BAB II

LANDASAN TEORI

2.1. Tinjauan Jurnal

Dalam hal penelitian ini penulis menyajikan 2 butir jurnal ilmiah yang terkait dengan permasalahan atau penelitian ini. Berikut penjelasan dari jurnal tersebut:

Menurut Masero (2013:21) Permasalahan yang sering timbul adalah faktor keamanan yang saat ini menjadi hal yang sangat penting untuk diperhatikan. Maka dibutuhkan suatu cara agar dapat memperoleh suatu informasi data, tukar menukar data, dilakukan dengan aman dan stabil. Oleh karena itu VPN diciptakan untuk menyelesaikan permasalahan dalam jaringan yang tidak aman.

> Menurut Triyono (2014:113) Secara Umum, VPN (*virtual private network*) adalah sebuah proses dimana jaringan umum (*public* network atau *internet*) diamankan kemudian difungsikan menjadi sebuah jaringan privat (*private network*). Sebuah VPN tidak didefinisikan oleh rangkaian khusus atau *router*, tetapi didefinisikan oleh mekanisme keamanan dan prosedur-prosedur yang hanya mengijinkan penggunanya yang ditunjuk akses ke VPN dan informasi yang mengalir melaluinya. Sementara untuk berhubungan dengan antar kantor dan antar kantor menggunakan *internet* dan *email* untuk mengirim data dan berkomunikasi. Sehingga dibutuhkan jaringan privat untuk mempermudah akses *file* terhadap suatu tempat yang berbeda lokasi.

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 adalah jaringan komputer yang cakupannya lebih luas dibandingkan LAN. Kategori ini dapat dikatakan gabungan dari beberapa jaringan LAN. Cakupan lokasinya mencapai satu atau lebih dari suatu kota. MAN biasanya digunakan untuk menghubungkan kantor-kantor perusahaan yang berdekatan dan dapat dimanfaatkan untuk keperluan pribadi (swasta) atau umum.

3. *Wide Area Network* (WAN)

Wide Area Network (WAN) Wide Area Network adalah jaringan komputer yang mencakup daerah geografis yang luas, sering kali mencakup sebuah negara atau benua.

4. *Internet*

Internet Internet (Interconnection Networking) adalah seluruh jaringan komputer yang saling terhubung menggunakan standar sistem global Transmission Control Protocol/Internet Protocol Suite (TCP/IP) sebagai protokol pertukaran paket (packet switching communication protocol) untuk melayani miliaran pengguna di seluruh dunia, bahkan antar planet.

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

Sistem operasi jaringan model *Peer-to-Peer* memungkinkan seorang pemakai jaringan computer membagi sumber daya yang ada dikomputernya, baik itu *file* data, printer dan mengakses sumber daya computer yang lainnya. Adapun gambar topologi *Peer-to-Peer.* Model ini tidak mempunyai sebuah file server atau induk server yang terpusat, seluruh komputer memiliki kemampuan atau hak yang sama untuk memakai sumber daya yang tersedia dijaringan komputer tersebut.

2.3. Peralatan Pendukung

Dalam hal membangun sebuah jaringan yang baik, diperlukan peralatan khusus yang baik. Beberapa peralatan jaringan standar yang sering digunakan untuk *internetworking* adalah:

1. Router

> Menurut Moch. Linto Herlambang dan Azis Catur (2008:9) bahwa:
> *Router* merupakan perangkat yang dikhususkan untuk menangani koneksi antara dua atau lebih jaringan yang terhubung melalui paket *switching*. *Router* bekerja dengan melihat alamat asal dan alamat tujuan dari paket yang melewatinya dan memutuskan rute yang akan dilewati paket tersebut untuk sampai ke tujuan. *Router* mengetahui alamat masing-masing komputer di lingkungan jaringan lokalnya, mengetahui alamat *bridge*, dan *router* lainnya.

Sumber: www.cisco.com

Gambar II.1.*Router*

2. NIC (*Network Interface Card*)

Yang dimaksud dengan NIC adalah kartu jaringan atau LAN Card. Menurut Madcoms (2010:8) bahwa "Kartu Jaringan merupakan perangkat yang dipasang pada sebuah PC yang berfungsi untuk dapat berkomunikasi dengan komputer lain melalui jaringan LAN (*Local Area Network*)".

