BAB 2

LANDASAN TEORI

2.1 Pengertian Jaringan

Menurut Forouzan, 2007, p7: Jaringan adalah serangkaian kumpulan alat (sering disebut *node)* yang terhubung oleh *link* komunikasi. *Node* dapat berupa komputer, *printer* atau beberapa *device* lainnya yang terhubung dengan jaringan yang mampu mengirim dan menerima data yang dihasilkan oleh *node* lainnya pada jaringan. Sebuah jaringan harus dapat memenuhi sejumlah kriteria. Kriteria yang terpenting adalah terdiri dari performa, kehandalan, dan keamanan.

Performa dapat diukur dengan berbagai cara, termasuk waktu transit dan waktu respon. Waktu transit adalah jumlah waktu yang diperlukan untuk sebuah pesan dikirim dari satu *device* ke *device* lain. Waktu respon adalah waktu yang berlangsung antara pemeriksaan informasi dan respon. Performa sebuah jaringan bergantung pada sejumlah faktor, termasuk jumlah pengguna, jenis media transmisi, kemampuan *hardware* yang terhubung, dan efisiensi *software.*

- Kehandalan

  Selain pengiriman akurasi, kehandalan jaringan diukur berdasarkan frekuensi kegagalan, waktu yang dibutuhkan sebuah *link* untuk pulih dari kegagalan, dan ketahanan jaringan dalam bencana.

- Keamanan

Masalah-masalah keamanan jaringan termasuk melindungi data dari akses yang tidak sah, melindungi data dari kerusakan, dan pelaksanaan kebijakan dan prosedur untuk pemulihan dari pelanggaran dan kehilangan data.

Jaringan komputer menjadi penting karena digunakan dalam komunikasi dan pertukaran data. Hampir di setiap perusahaan terdapat jaringan komputer untuk memperlancar arus informasi didalam perusahaan tersebut, sehingga dengan adanya jaringan komputer sangat membantu dalam meningkatkan efisiensi bisnis.

Sebuah jaringan pada awalnya hanyalah berskala kecil yaitu biasanya dengan teknologi *Local Area Network* (LAN), yang umumnya hanya dibatasi oleh area lingkungan seperti perkantoran disebuah gedung. Kemudian berkembang menjadi lingkup area yang luas dengan teknologi *Metropolitan Area Network* (MAN) misalnya untuk antar wilayah dan *Wide Area Network* (WAN) untuk antar negara, sehingga pengguna pada daerah geografis yang luas dapat dihubungkan.

Internet merupakan suatu jaringan komputer raksasa yakni terdiri dari jutaan LAN, MAN dan WAN yang terhubung dan dapat saling berinteraksi. Hal ini dapat terjadi karena adanya perkembangan teknologi jaringan yang sangat pesat, sehingga dalam beberapa tahun saja jumlah

pengguna jaringan komputer yang tergabung dalam internet berlipat ganda, karena dengan internet para pengguna dapat melakukan komunikasi tanpa adanya batasan geografis.

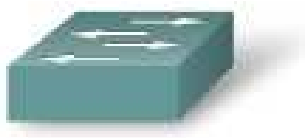
2.2 Peralatan Jaringan Komputer

Peralatan yang terhubung langsung ke segmen jaringan disebut sebagai sebuah *device. Device* ini dipecah menjadi dua klasifikasi. Klasifikasi pertama adalah *end-user device* (device untuk pengguna akhir). *End-user devices* mencakup komputer, *printer*, *scanner* dan *device* lain yang menyediakan *service* langsung ke *user*. Klasifikasi kedua adalah *network device. Network devices* mencakup semua *device* yang menghubungkan *end-user device* bersamaan untuk memungkinkan mereka berkomunikasi (Cisco Press, 2005, p48). Contoh *network device* diantaranya:

- ***Switch***

  Switch merupakan *network device* yang bekerja pada *Layer* 2 model OSI, yang mampu melakukan manajemen transfer data yaitu hanya meneruskan data ke *segmen* yang dituju. *Switch* tidak melakukan konversi format data. *Switch* mempelajari *host* mana saja yang terhubung ke suatu *port* dengan membaca *Media Access Control* (MAC) *Address* asal yang ada di dalam *frame* kemudian *switch* membuka sirkuit *virtual* antara *node* sumber dengan *node* tujuan. Dengan demikian komunikasi dua *port* tersebut tidak mempengaruhi *traffic* dari *port* lain. Hal terebut membuat LAN lebih

efisien. (Cisco Press, 2005, p53). Gambar berikut adalah simbol *switch* :



Gambar 2. 1 Switch Symbol

(Sumber : Cisco Press, 2005, pXXVII)

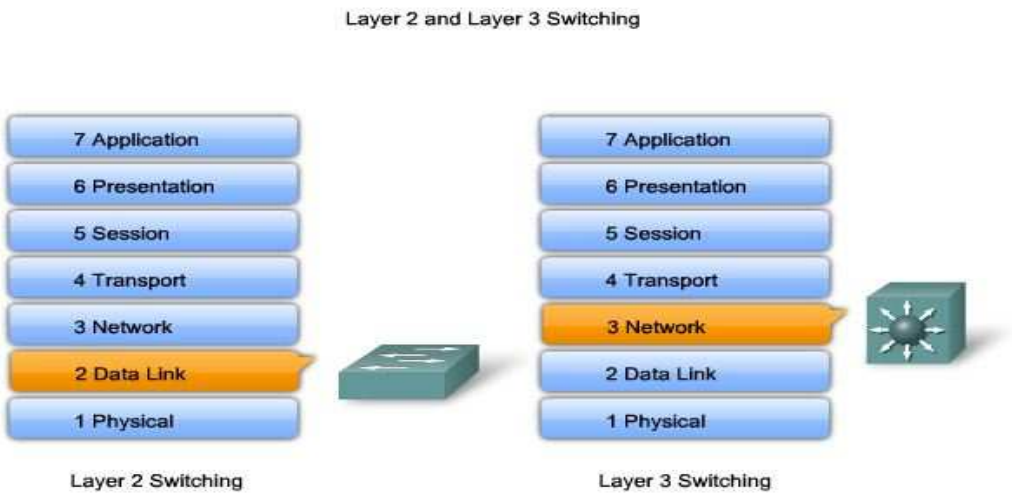
- ***Multi Layerswitch***

Menurut David, 2004, p310 : Multi Layerswitch adalah Sebuah switch layer 2 dapat melakukan switching dan filtering berdasarkan pada MAC address yang ada pada layer 2. Switch ini membuat sebuah table MAC address yang digunakan untuk keperluan forwarding data.

Sebuah switch layer 3 atau yang biasa disebut multilayer switch, contohnya Catalyst 3560, berfungsi mirip seperti switch biasa. Namun multilayer switch ini tidak hanya menggunakan MAC address dalam forwarding data, tapi juga dapat menggunakan IP address pada layer 3. Multilayer switch tidak hanya mempelajari MAC address yang berhubungan dengan port nya tapi juga dapat mempelajari IP address yang berhubungan di tiap interfacenya. Kemampuan ini membuat multilayer switch dapat mengarahkan traffic data dalam jaringan berdasarkan informasi IP address.

Multilayer switch juga dapat melakukan fungsi routing pada layer 3 yang dilakukan oleh router. Hal ini dalam membantu dalam mengurangi

perlunya router dalam jaringan LAN. Karena multilayer switch memiliki hardware yang special untuk keperluan switching, multilayer switch juga dapat melakukan fungsi routing secepat fungsi switching.



