# BAB I

## PENDAHULUAN

### Latar Belakang

Perkembangan IT saat ini menuju dengan konsep-kosenp social networkingnya, openess, share, colaborations, mobile, easy maintenance, one click, terdistribusi / tersebar, scalability, Concurency dan Transparan, Saat ini terdapat trend teknologi yang masih terus digali dalam penelitian-penelitian para pakar IT di dunia, yaitu Cloud Computing.

Routing adalah suatu protokol yang digunakan untuk mendapatkan rute dari satu jaringan ke jaringan yang lain. Rute ini disebut dengan route dan informasi route secara dinamis dapat diberikan ke router yang lain ataupun dapat diberikan secara statis ke router lain.

Konsep dasar dari routing adalah bahwa router meneruskan paket-paket IP berdasarkan pada IP address tujuan yang ada dalam header IP paket. Dia mencocokkan IP address tujuan dengan routing table dengan harapan menemukan kecocokan entri; suatu entri yang menyatakan kepada router ke mana paket selanjutnya harus diteruskan. Jika tidak ada kecocokan entri yang ada dalam routing table, dan tidak ada default route, maka router tersebut akan membuang paket tersebut. Untuk itu adalah sangat penting untuk mempunyai isian routing table yang tepat dan benar.

Agar isian pada tabel routing tepat dan benar, maka perlu bantuan dari adminstrator untuk mengisikannya, oleh karena itu routing static adalah pilihan tepat untuk membangun sebuah jaringan, terutama untuk jaringan berskala kecil

Apabila jaringan memiliki lebih dari satu kemungkinan rute untuk tujuan yang sama maka perlu digunakan dynamic routing. Sebuah dynamic routing dibangun berdasarkan informasi yang dikumpulkan oleh protokol routing. Protokol ini didesain untuk mendistribusikan informasi yang secara dinamis mengikuti perubahan kondisi jaringan. Protokol routing mengatasi situasi routing yang kompleks secara cepat dan akurat. Protokol routing didesain tidak hanya untuk mengubah ke rute backup bila rute utama tidak berhasil, namun juga didesain untuk menentukan rute mana yang terbaik untuk mencapai tujuan tersebut. Pengisian dan pemeliharaan tabel routing tidak dilakukan secara manual oleh admin. Router saling bertukar informasi routing agar dapat mengetahui alamat tujuan dan menerima tabel routing. Pemeliharaan jalur dilakukan oleh Routing Dinamic.

Berdasarkan penjelasan diatas maka kami kelompok 8 akan membahas mengenai static routing dan dynamic routing.

### Identifikasi Masalah

Berdasarakan latar belakang diatas, dapat dikemukaan beberapa permasalahan yang dapat diidentifikasi yaitu:

Apa itu routing static dan dinamyc?

Apa saja contoh dari routing static dan dinamic?

Bagaimana konfigurasi routing static dan dinamic ?

### Batasan Masalah

Dari identifikasi maslah diatas maka kami akanmembatasi ruang lingkup pembahasan yaitu:

Makalah ini hanya membahas mengenai routing static dan dynamic.

Contoh-contoh protocol dari routing static dan dynamic

Konfigurasi routing static dan dynamic

### Rumusan Masalah

Berdasarkan latar belakang dan identifikasi maslah, dapat dirumuskan permasalahkan yang akan diselesaikan yaitu bagaimana konsep peroutingan routing static dan routing dynamic.

### Tujuan Penulisan

Tujuan yang bisa didapat dari penulisan makalah ini adalah :

Untuk mengetahui apa itu Routing static dan dinamic

Untuk mengetahui jenis-jenis protocol dari Routing static dan dinamic.

Untuk mengetahui bagaimana cara mengkonfigurasikan Routing static dan routing dinamic.

# BAB II

## PEMBAHASAN

Pengertian Routing

Routing adalah proses pengiriman data dari satu host dalam satu network ke host dalam network yang lain melalui suatu router. Agar router dapat mengetahui bagaimana meneruskan paket paket ke alamat yang dituju dengan mengunakan jalur terbaik, router menggunakan peta atau tabel routing. Table routing adalah table yang memuat seluruh informasi IP address dari interfaces router yang lain sehingga router yang satu dengan router lainnya bisa berkomunikasi.

Bila kita mengacu pada pemodelan OSI (Open System Interconnection), maka proses routing terjadi pada Layer 3 (Network Layer). Karena terjadi pada Layer Network, maka proses routing erat kaitannya dengan pengalamatan logika atau IP Address. Untuk bentuk data yang akan diolah pada proses routing adalah packet yang merupakan Protocol Data Unit (PDU) di Layer 3, dimana Protocol Data Unit yang diolah di Layer 1 disebut bit, Layer 2 disebut frame, Layer3 disebut packet, Layer 4 disebut segmen sedangkan Layer 5 sampai 7 disebut data.

Didalam tabel routing informasi routing akan disimpan dalam bentuk entry-entry route (rute). Setiap entry route akan menunjukkan network address dari network yang dapat dituju oleh router tersebut. Entry route ini juga berisi tentang informasi bagaimana cara mencapai network tersebut. Entry Route pada tabel routing tersebut dapat dibuat atau dikonfigurasi secara manual oleh Administrator jaringan atau dapat juga diperoleh router secara otomatis dengan melakukan pertukaran informasi routing dengan router lain.

Routing dapat menghubungkan beberapa jaringan yang terhubung langsung pada interfacenya, seperti pada gambar 2.1. Pada jaringan tersebut tidak dibutuhkan teknik routing yang rumit karena merupakan jaringan yang sangat sederhana. Kita hanya perlu mengaktifkan IP Address pada masing-masing interface router dan kedua jaringan tersebut sudah dapat terhubung.

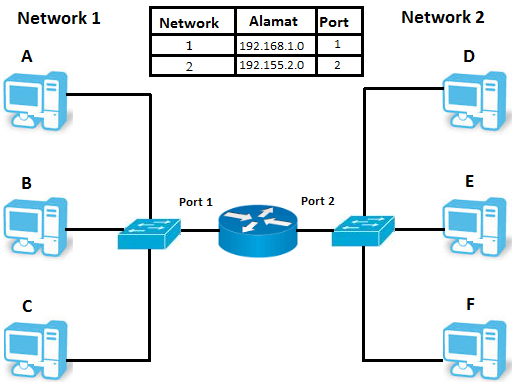


Figure 1.0 Dua network terhubung dengan sebuah router

Tabel Routing

Seperti yang kita ketahui router berfungsi untuk mengirimkan paket data dari satu network ke network lain sekaligus menentukan jalur terbaik (best path) untuk mencapai network tujuan. Untuk menjalankan fungsi tersebut router menggunakan tabel yang disebut tabel routing (routing tabel). Tabel tersebut berisi informasi keberadaan beberapa network, baik network yang terhubung langsung (directly connected network) maupun network yang tidak terhubung langsung (remote network).

Tabel ini juga berisi informasi bagaimana cara router tersebut mencapai suatu network. Tabel routing ini sangat penting karena digunakan router sebagai pedoman untuk mengirimkan setiap paket data yang diterimanya.

Informasi dalam tabel routing berupa baris-baris network address yang disebut entry route (kadang cukup disebut route). Dalam setiap entry route juga telah ada informasi tentang interface mana yang dapat digunakan router tersebut untuk mengirimkan paket data. Kita dapat mengambil analogi bandar udara sebagai router, penumpang sebagai paket data, papan informasi perjalanan sebagai tabel routing dan pintu keberangkatan sebagai interface router.

Jika kita adalah penumpang yang ingin berpergian ke luar kota maka kita harus menuju bandar udara, karena di bandar udaralah tersedia pesawat-pesawat yang dapat mengantarkan anda ke kota lain. Begitu juga dengan sebuah paket data yang ingin dikirimkan ke network lain, harus diberikan kepada router, karena routerlah yang mempunyai kemampuan menghubungkan beberapa network itu.