Sumber: www.tenda-indonesia.co.id

Gambar II.2.Kartu Jaringan

3. Switch

Menurut Madcoms (2010:9) mengemukakan bahwa:
Switch merupakan perangkat jaringan yang bekerja pada *OSI Layer* 2 (*Data Link Layer*). *Switch* berfungsi hampir sama seperti *hub*. *Switch* mengenal *MAC Address* yang digunakan untuk memilah data mana yang harus ditransmisikan. *Switch* menampung daftar *MAC Address* yang dihubungkan dengan port-port yang digunakan untuk menentukan kemana harus mengirim paket, sehingga akan mengurangi *traffic* pada jaringan. *Switch* menggunakan transmisi *Full Duplex* dimana memiliki jalur antara *receive* dan *transmit* data yang terpisah. Walaupun *collision* masih mungkin dapat terjadi, tetapi sudah diminimalisir.

Sumber: www.dlink.com

Gambar II.3.*Switch*

4. HUB

Menurut Madcoms (2010:8) bahwa "*Hub* merupakan perangkat jaringan yang bekerja di *OSI Layer* 1 (*Physical Layer*). *Hub* berfungsi sebagai penerima sinyal dari sebuah komputer, kemudian mentransmisikan ke komputer lain". Dengan kata lain, *hub* bekerja sebagai penyambung, *concentrator*, dan sebagai penguat sinyal pada kabel UTP.

Hub tidak mengenal *MAC Address* atau *Physical Address*, sehingga tidak dapat memilah data yang harus ditransmisikan, sehingga *collision* pada sebuah jaringan tidak dapat dihindari. *Collision* (tabrakan) merupakan suatu kondisi apabila terdapat dua *device* yang mengirim data pada saat bersamaan yang akan berakibat hilangnya data.

Sebuah *hub* dapat berfungsi sebagai *hub* aktif ataupun sebagai *hub* pasif. *Hub* aktif dapat difungsikan sebagai penguat sinyal sebelum sinyal tersebut dikirim kembali ke komputer lain. Sedangkan *Hub* pasif hanya berfungsi sebagai pembagi atau pemisah sinyal yang ditransmisikan pada sebuah jaringan. Pada sebuah *hub* terdapat beberapa *port* yang digunakan memasang konektor RJ45 yang sudah terpasang pada kabel UTP. (Madcoms, 2010:9)

Sumber: www.hw-group.com

Gambar II.4.*HUB*

5. Mikrotik

> Menurut Athailah (2013:18) menyimpulkan bahwa:
> MikroTik adalah sebuah merek dari sebuah perangkat jaringan, pada awalnya MikroTik hanyalah sebuah perangkat lunak atau *software* yang di-instal dalam komputer yang digunakan untuk mengontrol jaringan, tetapi dalam perkembangan saat ini telah menjadi sebuah *device* atau perangkat jaringan yang andal dan harga yang terjangkau, serta banyak digunakan pada level perusahaan penyedia jasa internet (ISP).

a. Sejarah Mikrotik

MikroTik adalah perusahaan kecil berkantor pusat di Latvia, bersebelahan dengan Rusia. Pembentukannya diprakarsai oleh John Trully dan Arnis Riekstins. John Trully adalah seorang Amerika yang berimigrasi ke Latvia. Di Latvia ia berjumpa dengan Arnis, seorang sarjana Fisika dan Mekanik sekitar tahun 1995.

Tahun 1996 John dan Arnis mulai me-*routing* dunia (visi MikroTik adalah *Routing the World*). Mulai dengan sistem Linux dan MS DOS yang dikombinasikan dengan teknologi *Wireless* LAN (W-LAN) Aeronet berkecepatan 2 Mbps di Molcova, tetangga Latvia, baru kemudian melayani lima pelanggannya di Latvia.

b. Jenis-Jenis Mikrotik

Menurut Moch. Linto Herlambang dan Azis Catur (2008:20-21) jenis-jenis MikroTik ada dua, yaitu:

1) MikroTik RouterOS

Adalah versi Mikrotik dalah bentuk perangkat lunak yang dapat diinstal pada komputer rumahan (PC) melalui CD. Anda dapat mengunduh file image MikroTik RouterOS dari website resmi MikroTik, www.mikrotik.com.

