BAB II
DASAR TEORI

2.1 Tinjauan Pustaka

Pada penelitian Dwi Aryanta yang berjudul Perancangan dan Analisis *Redistribution Routing Protocol* OSPF dan EIGRP [6]. Meneliti tentang simulasi proses *redistribution* antara *routing protocol* EIGRP (*Enhanced Interior Gateway Routing Protocol*) dan OSPF (*Open Shortest Path First*) yang kemudian akan dibandingkan kehandalannya dengan *single* routing *protocol* OSPF (*Open Shortest Path First*) dan EIGRP (*Enhanced Interior Gateway Routing Protocol*) menggunakan *software Packet Tracer* 5.3. Parameter pengujian dalam penelitian ini adalah nilai *time delay* dan *trace route*. Nilai *trace route* berdasarkan perhitungan langsung *cost* dan *metric* dibandingkan dengan hasil simulasi. Lalu hasil yang didapatkan oleh peneliti adalah nilai *delay redistribution* lebih baik 1% dibanding OSPF dan 2-3% di bawah EIGRP tergantung kepadatan *traffic*. Dalam perhitungan *trace route redistribution* dilakukan 2 perhitungan, yaitu *cost* untuk area OSPF dan m*etric* pada area EIGRP. Pengambilan jalur utama dan alternatif pengiriman paket berdasarkan nilai *cost* dan *metric* yang terkecil.

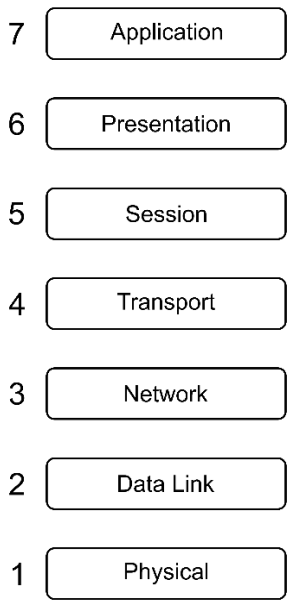
Selanjutnya pada penelitian Golap Kanti Dey, dkk. yang berjudul *Performance Analysis and Redistribution among RIPv2, EIGRP & OSPF Routing Protocol* [7]. Didalam topologi jaringan, sangat biasa menggunakan berbagai jenis *routing protocol* untuk meneruskan paket dimana tabel *routing* digunakan dalam memori *router* yang menyimpan jalur rute ke tujuan jaringan tertentu. *Routing protocol* yang digunakan adalah RIPv2 *(Routing Information Protocol version 2),* EIGRP (*Enhanced Interior Gateway Routing Protocol*) dan OSPF (*Open Shortest Path First*). Penelitian ini untuk menggambarkan perbandingan analisis kinerja ketiga *routing protocol* dinamis dan proses redistribusi antar *protocol* menggunakan delapan router Cisco dan switch dalam simulasi Packet Tracer dengan topologi jaringan empat router dengan *protocol* yang berbeda terhubung langsung dengan switch menggunakan redistribusi. Dari penelitian tersebut bahwa *protocol* EIGRP lebih baik daripada *routing*

protocol OSPF dan RIPv2, lalu OSPF lebih baik pada jaringan besar lainnya dimana sifat hirarkisnya meningkatkan skalabilitas dan RIPv2 berguna di jaringan area lokal yang kecil. Jadi perintah redistribusi menunjukkan cara untuk berkomunikasi dengan *routing protocol* yang berbeda.

2.2 Standarisasi OSI Dan TCP/IP

2.2.1 OSI (*Open System Interconnection*)

Dengan banyaknya atau bermacam komponen dan perangkat komputer dalam suatu jaringan, membutuhkan suatu standar *protocol* yang dapat digunakan oleh beragam perangkat tersebut. Salah satu standar *protocol* yang dikembangkan *International Standard Organization* (ISO) adalah model referensi *Open System Interconnection* (OSI). Model OSI merupakan model konseptual yang terdiri dari tujuh lapisan dimana setiap lapisannya mempunyai fungsi jaringan yang spesifik dan saling mendukung satu sama lain. Model ini telah dikembangkan oleh *International Organization For Standarization* (ISO) ditahun 1984, dan telah menjadi model arsitektur jaringan dan sebagai standarisasi dalam komunikasi antar komputer. Ketujuh lapisan OSI ini terlihat seperti gambar 2.1 [8]:



Gambar 2.1 Model OSI [9]

Pada gambar 2.1 merupakan urutan setiap lapisan OSI yang memiliki fungsi berbeda-beda, berikut adalah fungsi dari masing masing lapisan OSI [9]:

1. *Physical Layer*, lapisan yang paling dekat dengan *user*, bertanggung jawab atas proses data menjadi bit secara elektrik dan mengirimkannya serta menjaga koneksi.
2. *Data Link Layer*, befungsi memecah paket data yang akan dikirim menjadi beberapa paket data yang disebut *frame* dan bertanggung jawab memberikan *transfer* data yang terjamin bebas dari *eror* atau kesalahan.
3. *Network Layer*, untuk mengarahkan perjalanan (*routing*) melalui *internetwork* dan mengelola sistem pengalamatan *network*. *Router* merupakan perangkat yang bekerja dilapisan *network*.
4. *Transport Layer*, melakukan tugas pengiriman data secara *end-to-end protocol*. Lapisan ini bertanggung jawab terhadap keselamatan data dan segmentasi data.
5. *Session Layer*, bertugas untuk membangun, menjaga, mensinkronkan interaksi antar sistem yang berkomunikasi dan mengakhiri suatu hubungan komunikasi.
6. *Presentation Layer*, mengatur konversi dan translasi berbagai format data, seperti kompresi data dan enkripsi data, memastikan bahwa suatu data dapat terbaca oleh suatu sistem.
7. *Application Layer*, berfungsi sebagai *interface* antar *user* dan komputer. Bertanggungjawab dalam menyediakan pelayanan jaringan untuk proses aplikasi.

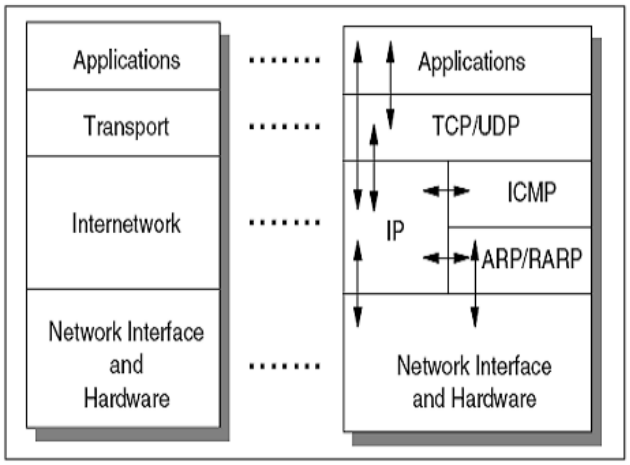
Tujuan model referensi OSI ini dibentuk dengan beberapa tujuan sebagai berikut [9]:

1. Menjadi pedoman dalam pengembangan prosedur komunikasi pada masa mendatang.
2. Mengatasi hubungan yang timbul antar pemakai dengan cara memberikan fasilitas yang sama dan memenuhi kebutuhan pemakai kini dan mendatang (berorientasi ke pengembangan masa depan).
3. Membagi permasalahan prosedur penyambungan menjadi substruktur.

4. *Open system* dengan tujuan agar dapat terjalin kerjasama antar terminal dan peralatan dari berbagai produk dan produsen yang berbeda.

2.2.2 TCP/IP (*Transmission Control Protocol/Internet Protocol)*

TCP/IP adalah sekumpulan *protocol* komunikasi yang distandarkan untuk intenet dan jaringan sejenis dalam proses pertukaran data dari satu komputer ke komputer lain. Tujuan dari TCP/IP adalah untuk membangun suatu koneksi antar jaringan *(network)*, dimana biasa disebut *internetwork*, atau intenet, yang menyediakan pelayanan komunikasi antar jaringan yang memiliki bentuk fisik yang beragam, berikut gambar 2.2 layer TCP/IP [1].



