BAB III

LANDASAN TEORI

Pada bab tiga penulis menjelaskan tentang teori penunjang kerja praktik yang telah di kerjakan.

3.1 *PACKET TRACER*

Packet Tracer adalah sebuah perangkat lunak (*software*) simulasi jaringan yang dikembangkan oleh Cisco, di mana perangkat tersebut berfungsi untuk membuat suatu simulator jaringan komputer yang sebelumnya telah didesain dan dikonfigurasi oleh pengguna. *Packet Tracer* memungkinkan para pengguna untuk melakukan simulasi berbagai macam protokol dengan mudah yang digunakan pada jaringan, baik secara realtime maupun dengan mode simulasi.

Dalam perangkat ini telah tersedia beberapa komponen atau alat-alat yang sering dipakai atau digunakan dalam jaringan sistem tersebut, antar lain seperti kabel LAN (*cross over*, *straight*, *console*, dll), Hub, Switches, Router, dan sebagainya. Ketika simulasi difungsikan, kita dapat mengetahui cara kerja pada tiap-tiap alat tersebut dan cara pengiriman sebuah pesan (paket data) dari komputer satu ke komputer lainnya dan dapat digunakan pula untuk simulasi dari desain, konfigurasi hingga pemecahan masalah (*troubleshooting*). Pengguna dapat secara langsung mengatur dan mengkonfigurasi jaringan yang akan di desainnya. (sopandi,2006)

3.2 SWITCH

Switch adalah suatu jenis komponen jaringan komputer yang digunakan untuk menghubungkan beberapa HUB dalam membentuk jaringan komputer yang lebih besar atau menghubungkan komputer-komputer yang memiliki kebutuhan akan *bandwidth* yang cukup besar.

Beberapa fungsi switch yaitu sebagai manajemen lalu lintas yang terdapat pada suatu jaringan komputer, switch bertugas bagaimana cara mengirimkan paket data untuk sampai ke tujuan dengan perangkat yang tepat, Switch juga bertugas untuk mencari jalur yang paling baik dan optimal serta memastikan pengiriman paket data yang efisien ketujuannya.

Switch merupakan *hardware* (perangkat keras) jaringan komputer yang sama dengan HUB, perbedaanya switch ini lebih pintar walaupun harganya sedikit lebih mahalan ketibang HUB. Cara kerja switch yaitu dengan cara menerima paket data pada suatu *port* lalu akan melihat MAC (*Media Access Control*) tujuannya dan membangun sebuah koneksi logika dengan *port* yang sudah terhubung dengan *node* atau perangkat tujuan, sehingga selain *port* yang dituju tidak dapat menerima paket data yang dikirimkan dan akan mengurangi terjadinya tabrakan data atau disebut dengan *collision*. Setiap perangkat yang terhubung ke *port* tertentu, *MAC address* nya akan dicatat di *MAC address table* yang nantinya disimpan pada memori *cache* switch, itulah bagaimana switch bekerja. (sofana, 2012)

Gambar 3.1 Switch

Switch terbagi menjadi dua macam, berdasarkan model OSI (*Open System Interconnection*) dimana terdapat switch layer dua dan layer tiga, penjelasannya di bawah ini:

Yang pertama, Switch layer 2 (dua) yang beroperasi *Data link layer* ada pada lapisan model OSI, dimana switch dapat meneruskan paket dengan melihat *MAC address* tujuan, switch juga dapat melakukan fungsi *bridge* antara segmen-segmen LAN (*Local Area Network*) sebab switch mengirimkan paket-paket data dengan cara melihat alamat yang ditujunya tanpa mengetahui protokol jaringan yang dipakai. Itulah penjelasan mengenai Switch layer 2.

Dan yang kedua, switch layer 3 (tiga) berada pada *Network layer* yang ada pada lapisan model OSI, dimana switch dapat meneruskan paket data menggunakan *IP address*. Switch layer 3 (tiga) sering disebut dengan switch routing ataupun switch *multilayer*.