2) Built in Hardware MikroTik

Merupakan *MikroTik* dalam bentuk perangkat keras yang khusus dikemas dalam *board router* yang di dalamnya sudah terinstal *MikroTik RouterOS*. Untuk versi ini, lisensi sudah termasuk dalam harga *router board* MikroTik.

Sumber: www.routerboard.com

Gambar II.5.*MikroTik Router Board*

c. Fitur-Fitur Mikrotik

1) Address List

Pengelompokan *IP address* berdasarkan nama.

2) Asynchronous

Mendukung serial PPP *dial-in*/ *dial out*, dengan otentikasi CHAP, PAP, MSCHAPv1 dan MSCHAPv2, *Radius*, *dial on demand*, *modem pool* hingga 128 *ports*.

3) Bonding

Mendukung dalam pengkombinasian beberapa antarmuka *ethernet* ke dalam 1 pipa pada koneksi yang cepat.

4) Bridge

Mendukung fungsi *bridge spanning tree*, *multiple bridge interface*, *bridge firewalling*.

5) Data Rate Management

Qos berbasis HTB dengan menggunakan *burst*, PCQ, RED, SFQ, FIFO *queue*, CIR, MIR, *limit* antar *peer to peer*.

6) DHCP

Mendukung DHCP tiap antarmuka; DHCP *relay*; DHCP *client*; *multiple network* DHCP; *static and dynamic* DHCP *leases*.

7) Firewall and NAT

Mendukung pemfilteran koneksi *peer to peer*, *source* NAT dan *destination* NAT. Mampu memfilter berdasarkan MAC, *IP address*, *range port*, *protokol IP*, pemilihan opsi protokol seperti ICMP, TCP *flags* dan MSS.

8) Hotspot

Hotspot gateway dengan otentikasi RADIUS. Mendukung *limit data rate*, SSL, HTTPS.

9) IPSec

Protokol AH dan ESP untuk IPSec; MODP Diffie-Hellman group 1, 2, 5; MD5 dan algoritma SHA1 *hashing*; algoritma enkripsi menggunakan DES, 3DES, AES-128, AES-192, AES-256; *Perfect Forwarding Secresy* (PFS) MODP group 1, 2, 5.

10) ISDN

Mendukung ISDN *dial-in*/ *dial-out*. Dengan otentikasi PAP, CHAP, MSCHAPv1 dan MSCHAPv2, Radius. Mendukung 128K *bundle*, Cisco HDLC, x751, x75ui, x75bui *line* protokol.

11) M3P

MikroTik Protokol Paket Packet untuk *wireless links* dan *ethernet*.

12) MNDP

MikroTik Discovery Neighbor Protocol, juga mendukung *Cisco Discovery Protocol* (CDP).

13) Monitoring/Accounting

Laporan traffic IP, log, statistik *graphs* yang dapat diakses melalui HTTP.

14) NTP

Network Time Protocol untuk *server* dan *client*; sinkronisasi menggunakan system GPS.

15) Point to Point Tunneling Protocol

PPTP, PPPoE dan L2TP *Access Concentrators*; protokol otentikasi menggunakan PAP, CHAP, MSCHAPv1, MSCHAPv2; otentikasi dan laporan RADIUS; enkripsi MPPE; kompresi untuk PPPoE; *Limit data rate*.

16) Proxy

Cache untuk FTP dan HTTP proxy *server*; HTPPS proxy; *transparent* proxy untuk DNS dan HTTP; mendukung protokol SOKCS; mendukung *parent* proxy; statik DNS.

17) Routing

Routing statik dan dinamik; RIP v1/v2, OSPF v2, BGP v4.

18) SDSL

Mendukung *Single Line* DSL; *mode* pemutusan jalur koneksi dan jaringan.