Gambar 2.2 *Protocol* TCP/IP [1]

Gambar 2.2 adalah layer protocol TCP/IP adapun fungsi masing-masing dari layer TCP/IP adalah sebagai berikut [1] :

1. Lapisan *Network Interface* memiliki fungsi yang mirip dengan *data link* pada OSI. Lapisan ini mengatur penyaluran *frame-frame* data pada media fisik yang digunakan. Lapisan ini memberikan servis untuk deteksi dan koreksi kesalahan dari data yang ditransmisikan.
2. Lapisan *Internetnetwork* berfungsi untuk menghubungkan dua perangkat ke jaringan yang berbeda. Pada lapisan ini dipergunakan IP untuk menyediakan fungsi *routing* melintasi jaringan yang bermacam-macam. Tugas lapisan *internet* adalah untuk mengirimkan paket-paket IP ke tempat tujuan seharusnya.
3. Lapisan *Transport* berfungsi melakukan pengiriman data antara *end to end host*. Lapisan ini menjamin bahwa informasi yang diterima pada sisi

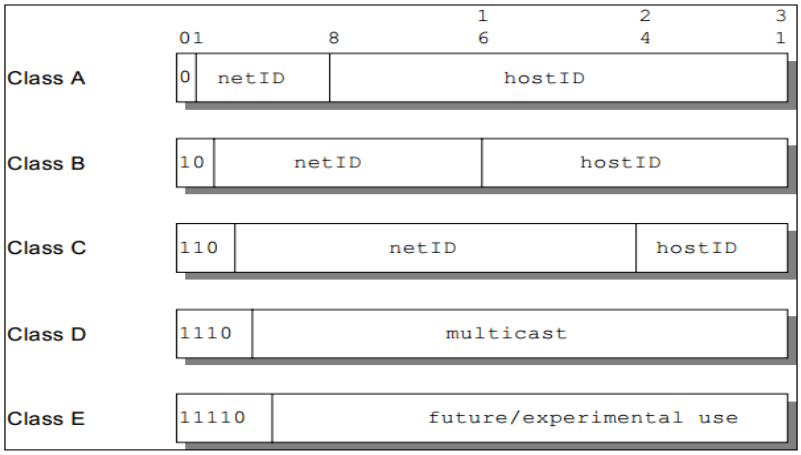
penerima adalah sama dengan informasi yang dikirimkan pada pengirim.

4. Lapisan *Application* Merupakan lapisan terkahir TCP/IP yang berfungsi mendefinisikan aplikasi yang dijalankan pada jaringan untuk berkomunikasi menggunakan TCP/IP. Contoh aplikasi antara lain Telnet dan *File Transfer Protocol* (FTP).

2.3 IP *(Internet Protocol)*

IP *address* atau *Internet Protocol Address* adalah bilangan yang digunakan sebagai pengenal tiap-tiap alat yang berada pada jaringan. IP *address* ditujukkan untuk mengetahui lokasi perangkat dalam sebuah jaringan dimana paket-paket data dikirimkan menggunakan *router* berdasarkan IP *address* yang sudah ditentukan. Awal perkembangan internet IP yang digunakan pertama yaitu IPv4 yang telah ada sejak awal tahun 1980an. IPv4 ini adalah generasi keempat dari internet *protocol* dan masih digunakan hingga sekarang secara luas. Internet *protocol* adalah bagian inti dari TCP/IP. Dalam model OSI, IP berada pada layer *network*. Fungsi utama dari IP ini adalah untuk mengidentifikasi host berdasarkan alamat, dengan tujuan untuk melakukan proses pertukaran paket data [10].

IP *address* terbagi menjadi 2 bagian yaitu *network adress* (*net* ID) berperan dalam menandai kelompok setiap jaringan dimana setiap mesin pada jaringan yang sama menggunakan *network address* yang sama dan *host address (host* ID) dipasang pada sebuah jaringan dimana tidak boleh terdapat dua atau lebih perangkat yang menggunakan alamat yang sama berikut gambar 2.3 pembagian kelas IPv4 [10].