Di bandar udara kita tentu dapat melihat papan informasi yang berisi informasi kota-kota tujuan beserta penerbangan apa yang dapat membawa kita ke kota tersebut. Dipapan informasi itu juga dijelaskan maskapai penerbangan apa dan pintu keberangkatan nomor berapa pesawat anda menunggu. Umumnya bandara memiliki beberapa pintu keberangkatan.

Ini sama saja dengan tabel routing yang berisi informasi network address yang dapat dituju oleh router, beserta interface mana yang dapat digunakan untuk menuju network address itu. Setelah kita menentukan kota mana yang akan dituju (tentunya dengan membeli tiket yang sesuai), maka kita akan dituntun menuju pintu keberangkatan dimana pesawat kita sudah menanti. Kita harus memilih pintu yang tepat untuk kota tujuan dan pesawat yang sudah kita pilih. Ini dapat disamakan dengan router yang mencocokan IP Address tujuan dari setiap paket data dengan entry yang ada dalam tabel routing.

Jika ternyata ada entry yang cocok, maka router akan mengalihkan paket data tersebut ke interface yang dapat digunakan untuk mencapai network luar, tetapi jika ternyata tidak ada enty yang cocok, maka router akan membuang paket data tersebut. Seperti kita yang harus menggunakan pintu keberangkatan yang tepat untuk kota yang tepat pula.

Ada 4 kategori entry dalam tabel routing, yaitu :

Directly Connected network

Entry ini akan muncul pada saat interface router diaktifkan dan dikonfigurasikan IP Address. Beberapa jenis router status default dari interfacenya adalah disable (non aktif) sehingga perlu diaktifkan oleh Administrator Jaringan.

Static Routes

Entry ini adalah entry yang diisi manual oleh Administrator jaringan, sehingga jika terjadi perubahan jaringan, maka entry ini juga harus dirubah secara manual pula.

Dynamic Routes

Entry ini adalah entry yang akan muncul karena hasil pertukaran informasi routing dari beberapa router. Pertukaran informasi routing akan menggunakan routing protocol. Entry ini tidak diisikan manual oleh Administrator jaringan. Dalam hal ini Administrator hanya perlu mengaktifkan routing protocol dan network yang akan di routing.

Default Routes

Entry ini digunakan untuk menentukan kemana sebuah paket akan dikirimkan jika alamat tujuan dari paket tersebut tidak terdapat pada tabel routing. Entry default routes bisa dikonfigurasikan secara manual (static) ataupun didapat dari pertukaran informasi dari routing protocol (dynamic).

Kemudian kita harus mengetahui tentang mana network yang merupakan directly connected network dan mana yang merupakan remote network dari sebuah router. Directly connected network adalah network atau jaringan yang terhubung langsung pada interface sebuah router. Sedangkan remote network adalah jaringan yang tidak terhubung secara langsung pada sebuah router. Untuk menjangkau remote network sebuah route memerlukan router lain sebagai next hop atau gateway.

Static Routing

Definisi Static Routing

Routing statik adalah teknik routing yang dilakukan dengan memasukkan entry route ke network tujuan (remote network) ke dalam tabel routing secara manual oleh Administrator Jaringan. Dalam memasukkan entry route tersebut Administrator harus dapat mengetahui dengan pasti gateway yang akan digunakan untuk mencapai remote network. Untuk jaringan yang terdiri dari beberapa router, maka penentuan gateway maupun jalur (path) harus dilakukan dengan lebih cermat.

Jika dalam jairngan terjadi perubahan topologi maupun perubahan pengalamatan (IP Address) maka Administrator juga harus secara manual melakukan perubahan pada tabel routing. Ini menjadi tidak efisien untuk jaringan berskala besar atau jaringan yang sering mengalami perubahan. Karena jika terjadi suatu perubahan kecil dalam jaringan maka Administrator jaringan harus mengkonfigurasikan kembali entry route pada setiap router yang ada dalam jaringan.

Prinsip Routing Static.

Dalam menerapkan routing static, kita akan mengisikan entry route pada tabel routing secara manual di setiap router yang ada dalam jaringan. Sebuah entry routing static yang akan dimasukkan ke tabel routing harus mengandung 3(tiga) informasi, yaitu :

Network Address, informasi ini merupakan network address dari network yang akan dituju (remote network).

Subnet Mask (prefix), informasi ini merupakan prefix atau subnet mask dari network yang akan dituju.

Next Hop atau Gateway, informasi ini berguna memberitahukan kepada router tentang bagaimana mencapai network tujuan yang telah didefinisikan di point (1). Next Hop merupakan IP Address dari router tetangga yang dapat digunakan untuk mencapai network tujuan (remote network).

Keuntungan dan Kekurangan Static Routing

Keuntungan Static Routing

keamanan network karena static routing hanya mengandung informasi yang telah dimasukkan secara manual.

Pengiriman paket data lebih cepat karena jalur atau rute sudah di ketahui terlebih dahulu.

Deteksi dan isolasi kesalahan pada topologi jaringan lebih mudah.

Beban kerja router terbilang lebih ringan karena pada saat konfigurasi router hanya mengupdate sekali saja ip table yang ada.

Kerugian Static Routing

Waktu konfigurasi lama

Harus tahu semua alamat network yang akan dituju beserta subnet mask dan next hoopnya (gatewaynya).

Tidak cocok untuk jaringan berskala besar.

Pengembangan network

Jika suatu network ditambah atau dipindahkan maka static routig harus diperbaharui oleh administrator.

Rentan terhadap kesalahan saat entri data static route dengan cara manual.

Administrasinya adalah cukup rumit dibanding dynamic route, khususnya terdiri dari banyak router yang perlu dikonfigurasi secara manual.

Pembatasan static router dapat menjadi keuntungan apabila untuk sampai pada tujuan hanya melalui satu router.

Konfigurasi Routing Static

Mari kita perhatikan gambar 2.2 yang merupakan topologi sederhana network 192.168.10.0/24 dan 192.168.20.0/24 yang dihubungkan oleh Router R0 dan Router R1. Kedua buah router tersebut masih dihubungkan lagi dengan sebuah network yaitu network 10.10.10.0/24.

Gambar 2.2 Dua jaringan yang dihubungkan dengan dua router

R0 memiliki dua directly connected network, yaitu network 192.168.10.0/24 dan 10.10.10.0/24, sehingga setelah kita mengkonfigurasikan IP Address pada Fa1/0 dengan 10.10.10.1/24 dan Fa0/0 dengan 192.168.10.1/24 maka entry untuk network 192.168.10.0/24 dan 10.10.10.0/24 akan secara otomatis masuk ke dalam tabel routing seperti berikut :

Dari tabel routing diatas, R0 tidak mengetahui keberadaan remote network 192.168.20.0/24 yang terhubung ke interface Fa0/0 dari R1. Untuk memberitahukan keberadaan network 192.168.20.0/24 tersebut maka kita harus memberitahukan informasi sebagai berikut :

Network Address = 168.20.0, yang merupakan network address dari remote network yang akan dituju.

Prefix = /24, merupakan prefix dari network 192.168.20.0

Next hop (Gateway) = 10.10.2, yang merupakan IP Address dari Fa1/0 dari R2, interface ini dapat digunakan oleh R1 untuk mencapai network 192.168.20.0/24

Perintah yang digunakan untuk mengkonfigurasi routing static untuk mendapatkan entry route ke network 192.168.20.0/24 sebagai berikut :

Dengan begitu maka R0 akan memiliki informasi keberadaan network 192.168.20.0/24 dan dapat dicapai melalui IP Address 10.10.10.2, sampai disini konfigurasi static pada R0 telah selesai, berikut hasilnya :

Konfigurasi selanjutnya harus dilanjutkan pada R1 dengan tujuan memberitahukan keberadaan network 192.168.10.0/24 yang dapat dicapai dengan menggunakan next hop 10.10.10.1 (Fa1/0), pada R1 untuk mendapatkan entry route ke network 192.168.10.0/24 seperti berikut :

Sehinga pada tabel routing di R1 telah mengetahui keberadaan network 192.168.10.0/24 yang dapat dicapai melalui interface Fa1/0 10.10.10.1 seperti berikut :

