BAB II
LANDASAN TEORI

A. Konsep VLAN

Jaringan *Local Area Network* atau LAN merupakan suatu jaringan yang menggabungkan perangkat keras dan perangkat lunak komputer yang dibutuhkan agar dapat saling berkomunikasi dalam daerah yang terbatas (*local*). Namun implementasi penggunaan *jaringan Local Area Network (LAN)*, terkadang menimbulkan beberapa permasalahan terkait dengan penggunaan pada jaringan tersebut. Permasalahan tersebut berupa kurangnya manajemen, konfigurasi keamanan dan terkait masalah komunikasi data dan informasi, terlebih jika pengguna yang terhubung pada infastruktur jaringan tersebut cukup banyak. Maka dari itu dibutuhkan manajemen jaringan *Local Area Network (*LAN) berupa *Virtual Local Area Network (*VLAN*)* untuk manajemen jaringan, dan segmentasi jaringan.

VLAN *(Virtual Area Network)* memiliki banyak keuntungan yang dapat diperoleh dari penggunaannya. Konsep VLAN *(Virtual Area Network*) memungkinkan untuk membuat banyak jaringan komputer (segmentasi) dan mendistribusikan hanya menggunakan saluran distribusi media dan dapat untuk menghubungkan jaringan area lokal (LAN) tanpa mengikuti lokasi geografis.

Jaringan *Local Area Network* (LAN) dibangun dalam bentuk grup *Virtual Local Area Network* (VLAN). Alamat IP DHCP yang diberikan oleh *router* ke PC yang terletak di jaringan. NAT (*Network Address Translation)* merupakan metode yang digunakan sebagai terjemahan alamat IP untuk dapat masuk ke jaringan yang berbeda. NAT (*Network Address Translation*) memungkinkan host untuk masuk ke jaringan yang berbeda tanpa mengizinkan host yang dimaksudkan untuk memanfaatkan jaringan mereka menggunakan VLAN. Sehingga dua jaringan yang berbeda menjadi satu saklar yang dapat terhubung. Memberikan DHCP IP akan memungkinkan *administrator* jaringan untuk memberikan alamat IP ke semua PC yang terdapat pada satu grup jaringan.. Host IP kemudian diteruskan dalam jaringan dengan NAT[1].

B. Teknik *Routing*

1. *Static Route*

   Static route merupakan suatu teknik memasukan rute-rute ke *host* atau jaringan tujuan secara manual oleh *administrator* jaringan ke *route table* suatu *router*. *Static route* akan mendefinisikan alamat IP *hop router* berikutnya dan *interface* lokal yang digunakan untuk mem-*forward* paket ke tujuan tertentu (*hop router* berikutnya). Keunggulan yang dimiliki oleh penggunaan teknik static route yaitu menghemat *bandwidth* jaringan karena *static route* tidak membangkitkan trafik *route update* untuk memberikan informasi perubahan rute yang berlaku (sah) saat ini ke *router-router* lain.

   Kekurangannya ketika *administrator* jaringan harus melengkapi *forwarding table* di setiap *router* yang jumlahnya tidak sedikit dalam jaringan yang besar. Apalagi ketika mengisi entri-entri di seluruh *router* di Internet yang jumlahnya banyak dan bertambah setiap hari. Jadi penggunaan *static route* membutuhkan waktu ekstra ketika memanajemen jaringan pada jaringan yang besar.