19) Simple Tunnels

Tunnel IPIP dan *EoIP* (*Ethernet over IP*)

20) SNMP

Mode akses read-only.

21) Synchronous

V.35, V.24, E1/T1, X21, DS3 (T3) media types;sync-PPP, Cisco HDLC; *Frame Relay line protocol*; ANSI-617d (ANDI atau annex D) dan Q933a (CCITT atau annex A); *Frame Relay* jenis LMI.

22) Tool

Ping*; traceroute; bandwidth test; ping flood; telnet; SSH; packet sniffer; Dinamik DNS update.*

23) Upnp

Mendukung antarmuka *universal Plug and Play*.

24) VLAN

Mendukung Virtual LAN IEEEE802.1q untuk jaringan *ethernet* dan *wireless*; *multiple* VLAN; VLAN *bridging*.

25) VOIP

Mendukung aplikasi *voice over IP*.

26) WinBox

Aplikasi mode GUI untuk meremote dan mengkonfigurasi MikroTik RouterOS.

2.3.1. Topologi Jaringan

Menurut Madcoms (2010:4) mengemukakan bahwa "Topologi jaringan merupakan gambaran pola hubungan antara komponen-komponen jaringan, yang meliputi komputer server, komputer *client/workstation*,

hub/switch, pengkabelan dan komponen jaringan yang lain". Topologi fisik menguraikan *layout* aktual dari perangkat keras (*hardware*) jaringan, sedangkan topologi logika menguraikan perilaku komputer pada jaringan dari sudut pandang operator manusianya (*brainware*).

Topologi itu sendiri mempunyai kelebihan dan kekurangan. Berikut penjelasan dari masing-masing topologi:

1. Topologi *Bus*

Menurut Madcoms (2010:4) menjelaskan bahwa "Topologi Bus merupakan topologi yang menghubungkan beberapa komputer ke sebuah kabel dengan beberapa terminal. Topologi *Bus* menggunakan jenis kabel *Coaxial* dengan beberapa konektor BNC".

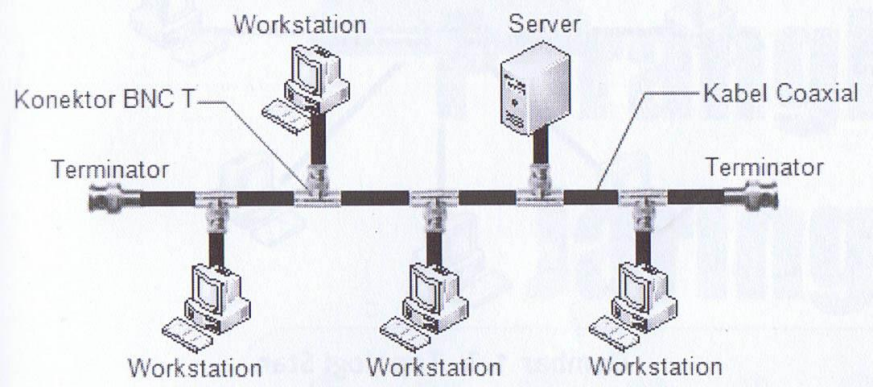
Menurut Wahana Komputer (2010:5) "Topologi *Bus* merupakan arsitektur jaringan dimana *client-client* yang ada dijaringan dihubungkan melalui *line* komunikasi yang ter-*share* yang disebut bus".

Keuntungan:

a. Hemat kabel
b. *layout* kabel sederhana
c. Setiap komputer dapat saling berhubungan langsung.

Kerugian:

a. Kepadatan lalu lintas data.
b. Sering terjadi hang (*crass talk*) ketika lebih dari satu pasang memakai jalur di waktu yang sama.



Sumber: Madcoms (2010:5)

Gambar II.6.Topologi *Bus*

2. Topologi *Ring*

Menurut Madcoms (2010:5) bahwa "Topologi *Ring* merupakan topologi yang menghubungkan beberapa komputer dengan membentuk lingkaran. Komputer yang terhubung dalam sebuah jaringan akan terkoneksi pada 2 komputer lain".

