PENGENALAN PROTOKOL ROUTING

Edi Surya Negara

Penerbit :
PPP-UBD Press

Dr. Edi Surya Negara, M.Kom

Pengenalan Protokol Routing

Penerbit:
Pusat Penerbitan dan Percetakan Universitas Bina Darma
Press
(PPP-UBD Press) Palembang
Jl. Jenderal Ahmad Yani No. 3 Plaju Palembang
Telp. 0711-515582
Email: universitas@binadarma.ac.id

Pengenalan Protokol Routing

Penulis: Edi Surya Negara
Editor: Rezki Syaputra
Tata Sampul: Dedek Juliansyah
Tata isi: Ria Andryani

Cetakan Pertama, Mei 2021

Pusat Penerbitan dan Percetakan Universitas Bina Darma Press (PPP-UBD Press) Palembang
Anggota IKAPI: 008/SMS/05

Jl. Jenderal A. Yani No. 3 Palembang Sumatera Selatan, Indonesia
Telp. 0711-515582
Email: universitas@binadarma.ac.id

ISBN 978-979-3877-44-0

Daftar Isi

Kata Pengantar

Rasa syukur dan segala puji atas karunia dan nikmat yang diberikan oleh Allah SWT kepada tim penulis, sehingga buku Pengenalan Protokol Routing dapat diselesaikan.

Routing merupakan sebuah mekanisme pada jaringan komputer dalam melakukan pengiriman paket data dari satu network ke network yang lain. Pada router, biasanya memiliki satu atau beberapa tabel routing yang menyimpan informasi jalur routing yang digunakan saat mentransfer data melalui router. Proses perutean terjadi pada lapisan 3 pada Open Sistem Interconection layer (OSI) . Buku ini akan menyajikan pengenalan protokol routing yang sering digunakan dalam dunia jaringan komputer.

Buku ini terdiri dari 10 bab, yaitu:

Bab 1 Penganalan Routing
Bab 2 Perutean Statis
Bab 3 Tabel Perutean
Bab 4 Protokol Perutean Vektor Jarak
Bab 5 Routing Information Protocol Versi 1
Bab 6 VLSM dan CIDR
Bab 7 Routing Information Protocol Versi 2 (RIPv2)
Bab 8 Enhanced Interior Gateway Routing Protocol (EIGRP)
Bab 9 Protokol Perutean Link-State
Bab 10 Buka Jalur Terpendek Pertama (OSPF)

Akhir kata penulis mengucapkan banyak terima kasih kepada semua pihak yang telah memberikan masukan-masukan positif selama penulisan buku ini. Semoga buku ini dapat memberikan manfaat kepada kita semua.

Palembang, Mei 2021

Penulis

Bab 1

Pengenalan Routing

1.1 Pengenalan Routing

Pada saat ini jaringan memiliki dampak yang signifikan pada kehidupan kita - mengubah cara kita hidup, bekerja, dan bermain. Jaringan komputer - dan dalam konteks yang lebih besar Internet - memungkinkan orang untuk berkomunikasi, berkolaborasi, dan berinteraksi dengan cara yang tidak pernah kita lakukan sebelumnya. Kita menggunakan jaringan dalam berbagai cara, termasuk aplikasi web, IP telephony, video conferencing, game interaktif, perdagangan elektronik, pendidikan, dan banyak lagi [1][2].

Di pusat jaringan terdapat router. Router bertanggung jawab untuk pengiriman paket di seluruh jaringan yang berbeda [3]. Tujuan dari paket IP mungkin web server di negara lain atau e-mail server pada jaringan area lokal [3]. Adalah tanggung jawab router untuk memberikan paket tersebut secara tepat. Efektivitas komunikasi internetwork tergantung pada kemampuan router untuk meneruskan paket dengan cara yang paling efisien mungkin untuk tingkat besar.

Pada saat ini Router telah ditambahkan ke satelit di ruang angkasa. Router ini memiliki kemampuan untuk me-route IP traffic antara satelit di ruang angkasa dalam banyak cara yang sama sebagaimana paket-paket dipindahkan di Bumi, sehingga mengurangi penundaan dan menawarkan fleksibilitas jaringan yang lebih [3].

Selain paket forwarding, router menyediakan layanan lain juga. Untuk memenuhi tuntutan jaringan pada saat ini, router juga digunakan untuk [3]:

- Memastikan ketersediaan 24x7 (24 jam sehari, 7 hari seminggu). Untuk membantu pencapaian penjaminan jaringan, router menggunakan jalur alternatif jika jalan utama gagal.
- Menyediakan pelayanan terpadu data, video, dan suara melalui jaringan kabel dan nirkabel. Router menggunakan Quality of service (QoS) paket IP untuk memastikan bahwa lalu lintas real-time, seperti data suara, video dan data kritis tidak drop atau tertunda.
- Mengurangi dampak dari worm, virus, dan serangan lain pada jaringan dengan mengijinkan atau menolak penyampaian paket.

Semua layanan ini dibangun di sekitar router dan tanggung jawab utamanya adalah mem-forward paket dari satu jaringan ke jaringan yang berikutnya. Hanya karena kemampuan router untuk me-route paket antar jaringan maka perangkat pada jaringan yang berbeda dapat berkomunikasi. Bab ini akan memperkenalkan Anda ke router, perannya dalam jaringan, utamanya perangkat keras dan komponen perangkat lunak, dan proses routing itu sendiri.