Beberapa Teknik Static Routing

Teknik Static Routing dengan Summarization

Sebelum kita melakukan routing dengan Summarization, terlebih dahulu kita mengenal route summarization yang merupakan teknik merangkum atau meringkas beberapa network menjadi sebuah network address, teknik ini juga dikenal dengan nama Route Aggregation atau Supernetting. Router summarization digunakan untuk menyederhanakan tabel routing yang ada pada router. Topologi yang akan digunakan untuk mengimplementasikan route summarization terlihat seperti gambar 2.3

Gambar 2.3 Route Summarization

Penerapan route summarization hanya akan mengambil implementasi dari Router4. Ini karena Rrouter4 memiliki beberapa remote network yang dapat dicapai melalui IP Address 10.10.10.2 Jika tidak menerapkan route summarization , maka perintah yang harus kita masukkan pada Router4 adalah sebagai berikut :

Sedangkan tabel routing yang akan dihasilkan dari tabel routing diatas sebagai berikut :

Namun jika menerapkan route summarization, maka entry yang akan perlu dimasukkan ke Router4 hanyalah sebuah entry 192.168.0.0/21 dengan gateway 10.10.10.2 seperti berikut :

Sedangkan tabel routing yang dihasilkan dengan menerapkan route summarization adalah sebagai berikut :

Kita lihat dari tabel routing diatas, Router4 sanggup menjangkau network lainya, hal ini dikarenakan entry 192.168.0.0/21 mewakili keberadaan enam jaringan tersebut. Cara untuk melakukan summarization ialah sebagai berikut :

Kita akan meringkas enam Network Address menjadi satu Network Address. Network Address hasil summarization tersebut harus mewakili enam jaringan tersebut. Perhitungan untuk melakukan Route Summarization diuraikan sebagai berikut :

Net I 192.168.0.0 = 11000000.10101000.00000000.00000000

Net II 192.168.1.0 = 11000000.10101000.00000001.00000000

Net III 192.168.2.0 = 11000000.10101000.00000010.00000000

Net IV 192.168.3.0 = 11000000.10101000.00000011.00000000

Net V 192.168.4.0 = 11000000.10101000.00000101.00000000

Hasil Summarization = 192.168.0.0/21

Untuk mencari hasil summarization, kita tuliskan kembali Network Address masing-masing sub network ke dalam notasi biner, kemudian kita harus mencari sampai bit keberapa susunan Network Address tersebut memiliki persamaan. Uraian diatas memperlihatkan bahwa sampai pada bit ke-21 bilangan biner dari keenam Network Address tersebut masih sama. Jumlah bit-bit yang sama Network Address yang sama inilah yang akan menjadi prefix baru hasil route summarization adalah /21.

Fail Over

Fail Over adalah teknik yang menerapkan beberapa jalur untuk mencapai suatu network tujuan. Namun dalam keadaan normal hanya ada satu link yang digunakan. Link yang lain hanya berfungsi sebagai cadangan (redudant) dan hanya akan digunakan bila link utama terputus.

Pada gambar 2.4, kita dapat menentukan mana link yang akan digunakan sebagai link utama dan mana link yang akan digunakan sebagai cadangan. Sebagai contoh implementasi, network 10.10.10.0/24 akan menjadi link utama sedangkan network 172.16.10.0/24 akan menjadi link cadangan.

Gambar 2.4 Fail Over Dengan Jalur Utama Pada Network 10.10.10.0/24

Konfigurasi static routing yang perlu kita lakukan pada R1 adalah sebagai berikut:

Pada konfigurasi static diatas, dapat kita lihat bahwa ada dua entry yang dimaksukkan untuk menuju network 192.168.20.0/24. Satu entry menggunakan gateway 10.10.10.2 dan satu entry dengan menggunakan gateway 172.16.10.2. Namun untuk entry yang kedua ditambahkan nilai distance 250 (Administrative Distance).

Nilai Administrative Distance (AD) merupakan nilai kepercayaan dari sebuah entry route. Semakin kecil nilai AD maka semakin tinggi nilai kepercayaan terhadap entry tersebut. Jika kita kembali pada baris konfigurasi routing statik pada R0, pada baris pertama tidak ditambahkan nilai distance, yang artinya entry tersebut akan menggunakan nilai default AD dari routing statik yaitu 1. Sedangkan baris kedua ditambahkan nilai distance sebesar 250 yang menandakan entry tersebut memiliki nilai AD sebesar 250. Pemilihan nilai 250 sebagai AD dalam implementasi ini hanyalah sebagai pemisalan. Kita dapat memilih nilai AD yang lain namun kita harus memperhatikan nilai-nilai AD dari protokol routing yang lain. Dibawah ini adalah daftar administrative distance untuk tiap routing.

Tabel 2.1 Administrative Distance Untuk Tiap Routing

Tipe Routing Administrative Distance (AD)

Connected 0

Static 1

Enhanced Interior Gateway Routing Protocol (EIGRP) summary route 5

Exterior Border Gateway Protocol (eBGP) 20

EIGRP (internal) 90

Open Shortest Path First Protocol (OSPF) 110

Intermediate System-to-Intermediate System Protocol (IS-IS) 115

RIP 120

Exterior Gateway Protocol 140

On-Demand Routing 160

EIGRP (external) 170

Internal Border Gateway Protocol (iBGP) (external) 200

Unknown 255

Tabel routing R0 dapat kita lihat seperti berikut :

Jika melihat tabel routing dari R0, kita dapat melihat sebuah entry untuk menuju network 192.168.20.0/24 yang menggunakan Gateway 10.10.10.2, sedangkan kita tadi juga memasukkan entry untuk menuju network 192.168.20.0/24 yang menggunakan Gateway 172.16.10.2, akan tetapi tidak ada didalam tabel routingnya, sementara di menu konfigurasi R0 dapat kita lihat seperti ini :

Hal ini menandakan entry route dengan gateway 10.10.10.2 merupakan entry yang aktif yang dapat digunakan untuk mengirimkan data (link utama). Sedangkan entry route dengan gateway 172.16.10.2 merupakan entry yang tidak digunakan atau cadangan (link cadangan).

Ssedangkan konfigurasi routing statik untuk R2 beserta tabel routingnya dapat kita lihat sebagai berikut :

Sehingga tabel routingnya sebagai berikut :

Pada tabel routing R1, terdapat dua entry untuk menuju network 192.168.10.0/24. Entry dengan Gateway 10.10.10.1 sedangkan dengan Gateway 172.16.10.0 merupakan entry yang tidak aktif atau cadangan.

Dynamic Routing

Definisi Dynamic Routing

Routing dinamik (dynamic routing) merupakan teknik routing dimana router akan memasukkan sendiri entry route kedalam tabel routingnya untuk melakukan itu, router akan saling bertukar informasi routing dengan router yang lain tentang jaringan yang mereka ketahui masing-masing setelah mempelajari keberadaan jaringan lain beserta cara mencapai jaringan tersebut, route akan membuat entry route dan pada akhirnya memasukkannya ke dalam tabel routing.

Untuk bisa melakukan pertukaran informasi routing, router-router tersebut harus menggunakan protokol routing jika dua buah router ingin bertukar informasi routing, maka keduanya harus menggunakan protokol routing yang sama. Berikut protokol routing yang paling banyak digunakan:

Routing Information Protocol (RIP)

Interior Gateway Routing Protocol (IGRP)

Enchanced Interior Gateway Routing Protocol (EIGRP)

Open Shortest Path First (OSPF)

Intermediate System-to-Intermediate System (IS-IS)

Border Gateway Protocol (BGP)

Pada jaringan yang menerapkan routing dinamic jika terjadi perubahan pengalamatan maupun topologi maka router-router akan mengirimkan informasi perubahan tersebut kerouter lain. Router-router tersebut akan bertukar informasi tentang perubahan yang terjadi dari pertukaran informasi routing tersebut akan menghasilkan perubahan entry route pada tabel routing secara otomatis pula.