Setiap informasi yang diperoleh diperiksa alamat-alamatnya oleh terminal yang dilewati. Jika informasi itu bukan untuknya maka informasi itu di putar lagi sampai menemukan alamat yang benar. Setiap terminal LAN saling bergantungan, sehingga jika terjadi kerusakan satu terminal saja, keseluruhan LAN akan terganggu. Media koneksi yang digunakan adalah kabel UTP cat 3.

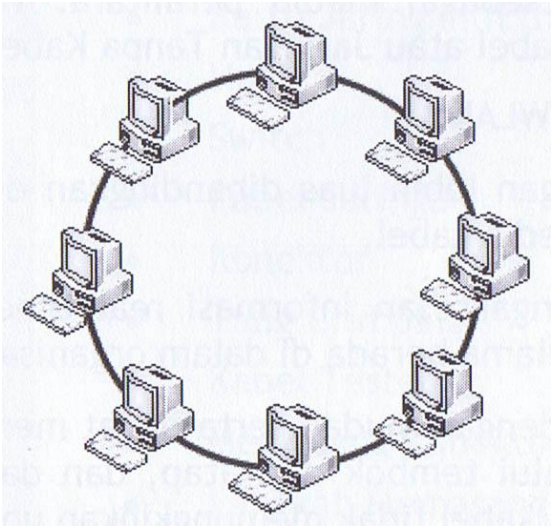
Keuntungan:

a. Laju data tinggi
b. Dapat melayani lalu lintas yang padat
c. Komunikasi antar terminal yang mudah

Kerugiannya:

a. Kerusakan pada satu terminal melumpuhkan jaringan.

b. Bila ada kerusakan pada media pengiriman data dapat menghentikan kerja seluruh jaringan.



Sumber: Madcoms (2010:5)

Gambar II.7.Topologi Ring

3. Topologi *Star*

Menurut Madcoms (2010:5) “Topologi *Star* merupakan topologi yang menghubungkan beberapa komputer dengan menggunakan perangkat yaitu *Hub* atau *Switch*”.

Dengan menggunakan topologi jenis ini maka jaringan mudah dikembangkan dengan menarik kabel ke konsentrator atau *node* pusat. Media koneksi yang digunakan adalah kabel UTP (10/100/1000Base-T).

Keuntungan:

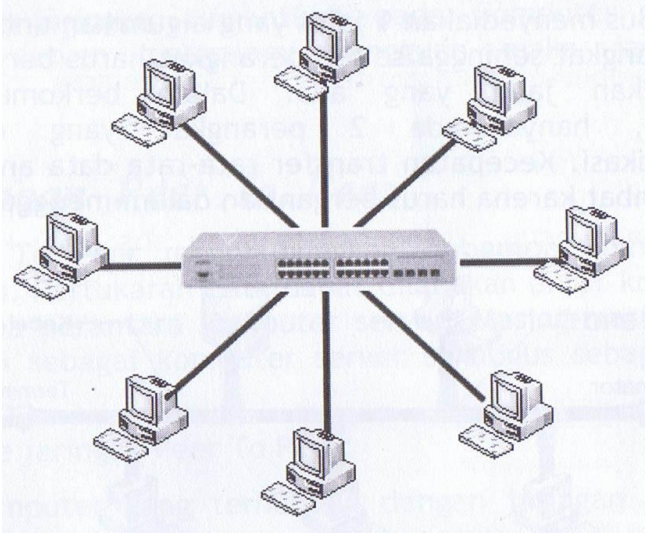
a. Paling fleksibel
b. Pemasangan atau perubahan stasiun sangat mudah dan tidak mengganggu bagian jaringan lain.
c. Kemudahan deteksi dan isolasi kesalahan atau kerusakan

Kerugian:

a. Boros kabel

b. Perlu penanganan khusus

c. Kontrol terpusat (*HUB, Switch*) jadi elemen kritis



Sumber: Madcoms (2010:6)

Gambar II.8.Topologi *Star*

4. Topologi *Mesh*

Menurut Arifin (2011:31) menjelaskan bahwa "pada topologi *mesh*, semua titik terminal akan saling terhubung dengan titik yang lain, sehingga membentuk jaringan yang kompleks".