Gambar 1.1 Router

1.2 Router adalah Komputer

Sebuah router adalah komputer, seperti komputer lain termasuk PC. Router yang pertama, digunakan untuk Jaringan Advanced Research Projects Agency (ARPANET), adalah Interface Message Processor (IMP). IMP 316 adalah komputer mini Honeywell; komputer ini menghidupkan ARPANET pada tanggal 30 Agustus 1969. Catatan: ARPANET dikembangkan oleh Advanced Research Projects Agency (ARPA) dari Amerika Serikat Departemen Pertahanan. ARPANET adalah jaringan packet switching dunia pertama dan merupakan pendahulu Internet saat ini [3].

Router mempunyai banyak persamaan komponen hardware dan software yang ditemukan di computer lain termasuk:

- CPU
- RAM
- ROM
- Operating System

Gambar 1.2. Bagian dalam router

Router berada di pusat jaringan

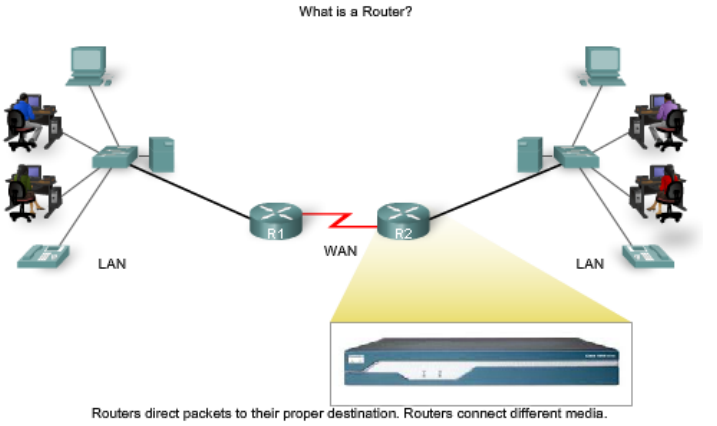
User pada umumnya mungkin tidak menyadari kehadiran banyak router dalam jaringan mereka sendiri atau di Internet. User berharap dapat mengakses halaman web, mengirim e-mail, dan download musik – tidak peduli apakah server mereka mengakses pada jaringan mereka sendiri atau pada jaringan lain di seluruh dunia. Namun, profesional network tahu bahwa router yang bertanggung jawab untuk meneruskan paket dari jaringan-ke-jaringan dari source ke destination.

Sebuah router menghubungkan beberapa jaringan. Ini berarti bahwa router memiliki beberapa interface yang masing-masing memiliki jaringan IP yang berbeda. Ketika router menerima paket IP pada satu interface, router menentukan interface mana yang digunakan untuk meneruskan paket ke tujuannya. Interface yang digunakan router untuk meneruskan paket mungkin

jaringan dari tujuan akhir paket tersebut (jaringan dengan alamat IP tujuan dari paket ini), atau mungkin jaringan yang terhubung ke router lain yang digunakan untuk mencapai tujuan akhir jaringan.

Setiap jaringan yang terhubung ke router biasanya membutuhkan interface yang terpisah. Interface ini digunakan untuk menghubungkan kombinasi keduanya Local Area Network (LAN) dan Wide Area Networks (WAN). LAN adalah jaringan Ethernet yang umumnya mengandung perangkat seperti PC, printer, dan server. WAN digunakan untuk menghubungkan jaringan di wilayah geografis yang luas. Sebagai contoh, sebuah koneksi WAN umumnya digunakan untuk menghubungkan LAN ke jaringan Internet Service Provider (ISP) [3].

Pada gambar, terlihat bahwa router R1 dan R2 bertanggung jawab untuk menerima paket pada satu jaringan dan mem-forward paket keluar jaringan lain menuju jaringan tujuan.



Gambar 1.3. Router menghubungkan media yang berbeda

Router menentukan jalur terbaik

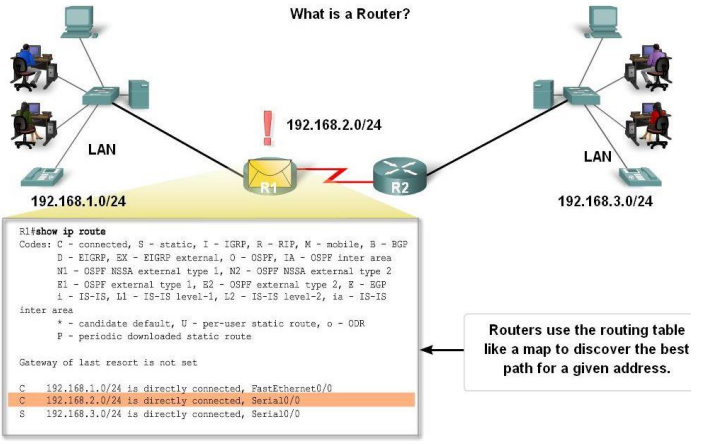
Tanggung jawab utama dari sebuah router adalah untuk mengarahkan paket yang ditujukan untuk local network dan remote network dengan:

- Menentukan jalan terbaik untuk mengirim paket
- Meneruskan paket ke tujuan

Router menggunakan tabel routing untuk menentukan jalur terbaik untuk mem-forward paket. Ketika router menerima sebuah paket, maka router mengkaji tujuan alamat IP-nya dan mencari yang paling cocok dengan alamat jaringan dalam tabel routing router. Tabel routing juga mencakup interface jaringan yang akan digunakan untuk meneruskan paket. Setelah kecocokan ditemukan, router mengenkapsulasi paket IP ke dalam frame data link dari interface yang keluar, dan paket ini kemudian diteruskan ke tujuan.

