BAB II

LANDASAN TEORI

2.1 Tinjauan Jurnal

Pratiwi, Triyono, dan Andayati (2013:21) menyimpulkan bahwa perkembangan dibidang informasi begitu cepat, hal ini diikuti dengan perkembangan teknologi komunikasi khususnya internet. Kehadiran internet di indonesia sudah sangat dibutuhkan mengingat bahwa teknologi informasi ini telah memberikan kemudahan proses komunikasi yakni dengan meniadakan jarak dan waktu yang selama ini dirasakan sebagai faktor penghambat. Maka dari itu, diperlukan sebuah jaringan yang dapat digunakan sebagai sarana untuk mengakses internet maupun saling bertukar informasi. Namun permasalahan yang sering timbul adalah faktor keamanan yang saat ini menjadi hal yang sangat penting untuk diperhatikan. Oleh karena itu, VPN diciptakan untuk menyelesaikan permasalah dalam jaringan yang tidak aman. *Private network* dianggap lebih efisien karena kecepatan transfer data yang lebih besar daripada kecepatan transfer data pada jaringan internet, selain itu masalah keamanan lebih bagus karena hanya bergerak dalam lingkup terbatas saja.

Nugroho, Widada, dan Kustanto (2015:1) menyimuplkan bahwa teknologi *virtual private network* (VPN) sangat berperan besar dalam dunia komunikasi sekarang ini. Dikarenakan VPN mampu membuat jaringan lokal dengan menggunakan fasilitas publik. Karena dengan VPN perusahaan bisa menjalin suatu koneksi data yang mudah dan aman.Dan jaringan VPN dengan koneksi internet disisi *server* akan membuat jaringan VPN lebih stabil dan tidak banyak timbul perbedaan pada PPTP maupun IPSec dan pada performansi IPSec dengan *server* yang lebih besar membuatnya lebih baik dibandingkan dengan PPTP.

2.2 Konsep Dasar Jaringan

A. Jaringan Komputer

Wahidin (2007:1) mendefinisikan bahwa “Jaringan komputer sebagai kumpulan beberapa komputer dan peralatan lain yang saling berhubungan menggunakan aturan – aturan tertentu”. Hubungan ini dapat terjadi menggunakan media fisik berupa kabel ataupun melalui gelombang radio, *infrared*, bahkan

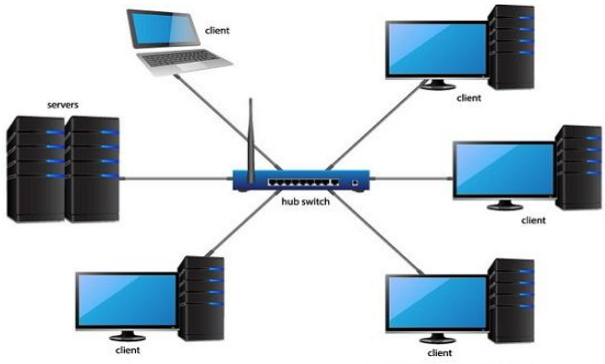
satelit. Setiap peralatan yang tersambung kejaringan disebut node. Sebuah jaringan biasanya terdiri dari 2 atau lebih komputer yang saling berhubungan diantara satu dengan yang lain, dan saling berbagi sumber daya misalnya *CDROM* dan *Printer*.

B. Jenis – Jenis Jaringan

Ada 3 macam jenis – jenis *networking* yaitu :

1. *Local Area Network* (LAN)

Sofana (2008:2) mendefinisikan bahwa "LAN adalah jaringan komputer yang masih berada dalam gedung atau ruangan". Jenis jaringan ini terletak pada suatu lokasi dengan jangkauan dua area terbatas, misalnya dalam lokasi gedung. Beberapa model konfigurasi LAN, satu komputer biasanya dijadikan sebuah *file server* yang mana digunakan untuk menyimpan perangkat lunak yang mengatur aktifitas jaringan ataupun sebagai perangkat lunak yang dapat digunakan oleh komputer-komputer yang terhubung kedalam jaringan. Komputer-komputer yang terhubung kedalam jaringan biasanya disebut *workstation.*

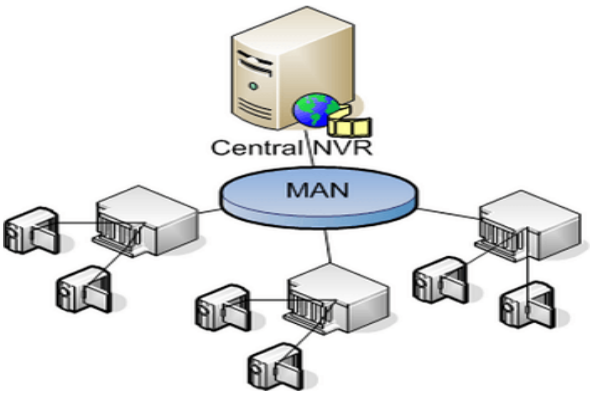


Sumber: www.nesabamedia.com/pengertian-jaringan-lan/

Gambar II.1 Jaringan LAN

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

Sofana (2010:111) mendefinisikan bahwa"MAN adalah sebuah jaringan komputer gabungan dari beberapa jaringan LAN yang mencakup daerah yang cukup luas". Dalam hal ini jaringan menghubungkan beberapa buah jaringan-jaringan kecil kedalam lingkungan area yang lebih besar.



Sumber: www.nesabamedia.com/pengertian-jaringan-man/

Gambar II.2 Jaringan MAN

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

Sofana (2010:127) menjelaskan bahwa "WAN merupakan gabungan beberapa jaringan MAN yang cakupannya bisa mencapai Negara ataupun antar Negara". Menggunakan sarana WAN, contohnya di sebuah kampus yang berada di Bandung bisa menghubungi kantor cabangnya yang berada di daerah Surabaya hanya dalam beberapa menit. Biasanya WAN agak rumit dan sangat kompleks karna menggunakan banyak sarana untuk menghubungkan antara LAN dan WAN kedalam komunikasi global seperti internet.