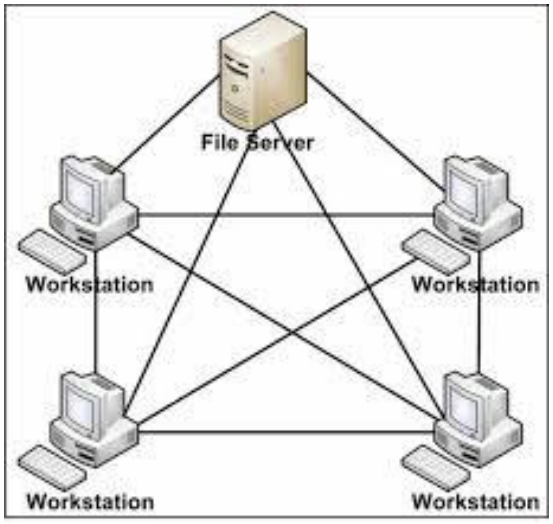
Pada topologi *Full Mesh*, setiap komponen jaringan memiliki hubungan langsung atau jalur khusus ke setiap komponen jaringan yang lain dalam segmen tersebut. Jika satu saja dari jalur khusus tersebut dihilangkan, maka topologi yang terbentuk tidak dapat lagi disebut *Full Mesh* melainkan menjadi *partial Mesh*.

Keuntungan:

a. Pengiriman data, dari satu *node* ke sejumlah simpul yang lain dapat dilakukan secara bersamaan.
b. Pemecahan masalah lebih mudah dibandingkan dengan topologi jaringan komputer lainnya.
c. Jika ada exspansi jaringan, tidak akan menyebabkan gangguan pada pengguna jaringan lainnya.

Kekurangan:

a. Membutuhkan lebih banyak perangkat keras jaringan (misalnya: kabel jaringan, dan lain-lain) dibandingkan dengan topologi yang lainnya.
b. Pelaksanaan (*instalasi* dan konfigurasi) topologi ini sangat rumit dan mungkin sangat berantakan. Sejumlah besar input atau output port diperlukan.
c. Biaya instalasi dan pemeliharaan jaringan komputer mesh cukup tinggi.



Sumber: www.kajianpustaka.com

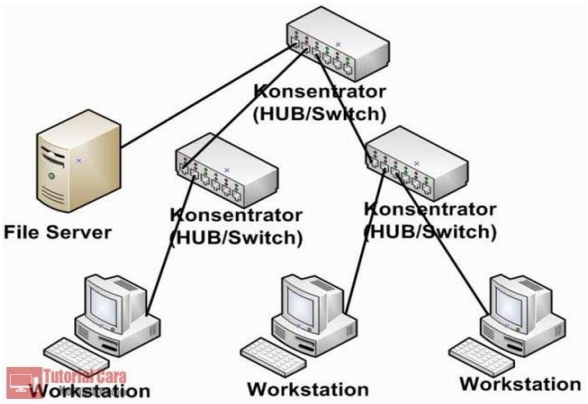
Gambar II.9.Topologi *Mesh*

5. Topologi Tree

Menurut Sofana (2013:54) bahwa "Topologi *tree* merupakan gabungan beberapa topologi *star* yang dihubungkan dengan topologi *bus*. Topologi *tree* digunakan untuk menghubungkan beberapa LAN dengan LAN lain. Hubungan antara LAN dilakukan *via hub*. Masing-masing *hub* dapat dianggap sebagai akar (*root*) dari masing-masing pohon (*tree*)".

Topologi *tree* dapat mengatasi kekurangan topologi *bus* yang disebabkan persoalan *broadcast traffic*, dan kekurangan topologi *star* yang disebabkan oleh keterbatasan kapasitas *port hub*.

Karakteristik yang dimiliki topologi *tree* mirip dengan topologi *bus* dan *star*. Begitu juga dengan peralatan, kabel, dan teknik pemasangan.