Sangat dimungkin bahwa router akan menerima paket yang di-enkapsulasi dalam satu jenis data link frame, seperti sebuah frame Ethernet dan ketika mem-forward paket, router akan meng-enkapsulasi data link frame dalam jenis yang berbeda, seperti Point -to-point Protocol (PPP). Enkapsulasi data link tergantung pada jenis interface pada router dan jenis media yang. Teknologi data link yang berbeda yang terhubung ke router dapat mencakup teknologi LAN, seperti Ethernet, dan koneksi serial WAN, seperti koneksi T1 menggunakan PPP, Frame Relay, dan Asynchronous Transfer Mode (ATM).

Pada gambar, kita dapat mengikuti sebuah paket dari PC sumber ke PC tujuan. Perhatikan bahwa adalah tanggung jawab router untuk menemukan jaringan tujuan dalam tabel routing dan meneruskan paket pada arah tujuan. Dalam contoh ini, router R1 menerima paket dikemas dalam sebuah frame Ethernet. Setelah decapsulasi paket, R1 menggunakan alamat IP tujuan dari paket untuk mencari tabel routing untuk alamat jaringan yang cocok. Setelah alamat jaringan tujuan ditemukan pada tabel routing, R1 merangkum paket di dalam sebuah frame PPP dan meneruskan paket ke R2. Sebuah proses yang serupa dilakukan oleh R2.



Gambar 1.4. router menggunakan routing table

Protokol Static route dan protokol dynamic route digunakan oleh router untuk mempelajari remote network dan membangun tabel routing. route dan protokol ini merupakan fokus utama dan akan dibahas secara rinci di bab berikutnya bersama dengan proses yang digunakan dalam pencarian routing table dan mem-forward paket.

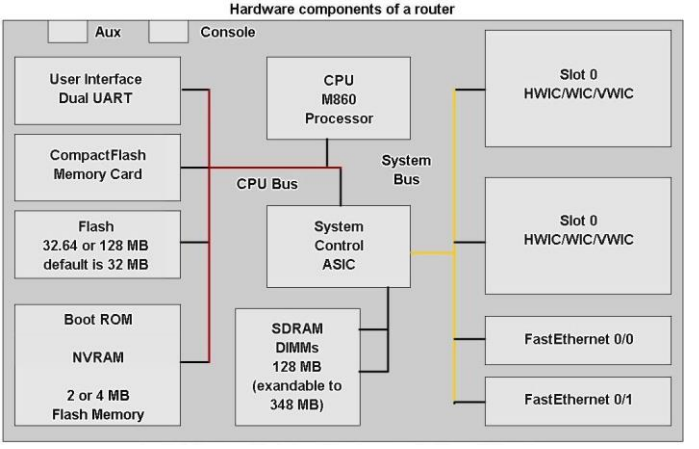
1.3 Router CPU dan Memory

Meskipun ada beberapa jenis dan model router, setiap router memiliki komponen hardware yang sama umum. Tergantung pada model, komponen-komponen tersebut terletak di tempat yang berbeda di dalam router. Gambar ini menunjukkan komponen internal sebuah router 1841. Untuk melihat komponen internal router, Anda harus melepaskan penutup logam dan melepasnya dari router. Biasanya Anda tidak perlu membuka router kecuali Anda meng-upgrade memori [3].

Gambar 1.7. komponen internal router 1841

Seperti PC, sebuah router terdiri dari:

- Central Processing Unit (CPU)
- Random-Access Memory (RAM)
- Read-Only Memory (ROM)



Gambar 1.8. komponen hardware router

CPU

CPU mengeksekusi instruksi sistem operasi, seperti inisialisasi sistem, fungsi routing, dan fungsi switching.

RAM

RAM menyimpan instruksi dan data yang diperlukan untuk dieksekusi oleh CPU. RAM digunakan untuk menyimpan komponen-komponen:

- Operating System: Cisco IOS (Internetwork Operating System) disalin kedalam RAM selama bootup.
- Running Configuration File: Ini adalah file konfigurasi yang menyimpan perintah konfigurasi yang IOS router gunakan. Dengan sedikit pengecualian, semua perintah dikonfigurasi di router disimpan di running configuration file, yang dikenal sebagai running-config.
- IP Routing Table: File ini menyimpan informasi tentang directly connected dan remote networks. Digunakan untuk menentukan jalur terbaik untuk mem-forward paket.
- ARP Cache: Cache ini berisi alamat IPv4 ke pemetaan alamat MAC, mirip dengan ARP cache pada PC. Cache ARP digunakan pada router yang memiliki LAN interface seperti interface Ethernet.
- Packet Buffer: Paket disimpan sementara dalam buffer ketika diterima sebuah interface atau sebelum keluar sebuah interface.

RAM adalah memori volatile dan kehilangan isinya ketika router dimatikan atau restart. Namun, router juga berisi area penyimpanan permanen, seperti ROM, flash dan NVRAM.

ROM

ROM adalah penyimpanan permanen. Perangkat Cisco menggunakan ROM untuk menyimpan:

- Instruksi-instruksi bootstrap
- Diagnostic software dasar
- Scaled-down versi IOS

ROM menggunakan firmware, yang merupakan perangkat lunak yang tertanam di dalam integrated circuit. Firmware termasuk software yang biasanya tidak perlu diubah atau ditingkatkan, seperti instruksi bootup. Banyak dari fitur ini, termasuk software monitor ROM, akan dibahas kemudian. ROM tidak kehilangan isinya ketika router kehilangan power atau restart.