Pada saat terjadi perubahan dalam jaringan, router tidak serta merta langsung mengganti entry pada tabel routingnya. Dibutuhkan selang waktu tertentu sehingga entry pada tabel routing bisa berubah. Waktu yang diperlukan dari saat terjadi perubahan aringan sampai terjadinya perubahan entry route pada tabel routing disebut waktu convergence. Semakin pendek waktu convergence maka semakin baik untuk kestabilan sebuah jaringan, karena pada saat belum convergence tentu ada entry-entry route yang tidak valid lagi, sehingga pengiriman paket dari satu host ke host lain yang berbeda jaringan akan gagal.

Secara lengkap penggunaan protokol berdasarkan jenis pengalamatan jaringan dapat dilihat pada tabel berikut :

Tabel 2.2 Versi Routing Protocol

Pengalamatan Protokol Routing

IPv4 RIPv1, RIPv2, IGRP, EIGRP, OSPFv2, IS-IS, BGPv4

IPv6 RIPng, EIGRP for IPv6, OSPFv3, IS—IS for IPv6, BGPv4 for IPv6

IGRP dan EIGRP merupakan protokol routing proprietary dari Cisco System, sehingga kedua protokol routing ini hanya ada pada router Cisco.

Classful dan Classless

Dalam mengirimkan update routing, beberapa protokol routing hanya mengirimkan informasi network address tanpa menyertakan subnetmask atau prefix dari jaringan yang dikelolanya. Beberapa lainnya menertakan subnetmask atau prefix pada saat akan mengirimkan informasi network address. Protokol routing yang tidak menyertakan subnetmask (prefix) disebut protocol routing classful (classful routing protocol). Sedangkan protocol routing yang menyertakan subnetmask (prefix) pada saat mengirimkan informasi routing disebut classless (classless routing protocol).

Yang termasuk protokol routing classful adalah RIPv1 dan IGRP, sedangkan yang merupakan protokol routing classless adalah RIPv2, EIGRP, OSPF, IS-IS serta BGP.

Metric

Sesuai dengan fungsinya router akan memilih jalur terbaik, namun apakah yang akan digunakan sebuah router untuk menentukan jalur terbaik tersebut ?

Untuk menentukan jalur terbaik maka router menggunakan metric atau sering disebut routing metric. Metric itu sendiri terdiri dari beberapa jenis dan metric antara protokol routing yang satu dengan lainnya tidaklah selalu sama. Sehingga sebuah jalur bisa saja menjadi jalur terbaik untuk suatu protokol routing namun tidak menjadi jalur terbaik bagi protokol routing yang lain.

Adapun berbagai jenis matric yang digunakan oleh protocol routing adalah sebagai berikut :

Hop Count’

Protokol routing yang menggunakan hop count akan menghitung jumlah lompatan (hop) untuk mencapai remote network. Jumlah lompatan terkecil merupakan nilai yang terbaik.

Cost

Metric ini akan memberikan harga (cost) pada setiap link yang ada dalam jaringan. Path yang memiliki cost dengan nilai terkecil yang akan menjadi best path (jalur terbaik).

Bandwidth

Penggunaan bandwidth sebagai matric hampir sama dengan penggunaan cost. Protokol routing akan menghitung bandwidth pada setiap path dan akan menjadikan path dengan bandwidth terbesar sebgai best path.

Load

Jika load yang dijadikan metric, maka protokol routing akan menghitung beban dari setiap path dan akan menjadikan beban terkecil sebagai best path.

Delay

Delay adalah waktu yang diperlukan untuk mengirimkan paket data dari setiap path, tentunya delay terkecil yang akan menjadi best path.

Reliability

Reliability adalah nilai kehandalan dari sebuah path, misalnya sering tidak terjadinya error atau kegagalan dalam link tersebut. Nilai reliability tertinggi yang akan menjadi best path.

Metric antara satu protokol routing dengan protokol routing yang lainnya tidaklah sama. Berikut metric yang digunakan oleh masing-masing protocol routing.

Tabel 2.3 Routing Metric

Protokol Routing Metric

RIP Hop count

IGRP dan EIGRP Menggunakan gabungan bandwidth, load, delay, reliability

OSPF dan IS-IS Cost (berdasarkan bandwidth)

Perhatikan jaringan pada gambar 2.5. pada gambar tersebut R0 memiliki dua buah path untuk menuju network 172.16.2.0/24. Path pertama melalui R1 baru kemudian ke R2 (hop count = 3), sedangkan path kedua adalah melalui R3 kemudian R4 dan selanjutnya baru ke R2 (hop count = 4). Jika protocol routing yang digunakan pada jaringan tersebut adalah RIP (menggunakan hop count sebagai matric) maka yang merupakan best path adalah path yang memiliki nilai hopt count-nya yang terkecil, yaitu melalui R1.

Gambar 2.5 Hop count dan Bandwidth sebagai metric

Kondisi tersebut akan berbeda jika yang digunakan adalah protokol routing yang menggunakan bandwidth sebagai metric, misalnya OSPF, jika yang digunakan adalah OSPF (menggunakan cost berdasarkan bandwith sebagai metric), maka yang akan menjadi best path adalah path melalui R3 karena memiliki bandwidth yang lebih besar, meskipun path ini memiliki nilai lompatan (hop) yang lebih besar.

Apabila yang terjadi jika terdapat dua atau beberapa path yang ternyata memiliki nilai metric yang sama, maka router akan menggunakan keseluruhan path tersebut untuk menuju remote network. Kondisi ini disebut equal cost load blancing atau load blancing. Semua protokol routing mendukung fitur load blancing dan akan memasukkan keseluruhan best path tersebut ke dalam tabel routing, contohnya seperti gambar 2.6 sebagai berikut.

Gambar 2.6 R1 memiliki dua best path

Kelebihan dan kekurangan routing dinamic

Kelebihan

Waktu konfigurasi lebih cepat

Untuk mengkonfgurasikan protokol routing pada router relatif tidak membutuhkan waktu yang lama. Kita cukup mengkonfigurasikan ip address pada setiap interface kemudian mengaktifkan protokol routing dan kemudian mengenalkan jaringan yang terhubung langsung dengan router tersebut

Dapat langsung beradaptasi pada perubahan jaringan

Karena menggunakan protokol routing yang secara dinamic memeriksa kondisi jaringan, maka perubahan jaringan akan dapat diketahui dengan cepat oleh router-router. setelah mengetahui perubahan tersebut, router-router akan kembali memperbaiki tabel routingnya

Kemungkinan kesalahan konfigurasi kecil

Karena konfigurasi yang dilakukan tidak dengan menentukan secara manual setiap entry route, maka kemungkinan kesalahan penentuan jalur jauh lebih kecil,. Kesalahan entry route hanya akan diakibatkan oleh kesalahan router dalam membaca informasi routing dari router lain.

Mendukung untuk jaringan besar

Protokol routing dapat dengan cepat beradaptasi terhadap perubahan jaringan, sehingga untuk jaringan yang berskala besar akan sangat efisien.

Kekurangan

Membutuhkan resource yang besar

Protokol routing akan menjalankan algoritma routing, membuat database jaringan sampai dengan urusan kirim mengirim pesan informasi routing (update routing). Kesemuanya itu membutuhkan CPU dan memori yang lebih besar dibandingkan jika hanya menjelankan routing static.

Membutuhkan kemampuan yang lebih dari administrator

Beberapa protokol routing memang tidak terlalu rumit untuk dikonfigurasikan. Namu ada juga protokol routing tertentu yang penerapannya membutuhkan administrator dengan pengetahuan yang lebih tentang konteks, konfigurasi, pengujian dan troubelshoot routing.

Relatif kurang aman

Dikatakan kurang aman, karena router akan menentukan sendiri entry route yang akan digunakan. Ini bisa mengakibatkan salah penentuan jalur oleh router-router yang akan mengakibatkan terjadinya routing loop. Selain itu pertukaran informasi routing dapat dikacaukan oleh pihak-pihak yang tidak bertanggung jawab ini akan mengakibatkan terjadinya entry route palsu dalam jaringan.