Sumber: www.tutorialcarakomputer.com

Gambar: II.10.Topologi *Tree*

2.3.2. IP Address

Menurut Madcoms (2010:21) mengemukakan bahwa "IP (*Internet Protocol*) *Address* merupakan alamat yang diberikan kepada komputer-komputer yang terhubung dalam suatu jaringan. *IP Address* terdiri dari dua bagian, yaitu: *Network ID* dan *Host ID*".

Menurut Madcoms (2010:21), *IP Address* berdasarkan perkembangannya dibagi menjadi dua jenis yaitu:

a. IPv4 (*Internet Protocol* versi 4), merupakan *IP Address* yang terdiri dari 32 bit yang dibagi menjadi 4 segmen berukuran 8 bit.
b. IPv6 (*Internet Protocol* versi 6), merupakan *IP Address* yang terdiri dari 128 bit yang digunakan untuk mengatasi permintaan IP Address yang semakin meningkat.

IP Address terdiri dari 32 bit angka biner yang dituliskan dalam bentuk empat kelompok dan masing-masing kelompok terdiri dari delapan (oktat) bit yang dipisahkan oleh tanda titik.

Contoh: 11000000.10101000.00000000.01100100

IP Addrees dapat juga ditulis dalam bentuk angka desimal dalam empat kelompok, dari angka 0-255.

Contoh : 192.168.0.100

Untuk memudahkan pengaturan *IP address* seluruh komputer pengguna jaringan *internet*, dibentuklah suatu badan yang mengatur pembagian *IP address*. Badan tersebut bernama InterNIC (*Internet Network Information Center*). InterNIC membagi-bagi *IP address* menjadi beberapa kelas. Kelas-kelas tersebut meliputi:

1. Kelas A

IP kelas A terdiri dari 8 bit pertama digunakan untuk Network ID, dan 24 bit berikutnya merupakan Host ID. IP kelas A memiliki 126 Network, yaitu dari nomor 1.xxx.xxx.xxx sampai dengan 126.xxx.xxx.xxx (xxx merupakan variabel yang nilainya dari 0 sampai dengan 255).

2. Kelas B

IP kelas B terdiri dari 16 bit pertama digunakan untuk Network ID, dan 16 bit berikutnya merupakan Host ID. IP kelas B memiliki 16.384 network, yaitu dari nomor 128.0.xxx.xxx sampai dengan 191.255.xxx.xxx.

3. Kelas C

IP kelas C terdiri dari 24 bit pertama digunakan untuk Network ID, dan 8 bit berikutnya merupakan Host ID. IP kelas C memiliki 2.097.152 network, yaitu dari nomor 192.0.0.xxx sampai dengan 223.255.255.xxx.

2.4. VPN (Virtual Private Network)

2.4.1. Pengertian VPN

Menurut Sofana (2013:536) "VPN merupakan sebuah model jaringan yang dapat menghubungkan beberapa LAN yang lokasinya berjauhan. Media yang digunakan untuk menghubungkan antarlokasi adalah media jaringan *public*".

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, ketiga fungsi utama tersebut antara lain:

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.

Berikut ini merupakan tipe-tipe VPN secara garis besar yaitu:

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.

2.4.2 Keamanan VPN

Terdapat beberapa fitur penting yang ada dalam VPN:

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.

3. IPSec

IPSec menyediakan layanan *security* dengan mengizinkan sistem untuk memilih protokol keamanan yang diperlukan, memperkirakan algoritma apa yang akan digunakan pada layanan, dan menempatkan *key* yang diperlukan untuk menyediakan layanan yang diminta. Pada IPSec terdapat *negotiation protocol*:

a. AH *(Authentication Header*) menyediakan layanan *authentication* (menyatakan bahwa data yang dikirim berasal dari pengirim yang benar), *integrity* (keaslian data), dan melakukan pengamanan terhadap IP *Header.*

b. ESP (*Encapsulated Security Payload*) menyediakan layanan *authentication*, *integrity, reply protection,* dan *confidentiality* terhadap data. ESP melakukan pengamanan data terhadap segala sesuatu dalam paket data setelah *header* (enkripsi).