




Sumber: http://jaringan-komputer.cv-sysneta.com

Gambar II.5. Topologi Tree

Keunggulan topologi Tree:

a. Mudah dalam pengembangan jaringan.
b. Mudah dalam mendeteksi kerusakan.
c. Jika salah satu kabel sub-Node, maka sub-Node yang lain tidak akan terganggu.

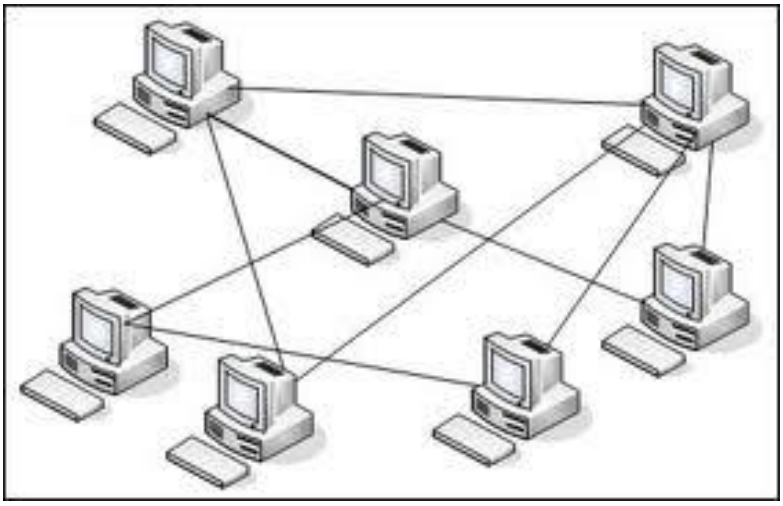
Kelemahan topologi Tree:

a. Jika salah satu konsentrator atau sentral Node mengalami kerusakan, maka sub Node yang ada dibawahnya akan terganggu.

**5) Topologi Mesh**

Daryanto (2010:34) berpendapat bahwa ”Topologi ini disebut sebagai jaring, karena setiap komputer akan berhubungan pada tiap-tiap komputer lain yang tersambung”.

Topologi Mesh biasanya digunakan pada *Internet Service Provider* (ISP) untuk memastikan bila terjadi kerusakan pada salah satu komputer maka tidak akan mengganggu hubungan jaringan dengan komputer lain dalam jaringan.



Sumber: http://kopihijau.info

Gambar II.6. Topologi Mesh

Keunggulan topologi Mesh:

a. Topologi Mesh memiliki tingkat *Redundancy* yang tinggi, sehingga jika terdapat satu *Link* yang rusak maka suatu Node (*Station*) dapat mencari *Link* yang lainnya.

Kelemahan topologi Mesh:

a. Membutuhkan biaya yang cukup besar, karena membutuhkan banyak kabel, setiap Node harus dipasang LAN *Card* sebanyak n-1 (n=Jumlah Node).

b. Jaringan ini tidak praktis.

### 2.4.3. IP Address

#### 1) Model TCP/IP

Rizal Rahman (2013:3) menyimpulkan bahwa ”*Transmission Control Protocol and Internet Protocol* adalah sebuah aturan standar yang digunakan untuk komunikasi antar berbagai jenis komputer yang terhubung dalam sebuah jaringan komputer”.

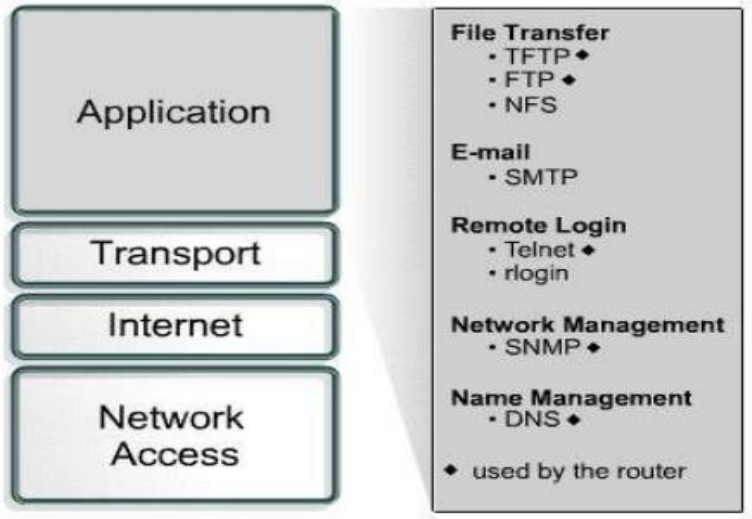
*Transmission Control Protocol and Internet Protocol* memiliki Beberapa keunggulan , antara lain:

a) *Open Protocol Standard*, yaitu tersedia secara bebas dan dikembangkan independen terhadap komputer hardware ataupun sistem operasi apapun. Karena didukung secara meluas di dunia komunikasi, TCP/IP sangat ideal untuk menyatukan bermacam *hardware* dan *software*, walaupun tidak berkomunikasi lewat internet bisa pada jaringan lokal.

b) Independen dari *physical network hardware*, ini menyebabkan TCP/IP dapat mengitegrasikan bermacam, *network*, baik melalui *ethernet*, *token ring*, *dial-up*,X.25/AX.25 dan media transmisi fisik lainnya.

c) Skema pengalamatan yang umum menyebabkan *device* yang menggunakan TCP/IP dapat menghubungi alamat device–device lain diseluruh *network*, bahkan internet sekalipun.

d) *High level protocol standard*, yang dapat melayani *user* secara luas.




Sumber: Musajid (2013:6)

Gambar II.7. Model layer TCP/IP

Menurut Musajid (2013:4) “TCP/IP didefinisikan sebagai koleksi (suit) protokol jaringan yang berperan dalam membangun lingkungan jaringan global seperti Internet”.

Nama TCP/IP diambil dari dua 'keluarga' protokol fundamental, yaitu TCP dan IP. Meskipun demikian suit masih memiliki protokol utama lainnya, seperti UDP dan ICMP. Protokol bekerja sama dalam memberikan *framework networking* yang digunakan oleh banyak protokol aplikasi berbeda , dimana masing-masing digunakan untuk tujuan berbeda.

***2) Subnetting***

Musajid (2013:15) memberikan penjelasan bahwa ”Subnetting adalah cara membagi satu jaringan menjadi beberapa sub jaringan”.

Beberapa bit dari bagian host ID dialokasikan menjadi bit tambahan pada bagian network ID. Cara ini menciptakan sejumlah Network ID tambahan dan mengurangi jumlah maksimum *host* yang ada dalam tiap jaringan tersebut. Jumlah bit yang dipindahkan ini dapat bervariasi yang ditentukan oleh nilai *subnetmask*. Sebagai contoh, *network* ID kelas B yaitu172.16.0.0, *subnetting* dapat dilakukan dengan cara sebagai berikut.

Tabel II.2 Address kelas B (sebelum *subnetting*)

| Network ID | Network ID | Host ID | Host ID |
|---|---|---|---|
| 172 | 16 | 0 | 0 |

Sumber: Musajid (2013:15)

Tabel II.3 Address kelas B (setelah *subnetting*)

| Network ID | Network ID | Host ID | Host ID |
|---|---|---|---|
| 172 | 16 | 2 | 0 |

Sumber: Musajid (2013:16)

Beberapa alasan membangun *subnetting* adalah mereduksi *traffik* jaringan. Alasan utama menggunakan subnetting yaitu untuk mereduksi ukuran *broadcast* domain.

1. Mengoptimasi penggunaan jaringan.
2. Memudahkan manajemen
3. Mengefektifkan jaringan yang dibatasi area geografis yang luas.

Sebuah hal yang harus diketahui untuk melakukan *subnetting* adalah mengingat nilai dari bit-bit *subnet mask*. Nilai ini yang akan dijadikan panduan dalam proses *subnetting*.

Perhatikan tabel dibawah ini.