Protokol Dynamic Routing

IGP dan EGP

Pada jaringan berskala besar, dikenal penggunaan Autonomous System (AS) atau domain routing. Autonomous System merupakan kumpulan router yang berada dibawah satu kendali administrator dan menggunakan strategi routing yang sama. Berdasarkan penggunaan dalam Autonomous System, protokol routing dapat dibagai menjadi dua, yaitu :

Interior Gateway Protocol (IGP)

Interior Gateway Protokol adalah protocol routing yang digunakan pada router-router yang berada dalam satu Autonomous System. Atau dengan kata lain IGP digunakan untuk menghubungkan jaringan-jaringan dalam sebuah Autonomous System. Sebagai contoh bila kita ingin menerapkan routing pada sebuah jaringan internal kampus atau internal sebuah perusahaan, maka kita harus menggunakan protokol routing kategor IGP. Protokol routing yang termasuk IGP adalah RIP, IGRP, EIGRP, OSPF dan IS-IS.

Exterior Gateway Protocol (EGP)

Exterior Gateway Protocol adalah Protokol routing yang digunakan pada router-router yang berasal dari Autonomous System yang berbeda. Atau dapat dikatakan EGP digunakan untuk menghubungkan jaringan-jaringan yang berasal dari Autonomous System yang berbeda. Contoh penggunaan EGP dapat dilihat jika ingin dilakukan routing antar kampus atau antar ISP. Satu-satunya protokol routing yang digunakan untuk keperluan ini adalah BGP.

Contoh implementasi IGP dan EGP dapat kita lihat pada gambar 2.7. Pada gambar tersebut terdapat dua buah jaringan yang berbeda Autonomous System (AS). Jaringan yang pertama dengan AS Nnumber 200 memiliki 3 buah router yang menjalankan protokol routing OSPF.

Begitu juga dengan jaringan dengan AS Number 300 yang memiliki 3 buah router yang menjalankan protocol routing EIGRP. Kedua jaringan berada dibawah kendali Administrator yang berbeda, sehingga Administrator dari AS Number 200 tidak mengetahui strategi routing, topologi, pengalamatan maupun konfigurasi jaringan pada network dengan AS Number 300. Administrator dari AS Number 200 tidak memiliki otoritas atau kekuasaan untuk mengkonfigurasi router-router yang ada pada jaringan AS Number 300, begitu juga sebaliknya.

Gambar 2.7 Penggunaan IGP dan EGP

Untuk membangun kedua jaringan ini, maka kedua Administrator menghubungkan kedua router terluar mereka. Kemudian mengkonfigurasikan protocol routing BGP pada kedua router tersebut. OSPF dan EIGRP pada kedua router digunakan untuk melakukan routing pada jaringan internal masing-masing Autonomous System (AS), sedangkan BGP digunakan untuk melakukan routing antara jaringan dengan AS Number 200 dan jaringan dengan AS Number 300.

Routing Information Protocol Versi 1 (RIPv1)

RIPv1 merupakan protokol routing yang sangat sederhana dan memiliki banyak kekurangan. Namun salah satu kelebihan RIPv1 adalah kemudahan saat akan diimplementasikan (dikonfigurasi). Sehingga untuk jaringan yang berskala kecil, RIPv1 ini masih memungkin untuk digunakan. RIPv1 juga terus dikembangkan dengan disempurnakan menjadi RIPv2 dan RIPng (RIP next Generation). RIPng merupakan protocol routing untuk jaringan yang menggunakan pengalamatan IPv6. Dengan adanya RIPng menandakan bahwa protocol routing ini masih akan tetap digunakan dimasa mendatang.

RIP merupakan protocol routing yang paling tua dan merupakan pengembangan dari protocol routing sebelumnya ada yaitu Gateway Information Protocol (GWINFO).

Pada tahun 1988, Charles Hadrik menuliskan kembali spesifikasi RIP dalam RFC 1058 sebagai standarisasi yang akan digunakan secara menyeluruh. RIP yang tertuang dalam RFC 1058 inilah yang dikenal sebagai RIPv1. Sedangkan pada tahun 1994 RIP ditulis kembali dalam RFC 1723 sebagai RIPv2. Dan pada tahun 1997, RFC 2080 memuat standarisai tentang RIPng.

Karakteristik RIPv1

Merupakan protocol routing distance vector

Menggunakan jumlah lompatan network (hop count) sebagai metric routing.

Network tujuan dengan hop count 16 dianggap invalid (tidak dapat dituju).

Proses pengiriman informasi routing (routing update) ke router tetangga (neighbor) terjadi setiap detik dan dilakukan secara broadcast.

Pengiriman routing update menggunakan protocol UDP dengan source port dan destination port 520.

Merupakan classful routing protocol

Menggunakan split horizon, route poisoning dan holdown timer untuk mencegah routing loop.

Secara default nilai administrative distance adalah 120.

RIPv1 bekerja dengan menggunakan algoritma Bellman Ford dan merupakan protocol routing distance vector, yang artinya RIPv1 hanya bekerja berdasarkan arah dan jarak. RIP v1 hanya mengetahui kemana arah (vector) dan jarak (distance) untuk mencapai suatu remote network. RIP tidak memiliki pengetahuan yang lengkap tentang topologi jaringan. Padahal topologi tersebut sangat berguna sebagai pedoman untuk mencapai remote network. Inilah yang merupakan salah sat kekurangan dari RIPv1.

Karena tidak memiliki pengetahuan yang baik tentang gambaran topologi jaringan, maka penggunaan RIPv1 dapat mengakibatkan terjadinya routing loop. Ini dangat berbeda dengan OSPF yang memiliki gambaran topologi jaringan, sehingga dapat mengetahui dengan baik jalur (path) yang dapat digunakan untuk mencapai network tujuan.

Hop Count Sebagai Matric

RIP menggunakan hop count (jumlah jaringan yang dilewati) sebagai nilai matric, dengan metric terendah sebagai metric terbaik. Bila untuk mencapai network tujuan terdapat beberapa jalur (path) dengan nilai hop count yang berbeda-beda, maka hop count yang terendah yanga akan dipih oleh RIP untuk dimasukkan kedalam table routing.

RIP Request dan RIP Response

RIPv1 menggunakan dua jenis informasi routing (pesan) untuk menjaga dan memelihara table routing, dengan tujuan dapat selalu mengetahui perubahan-perubahan yang terjadi dalam jaringan. Dua jenis pesan (message) itu adalah RIP request message dan RIP response message.

RIP response message sebenarnya adalah informasi routing yang dikirmkan sebuah router ke router tetangganya. RIP response message ini berisi network-network yang diketahui oleh sebuah router, lengkap dengan metric untuk setiap network. RIP response message.

Sedangkan RIP request message adalah pesan (message) yang dikirm sebuah router ke router tetangganya untuk meminta informasi routing. Singkatnya, RIP request message dikirim untuk meminta rip response message dari router tetangga. Hubungan antara RIP request message dan RIP response message dapat dilihat pada gambar berikut

Gambar 2.8 RIP Request Message dan Response Message

Jika R1 mengirim RIP request message ke R2, maka dengan tidak menunggu interval waktu 30 detik, R2 akan segera mengirimkan RIP response message ke R1. Padahal kita ketahui sebelumnya bahwa pengiriman routing update atau RIP response message adalah setiap 30 detik. Routing uodate tersebut akan diterima oleh R1, dan R1 segera memeriksa table routingnya. Jika dalam routing update terdapat informasi network yang lebih baru maka R1 akan memasukkan network tersebut kedalam table routingnya. Namun, jika ternyata informasi network dalam routing update tersebut sudah ada dalam table routing, R1 akan memeriksa apakah metric dalam update tersebut lebih baik dari metric yang ada dalam table routing.

Jika ternyata metric yang ada pada update tersebut lebih baik, maka informasi network yang telah ada sebelumnya dalam table routing akan digantikan dengan informasi yang lebih baru yang ada dalam routing update.

RIP request message akan dikeluarkan sebuah router pada saat router itu hidup (boot) dan saat kita mengaktifkan RIP pada router.

RIPv1 Dalam Discontiguous Network

Proses pemberian subnet mask atau prefix pada informasi network address yang diterima dari router lain akan berbeda tergantung pada jenis jaringan. Apakah jaringan tersebut merupakan contiguous network atau discontiguous network.