3.3 ROUTER

Router adalah sebuah alat yang mengirimkan paket data melalui sebuah jaringan atau Internet menuju tujuannya, melalui sebuah proses yang dikenal sebagai *routing*. Proses routing terjadi pada lapisan 3 (Lapisan jaringan seperti *Internet Protocol*) dari stack protokol tujuh-lapis OSI.

Router berfungsi sebagai penghubung antar dua atau lebih jaringan untuk meneruskan data dari satu jaringan ke jaringan lainnya. Router berbeda dengan switch. Switch merupakan penghubung beberapa alat untuk membentuk suatu *Local Area Network* (LAN).

Sebagai ilustrasi perbedaan fungsi dari router dan switch merupakan suatu jalanan, dan router merupakan penghubung antar jalan. Masing-masing rumah berada pada jalan yang memiliki alamat dalam suatu urutan tertentu. Dengan cara yang sama, switch menghubungkan berbagai macam alat, dimana masing-masing alat memiliki alamat IP sendiri pada sebuah LAN.(sofana. 2012)

Router sangat banyak digunakan dalam jaringan berbasis teknologi protokol TCP/IP, dan router jenis itu disebut juga dengan *IP Router*. Selain *IP Router*, ada lagi *AppleTalk Router*, dan masih ada beberapa jenis router lainnya. Internet merupakan contoh utama dari sebuah jaringan yang memiliki banyak router IP.

Router dapat digunakan untuk menghubungkan banyak jaringan kecil ke sebuah jaringan yang lebih besar, yang disebut dengan *internetwork*, atau untuk membagi sebuah jaringan besar ke dalam beberapa *subnetwork* untuk meningkatkan kinerja dan juga mempermudah manajemennya. Router juga kadang digunakan untuk mengoneksikan dua buah jaringan yang menggunakan media yang berbeda (seperti halnya router *wireless* yang pada umumnya selain ia dapat menghubungkan komputer dengan menggunakan radio, ia juga mendukung penghubungan komputer dengan kabel UTP), atau berbeda arsitektur jaringan, seperti halnya dari *Ethernet* ke *Token Ring*.

Router juga dapat digunakan untuk menghubungkan LAN ke sebuah layanan telekomunikasi seperti halnya telekomunikasi *leased line* atau *Digital Subscriber Line* (DSL). Router yang digunakan untuk menghubungkan LAN ke sebuah koneksi leased line seperti T1, atau T3, sering disebut sebagai *access server*. Sementara itu, router yang digunakan untuk menghubungkan jaringan lokal ke sebuah koneksi DSL disebut juga dengan DSL router. Router-router jenis tersebut

umumnya memiliki fungsi *firewall* untuk melakukan penapisan paket berdasarkan alamat sumber dan alamat tujuan paket tersebut, meski beberapa router tidak memilikinya. Router yang memiliki fitur penapisan paket disebut juga dengan *packet-filtering* router. Router umumnya memblokir lalu lintas data yang dipancarkan secara broadcast sehingga dapat mencegah adanya broadcast *storm* yang mampu memperlambat kinerja jaringan.

Gambar 3.2 Router

Fungsi utama Router adalah merutekan paket (informasi). Sebuah Router memiliki kemampuan Routing, artinya Router secara cerdas dapat mengetahui kemana rute perjalanan informasi (paket) akan dilewatkan, apakah ditujukan untuk host lain yang satu network ataukah berada di network yang berbeda.

Jika paket-paket ditujukan untuk host pada network lain maka router akan meneruskannya ke network tersebut. Sebaliknya, jika paket-paket ditujukan untuk host yang satu network maka router akan menghalangi paket-paket keluar.