Gambar 2. 2 Layer pada MLS

(Sumber :

http://www.cisco.com/web/learning/netacad/coursecataloge/packetTreacer.html**)**

Keuntungan menggunakan multilayer switch :

- Paket (data) diforward pada layer 3 sama seperti router.
- Paket (data) diteruskan (switched) menggunakan hardware special , ASIC, untuk kecepatan tinggi dan latency yang rendah.
- Paket (data) diforward dengan control keamanan dan QoS (Quality of Service) menggunakan informasi alamat layer 3 (IP address).
- Multilayer switch didesain untuk memeriksa dan mneruskan paket dalam lingkungan LAN berkecepatan tinggi. Di mana router dapat menghadapi

masalah berupa *bottleneck* sedangkan multilayer switch dapat ditempatkan di mana saja dalam jaringan tanpa mengalami sedikit atau tanpa masalah. Gambar berikut adalah simbol *multilayer switch :*

Gambar 2. 3 Multilayer Switch Symbol

(Sumber : Cisco Press, 2005, pXXVII)

- ***Router***

Menurut Lammle, 2005, p233 : *Router* adalah sebuah alat atau perangkat lunak dalam komputer yang menentukan kemana jaringan berikutnya akan dikirim kepada atau menuju tujuannya. *Router* ini biasanya dihubungkan dengan kurang lebih dua jaringan dan memilih jalan atau cara untuk mengirimkan tiap informasi didasari pada jaringan yang berhubungan dengan *router.*

Router biasanya bertugas melakukan *routing* paket data dari *source* ke *destination* pada LAN, dan menyediakan koneksi ke WAN. Dalam lingkungan LAN, *router* membatasi *broadcast domain*, menyediakan layanan *local address resolution* seperti ARP *(Address Resolution Protocol)* dan RARP *(Reverse Address Resolution Protocol)*, dan membagi *network* dengan menggunakan struktur *subnetwork.*

Gambar berikut adalah simbol *router* :

Gambar 2. 4 Router Symbol

(Sumber : Cisco Press, 2005, pXXVII)

2.3 Macam - Macam Jaringan

2.3.1 Local Area Network (LAN)

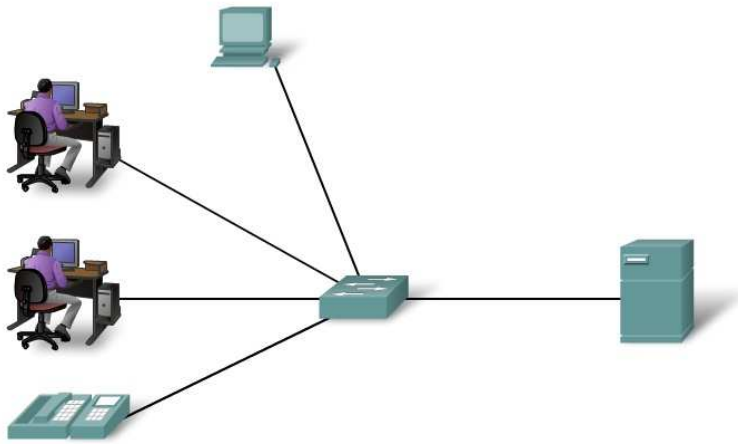
Menurut Reynolds, 2009, p8 : Local area network (LAN) merupakan suatu jaringan komputer yang menghubungkan suatu komputer dengan komputer lain untuk pemakaian bersamaan dengan jarak yang terbatas. LAN memungkinkan user untuk berbagi akses file yang sama dan membentuk komunikasi internal serta pemakaian bersama perangkat elektronik seperti printer dan scanner sehingga lebih efisien. LAN ditandai oleh berikut:

- Mentransfer data dengan kecepatan tinggi.
- Ada dalam wilayah geografis yang terbatas.
- Umumnya lebih murah.

LAN dapat digambarkan secara sederhana seperti dua buah PC dan *printer* yang terdapat pada *home office,* atau secara luas dapat dilihat pada

perusahaan yang dalam perusahaan tersebut suara, bunyi, dan video *peripherals* termasuk didalamnya. LAN hanya dapat terhubung dengan beberapa kilometer saja.

Gambar berikut menggambarkan jaringan *Local Area Network* (LAN).



Gambar 2. 5 Local Area Network (LAN)

(Sumber : Cisco Press, 2005, p70)

Setiap *personal computer* (PC) yang menggunakan LAN, membutuhkan *Network Inteface Card* (NIC) atau *Network Adapter Card* (NAC). Card ini berfungsi untuk memindahkan data dari PC ke jaringan dan dari jaringan ke PC.

Ukuran LAN dapat ditentukan dengan pembatasan jumlah user per *software*, atau dengan pembatasan jumlah pengguna untuk mengakses sistem operasi. Selain ukuran, LAN dibedakan dari jenis jaringan lainnya oleh media transmisi dan topologi. Secara umum, LAN tertentu akan

menggunakan hanya satu jenis medium transmisi. Dan secara khusus, LAN memiliki jangkauan kecepatan data sebesar 4-16 Mbps. Akan tetapi sangat umum untuk LAN untuk memiliki kecepatan data sebesar 100 Mbps atau 1 Gbps.

Biasanya, LAN menggunakan pendekatan jaringan *broadcast* lebih daripada pendekatan *switching*. Dengan *broadcast communication network*, tidak ada *node-node* penengah. Pada masing-masing *station*, terdapat sebuah *transmitter/receiver* yang menghubungkan media dengan *station* dengan *station* lain. Sebuah transmisi dari satu *station* disiarkan dan diterima oleh semua *station-station* lain. Data biasanya transmisikan dalam bentuk paket. Karena medianya dibagi, maka hanya ada satu *station* pada saat itu yang dapat mentransmisikan paket.

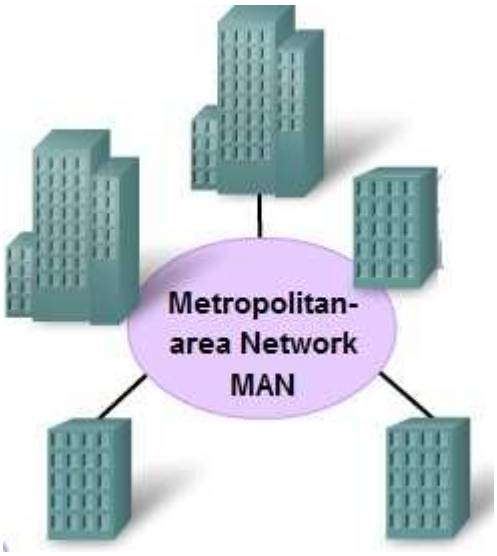
2.3.2 Metropolitan Area Network (MAN)

Menurut Forouzan , 2007, p15: *Metropolitan Area Network* (MAN) adalah jaringan dengan ukuran berada diantara LAN dan WAN. MAN dapat mencakup kantor-kantor perusahaan yang letaknya berdekatan atau juga antar kota dan dapat dimanfaatkan untuk keperluan pribadi (swasta) atau umum.

MAN mampu menunjang data dan suara, bahkan dapat berhubungan dengan jaringan televisi kabel. MAN adalah satu rangkaian komputer yang disambungkan antara satu sama lain pada kedudukan geografi yang luas, gabungan LAN dan WAN pada satu lokasi kepada satu LAN dan WAN pada lokasi yang lain dengan penyambungan kepada *backbone* yang dijalankan

oleh standar telekomunikasi.

Gambar berikut menggambarkan *Metropolitan Area Network* (MAN).



Gambar 2. 6 Metropolitan Area Network (MAN)

(Sumber : Cisco Press, 2005, p73)

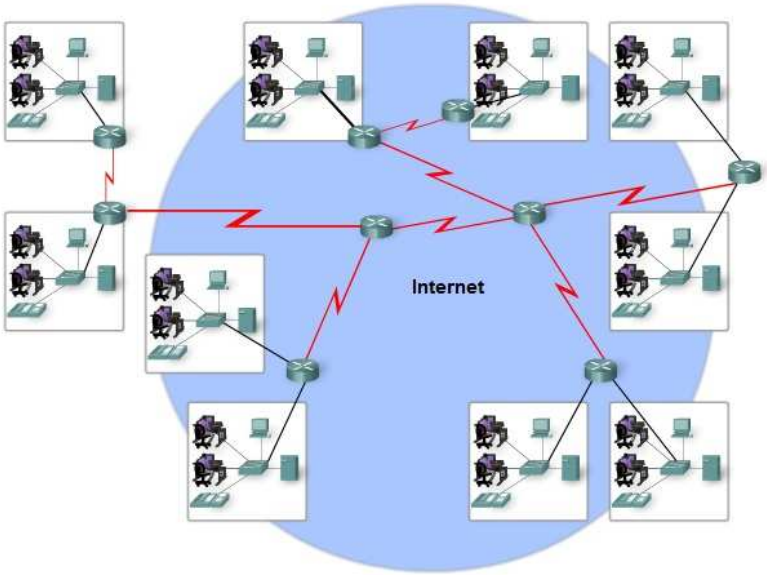
Keunggulan dari MAN itu sendiri, MAN dapat mentransfer data dengan berkecepatan tinggi, yang menghubungkan berbagai lokasi seperti kampus, perkantoran, pemerintahan, dan sebagainya.