Contiguous network adalah jaringan yang terdiri dari beberapa network dan menggunakan pengalamatan yang hierarki. Sedangkan discontiguous network (fragment network) adalah jaringan yang terdiri dari beberapa network yang tidak penggunakan pengalamatan yang hierarki. Contoh discontiguous adalah jaringan yang tediri dari beberapa network dimana ada dua atau lebih network dipisahkan oleh sebuah network yang berbeda mayor address-nya. Mayor network address sendiri mengacu pada pengalamatan classfull.

Router yang menjalankan RIPv1 akan melakukan dua metode untuk menambahkan subnet mask pada informasi network address yang diterimanya dari router tetangga, yaitu:

Jika mayor network address yang ada pada informasi routing diterima pada interface yang major network address-nya berbeda, maka subnet mask yang digunakan bagi network address tersebut adalah default subnet mask sesuai pembagian kelas IP Address. Inilah yang terjadi oada discontiguous network

Jika major network yang ada pada informasi routing, diterima pada pada interface yang major networknya smaa, maka subnet mask yang digunakan bagi network address tersebut adalah subnet mask pada interface yang menerima routing update tersebut.

Konfigurasi RIPv1

Tahap-tahap konfigurasi RIPv1 pada berbagai jenis/merk router umumnya sama. Tahapan dapat diuraikan sebagai berikut:

Mengaktifkan RIPv1 pada router

Tahapan ini bertujuan agar interface dari router dapat menerima dan mengirimkan informasi routing (routing update) kepada orang lain.

Meng-advertise Network

Pada tahap ini, kita diminta untuk memasukkan network. Network yang akan diperkenal kan (di advertise) kepada router lain melalui protocol RIPv1. Network address dari network yang telah di advertise akan diserahkan pada routing update.

Routing Informasi Protocol Versi 2 (RIPv2)

RIPv2 merupakan penyempurnaan dari RIPv1 sehingga dalam beberapa karakteristik kedua protocol routing ini adalah sama. RIPv2 dikembangkan untuk menutupi kelemahan-kelemahan RIPv1 terutama dalam penerapan pada jaringan yang menggunakan pengalamatan classless atau jaringan yang menggunakan pengalamatan Variable Length Subnet Mask (VLSM).

Karakteristik RIPv2

Jika diperbandingkan dengan RIPv1, maka RIPv2 memiliki persamaan dalam beberapa hal, yaitu:

Keduanya merupakan protocol routing distance vector yang menggunakan algoritma Bellman Ford

Keduanya menggunakan hop count sebagai metric-nya.

Keduanya menganggap network dengan hop count 16 adalah network invalid (atau network yang tidak dapat dituju)

Secara default keduanya akan melakukan pengiriman informasi routing (routing update) setiap 30 detik.

Keduanya akan mengirim routing update dengan mengunakan protocol UDP dengan port pengiriman dan penerima adalah 520.

Keduanya akan mengirimkan keseluruhan isi table routingnya kepada router tetangga (neighbor) pada saat melakukan pengiriman routing update.

Keduanya menggunakan split horizon, route poisoning, dan holdown timer untuk mencegah routing loop.

Sedangkan perbedaan dari kedua protocol routing ini adalah sebagai berikut:

Jika proses pengiriman informasi routing (routing update) RIPv1 dikirim secara broadcast, maka RIPv2 akan mengirimkannya secara multicast

Jika routing update RIPv1 tidak menyertakan prefix, maka RIPv2 akan menyertakan subnet mask atau prefix dari jaringan yang akan di advertise.

Jika RIPv1 merupakan protocol routing classful, maka RIPv2 merupakan protocol routing classless.

Jika RIPv1 tidak memiliki fitur authentication dalam proses pengiriman routing update, maka RIPv2 memiliki fitur authentication.

Single Ares OSPF

OSPF (Open Shortest Path First) merupakan protocol routing link state dan digunakan untuk menghubungkan router-router berada dalam satu Autonomous System (AS), sehingga protocol routing ini termasuk juga Kategori Interior Gateway Protocol (IGP). OSPF dikembangkan untuk menutupi kekurangan-kekurangan yang dimiliki oleh RIP, terutama pengimplementasian dijaringan berskala besar.

Untuk dapat menangani jaringan berskala besar, maka OSPF menerapkan konsep area dalam implementasinya. Sehingga pengimplementasian OSPF dikenal dengan dua cara yaitu Singel Ares OSPF dan Multi Area OSPF. Untuk jaringan yang berskala kecil kita dapat menerapkan Singel Area OSPF(OSPF Singel Area), namun untuk jaringan berskala besar maka harus diterapkan Multi Area OSPF.

Karakteristik OSPF

Merupakan link state routing protocol, sehingga setiap router memiliki gambaran topologi jaringan.

Menggunakan Hello Packet untuk mengetahui keberadaan neighbor router.

Routing update hanya dikirim bila terjadi perubahan dalam jaringan dan dikirim secara multicast.

Menggunakan cost sebagai metric, dengan cost terendah yang akan menjadi metric terbaik.

Tidak memiliki keterbatasan hop count, tidak seperti RIP yang hanya bias menjangkau 15 hop count.

Merupakan classless routing protocol.

Secara default nilai Administrative Distance 110.

Memiliki fitur authentication (seperti RIPv2) pada saat pengiriman routing update.

Router yang menjalankan OSPF hanya akan bertukar informasi routing dengan router OSPF lainnya yang berada dalam satu Autonomous System (AS). Namun sebelum melakukan pertukaran informasi routing tersebut, router-roter tersebut akan melakukan beberapa tahapan. Informasi routing yang dipertukarkan tidak sesederhana pad RIP yang hanya saling bertukar table routing melalui routing update. Router OSPF akan mengirimkan beberapa paker OSPF lainnya yang kesemuanya diguankan untuk membentuk table routing. Pada OSPF dikenal dengan kondisi adjacency antar router. Sebelum router-router tersebut bertukar informasi routing maka sebuah router harus terlebih dahulu mencapai kondisi adjacency dengan router tetangganya. Roter-router tidak akan bertukar routing update jika kondisi adjacency belum tercapai.

OSPF Packet

OSPF merupakan protocol routing yang sedikit lebih rumit. OSPF akan menggunakan 5 jenis paket data OSPF yang kesemuanya digunakan dalam tahapan pertukaran informasi routing (routing update).

Kelima jenis paket ini akan digunakan baik pada saat router-router akan mencapai kondisi adjacency maupun pada saat router-router tersebut akan saling mengirimkan Link State Advertisement (LSA). Kelima paket OSPF tersebut adalah sebagai berikut:

Hello Packet

Database Description (DBD) Packet

Link State Request (LSR) Packet

Link State Update (LSU) Packet

Link Stae Ack (LSAck) Packet

Hello Packet

Hello packet merupakan packet OSPF yang sangat penting, karena packet OSPF inilah yang akan menentukan apakah router-router yang bertetangga dapat mencapai kondisi adjacency atau tidak. Jika kondisi adjacency tidak tercapai maka tidak akan terjai pengiriman LSA antar router tersebut dan dengan tidak terkirimnya LSA maka pertukaran informasi routing juga tidak akan terjadi. Dan jika tidak terjadi pertukaran informasi routing maka jaringan tidak mencapai kondiri convergence. Network-network tidak akan saling terhubung satu sama lainnya.

Hello packet adalah paket yang hanya dikirim oleh router tetangga melalui interface router yang telah diaktifkan OSPF nya.

DataBase Description (DBD) Packet

DBD paket digunakan untuk kepentingan sinkronisai Link State Database. DBD packet berisi ringkasan Link State Database dan akan dikirim ke router lain. Router yang menerima DBD paket tersebut akan membandingkan dengan Link State Database yang dimilikinya untuk kemudian disinkronisasi.

Link State Request (LSR) Packet

LSR digunakan sebuah router untuk meminta informasi yang ada dalam Link State Database milik router-router lainnya. Informasi ini bias saja informasi spesifik maupun informasi tambahan yang dimiliki oleh router lain.

Link State Update (LSU) Packet

LSU Packet merupakan paket yang berisi informasi routing dari setiap router. Informasi routing ini berasal dari Link State Database. LSU packet merupakan jawaban dari LSR packet.