Tabel II.4 Bit-bit *subnet mask*

| **128** | **64** | **32** | **16** | **8** | **4** | **2** | **1** | | |
|---|---|---|---|---|---|---|---|---|---|
| **2^7** | **2^6** | **2^5** | **2^4** | **2^3** | **2^2** | **2^1** | **2^0** | | |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | = | 128 |
| 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | = | 192 |
| 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | = | 224 |
| 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | = | 240 |
| 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | = | 248 |
| 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | = | 252 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | O | = | 254 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | = | 255 |

Sumber: Musajid (2013:17)

Berdasarkan tabel diatas nilai *subnet mask* yang digunakan untuk *Subnetting* adalah 128, 192, 224, 240, 240, 248, 252, 254, dan 255.

Tabel II.5 Nilai *subnet mask* yang mungkin untuk *subnetting*

| Subnet Mask | CIDR | Subnet Mask | CIDR |
|---|---|---|---|
| 255.128.0.0 | /9 | 255.255.240.0 | /20 |
| 255.192.0.0 | /10 | 255.255.248.0 | /21 |
| 255.224.0.0 | /11 | 255.255.252.0 | /22 |
| 255.240.0.0 | /12 | 255.255.254.0 | /23 |
| 255.248.0.0 | /13 | 255.255.255.0 | /24 |
| 255.252.0.0 | /14 | 255.255.255.128 | /25 |

| | | | |
|---|---|---|---|
| 255.254.0.0 | /15 | 255.255.255.192 | /26 |
| 255.255.0.0 | /16 | 255.255.255.224 | /27 |
| 255.255.128.0 | /17 | 255.255.255.240 | /28 |
| 255.255.192.0 | /18 | 255.255.255.248 | /29 |
| 255.255.224.0 | /19 | 255.255.255.252 | /30 |

Sumber: Musajid (2013:18)

Contoh *subnetting* kelas C

Apabila sebuah network ID 192.168.10.0/30, maka untuk menentukan kelas dan *subnetmask* dari network ID adalah sebagai berikut:

IP 192.168.10.0 termasuk IP dari kelas C. *Subnetmask* /30 berarti 11111111.11111111.11111111.**111111**00

(128+64+32+16+8+4 =252). Sehingga subnet *mask* adalah 255.255.255.252.

Perhitungan tentang *subnetting* akan terfokus pada 4 hal, jumlah *subnet*, jumlah *host* per *subnet*, blok *subnet*, alamat *host* dan *broadcast* yang valid.

1. Jumlah*subnet*=$2^x$, dimana x adalah banyaknya bit1 padaoktet terahir *subnetmask* (2 oktet terahir untuk kelas B dan 3 oktet terakhir untuk kelas A). Jadi $2^6$ = 64subnet.
2. Jumlah *host* per subnet = $2^3 – 2$, dimana y adalah banyaknya bit 0 pada oktet terakhir subnet. Jadi jumlah *host* per *subnet* adalah $2^2 – 2 = 2$ host.
3. Blok *subnet* = 256–252 (nilai oktet terahir subnet *mask*) = 4. Jadi blok *subnet* lengkapnya adalah 0, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, ...., 252.
4. Alamat *host* dan *broadcast* yang valid dapat dilihat pada tabel di bawah ini. Sebagai catatan, host pertama adalah angka 1 setelah *subnet* dan *broadcast* adalah angka 1 angka sebelum subnet berikutnya.

Tabel II.6 Hasil *subnetting* 192.168.10.0/30

| | | | | |
|---|---|---|---|---|
| Network ID | 192.168.10.0 | 192.168.10.4 | ……. | 192.168.10.252 |
| Host Pertama | 192.168.10.1 | 192.168.10.5 | ……. | 192.168.10.253 |
| Host Terakhir | 192.168.10.2 | 192.168.10.6 | ……. | 192.168.10.254 |
| Broadcast | 192.168.10.3 | 192.168.10.7 | ……. | 192.168.10.255 |

Sumber: Musajid (2013:20)

Dengan konsep dan teknik yang sama, *subnetmask* yang bisa digunakan untuk kelas C adalah sebagai berikut:

Tabel II.7 Subnet *mask* yang dapat digunakan untuk *subnetting* kelas C

| Subnet Mask | CIDR |
|---|---|
| 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 |

Sumber: Musajid (2013:20)

Contoh *subnetting* kelas B

*Subnetmask* yang bisa digunakan untuk *subnetting* kelas B seperti pada tabel di bawah ini.