2.3.3 Wide Area Network (WAN)

Menurut Forouzan, 2007, p14 : *Wide Area Network* (WAN) merupakan jaringan komputer jarak jauh untuk transmisi data, gambar, audio, dan informasi video melalui area geografis yang besar yang mungkin terdiri dari suatu negara, sebuah benua, atau bahkan seluruh dunia. WAN ditandai oleh berikut:

- Ada dalam suatu wilayah geografis yang luas.
- Lebih rentan terhadap kesalahan karena jarak perjalanan data.
- Interkoneksi dari beberapa LAN.
- Lebih canggih dan kompleks daripada LAN.
- Teknologinya mahal.

Gambar berikut menggambarkan jaringan *Wide Area Network* (WAN).



Gambar 2. 7 Wide Area Networks (WAN)

(Sumber : Cisco Press, 2005, p71)

Biasanya, WAN diimplementasikan menggunakan satu dari dua teknologi ini : *Circuit Switching dan Packet Switching.*

Circuit Switching merupakan jalur komunikasi yang tepat dibangun diantara dua station melewati *node* atau persimpangan jaringan. Jalur yang

dimaksud adalah suatu rangkaian jaringan fisik yang terhubung diantara *node.* Pada masing-masing jaringan, suatu *logical channel* dimasukkan ke dalam proses koneksi ini. Data yang dikirimkan oleh sumber station ditransmisikan sepanjang jalur yang tepat secepat mungkin. Pada setiap *node*, data yang masuk diarahkan atau dialihkan ke *channel* keluar yang tepat tanpa mengalami penundaan sama sekali. Contoh yang paling umum dalam hal *circuit switching* adalah jaringan telepon.

Untuk jaringan *Packet Switching* menggunakan pendekatan yang berbeda. Dalam hal ini, tidak perlu menggunakan kapasitas transmisi sepanjang jalur melewati jaringan. Cukup dengan, data dikirim keluar dengan menggunakan rangkaian potongan-potongan kecil secara berurutan, yang disebut *packet.* Masing-masing *packet* melewati jaringan dari satu *node* ke *node* yang lain sepanjang jalur yang membentang dari sumber ke tujuan. Pada setiap *node*, seluruh *packet* diterima, disimpan dengan cepat, dan ditransimisikan ke *node* berikutnya. Jaringan *packet switching* umumnya dipergunakan untuk komunikasi dari terminal ke komputer dan dari komputer ke komputer.

2.4 Konsep Dasar VLAN (Jurnal)

Gozali dan Lo (2012: 70) Virtual Local Area Network atau dikenal dengan VLAN merupakan fungsi logik dari sebuah perangkat jaringan, dimana fungsi logik ini mampu membagi jaringan LAN yang secara fisik

tersambung dalam suatu jaringan global ke dalam beberapa jaringan yang bersifat virtual. Dengan menggunakan VLAN maka administrator jaringan dapat lebih mudah mengelompokkan workstation didalam jaringan berdasarkan fungsinya tanpa dibatasi oleh lokasi fisik workstation tersebut. Berbagai kelebihan VLANjika dibandingkan dengan LAN biasa, antara lain:

- ***Broadcast control***, dimana VLAN mampu membatasi *broadcast network* dari masing-masing grup.
- ***Security***, dimana VLAN membentengi akses ke sebuah grup dari group VLAN lain atau akses dari luar jaringan.
- ***Performance***, dimana pengelompokkan secara grup logik ini memberikan jalur data yangbersifat ***dedicated*** untuk tiap-tiap grup, sehingga secara otomatis masing-masing grup akan mendapat kinerja jalur data yang optimal.
- ***Management***, prinsip logik pada VLAN memberikan kemudahan seorang user dari suatu grup VLAN untukberpindah lokasi tanpa perlu mengganti koneksi/sambungan ke switch, dan administrator dapat dengan mudah mengubah keanggotaan suatu grup VLAN melalui aplikasi jaringan tanpa harus mengubah jaringan secara fisik.

Keanggotaan suatu workstation pada VLAN dapat dibedakan dalam dua kelompok yaitu yang bersifat statis dan bersifat dinamis.**VLAN Statis** merupakan cara umum dalam mengembangkan VLAN, dan sekaligus merupakan cara yang paling aman. Port pada switch bertugas untuk

mempertahankan konektifitas pada VLAN secara statis. Pada implementasi ini administrator secara manual mengubah penugasan atau keanggotaan dari port tersebut. Keanggotaan VLAN jenis ini, umumnya digunakan untuk jaringan komputer yang sederhana dan jumlah workstation yang terhubung sifatnya terbatas.

2.5 Topologi Jaringan

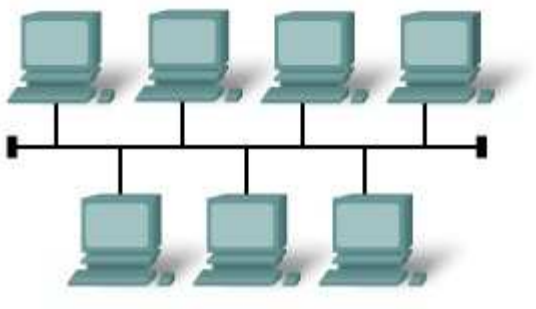
Topologi yang mendefinisikan bagaimana jaringan komputer, printer, perangkat jaringan, dan perangkat lainnya dapat terhubung. Dengan kata lain, topologi jaringan menggambarkan layout kabel dan perangkat serta jalur yang digunakan oleh pengiriman data. Topologi sangat mempengaruhi bagaimana jaringan bekerja. (Cisco Press, 2005, p62).

Berikut ini adalah beberapa topologi jaringan, yaitu:

a. Topologi *Bus*

Beberapa *node* dipasangkan dengan jalur data (bus). Masing-masing *node* dapat melakukan tugas-tugas dan operasi yang berbeda namun semua mempunyai hierarki yang sama. Topologi ini biasanya menggunakan kabel *coaxial,* yang sekarang sudah sangat jarang digunakan atau diimplementasikan. Pada topologi ini semua terminal terhubung ke jalur komunikasi. (Cisco Press, 2005, p63)

Gambar berikut adalah gambaran dari topologi *Bus* :



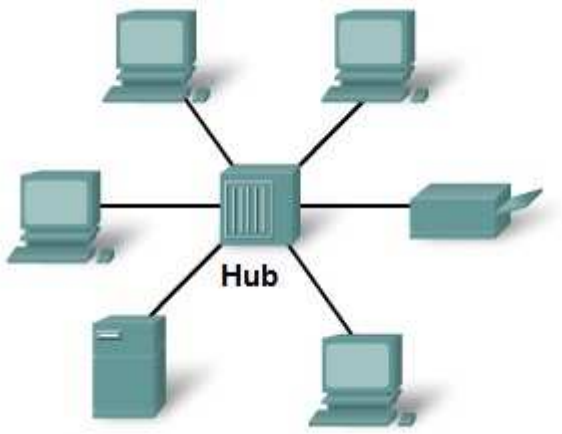
Gambar 2. 8 Topologi Bus

(Sumber : Cisco Press, 2005, p63)

b. Topologi *Star*

Beberapa *node* yang dipasangkan dengan simpul pusat, yang membentuk jaringan fisik seperti bintang, semua komunikasi ditangani langsung dan dikelola oleh *host* yang berupa *main frame* komputer seperti *switch* dan *hub.* Topologi *star* digunakan dalam jaringan yang padat, ketika *end point* dapat dicapai langsung dari lokasi pusat, kebutuhan untuk perluasan jaringan, dan membutuhkan kehandalan yang tinggi. Topologi ini merupakan susunan yang menggunakan lebih banyak kabel daripada *bus* dan karena semua komputer dan perangkat terhubung ke *central point.* Jadi bila ada salah satu komputer atau perangkat yang mengalami kerusakan maka tidak akan mempengaruhi yang jaringan yang lainnya. (Cisco Press, 2005, p64)