Sumber: www.rianlab.com/2014/11/mengenal-jenis-jenis-jaringan-komputer.html

Gambar II.3 Jaringan WAN

2.3 Manajemen Jaringan

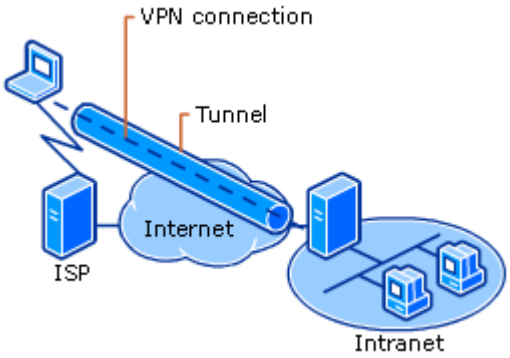
Manajemen jaringan merupakan hal terpenting dalam mengelola jaringan komputer untuk memastikan semua sistem jaringan bekerja sesuai apa yang diharapkan.

A. Pengertian VPN

Sofana (2012:228) mendefinisikan bahwa "*Virtual Private Network* (VPN) adalah teknologi jaringan komputer yang memanfaatkan media komunikasi publik (*open connection* atau *virtual circuit),* seperti *internet*, untuk menghubungkan beberapa jaringan lokal". Informasi yang berasal dari *node-node* VPN akan "dibungkus" (*tunneled)* dan kemudian mengalir melalui jaringan publik. Sehingga informasi menjadi aman dan tidak mudah dibaca oleh yang lain.

Umumnya VPN diimplementasikan oleh lembaga/perusahaan besar. Biasanya perusahaan semacam ini memiliki kantor cabang yang lokasinya cukup jauh dari kantor pusat. Sehingga diperlukan solusi yang tepat untuk mengatasi keterbatasan LAN. VPN dapat menjadi sebuah pilihan yang cukup tepat. Tentu saja VPN boleh

diimplementasikan oleh pengguna rumah atau oleh siapa pun yang membutuhkannya.



Sumber: http://www.technet.microsoft.com

Gambar II.4 Tampilan Jaringan VPN

Sukmaaji & Rianto (2008:176) mendefinisikan bahwa "Teknologi VPN menyediakan lima fungsi utama untuk penggunaannya". Kelima fungsi utama tersebut antara lain sebagai berikut :

a. Kerahasiaan, dengan kemampuan *scramble* dan *encrypt* pesan sepanjang jaringan yang tidak aman.

b. Kendali akses, menentukan siapa yang diberikan akses ke suatu sistem atau jaringan, sebagaimana informasi apa dan seberapa banyak seseorang dapat menerima.

c. *Autentikasi*, yaitu menguji identitas dari dua perusahaan yang mengadakan transaksi

d. *Integritas*, menjamin bahwa *file* atau pesan tidak berubah dalam perjalanan

e. *Non-repudiation*, yaitu mencegah dua perusahaan saling menyangkal bahwa mereka mengirim atau menerima sebuah *file*.

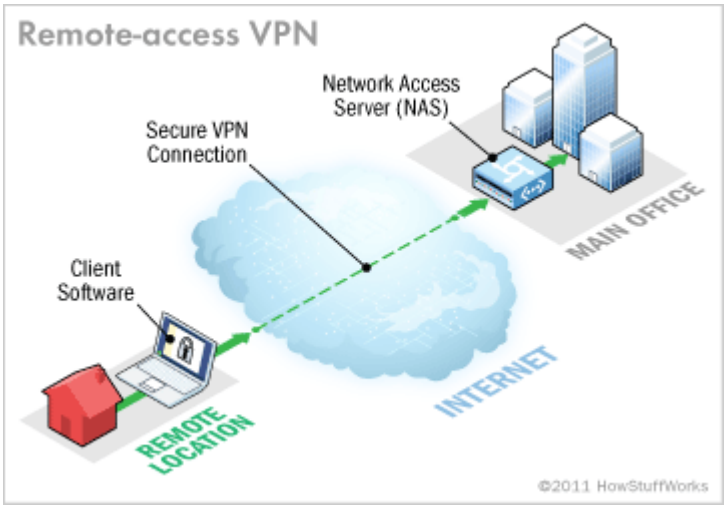
B. Jenis – Jenis *VPN*

Sofana (2012:229) mendefinisikan bahwa "VPN telah dikembangkan menjadi beberapa jenis". Para ahli berbeda pendapat tentang pembagian jenis VPN tersebut. Ada yang membagi VPN berdasarkan cakupan area, yaitu Intranet, Extranet, dan Internet, jenis proteksi data, dan sebagainya. Secara umum VPN dapat dikelompokkan menjadi:

1. Remote Access VPN

Sofana (2012:229) mendefinisikan bahwa "*Remote Access* VPN disebut juga *Virtual Private Dial-Up Network* (VPDN)". VPDN adalah jenis *user-to*-LAN *connection.* Artinya, *user* dapat melakukan koneksi ke *private network* dari manapun, apabila diperlukan. Biasanya VPDN dimanfaatkan oleh karyawan yang bekerja di luar kantor. Mereka dapat memanfaatkan komputer laptop yang sudah dilengkapi perangkat tertentu untuk melakukan koneksi dengan jaringan LAN di kantor.