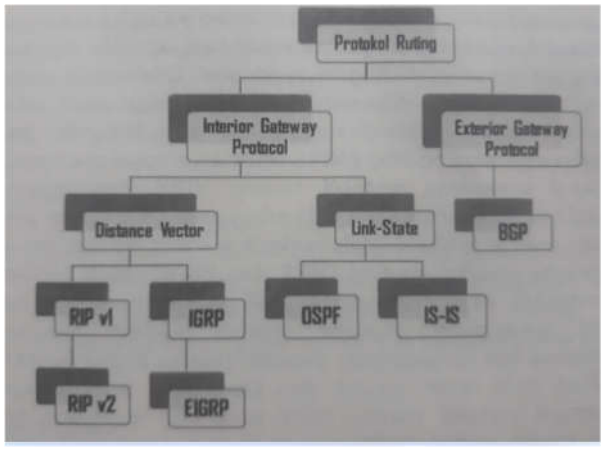
2. *Dynamic Routes*

   Routing dinamik merupakan cara yang digunakan untuk menghindari pengisisan entri-entri *forwarding table* secara manual. Pada *routing* dinamis, Protokol *routing* memiliki fungsi untuk mengatur *router-router* untuk dapat berkomunikasi satu dengan yang lain dan saling memberikan informasi *routing* sehingga dapat mengubah isi *forwarding table*, tergantung keadaan jaringannya. Semua *router* dapat mengetahui keadaan jaringan yang terakhir dan mampu meneruskan datagram ke arah yang benar. *Routing* dinamik mengacu pada dua tipe algoritma yaitu algoritma yang dikenalkan oleh Bellman Ford dengan algoritma *distance vector* nya dan algoritma yang dikenalkan oleh Djikstra dengan algoritma *link state* nya. Cisco kemudian mengembangkan *protocol* EIGRP yang merupakan gabungan dari kedua algoritma tersebut yang diberi nama [2].

C. Protokol *Routing*

Pada awalnya, protokol *routing* yang diaktifkan pada masing-masing *router* akan mempertukarkan informasi rute yang terdapat dalam tabel *routing*. Pada kondisi awal, informasi rute yang terdapat dalam tabel *routing* adalah tentang alamat *network* yang terhubung langsung saja. Informasi rute tersebut akan dikirimkan ke *router* tetangga yang terhubung langsung.

1. Pembagian Protokol Routing



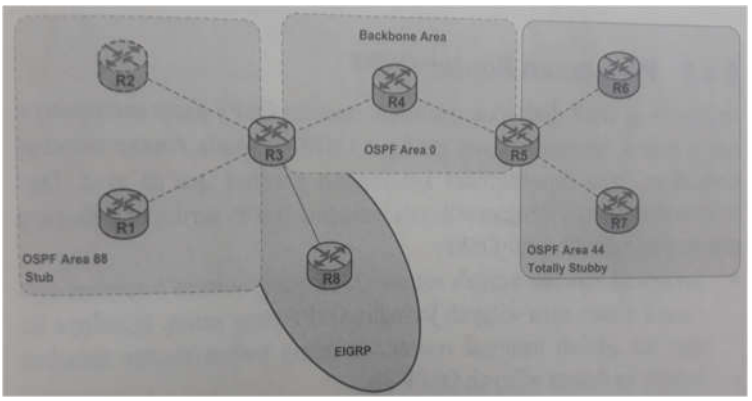
Gambar 2.1 Pembagian Protokol *Routing* [3]

Protokol *routing* dalam kategori IGP juga dapat diklasifikasikan menjadi dua bagian. Pembagian kategori protokol *routing* IGP lebih didasarkan atas cara kerja protokol tersebut dalam menghimpun informasi alamat *network* lawan. Cara kerja sebuah protokol *routing* lebih didasarkan pada algoritma *routing* yang digunakan. Protokol *routing* IGP dalam kategori *distance* vector menggunakan algoritma Bellman Ford. Protokol *routing* yang menggunakan algoritma Bellman Ford di antaranya adalah *Routing Information Protocol* (RIP) dan *Interior Gateway Routing Protocol* (IGRP). Sedangkan EIGRP (*Enhanced* IGRP) sedikit berbeda dengan IGRP walaupun sama-sama dikembangkan oleh Cisco yaitu menggunakan algoritma *routing Diffusing Update Algorithm* (DUAL). EIGRP dan IGRP hanya dapat digunakan oleh *router* produk Cisco saja. *Router* produk vendor lain tidak bisa menggunakan kedua protokol *routing* tersebut. Berbeda dengan keberadaan protokol *routing* RIP, baik itu RIP versi1 (RIP v1) dan versi 2 (RIP v2). Semua vendor pembuat perangkat *router* bisa menggunakan protokol *routing* tersebut.

2. Protokol OSPF

Open Shortest Path Fisrt (OSPF) adalah protokol *routing* dinamik yang sifatnya terbuka, artinya vendor pembuat perangkat *router* manapun bisa menggunakan protokol *routing*. Protokol routing OSPF dikembangkan oleh *Internet Engineering Task Force* (IETF) pada tahun 1987. Munculnya protokol *routing* OSPF lebih didasarkan pada perkembangan jaringan Internet yang semakin besar. Karena protokol *routing* OSPF tidak mengenal istilah jumlah hop dalam implementasinya.

3. Konsep Area OSPF



Gambar 2.2 Area OSPF [3]

Protokol *routing* OSPF tidak menggunakan batas jumlah *router* yang harus diaktifkan dalam sebuah jaringan. Tidak seperti penggunaan protokol *routing* RIP yang menggunakan batas jumlah *router* sebesar 15 hop. Namun keterbatasan kemampuan memory *router* dalam menampung informasi *update* dari *router* OSPF lawan, juga kecepatan pemrosesan data, diperlukan pembatasan wilayah jaringan OSPF. Sehingga dikenal istiah area (wilayah) dalam konsep jaringan OSPF.

