BAB II
TEORI PENUNJANG

2.1 Konsep *Routing*

Jaringan komputer selain melibatkan perangkat yang digunakan untuk membentuk sebuah konsep jaringan, juga akan melibatkan jalur yang digunakan untuk melewatkan paket yang dikirimkan oleh komputer sumber ke tujuan. Pada jaringan dengan skala besar, misalnya Internet pasti akan melibatkan banyak jalur. Paket yang dikirimkan dari komputer sumber akan melewati beberapa pilihan jalur sebelum sampai ke komputer tujuan. Dari beberapa pilihan jalur yang ada, kemungkinan besar tidak semua jalur akan dilewati oleh sebuah paket yang akan dikirimkan ke perangkat tujuan. Pasti ada salah satu atau beberapa jalur yang akan dipilih. Proses pemilihan jalur ini dinamakan dengan istilah *routing* dan perangkat yang difungsikan untuk melakukan proses *routing* tersebut adalah *router* atau perangkat yang bekerja-nya ada di layer 3 (layer *network*) pada konsep layer OSI, seperti perangkat switch layer 3. Dalam melakukan fungsi *routing* tersebut, perangkat router akan menggunakan informasi alamat IP tujuan dari paket yang diterima dan mencocokan alamat IP tujuan dengan daftar informasi rute yang terdapat dalam tabel *routing* sebuah *router* [2].

2.2 Protokol *Routing*

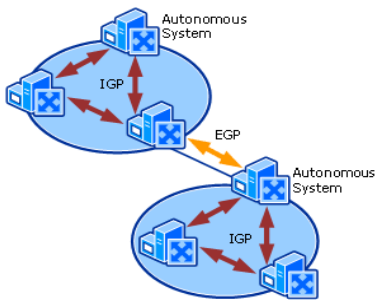
Proses pengumpulan informasi rute tentang alamat *network* yang tidak terhubung langsung dengan sebuah *router* yang dilakukan dengan cara otomatis menjadi pertimbangan tersendiri disaat alamat *network* yang harus dicatatkan kedalam tabel *routing* sebuah *router* relatif banyak. Bila seorang admin jaringan harus mendaftarkan seratus alamat *network* lain secara manual. Selain menguras tenaga terutama kekuatan tangan untuk menuliskan ke seratus alamat *network* tersebut, juga rawan terjadi kesalahan saat proses penulisan informasi rute tentang alamat *network* lain. Namun dengan cara otomatis, kita tidak perlu mencatatkan ke seratus alamat *network* lawan tersebut. Peran seorang admin jaringan cukup mengaktifkan protokol *routing* pada masing-masing *router*, nantinya protokol *routing* yang bekerja mencatat semua alamat *network* lawan ke dalam table

routing sebuah *router*. Jadi peran dari protokol *routing* sangatlah penting pada jaringan dengan skala besar, terlebih alamat network yang harus dicatatkan jumlahnya relatif banyak [2].

2.3 Klasifikasi Protokol *Routing*

Terdapat beberapa pilihan protokol routing yang dapat diaktifkan dalam sebuah *router*. Pemilihan protokol routing tersebut tergantung dari beberapa hal, diantaranya adalah wilayah *Autonomus System* (AS), jumlah router yang terdapat dalam sebuah jaringan, dan kecepatan konvergensi. *Autonomus System* (AS) dapat didefinisikan sebagai wilayah edar dari paket update yang dipertukarkan antar protokol routing yang telah diaktifkan dalam sebuah *router*, setiap ada paket update yang diterima oleh sebuah router, maka paket update tersebut akan disimpan dalam memori *router*. Bisa dibayangkan dalam jaringan skala besar misalnya Internet tanpa menggunakan konsep *Autonomus System* (AS) atau pembatasan wilayah edar paket update. Kemungkinan memory perangkat *router* akan tidak mampu untuk menampung seluruh informasi rute yang terdapat dalam jaringan Internet. Dengan semakin banyak informasi rute yang tersimpan dalam tabel *routing*, waktu yang dibutuhkan untuk melakukan fungsi *routing* juga akan semakin lama. Proses *routing* yang lama juga akan berpengaruh pada waktu konvergensi jaringan. Karena semua router harus mengetahui keseluruhan informasi alamat *network* yang terdapat dalam jaringan dengan cepat [2].