Sebelum koneksi terjadi akan dilakukan proses *dial-up* ke *network access server* (NAS). Biasanya NAS disediakan oleh *provider* yang memberikan layanan VPN. Sedangkan pengguna cukup menyediakan komputer dan aplikasi untuk men-*dial* NAS. Secara umum VPDN hampir mirip dengan *dial-up* internet *connection.* Namun, secara teknis tentu saja VPN lebih canggih dan lebih *secure* dibandingkan *dial-up* internet. Koneksi biasanya hanya dilakukan sewaktu-waktu.



Sumber: https://computer.howstuffworks.com/vpn3.html

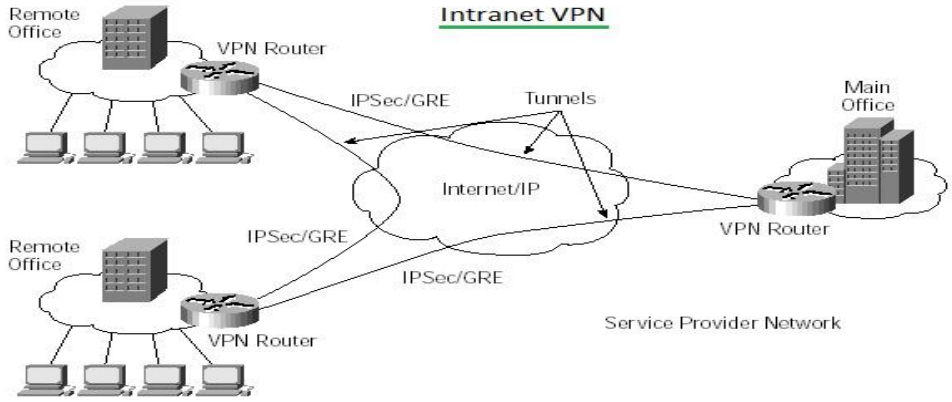
Gambar II.5 *Remote Access* VPN

2. Site-to-site VPN

Sofana (2012:230) mendefinisikan bahwa "*Site-to-site* VPN diimplementasikan dengan memanfaatkan perangkat *dedicated* yang dihubungkan via internet". *Site-to-site* VPN digunakan untuk menghubungkan berbagai area yang sudah *fixed* atau tetap, misal kantor cabang dengan kantor pusat. Koneksi antara lokasi-lokasi tersebut berlangsung secara terus menerus (24 jam) sehari. Jika ditinjau dari segi kendali atau *administrative control*. Secara umum *site-to-site* VPN dapat dibagi menjadi:

a. Intranet VPN

VPN hanya digunakan untuk menghubungkan beberapa lokasi yang masih satu instansi atau satu perusahaan. Seperti kantor pusat dihubungkan dengan kantor cabang. Dengan kata lain, *administrative control* berada sepenuhnya di bawah satu kendali.

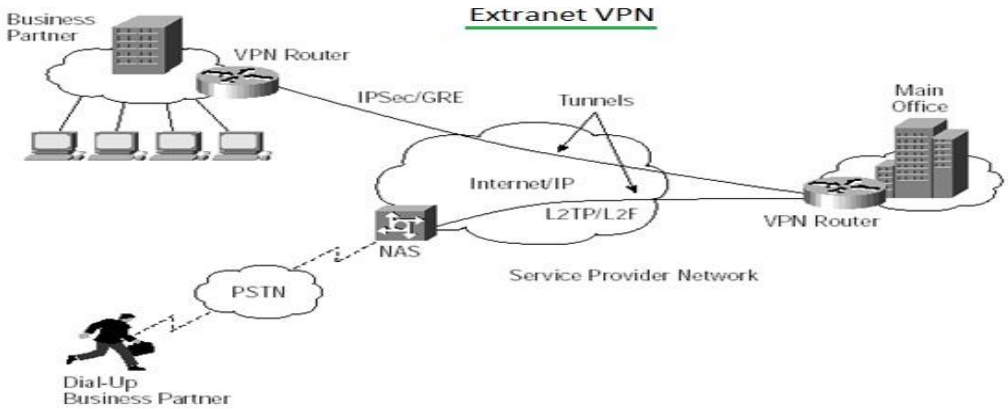


Sumber: www.rfwireles-world.com/Terminolgy/Intranet-VPN-vs-Extranet-VPN.html

Gambar II.6 Intranet VPN

b. Extranet VPN

VPN hanya digunakan untuk menghubungkan beberapa instansi atau perusahaan yang berbeda namun di antara mereka memiliki hubungan "dekat". Seperti perusahaan tekstil dengan perusahaan angkutan barang yang digunakan oleh perusahaan tekstil tersebut. Dengan kata lain *administrative control* berada di bawah kendali beberapa instansi terkait.



Sumber: www.rfwireles-world.com/Terminolgy/Intranet-VPN-vs-Extranet-VPN.html

Gambar II.7 Extranet VPN

C. Keamanan VPN

Sofana (2012:231) mendefinisikan bahwa untuk mengamankan informasi yang berasal dari jaringan *internal*, VPN menggunakan beberapa metode keamanan, seperti:

1. *Firewall*

Firewall menyediakan "penghalang" antara jaringan lokal dengan internet. Pada *firewall* dapat ditentukan *port-port* mana saja yang boleh dibuka, paket apa saja yang boleh melalui *firewall*, dan protokol apa saja yang dibolehkan.

2. Enkrpsi

Sofana (2012:232) mendefinisikan bahwa "Enkripsi merupakan metode yang umum untuk mengamankan data". Informasi akan "diacak" sedemikian rupa sehingga sukar dibaca oleh orang lain. Secara umum ada dua buah metode enkripsi, yaitu:

a. *Symmetric-key encryption*

Pada metode ini, masing-masing komputer pengirim dan penerima harus memiliki *"key"* yang sama. Informasi yang sudah di-enkripsi hanya dapat di-dekripsi menggunakan key tersebut.

b. *Public-key encryption*

Pada metode ini, komputer pengirim menggunakan *public key* milik komputer penerima untuk melakukan enkripsi. Setelah informasi dikirim maka proses dekripsi dapat dilakukan menggunakan *private key* komputer penerima.