Gambar berikut adalah gambaran dari topologi Star :



Gambar 2. 9 Topologi Star

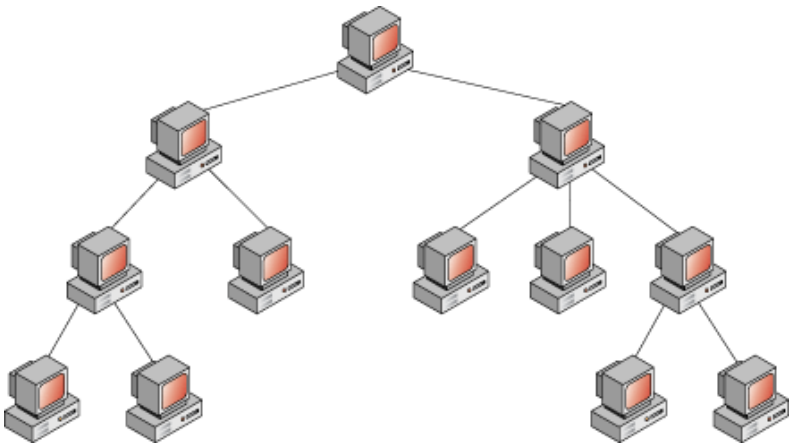
(Sumber : Cisco Press, 2005, p64)

Pada topologi ini semua transmisi dari stasioner yang satu ke stasioner yang lain harus melalui *server,* setelah itu baru dikirim ke alamat yang dituju.

c. Topologi *Hierarchical*

Berbentuk seperti pohon bercabang yang terdiri dari komputer induk (host) yang dipasangkan dengan simpul atau *node* lain secara berjenjang, jenjang yang lebih tinggi berfungsi sebagai pengatur kerja jenjang dibawahnya, biasanya topologi ini digunakan oleh perusahaan besar atau lembaga besar yang mempunyai beberapa cabang daerah, sehingga data dari pusat bisa didistribusikan ke cabang atau sebaliknya. (Cisco Press, 2005, p67)

Gambar berikut adalah gambaran dari topo topologi *Hierarchical* :



Gambar 2. 10 Topologi Hierarchical

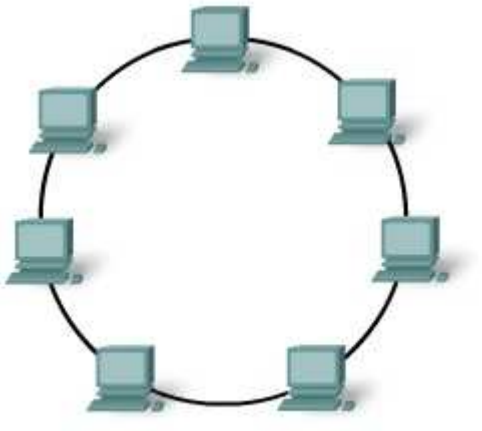
(Sumber : Cisco Press, 2005, p67)

d. Topologi *Ring*

Di dalam topologi *Ring* semua *workstation* dan *server* dihubungkan sehingga terbentuk suatu pola lingkaran atau cincin. Tiap *workstation* ataupun *server* akan menerima dan melewatkan informasi dari satu komputer ke komputer lain, bila alamat- alamat yang dimaksud sesuai maka informasi diterima dan bila tidak informasi akan dilewatkan. Kelemahan dari topologi ini adalah setiap *node* dalam jaringan akan selalu ikut serta mengelola informasi yang dilewatkan dalam jaringan, sehingga bila terdapat gangguan disuatu *node* maka seluruh jaringan akan terganggu. Keunggulan topologi *Ring* adalah tidak terjadinya *collision* atau tabrakan pengiriman data seperti pada topologi *Bus*, karena hanya satu *node* dapat mengirimkan data pada suatu saat, dan yang

lainnya menunggu hingga pengiriman data selesai. (Cisco Press, 2005, p66)

Gambar berikut adalah gambaran dari topo topologi *Ring* :



Gambar 2. 11 Topologi Ring

(Sumber : Cisco Press, 2005, p66)

2.5 Arsitektur Protokol Jaringan

2.5.1 Model Open System Interconnection (OSI)

Menurut Lukas , 2006, pp22-24: model *Open System Interconnection* (OSI) dikembangkan oleh *International Standard Organization* (ISO) sebagai model untuk merancang komunikasi komputer dan sebagai kerangka dasar untuk mengembangkan protokol lainnya. OSI terdiri dari tujuh layer dan standar OSI telah diterima di industri komunikasi yang mana dipakai untuk mengatur karakteristik, elektrik dan prosedur dari perlengkapan komunikasi.

Model *Open System Interconnection* (OSI) Layer digambarkan seperti pada gambar berikut :

Gambar 2. 12 Model OSI

(Sumber : Cisco Press, 2005, p94)

- *Application Layer*

  Berfungsi sebagai antarmuka dengan aplikasi dengan fungsionalitas jaringan, mengatur bagaimana aplikasi dapat mengakses jaringan, dan kemudian membuat pesan-pesan kesalahan. Protokol yang berada dalam lapisan ini adalah HTTP, FTP, SMTP, dan NFS.

- *Presentation Layer*

  Berfungsi untuk mentranslasikan data yang hendak ditransmisikan oleh aplikasi ke dalam format yang dapat ditransmisikan melalui jaringan. Protokol yang berada dalam level ini adalah perangkat lunak redirektor (redirector *software),* seperti layanan *Workstation* (dalam Windows NT)

dan juga *Network shell* (semacam *Virtual Network Computing* (VNC) atau *Remote Desktop Protocol* (RDP)).

- *Session Layer*

  Berfungsi untuk mendefinisikan bagaimana koneksi dapat dibuat, dipelihara, atau dihancurkan. Selain itu, di level ini juga dilakukan resolusi nama.

- *Transport Layer*

  Berfungsi untuk memecah data ke dalam paket-paket data serta memberikan nomor urut ke paket-paket tersebut sehingga dapat disusun kembali pada sisi tujuan setelah diterima. Selain itu, pada level ini juga membuat sebuah tanda bahwa paket diterima dengan sukses (acknowledgement), dan mentransmisikan ulang terhadp paket-paket yang hilang di tengah jalan.

- *Network Layer*

  Berfungsi untuk mendefinisikan alamat-alamat IP, membuat *header* untuk paket-paket, dan kemudian melakukan *routing* melalui *internetworking* dengan menggunakan *router* dan *switch layer-3.*

- *Data Link Layer*

  Befungsi untuk menentukan bagaimana bit-bit data dikelompokkan menjadi format yang disebut sebagai *frame.* Selain itu, pada level ini terjadi koreksi kesalahan, *flow control,* pengalamatan perangkat keras (seperti halnya Media Access Control Address (MAC Address)), dan menetukan bagaimana perangkat-perangkat jaringan seperti *hub, bridge,*

repeater, dan *switch layer 2* beroperasi. Spesifikasi IEEE 802, membagi *level* ini menjadi dua level anak, yaitu lapisan *Logical Link Control* (LLC) dan lapisan *Media Access Control* (MAC).

- *Physical Layer*

  Berfungsi untuk mendefinisikan media transmisi jaringan, metode pensinyalan, sinkronisasi bit, arsitektur jaringan (seperti halnya Ethernet atau Token Ring), topologi jaringan dan pengabelan. Selain itu, level ini juga mendefinisikan bagaimana *Network Interface Card* (NIC) dapat berinteraksi dengan media kabel atau radio.