Berdasarkan pembagian *Autonomus System* (AS), protokol *routing* yang dapat diaktifkan dalam sebuah router dapat dikategorikan menjadi dua macam: *Interior Gateway Protokol* (IGP) dan *Exterior Gateway Protokol* (EGP) [1]. Konsep *Autonomus System* (AS) dapat dilihat pada Gambar 2.1 berikut



Gambar 2.1 Konsep Autonomus System

Dengan semakin besar jaringan, dalam artian perangkat *router* yang digunakan dalam jaringan tersebut relatif banyak maka diperlukan penggunaan protokol *routing* yang khusus. Keberadaan protokol *routing* OSPF (*Open Shortest Path First*) digunakan sebagai penyempurna dari protokol *routing* RIP dan begitupula dengan keberadaan protokol *routing* EIGRP berfungsi sebagai penyempurna dari awal munculnya protokol *routing* IGRP. Penyempurnaan protokol routing tersebut lebih didasarkan pada kemampuan sebuah protokol *routing* ketika diimplementasikan pada jaringan dalam sebuah jaringan. Penggunaan protokol *routing* OSPF dan EIGRP lebih cenderung diimplementasikan pada jaringan skala besar. Namun penggunaan protokol *routing* EIGRP mempunyai keterbatasan dari sisi perangkat. Protokol *routing* EIGRP hanya bisa diaktifkan pada router produk Cisco saja. Berbeda dengan penggunaan protokol *routing* OSPF yang bisa digunakan untuk semua produk router. OSPF dan IS-IS (*Intermediate System to Intermediate System*) dikategorikan dalam protokol *routing link-state* dengan algoritma *routing* yang digunakan adalah Dijkstra [2].

2.3.1 EIGRP *(Enhanced Interior Gateway Routing Protocol)*

EIGRP (*Enhanced Interior Gateway Routing Protocol*) merupakan protokol *routing* produk dari Cisco, sehingga vendor yang bisa menggunakan protokol *routing* ini hanya Cisco saja. *Router* produk dari Mikrotik tidak bisa menggunakan protokol *routing* EIGRP. Dikeluarkan oleh Cisco sekitar tahun 1992. Keberadaan protokol *routing* EIGRP difungsikan sebagai penyempurna dari protokol *routing* yang sebelumnya telah dikembangkan oleh Cisco yaitu IGRP (*Interior Gateway Routing Protocol*) [2].

2.3.1.1 Tipe Paket EIGRP

Sebelum informasi rute tentang alamat *network* lawan dapat tersimpan dalam tabel *routing*, harus ada paket yang dipertukarkan antar *router* EIGRP. Proses awal yang harus dilakukan oleh *router* EIGRP adalah membuat hubungan/*adjacency* dengan *router* EIGRP lawan yang terhubung langsung. Dalam membuat proses *adjacency* tersebut, *router* EIGRP akan menggunakan paket *hello*. Paket yang akan dikirimkan oleh router EIGRP adalah paket *hello*.

Paket tersebut digunakan untuk mengecek keberadaan dari *router* EIGRP lawan [2].

Jika router tetangga yang menggunakan rotokol *routing* EIGRP membalas paket *hello* yang berisi tentang informasi masing-masing router, langkah selanjutnya yang dilakukan oleh *router* pengirim adalah dengan mengirimkan *paket update*. Isi yang terdapat dalam paket update adalah berupa informasi rute yang tersimpan dalam tabel *routing* pengirim. Ketika menerima *paket update*, router penerima harus memberikan balasan berupa pengiriman paket ACK (*Acknowledgement*). Tujuan dari pengiriman paket ACK adalah untuk memberitahukan kepada *router* pengirim bahwa *paket update* yang sebelumnya telah dikirimkan sudah diterima oleh *router* penerima [2].

2.3.2 OSPF *(Open Shortest Path First)*

OSPF (*Open Shortest Path First*) merupakan protokol routing yang dikembangkan oleh IETF (*Internet Engineering Task Force*) pada tahun 1987. Penggunaan protokol *routing* ini sifatnya open, artinya *vendor* pembuat perangkat *router* manapun bisa menggunakan protokol *routing* OSPF. Tidak terkecuali perangkat router produk dari Cisco dan Mikrotik. Munculnya protokol *routing* OSPF lebih didasarkan pada perkembangan jaringan Internet yang semaikn besar. Perlu penggunaan perangkat *router* dengan jumlah yang relatif banyak. Penggunaan protokol *routing* RIP hanya terbatas sampai 15 *hop*. Dengan kata lain penggunaan protokol *routing* RIP tidak cocok untuk diimplementasikan pada jaringan dengan skala besar, seperti Internet. Sehingga perlu dikembangkan protokol *routing* yang sudah tidak mengenal lagi dengan istilah jumlah *hop* yaitu OSPF [2].