Tabel II.8 Subnet *mask* yang digunakan *subnetting* kelas B

| Subnet Mask | CIDR | Subnet Mask | CIDR |
|---|---|---|---|
| 255.255.128.0 | /17 | 255.255.255.128 | /25 |
| 255.255.192.0 | /18 | 255.255.255.192 | /26 |
| 255.255.224.0 | /19 | 255.255.255.224 | /27 |
| 255.255.240.0 | /20 | 255.255.255.240 | /28 |
| 255.255.248.0 | /21 | 255.255.255.248 | /29 |
| 255.255.252.0 | /22 | 255.255.255.252 | /30 |
| 255.255.254.0 | /23 | | |
| 255.255.255.0 | /24 | | |

Sumber: Musajid (2013:21)

Contoh *subnetting* kelas B adalah sebagai berikut. Apabila alamat jaringan 172.16.0.0/18, maka *subnetting* dapat dilakukan sebgai berikut:

IP 172.16.0.0/18 merupakan IP kelas B, *subnetmask* /18 berarti:

11111111.11111111.11000000.00000000

(128 + 64 = 192 (Oktet ke 3))

Sehingga *subnet mask* adalah 255.255.192.0.

Perhitungan:

1. Jumlah *subnet* = $2^x$ , dimana x adalah banyak bit 1 pada oktet 2 terakhir. Jadi jumlah *subnet* adalah $2^2 = 4$ subnet.
2. Jumlah *host* per *subnet* adalah $2^y - 2$ , dimana y adalah banyaknya bit 0 pada 2 oktet terakhir. Jadi jumlah *host* per *subnet* adalah $2^{14} - 2 = 16.382$ host.
3. Blok subnet 256 – 192 = 64. Subnet lengkapnya adalah 0, 64, 128 dan 192. Alamat *host* dan *broadcast* yang valid seperti tabel di bawah ini.

Tabel II.9 Hasil *subnetting* 172.16.0.0/18

| | | | |
|---|---|---|---|
| Subnet | 172.16.0.0 | ….. | 172.16.192.0 |
| Host Pertama | 172.16.0.1 | ….. | 172.16.192.1 |
| Host Terakhir | 172.16.63.254 | ….. | 172.16.255.254 |
| Broadcast | 172.16.63.255 | ….. | 172.16.255.254 |

Sumber: Musajid (2013:23)

Contoh *subnetting* kelas A

Konsep *subnetting* kelas A sama dengan kelas B dan C, hanya berbeda oktet mana pada blok subnet yang akan dimainkan. Kalai kelas C dioktet 4, kelas B dioktet 3 dan 4 (2 oktet terakhir), kalai A dioktet2, 3 dan 4 (3 oktet terakhir). Kemudian *subnetmask* yang bisa digunakan untuk *subnetting* kelas A adalah semua *subnetmask* dari CIDR /8 sampai /30.

Contoh alamat jaringan 10.0.0.0/10, maka dapat ditentukan IP 10.0.0.0 tergolong IP kelas A. *Subnetmask* /10 adalah 11111111.11000000.00000000.00000000 (255.192.0.0).

Perhitungan:

1. Jumlah subnet $2^2 = 4$ *subnet*.
2. Jumlah host per subnet $2^{22} – 2 = 4.194.302$ host.
3. Blok subnet 256 – 192 = 64, jadi *subnet* lengkapnya adalah 0, 64, 128, 192.
4. Alamat *host* dan broadcast yang valid seperti tabel dibawah ini.

Tabel II.10 Hasil *subnetting* 10.0.0.0/10

| | | | |
|---|---|---|---|
| Subnet | 10.0.0.0 | ……. | 10.192.0.0 |
| Host Pertama | 10.0.0.1 | ……. | 10.192.0.1 |
| Host Terakhir | 10.0.0.254 | ……. | 10.255.255.254 |
| Broadcast | 10.63.255.255 | ……. | 10.255.255.255 |

Sumber: Musajid (2013:24)