Public key dapat disebarkan kepada siapa pun, namun *private key* hanya untuk pemilik yang sah saja.

3. IPSec

Sofana (2012:233) mendefinisikan bahwa “IPSec menyediakan fitur keamanan yang lebih baik”. Seperti algoritma enkripsi yang lebih bagus dan *comprehensive autohentication. IPSec* menggunakan dua buah metode enkripsi, yaitu:

a. Tunnel, melakukan emkripsi pada *header* dan *payload* masing-masing paket.

b. Transport, hanya melakukan enkripsi *payload* masing-masing paket.

4. Integritas Data

Setiap paket data yang dilewatkan pada jaringan publik, perlu adanya penjamin integritas data, apakah terjadi perubahan atau tidak pada data tersebut.

D. Protokol

1. *Point to Point Protocol* (PPP)

Towidjojo (2013a:198) menjelaskan bahwa “koneksi *point to point* (titik ke titik) dapat digunakan untuk menghubungkan secara langsung satu perangkat dengan perangkat lainnya”. Umumnya digunakan untuk menghubungkan jaringan lokal ke *Internet Service Provider*. Tujuan untuk membuat hubungan langsung atau *face to face* antara *provider* dengan *client* adalah untuk memudahkan manajemen jaringan dan memisahkan satu *client* dengan *client* lainnya. Untuk membuat topologi *point to point* ini digunakanlah *Point to Point Protocol.*

2. Point to Point Protocol Over Ethernet (PPPoE)

Towidjojo (2013b:198) menjelaskan bahwa “PPPoE adalah pengembangan dari PPP. Perbedaan keduanya terletak pada media dimana protokol ini di implementasikan”. Jika PPP digunakan pada jaringan yang menggunakan serial maupun GSM modem, maka PPPoE digunakan untuk membuat topologi *Point to Point* pada jaringan Ethernet.

3. *Point to Point Tunneling Protocol* (PPTP)

Habibi dan Arifin (2015:115) menjelaskan "salah satu protokol yang digunakan untuk membangun VPN adalah *Point to Point Tunneling Protocol* (PPTP). VPN akan menawarkan tingkat *encryption* yang lebih baik selain menawarkan fitur *authentication.* Inilah membuat VPN pilihan wajib jika anda membuat level keamanan yang lebih baik saat akan membuat *tunnel".*

4. *Layer 2 Tunneling Protocol* (L2TP)

Ramdhani, Periyadi dan Sularsa (2010:3) mendefinisikan "L2TP adalah sebuah *tunneling* protocol yang memadukan dan mengkombinasikan dua buah *tunneling* protokol yang bersifat *proprietary*, yaitu L2F *(Layer 2 Forwarding)* memiliki *cisco system* dengan PPTP milik *Microsoft".*

5. 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).

2.4 Konsep Penunjang Usulan

Untuk membuat suatu sistem jaringan diperlukan beberapa peralatan seperti:

1. *File server.*

Wahyudi dan Hanggara (2013:26) menjelaskan bahwa "Sebuah *file server* memungkinkan pengguna untuk berbagi informasi melalui jaringan tanpa harus secara fisik mengirim *file* dengan *floppy disk* atau beberapa perangkat penyimpanan *eksternal* lainnya."

2. Komputer sebagai tempat kerja atau disebut *Workstation*.

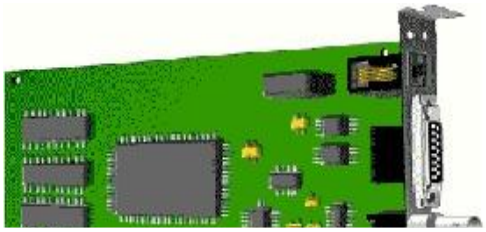
Syahrull dan Basalamah (2016:184) menjelaskan bahwa "*Workstation computer* menawarkan kapasitas komputasi yang lebih tinggi dan mempunyai kemampuan tampilan grafis yang lebih tangguh untuk pekerjaan saintifik dan rekayasa.

3. Peralatan jaringan seperti *Network Interface Card* atau Kartu Jaringan.

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

4. Media penghubung antar komputer seperti *Ethernet Card*

Micro (2012:13-14) menjelaskan bahwa " Kartu jaringan ethernet umumnya telah meyediakan *port* koneksi untuk kabel koaksial ataupun kabel *twisted pair*, jika didesain untuk kabel koaksial konnektornya adalah BNC, dan apabila didesain untuk kabel *twisted pair* maka akan punya konektor RJ-45". Beberapa kartu jaringan etthernet kadang juga punya konektor AUI. Semua itu dikoneksikan dengan koaksial, *twisted pair,* ataupun dengan kabel fiber optik.



Sumber : http://feriantoro.com/2013/09/nic-kartu-jaringan.html

Gambar II.8 *Network Interface Card*

5. *Local Talk Connector* untuk kapasitas data terhubung dengan komputer.