Flash Memory
Flash memori adalah memori komputer nonvolatile yang dapat disimpan dan dihapus secara elektrik. Flash digunakan sebagai penyimpanan permanen untuk sistem operasi, Cisco IOS. Pada kebanyakan model router Cisco, IOS secara permanen dalam memori flash dan disalin ke RAM selama proses booting, kemudian dieksekusi oleh CPU. Beberapa model lama dari router Cisco menjalankan IOS langsung dari flash. Flash terdiri dari kartu SIMM atau PCMCIA, yang dapat ditingkatkan untuk meningkatkan jumlah memori flash. Flash Memori tidak kehilangan isinya ketika router kehilangan power atau restart.

NVRAM
NVRAM (Non-Volatile RAM) tidak kehilangan informasinya ketika power dimatikan. Hal ini kontras dengan bentuk paling umum dari RAM, seperti DRAM, yang membutuhkan daya terus-menerus untuk menjaga informasinya. NVRAM digunakan oleh IOS Cisco sebagai penyimpanan permanen untuk file konfigurasi startup (startup-config). Semua perubahan konfigurasi disimpan dalam file running-config dalam RAM, dan dengan sedikit pengecualian, segera diimplementasikan oleh IOS. Untuk menyimpan perubahan-perubahan bila router restart atau kehilangan power, running-config harus disalin ke NVRAM, di mana ia disimpan sebagai file startup-config. NVRAM mempertahankan isinya bahkan router di-reload atau dimatikan.

ROM, RAM, NVRAM, dan flash dibahas pada bagian berikutnya yang memperkenalkan IOS dan proses bootup. Dibahas juga secara lebih rinci bagaimana mengelola IOS. Hal yang lebih penting bagi profesional networking untuk memahami fungsi komponen internal utama dari sebuah router dari pada lokasi yang tepat dari komponen-komponen di dalam router tertentu. Arsitektur internal fisik berbeda dari model ke model.
Links :
View the "Cisco 1800 Series Portfolio Multimedia Demo," http://www.cisco.com/en/US/products/ps5875/index.html

1.4 Internetwork Operating System

Software sistem operasi yang digunakan di router Cisco dikenal sebagai Cisco Internetwork Operating System (IOS). Seperti sistem operasi di komputer

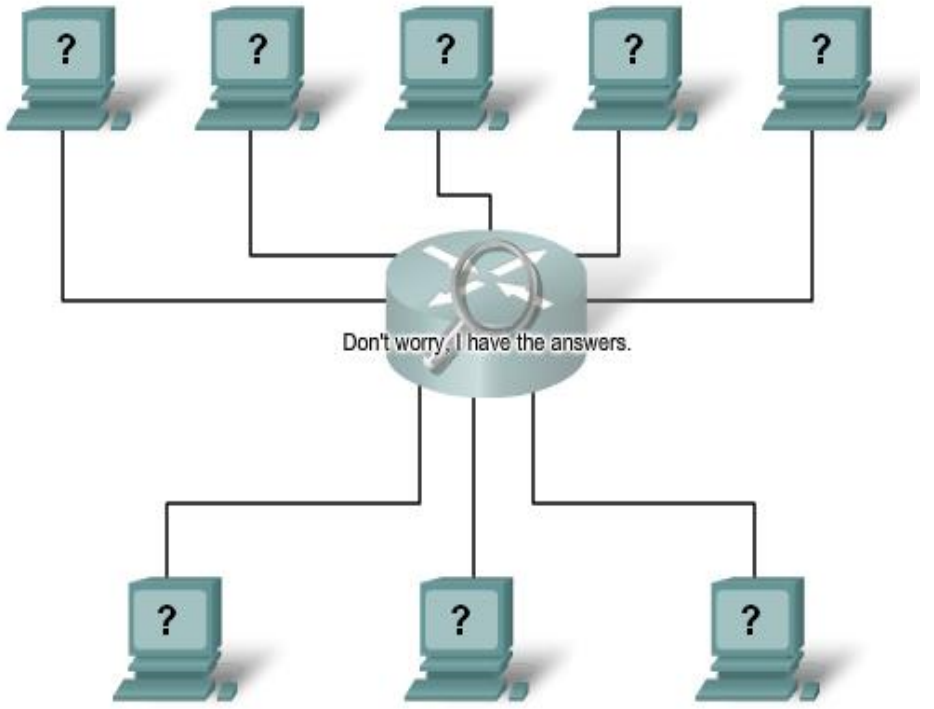
manapun, Cisco IOS mengelola sumber daya perangkat keras dan perangkat lunak router, termasuk alokasi memori, proses, keamanan, dan sistem file. Cisco IOS adalah sistem operasi multitasking yang terintegrasi dengan routing, switching, internetworking, dan fungsi telekomunikasi [3].

Meskipun Cisco IOS mungkin tampak sama pada banyak router, terdapat banyak IOS image yang berbeda. Sebuah IOS image adalah file yang berisi seluruh IOS untuk router. Cisco menciptakan berbagai jenis gambar IOS, tergantung pada model router dan fitur dalam IOS. Biasanya semakin banyak fitur dalam IOS, gambar yang lebih besar IOS, dan karenanya,semakin besar IOS image, dan oleh sebab itu semakin banyak flash dan RAM yang diperlukan untuk menyimpan dan memuat IOS. Sebagai contoh, beberapa fitur termasuk kemampuan untuk menjalankan IPv6 atau kemampuan router untuk melakukan NAT (Network Address Translation).

Seperti sistem operasi lain Cisco IOS memiliki user interface sendiri. Meskipun beberapa router menyediakan graphical user interface (GUI), command line interface (CLI) adalah metode yang jauh lebih umum mengkonfigurasi router Cisco.