Wilayah jaringan dalam konsep OSPF dibagi dua; *backbone* dan non *backbone*. area yang wajib dibuat (ada) dalam jaringan OSPF adalah area *backbone*. Kode yang diberikan untuk area *backbone* adalah 0 atau lebih sering disebut dengan istilah area 0 (*backbone*). Area *backbone* akan dihubungkan dengan area-area lain yang disebutdengan istilah area *non backbone*. Kode yang diberikan untuk area selain *backbone* harus selain 0. Dari pembagian area *non backbone* dibagi lagi menjadi dua macam; stub dan totally stubby. Pembagian area non *backbone* lebih ditekankan kepada

cara meringkas informasi rute yang didapatkan dari luar wilayah (area) OSPF.

Stub area merupakan area yang masih menerima informasi rute dari dalam wilayah OSPF namun tidak menerima informasi rute dari luar wilayah jaringan bukan OSPF. Misalnya jaringan lain yang mengaktifkan protokol *routing* selain OSPF, misalnya EIGRP atau RIP. Totally *stubby* merupakan area yang tidak menerima informasi rute dari luar wilayah OSPF ataupun wilayah jaringan lain yang tidak mengaktifkan protokol *routing* OSPF. Sebagai gantinya akan dibuat rute default sebagai alternatif solusi agar bisa menuju kejaringan luar[3].

D. DHCP Server

Server Dynamic Host Control Protocol (DHCP) merupakan protokol Internet dimana bertugas mendistribusikan segala informasi TCP/IP secara langsung kepada komputer yang menggunakan *protocol* TCP/IP dan saling terhubung. Protokol DHCP adalah hasil perkembangan protokol jaringan BOOTP atau yang dikenal dengan *Bootstrap Protocol* yang memiliki kelebihan berupa alokasi otomatis ke berbagai alamat jaringan yang terhubung satu sama lain.

DHCP berfungsi sebagai *persistent storage* yaitu sebagai media penyimpanan menetap dari jaringan parameter untuk *client*. DHCP menyimpan sebuah key-value dari setiap *client* karena *key-value* ini digunakan sebagai tanda pengenal yang unik dalam tiap komputer *client* dan mengandung parameter konfigurasi *client*. Tanda pengenal unik tersebut merupakan nomor subnet IP yang terdapat pada masing – masing komputer client.

DHCP juga berfungsi sebagai pengalokasi IP atau alamat jaringan *client* baik secara temporer maupun secara permanen. Pengalokasi ini bertujuan agar mekanisme DHCP tidak akan melakukan realokasi kepada alamat yang telah diberikan kepada *client* sebelumnya dan mencegah terjadinya pengiriman alamat yang sama setiap kali *client* meminta alamat kepada DHCP *Server*. Berdasarkan fungsi tersebut maka DHCP tidak akan mengirimkan alamat IP yang sama kepada *client* untuk lebih dari satu *node* (jumlah perangkat dalam

jaringan) pada saat yang sama, peraturan ini tetap berlaku walaupun *node* direstart berkali-kali[4].

E. EVE – NG

Gambar 2.3 *Simulator* EVE – NG[5]

Emulated Virtual Environment - New Generation (EVE-NG) merupakan platform *multi-vendor* dan *multi-user* gratis yang berfungsi untuk mensimulasikan berbagai topologi jaringan termasuk *router*, *switch*, perangkat keamanan, *workstation* dan *server*. *Emulator* ini mendukung sejumlah besar peralatan dari berbagai vendor, seperti Cisco, Juniper, HP, Checkpoint, Aruba, Alcatel.

Emulator ini dapat menambahkan image Cisco IOL, gambar dari VIRL (vIOS-L2 dan vIOS-L3), ASA *Firewall*, Cisco IPS, XRv dan CSR1000v, *Dynamips* dari GNS3, Cisco vWLC, vWSA dan Cisco IOU. *Emulator* ini dapat mengimplementasikan dukungan penuh untuk tingkat *switching* L2 dengan keterbatasan yang tidak signifikan. EVE-NG menggunakan sumber daya rendah terhadap perangkat keras komputer yang menjalankannya. Simulator ini mengimplementasikan antarmuka grafis yang serupa dengan GNS3, memiliki dukungan untuk gambar Microsoft Visio dan memiliki optimasi memori menggunakan UKSM (*Ultra Kernel Samepage Merging*)[5].