Micro (2012:14) mendefinsikan bahwa "*Local Talk* adalah peralatan jaringan untuk komputer macintosh, ini menggunakan sebuah kotak adapter khusus dan kabel yang terpasang ke *port* untuk *printer".*

Sumber : http://baharudin.web.id/hardware-jaringan-komputer.html

Gambar II.9 *Local Talk Connector*

6. **Token *Ring Card***

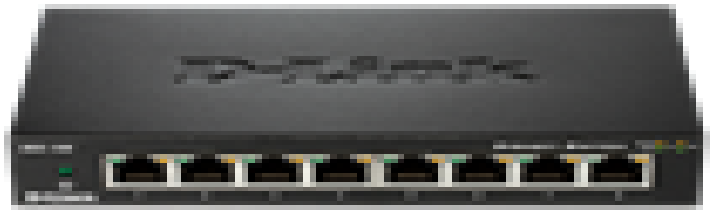
Madcoms (2010:8) menjelaskan bahwa "Kartu Jaringan merupakan perangkat yang dipasang pada sebuah PC yang berfungsi untuk dapat berkomunikasi dengan komputer lain melalui jaringan LAN *(Local Area Network).*

Sumber : http://us-instrument.com/object/catalog/product/img2126.jpg

Gambar II.10 Token *Ring Card*

7. Switch

Madcoms (2010:9) mendefinisikan 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.11 switch

8. *Bridge* / Jembatan

Sofana (2010:67) menjelaskan bahwa "*Bridge* adalah sebuah perangkat *network* yang menghubungkan dua buah atau membagi sebuah LAN menjadi beberapa *segmen*".. Fungsi dari *bridge* itu sama dengan fungsi *repeater* tapi *bridge* lebih *fleksibel* dan lebih cerdas daripada *repeater*. *Bridge* dapat menghubungkan jaringan yang menggunakan metode transmisi yang berbeda.

Misalnya *bridge* dapat menghubungkan *Ethernet baseband* dengan *Ethernet broadband*. *Bridge* juga dapat digunakan untuk menghubungkan jaringan yang menggunakan tipe kabel yang berbeda ataupun topologi yang berbeda pula. *Bridge* dapat mengetahui alamat masing-masing komputer di masing-masing sisi jaringan.

Berikut karakteristik *bridge* antara lain :

a. Koneksi internet dipakai pada pc saja, atau koneksi internet di *share* dengan sebagian pc menggunakan *server/access point*.
b. Koneksi internet menggunakan pilihan paket *quota*, sehingga tidak terhubung ke internet selama 24 jam.
c. Membuat kerja modem menjadi lebih mudah, dikarenakan bila koneksi di *share* maka modem tidak jadikan sebagai *server* untuk membagi *bandwidth*, hingga modem lebih awet, tetapi konsekuensinya untuk membagi *bandwidth* dibutuhkan tambahan *server/access point*.
d. Dapat memisahkan jaringan yang luas jadi sub jaringan yang lebih kecil.
e. Dapat mempelajari alamat, meneliti paket data serta menyampaikannya.
f. Mampu mengumpulkan serta melepaskan paket di antara dua *segmen* jaringan.
g. Dapat mengontol *broadcast* ke jaringan.
h. Dapat menjaga *address table*.

Kelebihan *Bridge*

a) Memperluas atau menambah jarak dari *network* yang ada.
b) Menambah jumlah *workstation* pada jaringan untuk mengurangi kemacetan *traffic.*

c) Menyediakan koneksi ke *network* yang tidak sama.

Kekurangan *Bridge*

a) *Bridge* tidak dapat memblokir paket *broadcast.*

b) Bila alamat yang diterima tidak dikenal oleh *bridge*, maka dapat disiarkan berita ke jaringan *segmen* lain serta perihal ini bisa mengakibatkan berlangsungnya *broadcast strom* (badai siaran) yang dampaknya bisa bikin jaringan macet keseluruhan.

c) Teknik *bridging* dapat mengonsumsi banyak *bandwidth.*

Sumber : http://www.nesabamedia.com/pengertian-bridge-dan-fungsi-bridge/

Gambar II.12 *Bridge*

9. Router

Linto dan Catur (2008:9) menjelaskan 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 dilingkungan jaringan lokalnya, mengetahui alamat *bridge,* dan *router* lainnya.

Fungsi dari sebuah *Router* yaitu sebagai berikut :

1. *Router* dapat menerjemahkan informasi diantara LAN dan internet .
2. *Router* akan mencarikan jalur yang terbaik untuk mengirimkan data melewati internet.
3. Mengatur jalur sinyal secara *effisien* dan dapat mengatur data yang mengalir diantara dua buah *protocol*.
4. Dapat mengatur aliran data diantara topologi jaringan *linear* bus dan *star*.
5. Dapat mengatur aliran data melewati kabel *fiber optic*, kabel *coaxsial* atau kabel *twisted pair*.

Sumber : http://www.nesabamedia.com/pengertian-router-dan-fungsi-router/

Gambar II.13 Router

10. Sistem Operasi Server

Sistem operasi server yaitu *Windows Server 2003, Windows Server 2008, Windows Server 2010, Window NT Server, Netware.*

11. Sistem Operasi untuk *workstation*

Sistem operasi untuk *workstation* yaitu *DOS, Windows Xp Profesional, Windows Vista, Windows 7, Linux, MAC.*

12. Modem

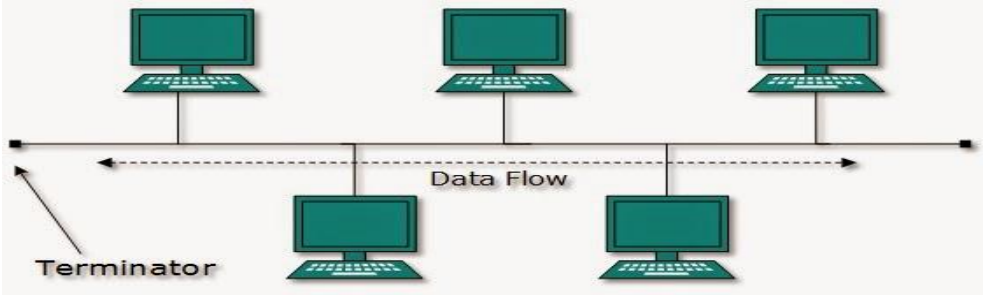
Aditya (2011:24) menjelaskan bahwa "Modem *(Modulator Demodulator),Modulator* merupakan bagian yang mengubah sinyal informasi ke dalam sinyal pembawa *(carrier),* sedangkan *Demodulator* adalah bagian yang memisahkan sinyal informasi yang berisi data atau pesan. Sehingga istilah modem adalah alat komunikasi dua arah (menggabungkan keduanya). Data dari komputer yang berbentuk sinyal *digital* diubah menjadi sinyal *analog* oleh modem. Sinyal *analog* tersebut kemudian dikirim melalui media telekomunikasi seperti telepon.