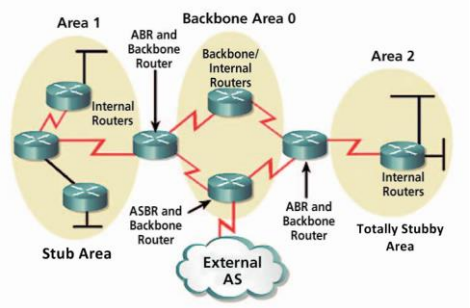
2.3.2.1 Tipe Paket OSPF

Sebelum informasi rute dipertukarkan antar *router* yang sudah diaktifkan protokol *routing* OSPF, terdapat pertukaran paket awal antar *router* OSPF yang saling dihubungkan. Misalnya terdapat dua *router* yang sudah diaktifkan protokol *routing* OSPF yaitu R1 dan R2. Ketika R1 dan R2 sudah diaktifkan protokol *routing* OSPF, masing-masing *router* akan saling mempertukarkan paket awal yang diberi nama *paket hello*. Fungsi dari keberadaan

paket *hello* ini adalah untuk membuat pertemanan antar dua *router* OSPF, istilah lainnya adalah *adjacency*. Setelah R1 yakin bahwa pada jalur yang aktif terdapat *router* lain yang sama-sama mengaktifkan protokol *routing* OSPF, R1 akan mengirimkan informasi rute lewat pengiriman paket DBD (*Database Description*). Biasanya paket DBD yang diterima oleh R2 tidak langsung disimpan dalam tabel *routing*. *Router* R2 akan meminta informasi tambahan dengan mengirimkan paket LSR (*Link-State Request*). Jawaban dengan cara mengirimkan paket LSR oleh R2 adalah dengan dikirimkannya paket LSU (*Link-State Update*) oleh R1. Isi yang terdapat dalam paket LSU adalah berupa informasi rute tambahan yang dimiliki oleh R1. Apabila paket LSU sudah diterima oleh R2, router R2 akan memberikan jawaban dengan mengirimkan paket LSAck (*Link-State Acknowledgement*) [2].

2.3.2.2 Konsep Area OSPF

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*, karena pertimbangan batas jumlah hop maksimal yang bisa dilewatkan oleh paket update RIP yaitu 15 *hop*. Berapapun jumlah *router* yang digunakan tidak menjadi masalah jika menggunakan protokol *routing* OSPF. Namun karena alasan keterbatasan kemampuan *memory router* dalam menampung informasi update dari *router* OSPF lawan, juga kecepatan pemrosesan data, diperlukan pembatasan wilayah jaringan OSPF. Sehingga dikenal istilah *area* (wilayah) dalam konsep jaringan OSPF [1]. Konsep area OSPF bisa dilihat pada gambar 2.2 berikut.



Gambar 2.2 Konsep area OSPF

Wilayah dalam konsep OSPF dibagi dua; *backbone* dan *nonbackbone*. Area yang wajib dibuat (ada) dalam jaringan OSPF adalah *area backbone*. Kode

yang dibeikan untuk area *backbone* adalah 0 atau lebih sering disebut dengan istilah area 0 (*backbone*). Area *backbone* akan dihubungkan dengan area-area lainnya yang disebut dengan istilah area *nonbackbone.* Kode yang diberikan untuk area selain backbone harus selain 0, misalnya area 1 atau area 2. Dan pembagian area *nonbackbone* dibagi lagi menjadi dua macam; *stub* dan *totally stubby*. Pembagian area *nonbackbone* lebih ditekankan kepada cara meringkas informasi route yang didapatkan dari luar wilayah (area) OSPF [2].

- *Stub area*: adalah 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 [2].
- *Totally stubby*: adalah 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 ke jaringan luar [2].

2.3.2.3 Wildcard Mask

Wildcard mask merupakan nilai kebalikan dari subnet mask. Jika dalam subnet mask diketahui nilai bit ‘1’, maka dalam nilai *wildcard mask* akan bernilai ‘0’. Begitupula sebaliknya, jika diketahui nilai bit pada subnet mask adalah ‘0’, maka pada *wildcard mask* akan bernilai bit ‘1’ [2].

2.4 IP Address

Alamat IP (*Internet Protocol Address* atau sering disingkat IP) adalah deretan angka biner antara 32 bit sampai 128 bit yang dipakai sebagai alamat identifikasi untuk tiap komputer host dalam jaringan Internet. Panjang dari angka ini adalah 32 bit (untuk IPv4 atau IP versi 4), dan 128 bit (untuk IPv6 atau IP versi 6) yang menunjukkan alamat dari komputer tersebut pada jaringan Internet berbasis TCP/IP. Pengiriman data dalam jaringan TCP/IP berdasarkan IP address komputer pengirim dan komputer penerima. IP address memiliki dua bagian, yaitu alamat jaringan (*network address*) dan alamat komputer lokal (*host address*) dalam sebuah jaringan [2].