LSAck Packet

LSA Ackknowledgment atau LSack merupakan paket yang berguna untuk memberitahu kepada router pengirim LSU bahwa LSU packet telah diterima.

OSPF Area

OSPF diterapkan dengan konsep area yang merupakan pengelompokkan beberapa router secara logika, bukan secara fisik. Ini berarti kita sendiri yang akan menentukan area-area tersebut beserta router-router untuk setiap area.

Area ini dimaksudkan untuk mengurangi besarnya flooding LSA pada saat terjadi perubahan jaringan. Jika jaringan yang menerapkan OSPF telah dikelompokkanmenjadi beberapa are, maka LSA hanya akan disebarkan (flooding) kepada router-router yang berada dalam satu area, LSA tidak akan di flood kerouter yang berbeda area. Juga dapat diterapkan route summarization antar area sehingga kita dapat mengurangi ukuran table routing.

Router-router OSPF yang berada dalam satu area akan menggunakan database yang sama dan selalu berusaha untuk mensinkronisasikan database tersebut.

Untuk mengidentifikasi area, maka setipa area memiliki pengenal yang disebut Area-ID. Area-ID ditulis menggunakan 32 bit bilangan biner dan ditulis dalam bentuk decimal seperti IP Adress (x.x.x.x). walaupun mirip dengan Ip Address akan tetapi perlu diingat area-Id bukan IP Address.

Dalam penerapan OSPF, area dpaat dibagi menjadi dua, yaitu:

Backbone Area, area ini memiliki Area-ID 0.0.0.0 dan merupakan area yang diharapkan dapat melakukan forward paket data (IP Packet) secepat-cepatnya. Area ini wajib ada jika ternyata hanya aka nada satu area (singe area) dalam suatu jaringan. Jika ternyata dalam jaringan tersebut dibuat beberapa area, maka backbone wajib ada karena berfungsi menghubungkan area-area yang lain. End user atau host tidak boleh ditempatkan pada Backbone Area.

Reguler Area, area ini adlaah area selain backbone (non backbone area) dan berfungsi menghubungkan end user. Jika dalam satu jaringan ada dua regular area, maka kedua area tersebut harus melewati backbone area untuk berkomunikasi.

Konfigurasi OSPF

Untuk konfigurasi OSPF setidaknya ada 2 hal yang perlu dilakukan yaitu:

Mengaktifkan interface router yang akan mengirimkan paket-paket OSPF

Mengkonfigurasikan network yang akan di advertise menggunakan routing protocol OSPF sekaligus menentukan network tersebut berada diarea mana.

BGP (Borde Gateway Protokol)

BGP merupakan salah satu jenis routing protokol yang digunakan untuk koneksi antar Autonomous System (AS), dan salah satu jenis routing protokol yang banyak digunakan di ISP besar (Telkomsel) ataupun perbankan. BGP termasuk dalam kategori routing protokol jenis Exterior Gateway Protokol (EGP).

Dengan adanya EGP, router dapat melakukan pertukaran rute dari dan ke luar jaringan lokal Auotonomous System (AS). BGP mempunyai skalabilitas yang tinggi karena dapat melayani pertukaran routing pada beberapa organisasi besar. Oleh karena itu BGP dikenal dengan routing protokol yang sangat rumit dan kompleks.

Border Gateway Protocol disingkat BGP adalah inti dari protokol routing Internet. Protocol ini yang menjadi backbone dari jaringan Internet dunia. BGP adalah protokol routing inti dari Internet yg digunakan untuk melakukan pertukaran informasi routing antar jaringan. BGP dijelaskan dalam RFC 4271. RFC 4276 menjelaskan implementasi report pada BGP-4, RFC 4277 menjelaskan hasil ujicoba penggunaan BGP-4. Ia bekerja dengan cara memetakan sebuah tabel IP network yang menunjuk ke jaringan yg dapat dicapai antar Autonomous System (AS). Hal ini digambarkan sebagai sebuah protokol path vector. BGP tidak menggunakan metrik IGP (Interior Gateway Protocol) tradisional, tapi membuat routing decision berdasarkan path, network policies, dan atau ruleset. BGP versi 4 masih digunakan hingga saat ini . BGP mendukung Class Inter-Domain Routing dan menggunakan route aggregation untuk mengurangi ukuran tabel routing. sejak tahun 1994, BGP-4 telah digunakan di Internet. semua versi dibawahnya sudah tidak digunakan. BGP diciptakan untuk menggantikan protokol routing EGP yang mengijinkan routing secara tersebar sehingga tidak harus mengacu pada satu jaringan backbone saja

Gambar 2.9 Penggunaan IGP dan EGP

Karakteristik BGP

Digunakan antara ISP dengan ISP dan client-client.

Digunakan untuk merutekan trafik internet antar autonomous system.

BGP adalah Path Vector routing protocol. Dalam proses menentukan rute-rute terbaiknya selalu mengacu kepada path yang terbaik dan terpilih yang didapatnya dari router BGP yang lainnya.

Router BGP membangun dan menjaga koneksi antar-peer menggunakan port nomor 179.

Koneksi antar-peer dijaga dengan menggunakan sinyal keep alive secara periodik.

Metrik (atribut) untuk menentukan rute terbaik sangat kompleks dan dapat dimodifikasi dengan fleksibel.

BGP memiliki routing table sendiri yang biasanya memuat prefiks-prefiks routing yang diterimanya dari router BGP lain.

Mengapa BGP?

BGP memiliki kemampuan untuk mengontrol dan mengatur trafik-trafik dari sumber berbeda di dalam network multi-home (tersambung ke lebih dari 1 ISP/Internet Service Provider). Tujuan utama BGP adalah untuk memperkenalkan kepada publik di luar network (upsteram provider atau peer) tentang rute atau porsi spasi address yang dimiliki dengan “meminta izin” membawa data ke suatu spasi address tujuan (meng-advertise).

Salah satu kelemahan yang mungkin dihadapi oleh BGP routing adalah ia mempublikasikan rute yang tidak diketahui bagaimana cara mencapainya. Ini dinamakan black-holing, yaitu melakukan advertise, atau meminta izin untuk membawa data, tetapi beberapa bagian spasi address adalah milik orang lain, akibatnya proses advertise malah menyulitkan.

Hubungan BGP Neighbor

Arisitektur Internet sebenarnya tersusun atas AS-AS yang saling terkoneksi. Router yang berkomunikasi langsung melalui BGP dikenal sebagai BGP speaker. Beberapa BGP speaker dapat ditempatkan pada AS yang sama atau AS yang berbeda. Dalam masing-masing AS ini, BGP speaker berkomunikasi satu sama lain untuk melakukan pertukaran informasi reachabilitas network berdasarkan set-set policy yang dibangun dalam AS-AS.

Beberapa versi BGP

BGP versi 1

Ukuran message 8 – 1024 byte.

Terdapat 8 bit field Direction yang menandkan arah yang diambil oleh informasi routing.

Lima kemungkinan field Direction: Up, Down, Horizontal, EGP-derived information, Incomplete

BGP versi 2

Ukuran message 19 – 4096 byte.

Menghilangkan konsep up, down, dan horizontal di antara AS-AS

Menambahkan konsep path-attribute.

BGP versi 3

Ukuran message 19 – 4096 byte

Mengklarifikasi prosedur pendistribusian rute-rute BGP di antara speaker-speaker dalam sebuah AS.

Meningkatkan restriksi terhadap penggunaan path attribute Next-hop

BGP versi 4

Ukuran message 19 – 4096 byte.

Path atribute AS telah dimodifikasi sehingga set AS-AS dapat digambarkan sebagaimana AS individual.

Inter-AS Metric path attribute telah didefinisikan ulang sebagai Multi-Exit Discriminator path attribute.

Local preference path attribute ditambahkan.

Aggregator path attribute ditambahkan.