Gambar 2.3 Pembagian Kelas IPv4 [10]

Pada gambar 2.3 pembagian IPv4 terbagi menjadi 5 kelas yang tergantung dari besarnya bagian *host* yaitu kelas A, kelas B, kelas C, kelas D dan kelas E [10]:

1. Kelas A, pada IP pada kelas A memiliki range IP dari 0.0.0.0 s/d 127.255.255.255. Sedangkan untuk alamat IP *private* yaitu 10.0.0.0 s/d 10.255.255.255.
2. Kelas B, pada IP kelas B ini memiliki range IP dari 128.0.0.0 s/d 192.255.255.255 dan untuk alamat IP *private* kelas B yaitu 172.16.0.0 s/d 172.31.255.255.
3. Kelas C, memiliki range IP dari 192.0.0.0 s/d 233.255.255.255 dan untuk alamat IP *private* kelas C yaitu 192.168.0.0 s/d 192.168.255.255.
4. Kelas D, alamat IP kelas D digunakan khusus untuk *multicasting*.
5. Kelas E, alamat IP kelas E digunakan untuk penelitian atau untuk keperluan khusus atau eksperimen.

2.4 *Routing Protocol*

Sebuah *routing protocol* adalah seperangkat aturan atau standar yang menentukan bagaimana *router* pada jaringan berkomunikasi dan bertukar informasi satu sama lain, memungkinkan mereka untuk memilih *rute* terbaik ke sebuah jaringan yang dituju. *Routing protcol* akan mencatatkan semua alamat *network* lawan kedalam tabel *routing router* begitu protokol ini diaktifkan. Protokol yang telah diaktifkan ini akan mempertukarkan informasi mengenai rute yang terdapat pada tabel *routing* [2]. Dengan adanya pertukaran informasi yang ada dalam setiap tabel *routing* suatu *router* maka *router* lainnya yang tidak terhubung langsung dapat mengetahui isi dari tabel *routing router* tetangga yang tidak terhubung langsung. Kondisi ketika semua alamat *network* dalam suatu jaringan telah tercatatkan dalam tabel *routing* dapat disebut dengan kondisi jaringan yang konvergen sehingga antar komputer dapat saling bertukar data dan saling terkoneksi. Secara umum ada dua jenis *routing protocol*, yaitu [4]:

1. *Distance Vector* (*Path Vector*) *Protocol* disebut *distance vector protocol* karena penentuan *routing* berdasarkan *distance* atau jarak terpendek, antara titik asal paket dengan titik tujuan. Contoh *distance vector* yaitu

RIP (*Routing Information Protocol*), IGRP (*Interior Gateway Routing Protocol*), dan EIGRP *(Enhanced Interior Gateway Routing Protocol)* adalah versi yang disempurnakan dari *routing protocol* IGRP, EIGRP menggunakanrouting *distance vector based* yang sama dengan yang digunakan IGRP dengan perbaikan adalah konvergensi dan efisiensi operasi.

2. *Link State Protocol* disebut *link state protocol* karena penentuan *routing* dilakukan berdasarkan informasi yang diperoleh dari *router-router* lain. *Link state* dikembangkan menggunakan algoritma *shortest path*, seperti algoritma dijkstra‟s. Algoritma dijkstra‟s merupakan algoritma yang paling sering digunakan dalam pencarian rute terpendek, sederhana penggunaannya dengan menggunakan simpul-simpul sederhana pada jaringan jalan yang tidak rumit. Adapun nama algoritma dijkstra‟s sendiri berasal dari penemunya yaitu Edsger dijkstra‟s. Dalam mencari solusi, algoritma dijkstra‟s menggunakan prinsip *greedy*, yaitu mencari solusi optimum pada setiap langkah yang dilalui, dengan tujuan untuk mendapatkan solusi optimum contoh *link state* adalah OSPF.

2.4.1 RIP *(Routing Information Protocol)*

RIP merupakan salah satu contoh dari algoritma *Distance vector*. RIP mengirimkan semua isi *routing* table ke *router* tetangga yang terhubung secara langsung (*directly connected*), secara periodik setiap 30 detik. *Router* yang menerima *routing* update akan meng-update *routing* table-nya dan kemudian mengirimkan *routing* update ke *router* di sampingnya lagi. Proses ini akan terus berulang melalui semua *router* yang ada pada jaringan. Setiap perpindahan 1 *router* maka nilai hop *count* akan bertambah 1. Bila paket data telah melalui 15 *router*, maka paket tersebut akan *di-discard* (dimusnahkan), meskipun belum mencapai tujuannya, dan *network* tujuan juga akan dianggap *unreachability* (tidak dapat dicapai). RIP menggunakan *hop count* sebagai *metric* dengan maksimal *hop count* adalah 15 sebagai upaya agar tidak sampai terjadi *count to infinity* dan *routing loop. RIP* merupakan *routing protocol* yang paling mudah untuk dikonfigurasi. *RIP* memiliki 3 versi yaitu [10] :