Setelah bootup, file startup-config dalam NVRAM disalin ke RAM dan disimpan sebagai file running-config. IOS mengeksekusi perintah konfigurasi di running-config. Setiap perubahan yang dimasukkan oleh administrator jaringan disimpan dalam running-config dan langsung diimplementasikan oleh IOS. Dalam bab ini, kita akan meninjau beberapa perintah IOS dasar yang digunakan untuk mengkonfigurasi router Cisco. Dalam bab-bab berikutnya, kita akan mempelajari perintah yang digunakan untuk mengkonfigurasi, memverifikasi, dan memecahkan masalah routing statis dan berbagai protokol routing seperti RIP, EIGRP, dan OSPF.

Catatan: Cisco IOS dan proses bootup didiskusikan lebih detail berikutnya.



Gambar 1.9. internetwork

1.5 Proses Bootup Router

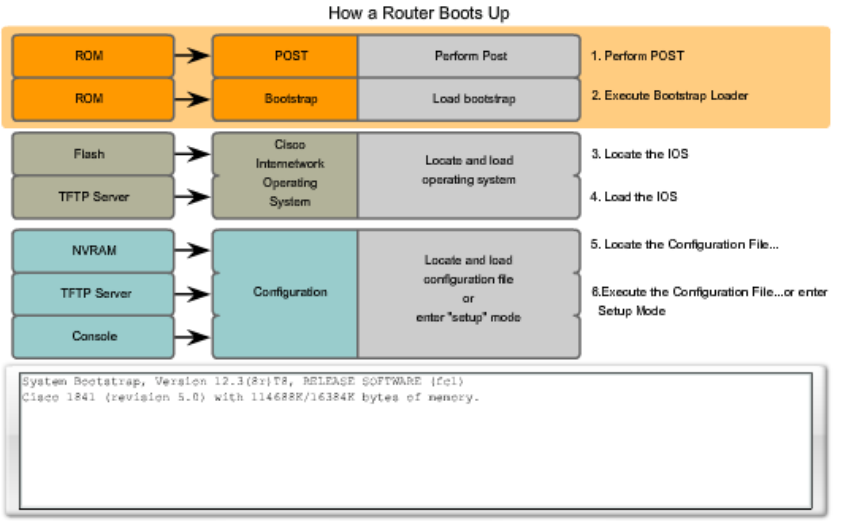
Terdapat empat tahapan utama proses bootup:

1. Melakukan POST

Power-On Self Test (POST) adalah proses umum yang terjadi pada hampir setiap komputer saat bootup. Proses POST digunakan untuk menguji perangkat keras router. Ketika router dinyalakan, perangkat lunak pada chip ROM yang melakukan POST. Selama self-test berlangsung, router menjalankan diagnosa dari ROM pada komponen beberapa hardware termasuk CPU, RAM, dan NVRAM. Setelah POST selesai, router mengeksekusi program bootstrap.

2. Memuat program bootstrap

Setelah POST, program bootstrap disalin dari ROM ke RAM. Selama di RAM, CPU mengeksekusi instruksi dalam program bootstrap. Tugas utama dari program bootstrap adalah untuk menemukan IOS Cisco dan memuatnya ke RAM.



Gambar 1.10. proses boot up 1 dan 2

Catatan: Pada titik ini, jika Anda memiliki koneksi konsol ke router, Anda akan mulai melihat output di layar.

3. Menemukan dan loading IOS Cisco

Menemukan software Cisco IOS. IOS biasanya disimpan dalam memori flash, tetapi juga dapat disimpan di tempat lain seperti server (Trivial File Transfer Protocol) TFTP.

Jika IOS image sepenuhnya tidak dapat ditemukan, versi skala-down dari IOS disalin dari ROM ke RAM. Versi IOS ini digunakan untuk membantu mendiagnosa masalah dan dapat digunakan untuk memuat versi lengkap dari IOS ke RAM.

Catatan: Sebuah server TFTP biasanya digunakan sebagai server cadangan untuk IOS tetapi juga dapat digunakan sebagai titik sentral untuk menyimpan dan loading IOS. Manajemen IOS dan menggunakan server TFTP dibahas kemudian.

Loading IOS. Beberapa router Cisco yang lebih tua mengerjakan IOS langsung dari flash, tetapi model terbaru menyalin IOS ke RAM untuk dieksekusi oleh CPU.
Catatan: Setelah IOS mulai di muat, mungkin terlihat tanda string pound (#), seperti yang ditunjukkan pada gambar, sementara image di-decompress.

4. Menemukan dan loading file konfigurasi startup atau masuk setup mode

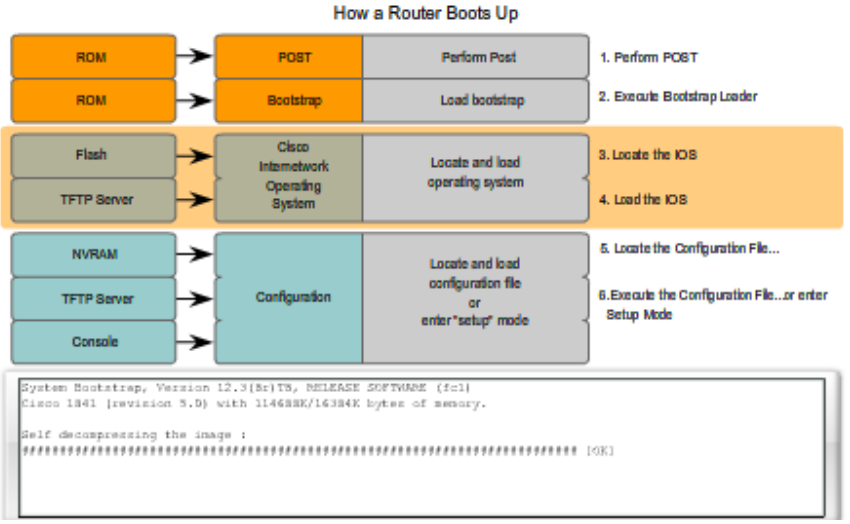
Menemukan Startup Configuration File. Setelah IOS dimuat, Program bootstrap mulai mencari startup configuration file, yang dikenal sebagai startup-config, dalam NVRAM. File ini memiliki perintah konfigurasi yang telah disimpan dan parameter-parameter didalamnya termasuk:

- Alamat interface
- Informasi routing
- passwords
- konfigurasi lainnya yang disimpan oleh administrator

Jika startup configuration file, startup-config, terletak di NVRAM, semua disalin ke RAM sebagai running configuration file, running-config.

Catatan: Jika startup configuration file tidak terdapat di NVRAM, router dapatmencari di TFTP server. Jika router mendeteksi bahwa itu memiliki link aktif ke router lain yang telah dikonfigurasi, router mengirimkan broadcast mencari file konfigurasi di link aktif. Kondisi ini akan menyebabkan router berhenti, tapi akhirnya akan terlihat pesan konsol seperti yang berikut ini:

<router pauses here while it broadcasts for a configuration file across an active link>
%Error opening tftp://255.255.255.255/network-confg (Timed out)
%Error opening tftp://255.255.255.255/cisconet.cfg (Timed out)



Gambar 1.11. proses boot up 3 & 4

Menjalankan Configuration File. Jika sebuah startup configuration file ditemukan dalam NVRAM, IOS me-load-kan file ke RAM sebagai running-config dan menjalankan perintah dalam file, satu baris pada satu waktu. File running-config berisi alamat interface, mulai proses routing, mengkonfigurasi password router dan mendefinisikan karakteristik lain dari router.

Masuk ke Setup Mode (Optional). Jika startup configuration file tidak dapat ditemukan, router meminta pengguna untuk memasukkan setup mode. Setup mode adalah serangkaian pertanyaan yang mendorong pengguna untuk memasukkan informasi konfigurasi dasar. Setup Mode ini tidak dimaksudkan untuk digunakan untuk memasukkan konfigurasi router yang kompleks, dan tidak umum digunakan oleh administrator jaringan.

Would you like to enter the initial configuration dialog? [yes/no]: no

Setup mode tidak akan digunakan untuk mengkonfigurasi router. Ketika diminta untuk masuk ke setup mode, selalu jawab dengan no. Jika dijawab dengan yes dan masuk ke setup mode, dapat menekan Ctrl-C kapanpun untuk keluar dari proses setup.

Ketika setup mode tidak digunakan, IOS menciptakan default running-config. Default running-config adalah dasar konfigurasi file yang memasukkan

interface router, managemen interfaces, dan default information. Default running-config tidak berisi alamat interface tertentu, informasi routing, password, atau informasi konfigurasi secara spesifik.

Command Line Interface

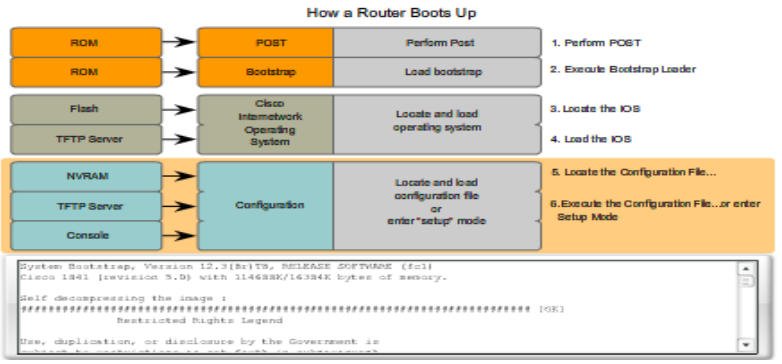
Tergantung pada platform dan IOS, router dapat mengajukan pertanyaan berikut sebelum menampilkan prompt:

Would you like to terminate autoinstall? [yes]: <Enter>
Press the Enter key to accept the default answer.
Router>

Catatan: Jika file konfigurasi ditemukan, running-config dapat berisi hostname dan prompt akan menampilkan hostname dari router.

Setelah prompt ditampilkan, router sekarang menjalankan IOS dengan running configuration file yang ada. Administrator jaringan sekarang dapat mulai menggunakan perintah-perintah IOS pada router ini.

Catatan: Proses bootup dibahas lebih rinci kemudian.



Gambar 1.12. proses boot up 5 & 6

Memverifikasi Proses Bootup Router

Perintah show version dapat digunakan untuk membantu memverifikasi dan memecahkan beberapa masalah komponen hardware dan software dasar router. Perintah show version menampilkan informasi tentan versi dari software Cisco IOS yang sedang berjalan di router, versi dari program bootstrap, dan informasi tentang konfigurasi hardware, termasuk jumlah dari system memory.

Output dari perintah show version termasuk:

IOS version
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)

Ini adalah versi software Cisco IOS dalam RAM yang digunakan oleh router.

ROM Bootstrap Program
ROM: System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)

Ini menunjukkan versi dari software system bootstrap, disimpan di memori ROM, yang menunjukkan inisialisasi yang digunakan router untuk boot up.

Lokasi dari IOS
System image file is "flash:c2600-i-mz.122-28.bin"

Ini menunjukkan dimana program bootstrap dan di load di Cisco IOs, dan nama lengkap dari IOS image.