3.4 VLAN (*VIRTUAL LOCAL AREA NETWORK*)

Virtual Local Area Netwok (VLAN) merupakan sebuah metode baru yang berjalan di dunia jaringan yang akhir – akhir ini berkembang dengan pesat. Dengan adanya media ini, suatu jaringan dapat dikonfigurasi secara virtual tanpa harus menuruti lokasi fisik peralatan. Penggunaan VLAN akan membuat pengaturan jaringan menjadi sangat fleksibel di mana dapat dibuat segmen yang bergantung

pada organisasi atau departemen, tanpa bergantung pada lokasi *workstation*.(sukmaaji,2008)

Perbedaan yang sangat jelas dari model jaringan *Local Area Network* dengan *Virtual Local Area Network* adalah bahwa bentuk jaringan dengan model *Local Area Network* sangat bergantung pada letak/fisik dari *workstation*, serta penggunaan hub dan repeater sebagai perangkat jaringan yang memiliki beberapa kelemahan. Sedangkan yang menjadi salah satu kelebihan dari model jaringan dengan VLAN adalah bahwa tiap-tiap workstation/ user yang tergabung dalam satu VLAN/ bagian (organisasi, kelompok dsb) dapat tetap saling berhubungan walaupun terpisah secara fisik. (rafiudin, 2006)

VLAN merupakan suatu model jaringan yang tidak terbatas pada lokasi fisik seperti LAN , hal ini mengakibatkan suatu *network* dapat dikonfigurasi secara virtual tanpa harus menuruti lokasi fisik peralatan. Penggunaan VLAN akan membuat pengaturan jaringan menjadi sangat fleksibel dimana dapat dibuat segmen yang bergantung pada organisasi atau departemen, tanpa bergantung pada lokasi *workstation*.

Tipe – Tipe Vlan :

1. Berdasarkan *Port*

   Keanggotaan pada suatu VLAN dapat di dasarkan pada *port* yang di gunakan oleh VLAN tersebut. Sebagai contoh, pada bridge/switch dengan 4 *port*, *port* 1, 2, dan 4 merupakan VLAN 1 sedang *port* 3 dimiliki oleh VLAN 2,

Tabel 3.1 VLAN berdasarkan *port*

Port	1	2	3	4
VLAN	2	2	1	2

Kelemahannya adalah user tidak bisa untuk berpindah pindah, apabila harus berpindah maka *Network Administrator* harus mengkonfigurasikan ulang.

2. Berdasarkan Mac Address

Keanggotaan suatu VLAN didasarkan pada *MAC address* dari setiap *workstation*/komputer yang dimiliki oleh user. Switch mendeteksi/mencatat semua *MAC address* yang dimiliki oleh setiap *Virtual* LAN. *MAC address* merupakan suatu bagian yang dimiliki oleh NIC *(Network Interface Card)* di setiap *workstation*. Kelebihannya apabila user berpindah pindah maka dia akan tetap terkonfigurasi sebagai anggota dari VLAN tersebut. Sedangkan kekurangannya bahwa setiap mesin harus di konfigurasikan secara manual, dan untuk jaringan yang memiliki ratusan *workstation* maka tipe ini kurang efissien untuk dilakukan.

Contoh:

Tabel 3.2 VLAN berdasarkan MAC address

MAC ADDRESS	VLAN
132516617738	1
272389579355	2
536666337777	2
24444125556	1

3. Berdasarkan Tipe Protokol yang digunakan

Keanggotaan VLAN juga bisa berdasarkan protocol yang digunakan.

Tabel 3.3 VLAN berdasarkan tipe protocol

Protokol	IP	IPX
VLAN	1	2

4. Berdasarkan Alamat Subnet IP

Subnet IP address pada suatu jaringan juga dapat digunakan untuk mengklasifikasi suatu VLAN.

Tabel 3.4 VLAN berdasarkan Subnet

IP subnet	22.3.24	46.20.45
VLAN	1	2

Konfigurasi ini tidak berhubungan dengan *routing* pada jaringan dan juga tidak mempermasalahkan funggsi router. IP address digunakan untuk memetakan keanggotaan VLAN. Keuntungannya seorang user tidak perlu mengkonfigurasikan ulang alamatnya di jaringan apabila berpindah tempat, hanya saja karena bekerja di layer yang lebih tinggi maka akan sedikit lebih lambat untuk meneruskan paket di banding menggunakan *MAC addresses*.