1. *RIPv1* Spesifikasi asli versi *RIP* yang pertama, didefinisikan dalam *RFC 1058*, *classfull* menggunakan *routing*. *Update routing* periodik pada versi ini tidak membawa informasi subnet kemudian kurang mendukung untuk *Variable Length Subnet Mask* (VLSM). Keterbatasan dari versi ini tidak dapat memiliki subnet berukuran berbeda dalam kelas jaringan yang sama. Dengan kata lain, semua subnet dalam kelas jaringan harus memiliki ukuran yang sama dan juga tidak ada dukungan untuk router otentikasi sehingga membuat versi ini rentan terhadap berbagai serangan.
2. *RIPv2* merupakan perkembangan kekurangan yang terdapat di dalam spesifikasi *RIP* asli, *RIP* versi 2 (RIPv2) dikembangkan pada tahun 1993 dan standar terakhir pada tahun 1998. Kemampuan dari *protocol RIP* versi ini yaitu mampu membawa informasi subnet, sehingga mendukung *Classless Inter-Domain Routing* (CIDR) dan juga mendukung *Variable Length Subnet Mask* (VLSM). Untuk menjaga kompatibilitas, maka batas hop masih tetap sampai 15 hop. *RIPv2* memiliki fasilitas yang sepenuhnya beroperasi dengan spesifikasi awal yaitu *RIPv1*. Upaya dalam menghindari terjadinya beban *host* yang tidak perlu dan host yang tidak berpartisipasi pada *routing*. *RIPv2* dengan fiturnya akan me-*multicast* seluruh tabel *routing* ke semua tabel *routing* yang berdekatan. Di dalam *protocol* versi ini, pengalamatan menggunakan *unicast* masih boleh dipergunakan untuk aplikasi khusus.
3. *RIPng* RIP *Next Generation* (RIPng), yang didefinisikan dalam *RFC 2080*, adalah perluasan dari *RIPv2* untuk mendukung *IPv6*, generasi *Internet Protocol* berikutnya.

2.4.2 EIGRP *(Enhanced Interior Gateway Routing Protocol)*

Enhanced Interior Gateway Routing Protocol (EIGRP) merupakan *routing protocol* yang telah ditingkatkan (*enhanced*) dari pendahulunya yaitu *Interior Gateway Routing Protocol* (IGRP) dan hanya dapat digunakan oleh *router* yang diproduksi oleh Cisco, Inc. EIGRP menggunakan konsep *Autonomous System* (AS) untuk menggambarkan *router-router* suatu jaringan yang beroperasi dengan *protocol* yang sama

dan saling berbagi informasi *routing* yang sama. EIGRP memiliki karakteristik sebagai berikut [4]:

1. Termasuk *routing protocol distance vector* tingkat lanjut.
2. Menggunakan *cost load balancing* yang tidak sama.
3. Menggunakan algoritma kombinasi antara *distance vector* dan *link state*.
4. Menggunakan *Diffusing Update Algorithm* (DUAL) untuk menghitung jalur terpendek.
5. *Update routing* dilakukan secara *multicast* apabila terjadi perubahan pada topologi jaringan.

EIGRP menggunakan algoritma DUAL untuk mencari dan menjaga jalur terbaik atau terpendek yang dapat melewati data ke setiap jaringan yang terpisah. DUAL memilih rute-rute berdasarkan tabel pada *feasible succesor* [11]. DUAL juga memperbolehkan sebuah *router* EIGRP menemukan rute alternatif, jadi ketika jalur mati atau terputus *router* EIGRP akan dengan cepat menanyakan kepada *router-router* tetangga untuk membantu mencarikan arah. Mengandalkan *router* lain dan memanfaatkan informasi merupakan alasan karakter *diffusing* atau membaur dari DUAL. Berikut cara kerja dari *routing protocol* EIGRP ini adalah sebagai berikut :

1. *Advertised Distance* (AD), merupakan laporan nilai *metric* dari *router* tentang *cost* menuju *network* yang dikirim ke *router* tetangga.
2. *Feasible Distance* (FD), adalah informasi rute terbaik yang diperoleh dari *routing table*.
3. *Successor*, adalah jalur terbaik untuk meneruskan trafik data ke suatu tujuan *network* yang terpisah.
4. *Feasible Successor*, adalah jalur yang jaraknya kurang dari *feasible distance* yang dianggap sebagai rute cadangan atau jalur *backup* dari *successor*.