CPU dan jumlah RAM
cisco 2621 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory

Bagian pertama dari baris ini menampilkan tipe CPU pada router ini. Bagian terakhir dari baris ini menampilkan jumlah DRAM. Beberapa seri router,. Seperti 2600, menggunakan sebagian kecil dari DRAM sebagai packet memory. Packet memory digunakan untuk buffering paket.

Untuk menentukan jumlah total DRAM di router, tambahkan kedua angka. Pada contoh ini, router Cisco 2621 mempunyai 60,416 KB (kilobytes) DRAM digunakan untuk penyimpanan sementara Cisco IOS dan proses system lainnya. 5,120 KB lainnya diperuntukkan packet memory. Jumlah total DRAM adalah 65,536K, atau 64 megabytes (MB).

Catatan: Mungkin perlu untuk meningkatkan jumlah RAM ketika melakukan upgrade IOS.

Interface
2 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)

Bagian ini menunjukkan physical interfaces pada router. Pada contoh ini, router Cisco 2621 mempunyai dua interface FastEthernet dan dua low-speed serial interfaces.

Jumlah NVRAM
32K bytes of non-volatile configuration memory.

Ini adalah jumlah NVRAM pada router. NVRAM digunakan untuk menyimpan startup-config file.
Ini adalah jumlah flash memory pada router. Flash digunakan secara permanen menyimpan Cisco IOS.

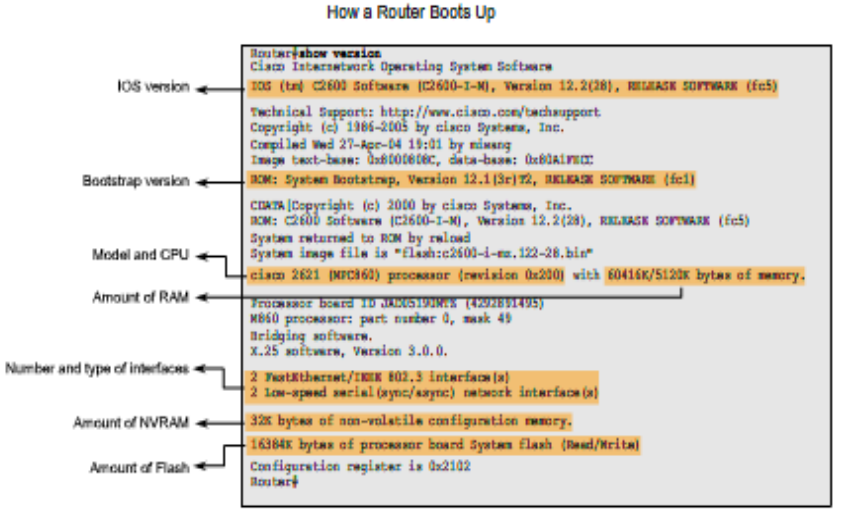
Catatan: Mungkin diperlukan menambah jumlah flash ketika meng- upgrade IOS.

Konfigurasi Register
Configuration register is 0x2102

Baris terakhir dari perintah show version menampilkan nilai software konfigurasi register terkini dalam hexadecimal. Jika terdapat nilai kedua ditampilkan dalam tanda kurung, ini menunjukkan nilai konfigurasi register yang akan digunakan selama reload selanjutnya.

Configuration register mempunyai beberapa fungsi, termasuk password recovery. Pengaturan standar untuk configuration register adalah 0x2102. Nilai ini menunjukkan bahwa router akan mencoba me-load Cisco IOS software image dari flash memory dan me- load startup configuration file dari NVRAM.

Catatan: Configuration register akan dibahas lebih rinci selanjutnya.



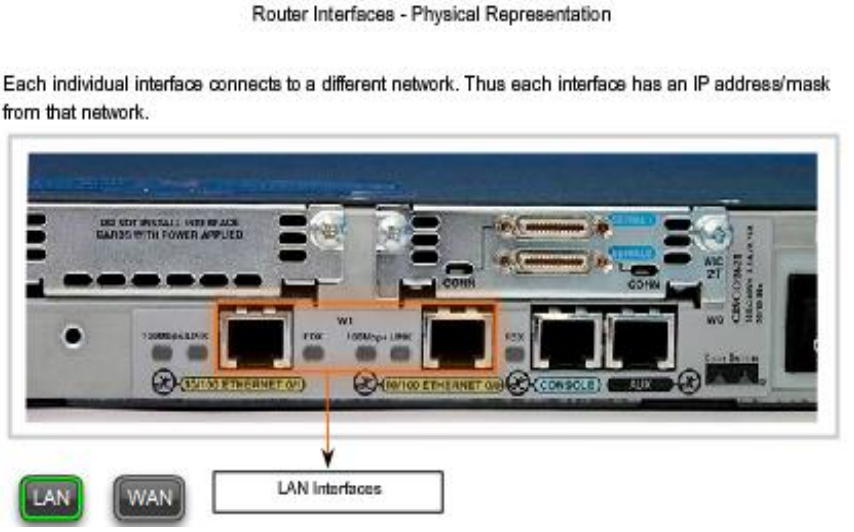
Gambar 1.13. output dari perintah show version