5. Berdasarkan Aplikasi atau Kombinasi Lain

Sangat dimungkinkan untuk menentukan suatu VLAN berdasarkan aplikasi yang dijalankan, atau kombinasi dari semua tipe di atas untuk diterapkan pada suatu jaringan. Misalkan: aplikasi FTP *(file transfer protocol)* hanya bisa digunakan oleh VLAN 1 dan Telnet hanya bisa digunakan pada VLAN 2.

Metode Keanggotaan Vlan

1. Metode *Static* :

konfigurasi secara manual *port* pada switch ditandai sebagai VLAN menggunakan Aplikasi pengelola VLAN atau langsung dikerjakan pada switch.

2. Metode Dinamis

   konfigurasi tidak mempercayakan pada *port* yang ditandai sebagai VLAN khusus melainkan menjadikan semua *port* adalah anggota VLAN.

Beberapa manfaat VLAN adalah ;

1. Performance.

   VLAN mampu mengurangi jumlah data yang dikirim ke tujuan yang tidak perlu. Sehingga lalu lintas data yang terjadi di jaringan tersebut dengan sendirinya akan berkurang.

2. Mempermudah Administrator Jaringan.

   Setiap kali komputer berpindah tempat, maka komputer tersebut harus di konfigurasi ulang agar mampu berkomunikasi dengan jaringan dimana komputer itu berada. Hal ini membuat komputer tersebut tidak dapat dioperasikan langsung setelah di pindahkan. Jaringan dengan Prinsip VLAN bisa meminimalkan atau bahkan menghapus langkah ini karena pada dasarnya ia tetap berada pada jaringan yang sama.

3. Mengurangi biaya.

   Dengan berpindahnya lokasi, maka seperti hal nya diatas, akan menyebabkan biaya instalasi ulang. Dalam jaringan yang menggunakan VLAN, hal ini dapat diminimallisir atau dihapuskan.

4. Keamanan

   VLAN bisa membatasi Pengguna yang bisa mengakses suatu data., sehingga mengurangi kemungkinan terjadinya penyalahgunaan hak akses.

3.5 VTP (*VLAN TRUNKING PROTOCOL*)

VTP adalah suatu protocol untuk mengenalkan suatu atau sekelompok VLAN yang telah ada agar dapat berkomunikasi dengan jaringan. Atau menurut sumber lain mengatakan suatu metode dalam hubungan jaringan LAN dengan *ethernet* untuk menyambungkan komunikasi dengan menggunakan informasi VLAN, khususnya ke VLAN. VLAN *Trunking Protocol* (VTP) merupakan fitur Layer 2 yang terdapat pada jajaran switch Cisco Catalyst, yang sangat berguna terutama dalam lingkungan switch skala besar yang meliputi beberapa *Virtual Local Area Network* (VLAN).

Tujuan mengonfigurasi VLAN *tagging* adalah agar *traffic* dari beberapa VLAN dapat melewati *trunk link* yang digunakan untuk menghubungkan antar-switch. Meskipun hal ini merupakan hal yang baik dalam lingkungan yang besar, VLAN *tagging* tidak melakukan apa-apa untuk mempermudah pengkonfigurasian VLAN pada beberapa switch. Di sinilah VTP mengambil bagian. (wagito,2005)

VLAN merupakan suatu *broadcast domain*, sekumpulan *port* atau user yang kita kelompokkan. VLAN dapat mencakup beberapa switch, hal ini dapat dilakukan dengan mengonfigurasi VLAN pada bebarapa switch dan kemudian menghubungkan switch tersebut, dengan satu pasang *port* per VLAN.

Kelemahan cara ini adalah banyaknya *port* switch yang menghubungkan switch tersebut. Cara ini juga lebih manual, membutuhkan lebih banyak waktu, dan sulit untuk dikelola. Oleh karena itu, muncullah *VLAN trunking* yang bertujuan untuk menghubungkan switch dengan *interlink* (*uplink*) kecepatan tinggi, dan beberapa VLAN dapat berbagi satu kabel.