EIGRP memlih jalur terbaik dalam suatu jaringan berdasarkan perhitungan *bandwidth* dan *delay* pada *interface router*. *Bandwidth* suatu *interface* adalah sebagai nilai konsumsi data yang tersedia, dihitung dalam satuan kbps. Sedangkan *delay* adalah waktu paket didalam sistem. Berikut adalah perhitungan *metric* [11] :

$$\text{EIGRP Metric} = \frac{max\ bandwidth}{min\ bandwidth} + \sum \frac{delay}{10} \times 256 \qquad (2.1)$$

Keterangan :

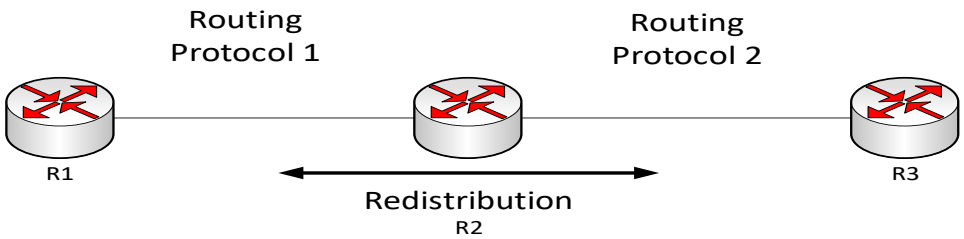
Max bandwidth = 10000000 (kbps)

Min bandwidth = *link* pada *interface* (kbps)

Delay = total *delay* pada *interface* dibagi 10 ms

2.5 *Redistribution Routing*

Redistribution adalah cara untuk meneruskan *routing tabel* yang dibentuk oleh suatu *routing protocol* untuk diteruskan ke *routing protocol* lain. Pada prinsipnya router menjadi penghubung antara *network* dengan *routing protocol* yang berbeda [4]. Berikut ilustrasi metode redistribusi



Gambar 2.4 Ilustrasi *Redistribution Routing*

Pada gambar 2.4 merupakan ilustrasi *redistribution routing* menggunakan *routing protocol* berbeda yang dipergunakan oleh kedua *network* tersebut, misal *Routing protocol* 1 menggunakan RIPv2 dan *Routing protocol* 2 menggunakan EIGRP. Untuk membuat agar *routing tabel* yang dibentuk oleh RIPv2 bisa diteruskan menuju ke EIGRP maka dipergunakan *redistribute* RIPv2 pada router 2 sebagai penghubung antara network routing protocol RIPv2 dan network routing protocol EIGRP, dan sebaliknya agar *routing tabel* yang terbentuk pada EIGRP bisa diteruskan menuju RIPv2 maka dipergunakanlah *redistribute* EIGRP.

Redistribute routing merupakan suatu cara untuk mengirimkan rute yang telah dipelajari oleh *routing protocol* yang berbeda. Penggunaan lebih dari satu jenis *routing protocol* didalam suatu jaringan biasanya dihadapkan pada beberapa hal seperti *company merger*, *multiple network administrator*, ataupun karena penggunaan perangkat dari vendor yang berbeda.

Redistribution menjadi pilihan yang bagus dalam memberikan informasi rute antara *routing protocol* yang berbeda karena mudah dalam konfigurasi. Penerapan *redistribute* harus diperhatikan seperti karakteristik dari setiap *routing protocol* yaitu *metric* dan *administrative distance routing* [4].

1. ***Metrics***

   Metrics merupakan nilai untuk menentukan prioritas dari pemilihan rute pada suatu *routing* tabel. *Metrics* yang digunakan pada setiap *routing* protocol berbeda seperti RIP menggunakan jumlah hop sebagai metrics nya. Sedangkan pada OSPF ataupun EIGRP *metrics* didapatkan dari nilai beberapa kondisi seperti *delay*, *bandwidth* , *load*. Berikut merupakan tabel *metrics* dari setiap *routing protocol* [4].