2.4.1 Topologi Jaringan Komputer

Wahidin (2007a:10) menjelaskan bahwa "Topologi Jaringan adalah "*konfigurasi* tentang bagaimana menghubungkan komputer secara fisik sehingga membentuk sebuah jaringan". Topologi yang sering digunakan adalah :

1. Topologi BUS

Wahidin (2007b:10) menjelaskan bahwa "Topologi Bus adalah komputer *server* dan *workstation* dihubungkan secara berantai melalui kabel tunggal". Topologi ini mudah dikembangkan dan sederhana namun bila salah satu *workstation* mati yang lain akan berpengaruh.

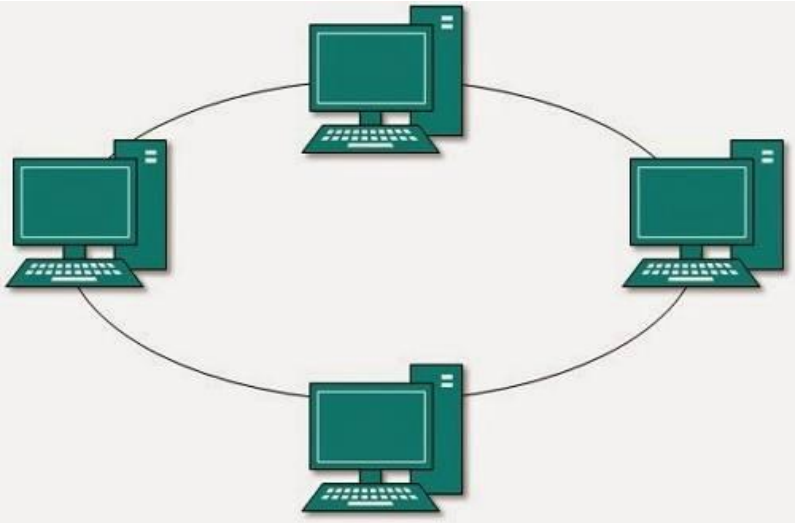


Sumber: http://www.nesabamedia.com/topologi-bus/

Gambar II.14 Topologi Bus

2. Topologi Token *Ring*

Topologi Token *Ring* mirip dengan topologi BUS, bedanya topologi ini ujungnya saling berhubungan seolah membentuk lingkaran cincin.Pada topologi Wahidin (2007c:10) menjelaskan bahwa "Token *Ring* adalah data mengalir searah, artinya seluruh komputer dalam jaringan akan ikut ambil bagian dalam mengelola informasi yang lewat sehingga bila salah satu rusak maka akan berpengaruh terhadap keseluruhan jaringan".



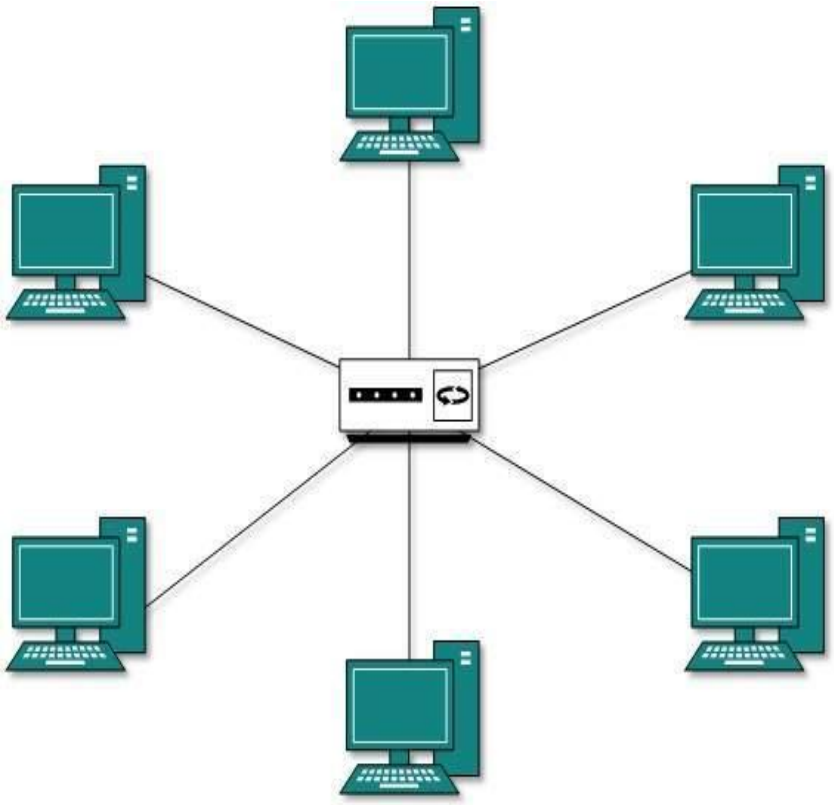
Sumber: http://www.nesabamedia.com/pengertian-topologi-ring/

Gambar II.15 Topologi Token *Ring*

3. Topologi *Star*

Dalam topologi *Star* setiap komputer atau *workstation* dihubungkan secara langsung melalui media perantara berupa *Switch*. Keunggulan dari topologi *Star* , Wahidin (2007a:11) menjelaskan "Bahwa dengan adanya kabel tersendiri pada setiap *workstation* ke *server*, maka *bandwidth* atau lebar jalur komunikasi dalam kabel akan semakin lebar sehingga akan meningkatkan kinerja jaringan secara keseluruhan". Kelemahan topologi *star* Wahidin (2008:11) menjelaskan bahwa

ialah “membutuhkan kabel yang lebih banyak dan juga kontrol terpusat (*Switch)* jadi elemen kritis”.