Alamat jaringan digunakan oleh router untuk mencari jaringan tempat sebuah komputer lokal berada, semantara alamat komputer lokal digunakan untuk mengenali sebuah komputer pada jaringan lokal. Informasi ini bisa diketahui dengan mengkombinasikan IP address dengan 32 bit angka subnet mask. IP address memiliki beberapa kelas berdasarkan kapasitasnya, yaitu Class A dengan kapasitas lebih dari 16 juta komputer, Class B dengan kapasitas lebih dari 65 ribu komputer, dan Class C dengan kapasitas 254 komputer [2].

2.4.1 Network Address

Network address adalah suatu metode untuk menghubungkan lebih dari satu komputer ke jaringan internet dengan menggunakan satu alamat IP. Banyaknya penggunaan metode ini disebabkan karena ketersediaan alamat IP yang terbatas, kebutuhan akan keamanan (*security*), dan kemudahan serta fleksibilitas dalam administrasi jaringan [2].

2.4.2 Subnet Mask

Subnet mask adalah istilah teknologi informasi yang mengacu kepada angka perduaan (*binary*) 32 bit yang digunakan untuk membedakan ID jaringan (*network ID*) dengan ID induk, yakni: menunjukkan letak suatu induk, entah berada di jaringan setempat atau di jaringan luar [2].

2.5 *Quality of Service* (QoS)

Quality of Service adalah kemampuan sebuah jaringan untuk menyediakan layanan yang lebih baik lagi bagi layanan trafik yang melewatinya. QoS merupakan sebuah sistem arsitektur end to end dan bukan merupakan sebuah feature yang dimiliki oleh jaringan. *Quality of Service* suatu network merujuk ke tingkat kecepatan dan keandalan penyampaian berbagai jenis beban data di dalam suatu komunikasi. Aplikasi yang berbeda memerlukan suatu persyaratan QoS tertentu agar selama proses pentransmisian tidak terlalu banyak paket yang hilang, layanan real-time yang baik, *delay* yang rendah, dan alokasi *bandwidth* yang baik. Performansi kecepatan dan mengacu keandalan ke tingkat penyampaian berbagai jenis beban data di dalam suatu komunikasi yang meliputi *troughput, delay* dan *paket loss* [3].

2.5.1 Delay

Delay (Latency) merupakan waktu yang dibutuhkan data untuk menempuh jarak dari asal ke tujuan. Delay dapat dipengaruhi oleh jarak, media fisik, *congesti* atau juga waktu proses yang lama [4].

2.5.2 Throughput

Throughput yaitu kecepatan (rate) transfer data efektif, yang diukur dalam bps (bit per second). *Throughput* adalah jumlah total kedatangan paket yang sukses yang diamati pada tujuan selama interval waktu tertentu dibagi oleh durasi interval waktu tersebut [4]. Adapun rumus mencari *throughput* sebagai berikut:

$$Throughput = \frac{ukuran\ file}{waktu\ pengiriman} \qquad (2.1)$$

2.6 Cisco Packet Tracer

Cisco Packet Tracer adalah software simulator jaringan yang diluncurkan oleh *Cisco System* yang difungsikan sebagai media pembelajaran, pelatihan, dan juga penelitian simulasi jaringan komputer. Software ini disediakan gratis untuk semua kalangan yang ingin belajar atau melakukan pelatihan dan penelitian. Tujuan utama *Cisco System* membuat aplikasi ini adalah untuk menyediakan alat bagi siswa dan pengajar maupun orang-orang yang berminat terhadap jaringan agar dapat memahami prinsip jaringan komputer dan juga membangun kemampuan di bidang peralatan jaringan Cisco [5].

Sebenarnya masih banyak software simulasi jaringan komputer yang dapat digunakan, seperti GNS3, *Boson Netsim*, dan lainnya, tetapi yang lebih mudah digunakan adalah *Cisco Packet Tracer* ini karena image devicenya telah disediakan menjadi satu paket d

alam software. Pada GNS3 Anda harus mencari image IOS device-nya terlebih dahulu yang akan digunakan untuk menjalankan *operating system* si perangkat jaringan yang dipilih [5].

Target *Packet Tracer* yang ditawarkan cisco adalah menyediakan simulasi jaringan yang *real* (asli), namun terdapat beberapa batasan berupa penghilangan

beberapa perintah yang digunakan pada alat aslinya, yaitu pengurangan *command* CISCO-IOS. *Packet Tracer* juga tidak bisa digunakan untuk memodelkan jaringan produktif/aktif. Namun demikian, software ini masih banyak digunakan dan menurut saya bagus untuk dikembangkan sebelum kita terjun langsung ke hardware jaringan yang sebenarnya [5].