Tabel 2.1 *Metrics Routing Protocol*

Routing Protocol	*Metric*
RIP	*Hop*
IGRP	*Bandwidth, Delay, Load*
OSPF	*Cost*
EIGRP	*Bandwidth, Delay*
IS-IS	*Cost*

Berikut penjelasan tabel 2.1 *metric* yang digunakan dalam *routing protocol* IP meliputi [4]:

a. *Hop count* : sebuah *metric* sederhana yang menghitung jumlah router yang harus dilalui sebuah paket.
b. *Bandwidth* : mempengaruhi pemilihan jalur dengan memilih nilai *bandwidth* yang paling tinggi.
c. *Load* : Mempertimbangkan penggunaan lalu lintas dari link tertentu.
d. *Delay* : Mempertimbangkan waktu yang dibutuhkan paket untuk melintasi rute.
e. *Cost* : Nilai yang ditentukan oleh IOS atau oleh *administrator* jaringan untuk ditunjukkan preferensi rute.

2. Administrative Distance

Saat *metrics* bernilai sama atau tidak maka akan digunakan *administrative distance*. *Administrative distance* menentukan prioritas dari penggunakan rute berdasarkan nilai yang terdapat didalamnya. Semakin rendah *administrative distance* pada suatu route maka *route* tersebut akan menjadi jalur utama berikut *default administrative distance* dari setiap *routing protocol* seperti tabel 1.2 [4].

Tabel 2.2 *Default Administrative Distance Routing Protocol*

Routing Protocol	*Administrative Distance*
RIP	120
IGRP	100
OSPF	110
EIGRP	90
IS-IS	115

Sebagai contoh jika sebuah router menerima informasi *routing* dari dua *protocol Open Shortest Path First* (OSPF) yang memiliki nilai administrative distance 110 dan *Interior Gateway Routing Protocol* (IGRP) yang memiliki nilai administrative distance 100, maka router akan memiliki menggunakan informasi *routing* yang dimiliki IGRP.

Jadi setiap *routing protocol* dinamis memiliki nilai administrasi yang unik, bersamaan dengan rute statis dan jaringan yang terhubung langsung. Semakin rendah nilai administrasi, semakin disukai sumber rutenya. Jaringan yang terhubung langsung merupakan sumber yang disukai, diikuti oleh rute statis dan kemudian berbagai *routing protocol* dinamis. Fitur ini digunakan untuk memilih jalur terbaik pada jaringan tujuan yang sama dari dua atau lebih sumber perutean yang berbeda [4].

2.6 QoS (*Quality Of Service*)

Quality of sevice menggabarkan nilai indikator dari kualitas sebuah laynan. Pada jaringan itu sendiri QoS merupakan kemapuan untuk memberikan jaminan performansi dalam jaringan tersebut. Performansi dalam sebuah jaringan dapat diukur dari kecepatan, kehandalan dalam

penyampaian berbagai jenis data pada sebuah sistem komunikasi [12]. Performansi QoS bisa dilihat dari parameter-parameter berikut yaitu *packet loss*, *delay*, dan *throughput.*

2.6.1 *Throughput*

Throughput adalah suatu kecepatan dalam transfer data efektif, yang akan diukur dalam bps. *throughput* sendiri berhubungan dengan *bandwidth* yang disediakan tetapi tidak semua tidak digunakan oleh aplikasi jaringan [12]. Untuk mengatahui *throughput* dapat dihitung dengan jumlah paket data yang telah diterima kemudian dibagi dengan lamanya pengamatan dalam satuan waktu. Berikut rumus yang digunakan untuk mengetahui jumah *throughput* :

$$\textit{Throughput}\ (\text{bps}) = \frac{\text{Jumlah data yang dikirim (bit)}}{\text{waktu pengiriman data (s)}} \qquad (2.2)$$

Keterangan :

- Jumlah data yang dikirim (bit) = total data yang dikirim dari *server* ke *client* (bit).
- Waktu pengiriman data = lama waktu pengiriman data dari *server* ke *client* (s).