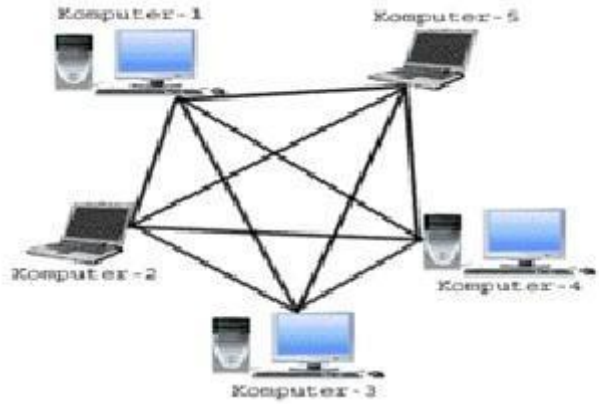


Sumber: https://www.thinglink.com/scene/733322731365335042

Gambar II.16 Topologi *Star*/Bintang

4. Topologi *Mesh*

Wahidin (2007b:11) mendefinisikan bahwa ”topologi *Mesh* setiap komputer bisa saling berhubungan satu sama lain, namun kabel yang diperlukan sangat banyak”. Apabila salah satu *client* mengalami masalah maka *client* lain berpengaruh. Oleh karena itu topologi ini jarang dipakai.



Sumber: http//www.amazinglight.info/tipe-jaringan-komputer.html

Gambar II.17 Topologi Mesh

Dalam praktiknya, pembangunan sebuah jaringan biasanya tidak menggunakan satu topologi saja melainkan gabungan dari beberapa topologi yang ada. Untuk menghubungkan jaringan yang berbeda Wahidin (2008:12) menjelaskan bahwa biasanya yang digunakan adalah "Topologi BUS".Sedangkan untuk menghubungkan komputer pada jaringan komputer digunakan topologi *STAR.*

2.4.2 Kabel

Komputer membutuhkan sebuah media transmisi untuk dapat terhubung dan melakukan segala bentuk kegiatan di jaringan.media transmisi ada beberapa macam, salah satunya adalah kabel. Kabel pada jaringan komputer di gunakan untuk meghubungkan antara suatu *server* dengan *workstation*, atau sebaliknya.

Berikut jenis bentuk kabel yang sering digunakan dalam jaringan komputer :

a. Kabel *Coaxcial*

Kabel *coaxial* tersusun atas inti tembaga pada intinya, dan tertutup secara menyeluruh oleh bahan *plastic insulator*.Bagian inti kabel terbuat dari bahan

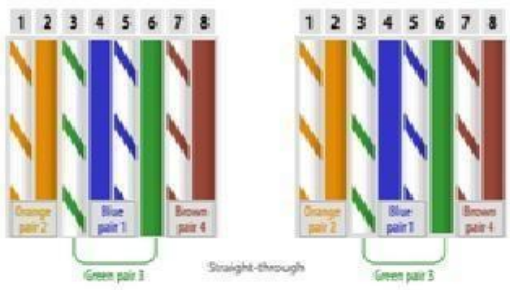
tembaga atau alumunium yang halus berupa anyaman.Bagian luar kabel berupa *plastic coating*. Di samping berfungsi untuk melindungi kabel bagian dalam sisi luar dari kabel *coaxial* juga berfungsi sebagai pentanahan (*grounding).*Kabel *coaxial* terdapat dua macam, yaitu *tinnet* dan *thicknet.*

b. Kabel *Twisted pair* (TP)

Kabel *Twisted pair* (TP) berintikan tembaga berukuran kecil. Pada masing-masing kabel berisikan 8 buah kabel kecil dengan warna yang berbeda antara satu dengan yang lainnya.Pembedaan warna pada kabel bertujuan untuk mempermudah dalam memasukannya pada konektor RG-45. Kabel *Twisted pair* (TP) terdiri dari dua macam, yaitu kabel *Unshielded Twisted Pair* (UTP) dan kabel *Shielded Twisted Pair* (STP). Berdasarkan cara pemasangannya dengan LAN *Card*, kabel *twisted pair* dapat dihubungkan dengan dua macam cara, yaitu menggunakan metode *straight* dan metode *crossover*.

1. Metode *Straight*

Metode *straight* digunakan untuk menghubungkan peralatan jaringan yang jenisnya berbeda misalnya antara komputer dengan *switch*. Pemasangan atau pengkabelannya sama dengan kabel standar. Pemasangan kabel antara warna ujung satu dengan ujung yang lain sama dengan warna dari ujung kabel standar, tidak ada yang perlu di ubah.

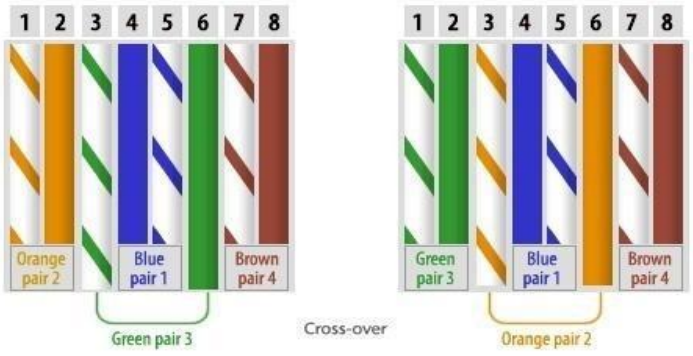


Sumber: www.trangosys/support/cat5-ethernet-cable-pin.out.shtml

Gambar II.18 Susunan Kabel *Straight Through*

2. Metode *Crossed-over*

Metode *crossed-over* digunakan untuk menghubungkan peralatan jaringan yang sejenis, misalnya antara komputer dengan komputer, *hub* dengan *hub*. Kabel yang digunakan dalam jaringan hanya 4 buah pin kabel saja. Pin-pin kabel yang dipakai adalah pin 1,pin 2, pin 3 dan pin 6. Dengan demikian pemasangan kabel *crossed-over* hanya dengan menyilangkan 4 buah pin tersebut, sedangkan kabel yang lainnya dipasang sesuai dengan kabel standar.