2.5.2 Model TCP/IP

Dalam perpindahan data pada jaringan komputer, sebagai alamat tujuan dalam jaringan adalah menggunakan *Internet Protocol address* atau yang biasa dikenal dengan IP *address*. IP *address* digunakan sebagai pengalamatan dalam jaringan komputer, konsep ini berdasarkan dari konsep TCP/IP, yang digunakan sebagai dasar dalam pembentukan jaringan komputer dewasa. Penentuan IP *address* dapat ditentukan dengan berbagai cara, namun ada aturan-aturan yang harus dipenuhi guna menjaga kemudahan dalam manajemen jaringan.

Transfer Control Protocol / Internet Protocol atau biasa dikenal dengan TCP/IP adalah hasil riset yang dikembangkan badan pertahanan Amerika Serikat yang awalnya diberi nama ARPANET. Sama seperti arsitektur OSI, TCP/IP juga menggunakan sistem *layering*. Jika arsitektur

OSI dikenal dengan *seven layer* OSI, karena memiliki tujuh *layer* arsitektur. Sedangkan TCP/IP hanya mempunyai empat *layer* arsitektur, yaitu *application layer* dan *transport layer* dari segi *protocol* dan internet serta *network access* pada bagian *networks.*

Model TCP/IP Layer digambarkan seperti pada gambar 2.12 berikut :

Gambar 2. 13 Model TCP/IP

(Sumber : Cisco Press, 2005, p94)

2.6 Dynamic host configuration protocol (DHCP)

Menurut Chris, 2003, p349 : DHCP adalah protokol yang berbasis arsitektur c*lient / server* yang digunakan untuk memudahkan pengalokasian alamat IP dalam suatu jaringan, tanpa harus memberikan alamat *IP* secara manual. Fungsi DHCP adalah sebagai berikut:

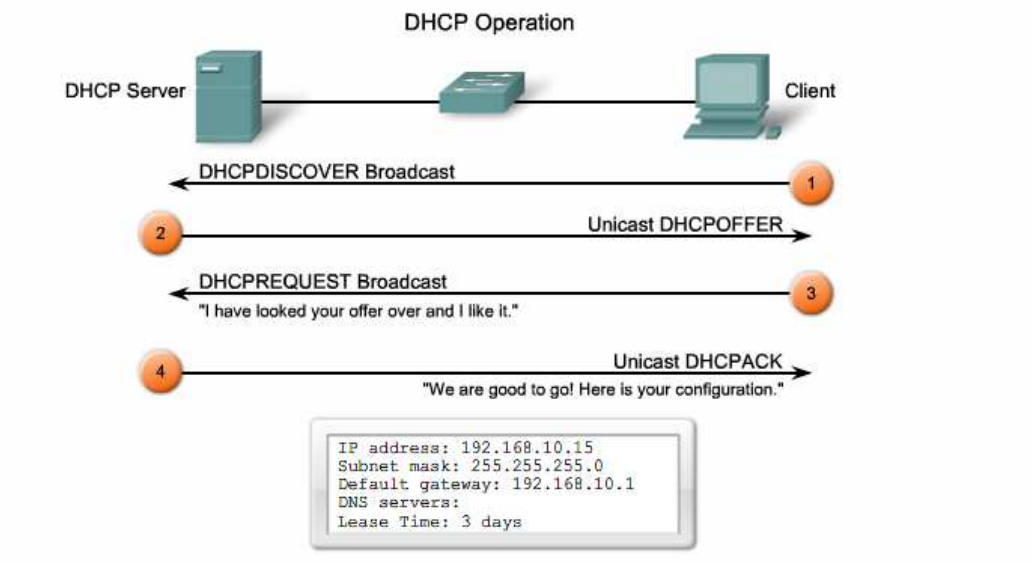
- DHCP *server* merupakan sebuah mesin yang menjalankan layanan yang dapat memberikan alamat IP dan informasi TCP /IP lainnya kepada semua klien yang memintanya.
- DHCP *client* merupakan mesin klien yang menjalankan perangkat lunak klien DHCP yang memungkinkan mereka untuk dapat berkomunikasi dengan DHCP server

DHCP *server* pada umum nya memiliki sekumpulan alamat yang diizinkan untuk didistribusikan kepada klien, yaitu disebut dengan DHCP *Pool.* Setiap klien akan menyewa alamat IP dari DHCP *Pool*. Setiap klien kemudian akan menyewa alamat ip dari DHCP *Pool* ini untuk waktu penyewaan alamat IP tersebut habis masanya, klien akan meminta kepada server untuk memberikan alamat IP yang baru atau memperpanjangnya.

Berikut adalah langkah-langkah dalam proses DHCP *operation*:

1. DHCP *Discover* : DHCP *client* akan menyebarkan request secara broadcast untuk mencari DHCP server yang aktif.
2. DHCP *Offer* : Setelah DHCP server mendengar broadcast dari DHCP client, DHCP server kemudian menawarkan sebuah alamat yang tersedia dalam DHCP *Pool* pada DHCP server yang bersangkutan
3. DHCP *Request* : Client meminta DHCP server untuk menyewakan alamat IP dari salah satu alamat yang tersedia dalam DHCP *Pool* pada DHCP server yang bersangkutan

4. DHCP *Pack* : DHCP server akan merespons permintaan dari klien dengan mengirimkan paket *acknowledgment*. Kemdian DHCP *server* akan menetapkan sebuah alamat (dan konfigurasi TCP / IP lainnya) kepada klien, dan memperbaharui basis data *database* miliknya. Klien selanjutnya akan memulai proses *binding* dengan tumpukan protocol TCP / IP dank arena telah memiliki alamat IP, klien pun dapat memulai komunikasi jaringan.



Gambar 2. 14 DHCP Operation

(Sumber :

http://www.cisco.com/web/learning/netacad/coursecataloge/packetTreacer.html**)**

2.7 Secure Shell (SSH)

Menurut Chris, 2003, P.232 : SSH adalah metode untuk melakukan otentikasi klien dan menjaga sesi beberapa layanan antara dua sistem. SSH

mendengarkan port 22 untuk permintaan koneksi masuk (Chris, 2003, P.232). Ketika dua sistem menjalankan SSH akan membentuk sambungan lalu melakukan validasi ke setiap perintah lain untuk setiap sistem yang telah divalidasi. *Triple* DES adalah penggunaan untuk enkripsi semua informasi yang pertukaran antara kedua sistem. Dua *host* otentikasi satu sama lain dalam sesi komunikasi dan berkala mengubah kunci enkripsi. Ini membantu untuk memastikan bahwa kekerasan atau serangan pemutaran tidak efektif.

SSH merupakan metode yang baik untuk mengamankan protokol yang tidak diketahui. misalnya, telnet dan FTP sesi pertukaran semua informasi otentikasi di jelas. ssh dapat merangkum sesi ini untuk memastikan bahwa tidak ada informasi yang jelas terlihat.

2.8 Keamanan Jaringan

Menurut Kizza, 2005, p49 : Keamanan adalah proses yang terus-menerus melindungi objek dari serangan. Objek tersebut mungkin orang, sebuah organisasi seperti bisnis, atau sistem komputer dan file.

Keamanan merupakan hal yang penting dalam sebuah jaringan komputer, karena faktor keamanan inilah yang menjadi pelindung bagi data-data yang mengalir di dalam jaringan komputer. Pada dasarnya ada tiga aspek yang dapat dikelompokkan dalam upaya mengamankan jaringan komputer dari ancaman-ancaman yang mungkin dapat merusak sistem yang sedang berjalan. Tiga hal yang menjadi segmentasi dalam melakukan keamanan jaringan yaitu:

- Pengamanan dari segi *hardware*

  Pengamanan dalam segi *hardware* adalah upaya kita untuk mengamankan *device-device* penting yang menjadi bagian dalam jaringan komputer seperti menempatkan *server* pada ruangan tertentu yang terlindungi. Atau memberikan pelindung kabel jaringan. Dan masih banyak hal yang bisa dilakukan untuk mengamankan *device* jaringan.