Dukungan untuk CIDR (Classless Inter Domain Routing)

Ringkasan Operasi BGP

Saat sebuah router BGP baru dibangun, peer-peer BGP dengan sendirinya melakukan pertukaran tabel routing yang mereka miliki, setelah itu peer-peer mengirim notifikasi atau pemberitauan berkaitan dengan perubahan yang terjadi pada tabel routing. Update message memberi informasi peer BGP hanya untuk satu path. Bila perubahan yang timbul mempengaruhi banyak path, maka multiupdate, message perlu dikirim.

Setelah BGP menghimpun update-update routingnya dari beragam AS, protokol akan membuat keputusan untuk mengambil path spesifik untuk masing-masing rute tujuan. Biasanya hanya satu path yang dibutuhkan untuk mencapai satu tujuan. BGP menggunakan atribut path (path attribute) yang dilepas kepadanya melalui update message agar bisa menentukan satu path terbaik bagi setiap tujuan.

Ada dua bentuk sistem koneksi transport protocol yang penting dimengerti. Mereka saling bertukar pesan (message) untuk membuka dan mengkonfirmasi parameter-parameter koneksi. Alur data awal yang dihasilkan tidak lain berupa keseluruhan tabel routing BGP, yang selanjutnya beberapa update penambahan dikirim sebagai perubahan pada tabel routing. BGP dalam hal ini tidak menuntut refresh secara periodik atas keseluruhan tabel routing. Oleh karena itu, BGP speaker harus memelihara versi terkini keseluruhan tabel routing BGP dari semua peer-nya selama durasi koneksi tertentu.

Pesan KeepAlive dikirim secara periodik untuk memastikan kelancaran koneksi. Pesan Notification dikirim untuk merespon adanya error atau kondisi-kondisi khusus yang terjadi. Jika sebuah koneksi menemukan sebuah error, pesan Notification segera dikirim dan koneksi pun ditutup.

Perangkat Hardware & Software untuk Komunikasi BGP

Perlengkapan yang dibutuhkan adalah router komersial seperti Cisco router dan Bay router atau klon-klon PC yang menjalankan Linux, BSD, atau varian Unix lainnya dibantu dengan program yang dinamakan gated untuk memanage BGP.

eBGP vs iBGP

BGP mensupport dua tipe pertukaran informasi routing:

Pertukaran di antara AS-AS yang berbeda (external BGP atau eBGP)

Pertukaran dalam satu AS tunggal (internal BGP atau iBGP)

Sebuah sistem BGP berbagi informasi reachabilitas network dengan sistem-sitem BGP berdekatan lainnya yang dikenal dengan neighbor atau peer. Sistem BGP tersusun atas grup-grup (groups). Dalam sebuah grup BGP internal, semua peer anggota grup (internal peer) berada dalam AS yang sama. Grup internal menggunakan rute-rute dari IGP untuk memutuskan penyampaian atau forwarding address-adress. Mereka juga menyebarkan rute-rute eksternal di antara router-router internal lain yang menjalankan BGP internal, menghitung next hop dengan mengambil hop BGP yang diterima dengan rute, lalu memutuskannya menggunakan informasi yang diperoleh dari salah satu IGP.

eBGP dan iBGP saling berbagi protokol level dasar yang sama untuk bertukar rute dan juga berbagi algoritma. Namun eBGP digunakan untuk bertukar rute di antara AS yang berbeda, sedang iBGP digunakan untuk bertukar rute di antara AS yang sama. Dalam faktanya, iBGP termasuk salah satu “interior routing protocol” yang dapat digunakan untuk melakukan routing aktif dalam sebuah network.

Perbedaan utama eBGP dan iBGP adalah bahwa eBGP tidak bosan-bosannya mencoba meng-advertise setiap rute BGP yang diketahui ke semua orang sehingga mungkin harus digunakan filter untuk menghentikannya. Sedang iBGP pada dasarnya cukup sulit bekerja karena iBGP tidak meredistribusi rute-rute. Speaker iBGP dalam lingkungan network harus melakukan peer dengan semua speaker iBGP lain untuk membuatnya dapat bekerja (routing mesh).

# BAB III

## PENUTUP

### KESIMPULAN

Suatu static route adalah suatu mekanisme routing yang tergantung dengan routing table dengan konfigurasi manual. Disisi lain, dynamic routing adalah suatu mekanisme routing di mana pertukaran routing table antar router yang ada pada jaringan dilakukan secara dynamic.

Dalam skala jaringan yang kecil yang mungkin terdiri dari dua atau tiga router saja, pemakaian static route lebih umum dipakai. Static router (yang menggunakan solusi static route) haruslah dikonfigurasi secara manual dan di-maintain secara terpisah karena tidak melakukan pertukaran informasi routing table secara dinamis dengan router-router lainnya.

Suatu static route akan berfungsi sempurna jika routing table berisi suatu route untuk setiap jaringan didalam internetwork yang mana dikonfigurasi secara manual oleh administrator jaringan. Setiap host pada jaringan harus dikonfigurasi untuk mengarah kepada default route atau default gateway agar cocok dengan IP address dari interface local router, di mana router memeriksa routing table dan menentukan route yang mana digunakan untuk meneruskan paket.

Konsep dasar dari routing adalah bahwa router meneruskan IP paket berdasarkan pada IP address tujuan yang ada dalam header IP paket. Dia mencocokkan IP address tujuan dengan routing table dengan harapan menemukan kecocokan entri–suatu entri yang menyatakan kepada router kemana paket selanjutnya harus diteruskan. Jika tidak ada kecocokan entri yang ada dalam routing table, dan tidak ada default route, maka router tersebut akan membuang paket tersebut. Untuk itu adalah sangat penting untuk mempunyai isian routing table yang tepat dan benar.

Keuntungan static route:

Static route lebih aman dibanding dynamic route

Static route kebal dari segala usaha hacker untuk men-spoof paket dynamic routing protocols dengan maksud melakukan konfigurasi router untuk tujuan membajak traffic.

Kerugian:

Administrasinya adalah cukup rumit dibanding dynamic routing, khususnya jika terdiri dari banyak router yang perlu dikonfigurasi secara manual.

Rentan terhadap kesalahan saat entri data static route dengan cara manual.

Sedangkan Routing Dinamik adalah jenis routing yang bisa berubah sesuai dengan kondisi yang diinginkan dengan parameter tertentu sesuai dengan protokolnya. Routing Dinamik diterapkan pada PC yang berfungsi sebagai router dan dibutuhkan router lain yang sama-sama menerapkan sistem routing dinamik, jadi tidak bisa berdiri sendiri seperti halnya Router static.

Routing Dinamik menentukan gateway untuk network destination berdasarkan parameter yang didapat dari router lainnya melalui Protokol Multicast, seperti metrik, cost dsb. Protocol RIP dan OSPF menggunakan multicast untuk pertukaran informasi antar router, sedangkan protokol BGP menggunakan koneksi TCP untuk pertukaran routingnya.

### SARAN

Dari kesimpulan makalah ini, maka berikut adalah saran yang dapat penulis berikan.

Penggunaan static route sebaiknya digunakan pada jaringan skala kecil, dan sebaliknya untuk jaringan skala besar lebih baik menggunakan dynamic route.

Penerapan protocol pada dynamic route harus disesuaikan dengan jaringan bentuk atau area yang akan dibangun.

Dalam melakukan entri data satic route, administrator diharap lebih hati-hati dan teliti, karena dalam pengentrian data dengan static route rentan terjadi kesalahan

Setiap Router memiliki kelebihan dan kekurangan sebaiknya gunakanlah router sesuai dengan kebutuhan masing-masing.

### DAFTAR PUSTAKA

Dodi Hriadi. 2012. Solusi Cerdas Menguasai Internetworking Packet Tracer. Yogyakarta: ANDI.

http://fahmpress.blogspot.com/2014/01/mengenal-konfigurasi-static-route-pada.html

http://santekno.blogspot.com/2013/01/bgp-border-gateway-protocol.html

http://id.wikipedia.org/wiki/Border\_Gateway\_Protocol

http://rachmad29.blogspot.com/2008/12/bagaimana-cara-kerja-router-menjalankan.html

https://deenugraha.wordpress.com/about/konfigurasi-routing-dinamik-dengan-packet-tracer/