Sumber: www.trangosys/support/cat5-ethernet-cable-pin.out.shtml

Gambar II.19 Susunan Kabel *Crossed - Over*

c. Kabel Fiber Optik

Kabel fiber optik berisi serat optik yang sangat halus digunakan untuk mentransfer data pada jaringan komputer.Pada inti kabel terdapat serat sebagai inti (*core*) atau sering dinamakan dengan *inner optik*.*Inner optic* ini dilapisi atau dilindungi oleh bahan gelas yang disebut dengan *cladding*.Pada fiber optik terdapat dua jenis sumber cahaya yang dapat digunakan untuk melakukan pensignalan, yaitu *Semi conductor Laser* dan *LED*. Kecepatan transfer kabel fiber optik dapat mencapai ratusan mega bit perdetik (Mbps). Oleh karena itu, serat optik juga dapat digunakan untuk mengirimkan sinyal listrik dengan bit *rate* yang rendah dalam lingkungan *noise* sekalipun. Kabel fiber optik menurut modelnya

ada dua macam, yaitu *single fiber* (*mono* mode) dan *several fiber* (*multi mode).* *Single fiber* mempunyai *bandwidth* yang lebar tetapi memiliki inti *(core)* yang sangat kecil, sehingga menyulitkan dalam penyambungan *(splice).* Contoh manfaat penggunaan kabel fiber optik dalam suatu jaringan komputer adalah apabila terhubung dengan internet maka kecepatan transfer data akan terasa lebih cepat, sehingga kita tidak perlu menunggu terlalu lama untuk membuka suatu situs *website*. Kurniawan (2007:48) menjelaskan bahwa keuntungan menggunakan *fiber optic* yaitu:

1. Sangat stabil dan konsisten dalam mengakses paket data
2. Apabila terdapat suatu hambatan dalam pengiriman paket data, biasanya kendala tersebut sangat kecil dan bukan hambatan yang berarti.
3. Kecepatan akses paket data sangat tinggi, dapat mencapai 1 Gbps
4. Apabila dalam suatu jaringan membutuhkan suatu *bandwith* dalam proses transmisi datanya, maka *fiber optic* dapat dijadikan sebagai *backbone.*

Kurniawan (2007:48) menjelaskan bahwa kerugian menggunakan *fiber optic* :

1. Pemasangan dan pemeliharaan kabel memerlukan keahlian khusus lebih mahal dibandingkan kabel t*wisted pair* (TP) maupun kabel *coaxial*.
2. Pemeliharaan kabel lebih sulit, karena berada di luar ruangan.
3. Apabila terjadi gangguan seperti kabel putus, maka akan sangat sulit sekali mendeteksinya. Perawatan kabel membutuhkan biaya investasi yang tidak sedikit, sehingga pengguna rumahan jarang memakai fiber optik untuk media akses jaringannya.
4. Umumnya hanya perusahaan besar saja yang menggunakan kabel ini untuk keperluan jaringan.

d. Konektor

Kurniawan (2007:49) menerangkan bahwa Konektor "adalah *peripheral* yang dipasangkan pada ujung kabel UTP". Tujuannya agar kabel dapat dipasang pada *port* LAN. Dalam jaringan komputer konektor yang dipakai adalah konektor RJ-45. Untuk dapat memasangkan ujung-ujung kabel UTP dengan konektor RJ-45, maka diperlukan sebuah alat yang dinamakan *crimping tool.*

Sumber : www.hobbes-europe.com/product.php5?products_id=65

Gambar II.20 Konektor RJ-45

2.4.3 Mikrotik

Towidjojo (2013:1) menjelaskan bahwa "Mikrotik dikenal luas sebagai *Router.Router* adalah perangkat jaringan yang digunakan untuk menghubungkan beberapa jaringan (*network).* Dalam jaringan yang lebih komples, *Router* digunakan untuk memilihkan jalan bagi paket data untuk mencapai komputer tujuan. Fasilitas pada mikrotik :

1. *Protocol routing* RIP, OSPF, BGP.

2. Statefull Firewell.

3. Hotspot Plug-amd-Play access.

4. Remote winbox GUI *admin.*

5. DHCP.

6. *IP Security.*

Mikrotik dapat di install pada komputer yang mempunyai spesifikasi *hardware* minimal: 2 NIC, RAM 128MB, HDD 4GB, *Processor Dual Core 1,7* GHz.

2.4.4 Winbox

Madcoms (2016:63) menjelaskan bahwa "*Winbox* adalah sebuah *utility* yang digunakan untuk melakukan *remote* ke *server mikrotik* anda dalam mode GUI". Jika untuk mengkonfigurasi *mikrotik* dalam *text* mode melalui PC itu sendiri, maka untuk mode GUI yang menggunakan *winbox* ini dapat mengkonfigurasi *mikrotik* melalui komputer *client.*

Fungsi utama *winbox* adalah untuk *setting* yang ada pada mikrotik, berarti tugas utama *winbox* adalah untuk mengatur mikrotik dengan GUI atau tampilan desktop.

2.4.5 IP *Address*

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*".

Madcoms (2010:21) menjelaskan bahwa 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.