- Pengamanan dari segi *software*

  Pengamanan dari segi *software* adalah pengamanan dari virus-virus yang banyak di internet. Banyak cara yang dapat dilakukan seperti memasang antivirus dan memasang *firewall.*

- Pengamanan dari *human error*

  Pengamanan dari *human error* atau penyusup dengan cara melakukan pelatihan pada operator, melakukan *backup* berkala. Untuk melindungi dari penyusup dapat diberikan *access list* pada jaringan dilengkapi dengan *user account.*

2.9 *Virtual* LAN (VLAN)

Menurut Forouzan, 2007, p458 : VLAN adalah kelompok *device* dalam sebuah LAN yang dikonfigurasi (menggunakan software manajemen) sehingga mereka dapat saling berkomunikasi asalkan dihubungkan dengan jaringan yang sama walaupun secara fisikal mereka berada pada segmen LAN yang berbeda.

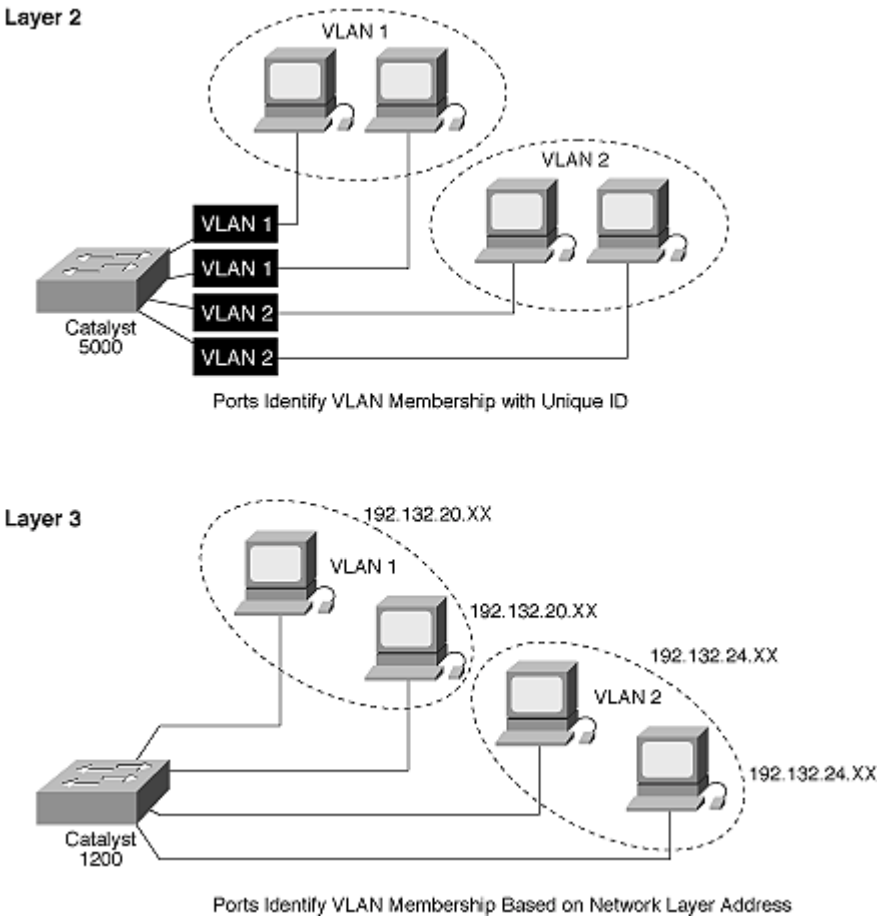
Virtual LAN (VLAN) menawarkan sebuah solusi dengan memungkinkan

pengguna di setiap lokasi untuk berpartisipasi dalam LAN. Keanggotaan VLAN dilakukan didalam *switch* dan dapat didasarkan pada asosiasi *port* fisik, MAC *address,* alamat jaringan atau karakteristik paket lainnya. Sebuah karakteristik kunci dari VLAN adalah bahwa setiap VLAN mewakili *broadcast domain* terpisah.

Berikut adalah beberapa cara VLAN dapat menyederhanakan manajemen jaringan. VLAN dapat mengelompokkan beberapa *broadcast domain* dalam beberapa *subnet logical.* Pengguna dapat menambah jaringan, memindahkan, dan melakukan perubahan dengan mengkonfigurasi *port* ke VLAN yang tepat :

- Pengguna dapat menempatkan sebuah kelompok pengguna yang memerlukan keamanan tinggi kedalam VLAN sehingga tidak ada pengguna diluar dari VLAN yang dapat berkomunikasi dengan mereka.
- VLAN dapat dianggap independen.
- VLAN dapat meningkatkan keamanan jaringan.

Penggunaan VLAN akan membuat pengaturan jaringan menjadi sangat fleksibel dimana dapat dibuat segmen yang bergantung pada organisasi, tanpa bergantung pada lokasi *workstation* seperti pada gambar dibawah ini :



Gambar 2. 15 Virtual LAN (VLAN)

(**Sumber :**

http://www.cisco.com/web/learning/netacad/coursecataloge/packetTreacer.html)

Beberapa keuntungan penggunaan VLAN antara lain:

1. *Security* – keamanan data dari setiap divisi dapat dibuat tersendiri, karena segmennya bisa dipisah secara logika. Lalu lintas data dibatasi segmennya.
2. *Higher performance* – pembagian jaringan *layer* 2 ke dalam beberapa

kelompok *broadcast domain* yang lebih kecil, yang tentunya akan mengurangi lalu lintas paket yang tidak dibutuhkan dalam jaringan.

3. *Broadcast storm mitigation* – pembagian jaringan ke dalam VLAN-VLAN akan mengurangi banyaknya *device* yang berpartisipasi dalam pembuatan broadcast *storm.* Hal ini terjadinya karena adanya pembatasan *broadcast domain.*
4. *Improved IT staff efficiency* – VLAN memudahkan manajemen jaringan karena pengguna yang membutuhkan sumber daya yang dibutuhkan berbagi dalam segmen yang sama.

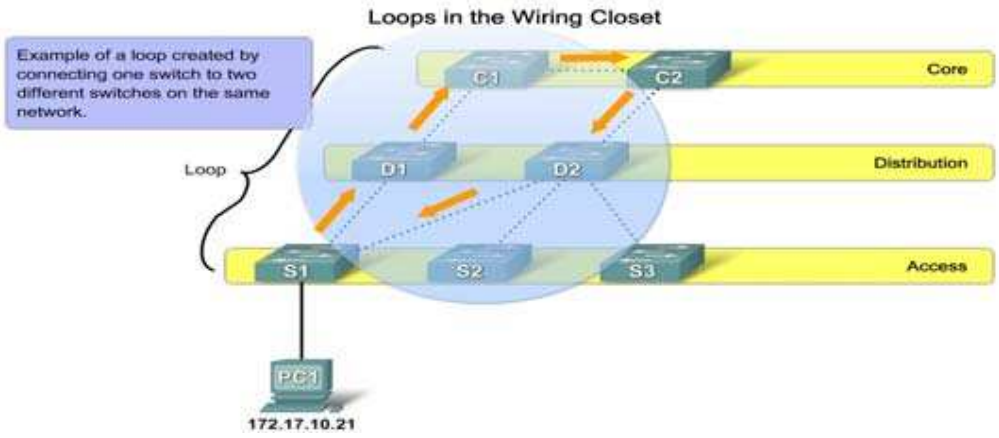
2.10 Spanning Tree Protocol (STP)

Menurut David, 2004, p217 : *Spanning Tree Protocol* adalah sebuah protokol manajemen link yang menyediakan jalur *backup* untuk mencegah terjadinya *loop* yang tidak diinginkan dalam jaringan. Pada jaringan Ethernet agar dapat berjalan dengan baik, hanya satu jalur yang dapat berada diantara dua titik. Jika ada jalur ganda, maka sangat mungkin akan terjadi penyampaian pesan ganda dan akan mengakibatkan tingginya *traffic.*

Redundancy adalah jalur jaringan alternatif yang digunakan untuk meningkatkan ketersediaan jaringan, sehingga jika dalam suatu jaringan terdapat link yang terputus maka jalur untuk data masih bisa terhubung tanpa mempengaruhi konektivitas perangkat pada jaringan tersebut.