Trunk link tidak dibuat untuk satu VLAN tertentu. Satu, beberapa, atau semua VLAN aktif dapat dilewati antar-switch dengan mengguunakan satu *trunk link*. Adalah mungkin untuk menghubungkan dua switch dengan link fisik terpisah untuk setiap VLAN. Namun dengan semakin banyaknya VLAN yang dibuat, maka jumlah link dapat bertambah dengan cepat. Cara yang lebih efisien adalah dengan menggunakan *trunking*. Untuk membedakan kepemilikan traffic pada trunk link, switch harus mempunyai metode untuk mengidentifikasi frame setiap LAN.

Sebenarnya fungsi dari VTP adalah memudahkan Jaringan yang mengakomodir dan *network administrator* dalam mengelola semua VLAN yang berskala besar dan telah dikonfigurasikan pada sebuah *internetwork* switch. Dalam artian bahwa dengan menggunakan fasilitas VTP, memungkinkan seorang jaringan atas untuk menambah, mengurangi, dan mengganti VLAN, dimana informasi VLAN tersebut kemudian disebarluaskan ke semua switch lainnya di domain VTP tersebut.

Adapun keuntungan yang dapat diperoleh dalam menerapkan konsep VTP adalah berupa:

- Konfigurasi VLAN yang lebih stabil di semua switch di *network*
- Pengiriman VLAN-*advertisement* terjadi hanya di trunk-*port*
- Menambahkan VLAN secara *plug –and-play*
- *Tracking* dan monitoring VLAN-VLAN yang akurat

3.6 *ACCESS LIST*

Access List merupakan sebuah daftar yang di rancang untuk menampung aturan – aturan yang berguna untuk mengontroll packet yang melintas dalam sebuah

jaringan, khususnya paket – paket datagram (HTTP, FTP, Telnet, UDP, DLL.) yang melewati sebuah router, sebelum terkena *Access List* Packet – packet tersebut harus mendapat izin Routing dari *Access List* untuk melintasi jaringan antar Router *(Permit/Deny*) yang telah di dapat, maka Process *Access List* tersebut di terapkan.(arpandi, 2012)

Access List bisa di terapkan di dua Pintu: pertama sebagai Pintu masuk (*INBOUND Access-List*) dan sebagai Pintu keluar (*OUTBOUND Access-List*).

- *Inbound Access – List*: sebuah Packet yang akan di proses Router oleh *Access – List* sebelum packet tersebut masuk ke dalam Router.
- *Outbound Access – List*: sebuah Packet yang akan di proses Router oleh *Access – List* sebelum packet tersebut keluar dari Router.

Access List terdapat dua type, diantaranya:

a. *Numbered*:

Untuk penerapan *Access List* dari dua tipe (*Numbered*) tersebut dengan cara memasukkan nomor yang telah di tentukan untuk konfigursinya, nomer ini menandakan jenis atau type dari ACL tersebut dan harus pada range tertentu dari nomer yang Valid untuk jenis daftar tersebut, berikut ini:

Tabel 3.5 Jenis Access List

Jenis Access List	Range Nomor Pengenal
IP Standard	1-99
IP Extended	100-199
IPX Standard	800-899
IPX Extended	900-999
Aplle Talk	600-699
IPX SAP Filter	1000-1099

- Standar *Access List*: berguna untuk melakukan Penyeleksiyan *Packet* berdasarkan Alamat IP pada pengirim (*source*) Packet.
- Extended *Access List*: berguna untuk melakukan Penyeleksian *Packet* berdasarkan Alamat IP pengirim (*source*) dan penerima (*Destination*), Protocol (HTTP, UDP, TCP, DLL) dan jenis *Port* (FTP, Telnet, WWW, DLL) *packet* yang di kirim (*source*).

b. Named

Mengidentifikasi konfigurasinya menggunakan Nama yang *Case-Sensitive* antara *Standard* atau *Extended List*, terdapat pada Cisco ios 11.2 dan sebelumnya.