2.6.2 *Delay*

Delay merupakan sebuah total waktu yang dibutuhkan sebuah paket untuk menempuh jarak dari pengiriman sampai dengan ke tujuan. Sebuah *delay* dapat dipengaruhi oleh jarak, media fisik, dan waktu proses yang lama [12]. Berdasarkan pengertian tersebut, *delay* dapat dihitung menggunakan Persamaan 2.3:

$$Delay = \frac{Total\ Delay}{Jumlah\ total\ paket} \quad (2.3)$$

Keterangan :

- Total delay = Jumlah *delta time* pada sisi *client*.
- Jumlah total paket = jumlah paket yang diterima pada sisi *client*.

Persamaan 2.3 dapat digunakan jika waktu paket di kedua sisi diketahui. Namun, jika waktu paket di salah satu sisi tidak diketahui, maka Persamaan 2.3 tidak dapat digunakan. Alternatifnya dapat menghitung

latency rata-rata menggunakan Persamaan 2.4 dengan asumsi pengiriman data berlangsung pada jalur komunikasi yang ideal.

$$Delay\ rata-rata\ (s) = \frac{Delta\ time\ rata-rata\ (s)}{2}$$

(2.4)

Keterangan :

- *Delta time* = waktu paket diterima saat ini dikurangi saat ini dikurangi waktu paket diterima sebelumnya (s).
- *Delta time* rata-rata = jumlah *delta time* dibagi dengan jumlah banyaknya *delta time* (s).

Nilai dari *delay* ini nantinya akan menentukan dari kualitas sebuah jaringan. Perhitungan nilai *delay* tersebut nanti dikategorikan kedalam tabel 2.3, terdapat standart untuk kualitas *delay* sebagaimana *versi Telecomunication and Internet Protocol Harmonization Over Network* (TIPHON) dapat dikelompokkan sebegai berikut [13] :

Tabel 2.3 Kategori *Delay* [13]

Kategori *Delay*	*Delay*
Sangat bagus	<150 ms
Bagus	150 ms s/d 300 ms
Sedang	300 ms s/d 450 ms
Buruk	>450 ms

Hasil perhitungan parameter *delay* pada rumus 2.4 akan dibagi menjadi empat kategori yaitu nilai standart *delay* sangat bagus bernilai kurang dari 150 milisecond, kategori *delay* bagus antara 150 milisecond sampai 300 milisecond, kategori *delay* sedang antara 300 milisecond sampai 450 milisecond, dan kategori *delay* buruk dengan nilai lebih dari 450 milisecond. Jadi semakin kecil nilai *delay*-nya maka semakin baik kualitas jaringannya

2.6.3 *Packet loss*

Packet loss merupakan suatu kegagalan atau sebuah paket yang tidak sampai dengan sempurna pada tujuannya. Kegagalan tersebut dapat disebabkan oleh beberapa faktor seperti terjadinya *overload traffic* pada jaringan, terjadinya tabrakan data, *error* pada media fisik. Untuk mendapatkan jaringan yang baik maka untuk hasil dari *packet loss* ini diharapkan memliki nilai yang kecil [13]. Berikut rumus yang digunakan untuk mendapatkan jumlah *packet loss* :

$$Packet\ Loss\ (\%) = \left(\frac{\text{Jumlah paket yang dikirim - Jumlah paket yang diterima}}{\text{Jumlah paket yang dikirim}} \right) \times 100\% \quad (2.5)$$

Keterangan :

- Jumlah paket yang dikirim = total paket yang dikirim *server*
- Jumlah paket yang diterima = total paket yang diterima *client*

Perhitungan nilai *packet loss* tersebut nanti dikategorikan kedalam tabel 2.4 sebagaimana *versi Telecomunication and Internet Protocol Harmonization Over Network* (TIPHON) dapat dikelompokkan sebegai berikut [13]:

Tabel 2.4 Kategori *Packet loss* [13]

Kategori *Packet loss*	*Packet loss*
Sangat bagus	0%
Bagus	3%
Sedang	15%
Buruk	25%

Hasil perhitungan parameter *packet loss* pada rumus 2.4 akan dibagi menjadi empat kategori yaitu nilai standart *packet loss* sangat bagus jumlah persentasenya adalah 0% sampai 3%, kategori *packet loss* bagus jumlah persentasenya adalah 3%, sampai 15%, kategori *packet loss* sedang jumlah persentasenya adalah 15% -25%, dan kategori *packet loss* buruk dengan nilai persentasenya adalah lebih dari 25%. Jadi hasil dari *packet loss* ini diharapkan memliki nilai persentase yang kecil.