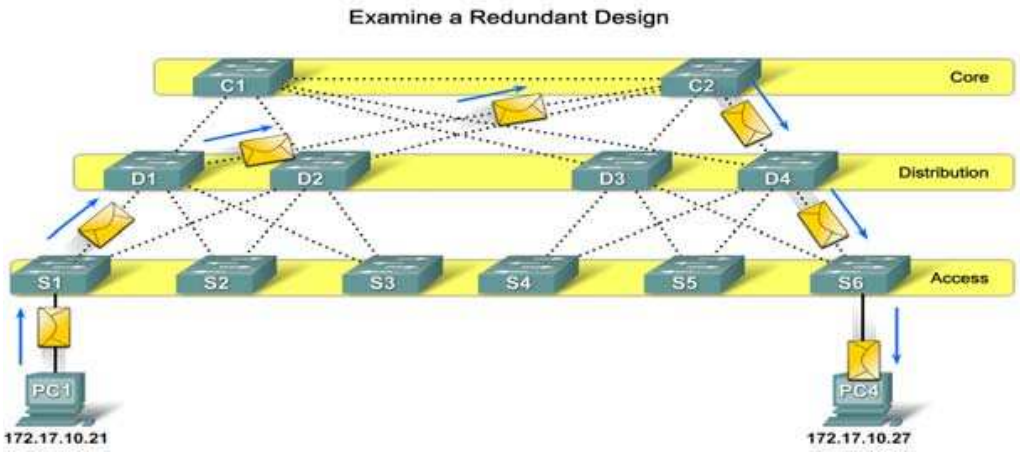
Loop terjadi karena adanya jalur lain antara satu titik. Untuk menyediakan jalur *backup* dan mencegah terjadinya *loop* yang tidak diinginkan pada suatu jaringan yang mengakibatkan *overload traffic* dan memakan banyak *bandwidth,* maka *spanning tree* melakukan *blocking* pada jalur *backup,* dan akan mengaktifkannya jika diperlukan. STP hanya mengijinkan satu jalur yang aktif diantara dua titik dan menjadikan jalur alternatif sebagai *backup* jalur yang diblok dan akan diaktifkan jika jalur utama *crash.*

Broadcast Storm terjadi ketika ada begitu banyak frame broadcast terperangkap dalam loop dan semua bandwitch yang tersedia dikonsumsi. Akibatnya, tidak ada bandwitch yang tersedia untuk lalu lintas yang lain. *Broadcast Storm* tidak dapat dihindari pada jaringan redudancy. Sebagai perangkat yang mengirim lebih broadcast keluar jaringan, lalu lintas semakin banyak tertangkap loop, dan akhirnya menciptakan broadcast syang menyebabkan jaringan gagal.



Gambar 2. 16 Loop yang terjadi

(http://www.cisco.com/web/learning/netacad/coursecataloge/packetTreacer.html)



Gambar 2. 17 Pemilihan jalur aktif

(http://www.cisco.com/web/learning/netacad/coursecataloge/packetTreacer.html)

STP mempunyai algoritma sendiri untuk menentukan jalur utama dan jalur yang mana yang akan diblok sehingga tidak terjadi *loop*, algoritma itu disebut dengan *Spanning Tree Algorithm.*

Berikut cara kerja *Spanning Tree Atgorithm* :

- *Semua switch* dalam LAN berpartisipasi dengan cara melakukan pertukaran data. Data yang ditukarkan adalah BPDU (Bridge *Protocol Data Unit).* Hal ini untuk menentukan *Root Bridge.*
- *Switch* dengan *Bridge* ID (BID) terkecil akan terpilih sebagai *Root Bridge.* Jika terdapat dua *Switch* dengan BID terkecil maka pemilihan dilakukan dengan melihat MAC *address* yang paling

kecil.

- Setelah *Root Bridge* terpilih, selanjutnya adalah memilih *Root Port.* Setiap *switch* yang tidak terpilih sebagai *Root Bridge* akan menentukan *port interface* mana yang akan menjadi *Root Port* dengan memilih *Shortest Path* (SP) dengan nilai terkecil.
- Jika ada dua *port interface* dengan nilai SP terkecil yang sama maka akan dipilih dengan melihat *port priority* terkecil, jika ada dua yang sama maka akan dipilih berdasarkan dengan *port* ID terkecil.
- Selanjutnya menentukan *Designed Port* dan *Non-designed Port.* Setiap *port interface* yang tidak terpilih sebagai *Root* Port akan menjadi *Designed Port* (DP), jika ada DP yang bersebelahan secara langsung maka DP dengan *port priority* yang lebih besar akan menjadi NDP.

Setiap *port* pada *switch* yang menggunakan *Spanning Tree* ada di salah satu dari lima *state* berikut.

- *Blocking*
- *Listening*
- *Learning*
- *Forwarding*
- *Disable*

2.11 VLAN Trunking Protocol (VTP)

Menurut David, 2004, p171 : VTP adalah *Layer* 2 *messaging protocol* yang digunakan untuk menjaga konsistensi dari konfigurasi VLAN dengan cara mengatur penambahan, penghapusan dan perubahan nama dari VLAN. Jika tidak mengunakan VTP maka perubahan-perubahan terhadap VLAN dilakukan secara manual pada setiap *switch.* Dengan VTP perubahan hanya dilakukan pada VTP *server* dan VTP *server* akan menyalurkan pesan perubahan ke semua *switch* yang terhubung. VTP memberikan manfaat sebagai berikut :

- Konfigurasi VLAN konsistensi diseluruh jaringan.
- Skema pemetaan yang memungkinkan suatu VLAN untuk menjadi *trunk* diatas media campuran.
- kurat pelacakan dan pemantauan VLAN.
- Pelaporan dinamis ditambahkan diseluruh jaringan VLAN.
- *Plug-and-play* saat menambahkan konfigurasi baru VLAN

2.11.1 VTP *Domain*

VTP *domain* merupakan kumpulan dari *switch – switch* yang mempunyai satu manajemen yang sama. Fungsi dari VTP adalah untuk melakukan pengaturan *switch* CISCO sebagai suatu kelompok *switch management* yang tergabung dalam VTP *domain.*

Satu *switch* hanya bisa menjadi bagian dari satu *switch management domain* dan secara *default* tidak menjadi bagian dari *switch management domain* manapun.

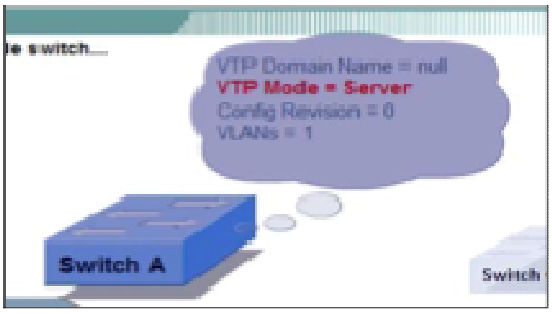
2.11.2 VTP *Mode*

Setting awal dari *switch* adalah tidak tergabung dalam *switch management domain* manapun, untuk membuatnya menjadi bagian dalam suatu *switch management domain* adalah dengan melakukan konfigurasi sehingga *switch* tersebut menjadi salah satu dari tiga jenis *mode* VTP untuk menentukan bagaimana cara suatu *switch* berkomunikasi dengan *switch* VTP lainnya dalam *switch management domain* tersebut. Berikut *mode* VTP yaitu:

- VTP *Server*

  VTP *server* dapat menambahkan, menghapus dan mengganti nama dari VLAN dan juga menyebarkan nama VTP *domain* dan nomor revisi dari konfigurasi VLAN. Secara *default, switch* akan mempunyai *setting* sebagai berikut:

  - VTP *domain name = null*
  - VTP *Mode = Server*
  - *Config Revison* = 0
  - VLANs = 1



Gambar 2. 18 Konfigurasi awal switch

(sumber:http://www.cisco.com/web/learning/netacad/coursecataloge/packetTreacer.html).

Dalam satu VTP *domain* minimal harus mempunyai satu *switch* dengan mode VTP *server* untuk keperluan pembuatan, penambahan, penghapusan dan perubahan nama VLAN.

- VTP *Client*

  VTP *Client* tidak dapat melakukan perubahan konfigurasi pada VLAN, pada mode ini *switch* hanya mendengarkan *advertisement* dari *switch* VTP yang lain kemudian memodifikasi konfigurasi hanya untuk dirinya sendiri. Informasi yang diterima dilanjutkan ke *switch* VTP tetangganya yang satu *domain.*

- VTP *Transparant*

  Switch dengan *mode* VTP *transparant* harus melakukan konfigurasi VLAN secara manual. Pada *mode* ini *switch* tidak berpartisipasi dengan VTP dan tidak menyebarkan konfigurasi

VLAN-nya. *Mode* ini hanya meneruskan *advertisement* yang lewat ke *switch* tetangganya dalam satu *domain.* Jika terjadi perubahan pada VLAN *switch* hanya menyimpan pada *memory* lokal tidak pada NVRAM, sehingga jika direset maka *settingan* akan hilang

.

2.12 Packet Tracer

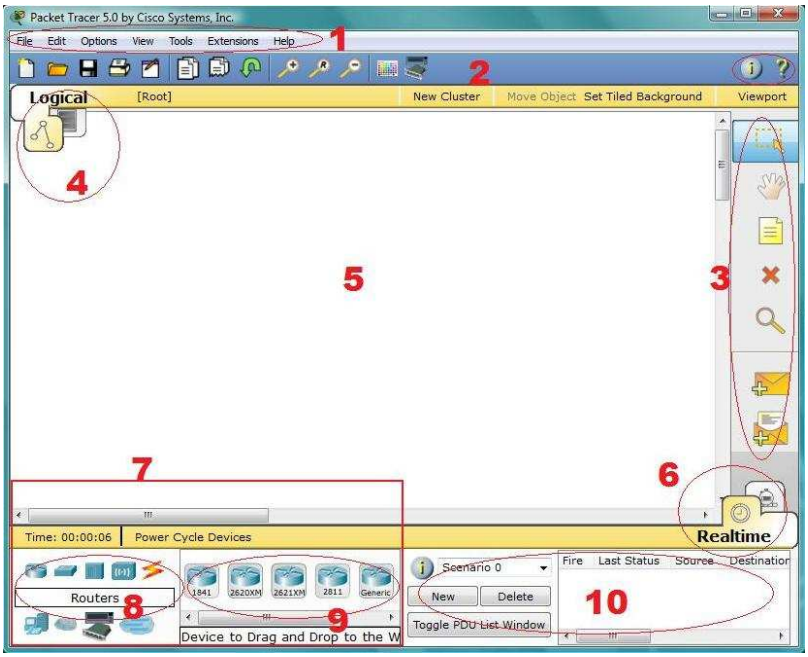
Packet Tracer adalah sebuah *software* yang dikembangkan oleh Cisco. *Packet Tracer* merupakan sebuah program simulasi jaringan yang memungkinkan siswa untuk bereksperimen dengan sistem jaringan dan bertanya tentang pertanyaan "bagaimana jika", dimana *software* tersebut berfungsi untuk membuat model suatu jaringan komputer dan mensimulasikan suatu jaringan. *Paket Tracer* memberikan simulasi, visualisasi, perancangan, penilaian, dan kemampuan kolaborasi serta memfasilitasi belajar dan mengajar dengan konsep teknologi yang kompleks.

(http://www.cisco.com/web/learning/netacad/coursecataloge/packetTreacer.html)

Dalam program ini telah tersedia beberapa komponen–kompenen atau alat– alat yang sering dipakai atau digunakan dalam sistem *network* tersebut, sehingga dapat dengan mudah membuat sebuah simulasi jaringan komputer didalam PC, simulasi ini berfungsi untuk mengetahui cara kerja pada tiap–tiap alat tersebut dan cara pengiriman sebuah pesan dari komputer yang satu ke

komputer lain juga dapat disimulasikan.

Jendela *Packet Tracer* dapat dapat terlihat pada gambar berikut :



Gambar 2. 19 Jendela packet tracer

Dalam program tersebut terdiri beberapa menu yang ditampilkan pada program ini diantaranya:

1. Kolom Menu

Kolom Menu pada bagian atas sebelah kiri ini merupakan bagian yang sering kita lihat dalam setiap software yang berguna sebagai pilihan menu dari sekelompok perintah dimana terdiri antara lain adalah menu *File*, *Edit*, *Options*, *View*, *Tools*, *Extensions*, dan *Help.*

2. Kolom *Shortcut*

Pada bagian ini, terdapat *shortcut* seperti *New, Open, Save, Print, Activity Wizard, Copy, Paste, Undo, Zoom In, Original Size, Zoom Out, Palette,* dan *Custom Devices Dialog.* Dan pada sisi kanan, juga akan ditemukan *shortcut Network Information* dan *Help.* Fungsi kolom ini adalah memudahkan untuk menjalankan suatu perintah yang diinginkan dengan cepat.

3. Kolom Alat Umum

Bagian ini menyediakan akses yang biasanya menggunakan peralatan *workspace.* Bagian ini merupakan sebuah perintah antara lain: memilih (Select), memindahkan tata ruang (Move *Layout),* menempatkan catatan (Place *Note),* menghapus (Delete), memeriksa **(Inspec),** serta menambahkan PDU sederhana dan kompleks.

4. Kolom *Logical/Physical Workspace*

Pada bagian ini disediakan dua macam *workspace,* yaitu *Physical* dan *logical workspace.* Dimana *logical workspace* merupakan tempat untuk membuat sebuah simuasi jaringan komputer. Dan *physical workspace* merupakan tempat yang untuk memberi suatu dimensi *physical* ke topologi jaringan komputer. Hal tersebut bisa memberikan pengertian skala dan penempatan sesuatu jaringan komputer pada suatu lingkungan separti kantor.

5. *Workspace* (Tempat kerja)

Area ini merupakan sebuah tempat dimana akan merencanakan atau membuat sebuah jaringan, mengamati simulasi pada jaringan tersebut serta mengamati beberapa macam informasi dan statistik.

6. Kolom *Realtime/Simulation*

Pada bagian ini tersedia dua *item* yang diantaranya mode Simulasi dan mode *Realtime*, dimana dalam mode *Realtime,* jaringan seperti *device* yang nyata dengan respon yang *real-time* untuk semua aktivitas jaringan. Dalam Mode Simulasi, *user* dapat melihat dan mengendalikan waktu interval, transfer data, serta penyebaran data melalui jaringan yang telah dirancang.

7. *Network Component Box*

Bagian ini merupakan tempat dimana untuk memilih alat dan koneksi yang akan digunakan pada *workspace* untuk membuat sebuah jaringan komputer. Dalam bagian ini juga terdapat dua *item* yaitu pemilihan peralatan dan koneksi serta pemilihan jenis peralatan dan koneksi yang lebih spesifik contohnya jenis penghubung dan jenis kabel

8. Kotak Pemilihan Jenis Alat/Koneksi

Bagian ini merupakan bagian dari kolom diatas dimana pada kolom tersebut digunakan untuk memilih sebuah alat yang digunakan dan ditempatkan pada *workspace.* Alat tersebut antara lain adalah *Routers, Switches, Hubs,*

Wireless Devices, Connections, End Devices, Wan Emulation, Custom Made Devices, dan *Multiuser Connection.*

9. Kotak Pemilihan Jenis Alat/Koneksi Spesifik

Bagian ini merupakan lanjutan dari bagian diatas dimana alat atau koneksi yang telah dipilih akan dibagikan jadi beberapa jenis-jenisnya secara lebih rinci. Alat dan koneksi yang telah dispesifikasikan tersebutlah yang akan digunakan dalam rancangan atau pembuatan jaringan yang sesuai dengan keinginan.

10. Jendela Informasi Status

Bagian ini merupakan keterangan untuk melihat informasi status dari paket serta untuk mengatur skenario selama berlangsungnya simulasi jaringan yang telah dibuat.