1.6 Interface Router

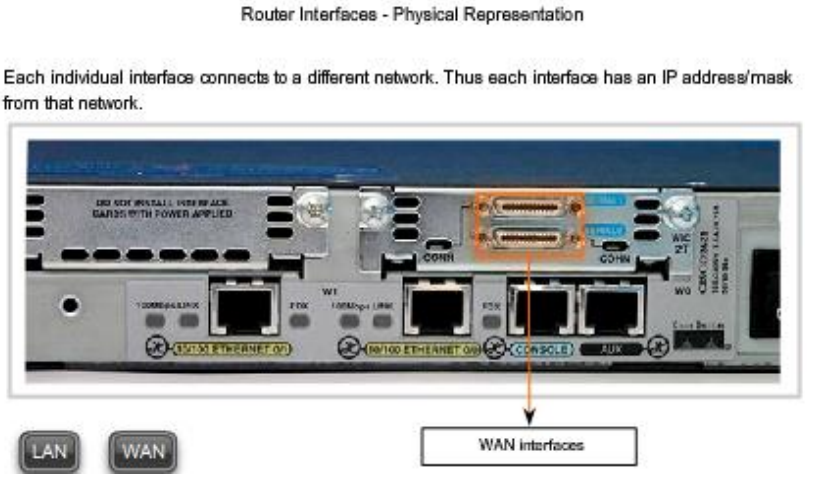
Managemen Port

Router mempunyai memiliki konektor fisik yang digunakan untuk mengelola router. Konektor ini dikenal sebagai management ports. Tidak seperti Ethernet dan serial interfaces, managemen port tidak digunakan untuk packet forwarding. Managemen port yang paling umum adalah console port. Console port digunakan untuk menghubungkan sebuah terminal, atau paling sering digunakan untuk menjalankan software terminal emulator PC, untuk mengkonfigurasi router tanpa perlu network access ke router. Console port harus digunakan selama inisialisasi konfigurasi router.

Management port yang lain adalah auxiliary port. Tidak semua router mempunyai auxiliary ports. Pada saat auxiliary port dapat digunakan caranya serupa dengan console port. Dapat juga digunakan untuk menyambungkan ke modem. Auxiliary ports tidak akan dibahas sekarang.
Gambar menunjukkan console dan AUX port pada router.



Gambar 1.14. interface untuk LAN

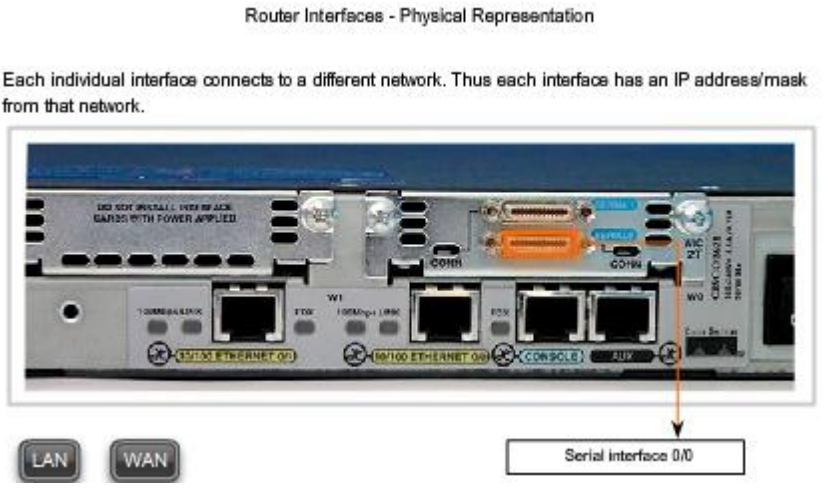


Gambar 1.15. interface untuk WAN

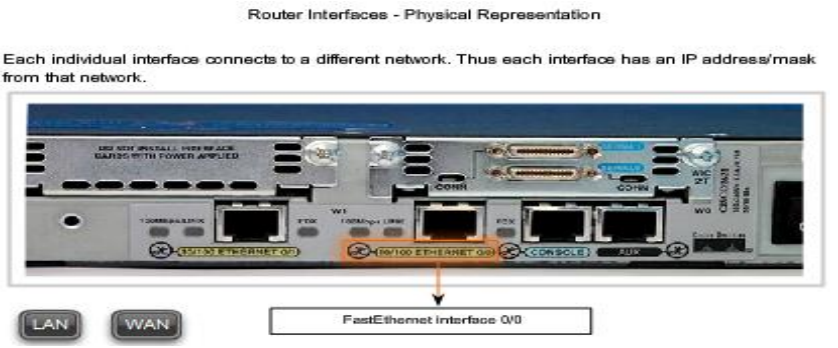
Interface Router

Istilah interface pada Cisco routers mengacu pada konektor secara fisik ada pada router yang fungsi utamanya adalah menerima dan mem- forward packet. Router punya banyak interfaces yang digunakan untuk menghubungkan banyak jaringan. Biasanya, interface terhubung ke berbagai jenis jaringan,

yang berarti bahwa diperlukan jenis media dan konektor yang berbeda. Sering kali router akan membutuhkan tipe interface yang berbeda. Contohnya, sebuah router biasanya memiliki interface FastEthernet untuk menghubungkan ke LAN yang berbeda dan banyak tipe interface WAN untuk menghubungkan berbagai macam serial link termasuk T1, DSL dan ISDN. Gambar menunjukkan FastEthernet dan serial interface pada router.



Gambar 1.16. serial interface



Gambar 1.17. fastethernet interface

Seperti interface pada PC, ports dan interface pada sebuah router terletak diluar router. Lokasi external mereka memungkinkan kemudahan pemakaian bagi kabel dan konektor jaringan yang sesuai.

Catatan: interface tunggal pada sebuah router dapat digunakan untuk menghubungkan ke multiple network; tetapi, ini diluar batas pembahasan dan akan dibahas kemudian.

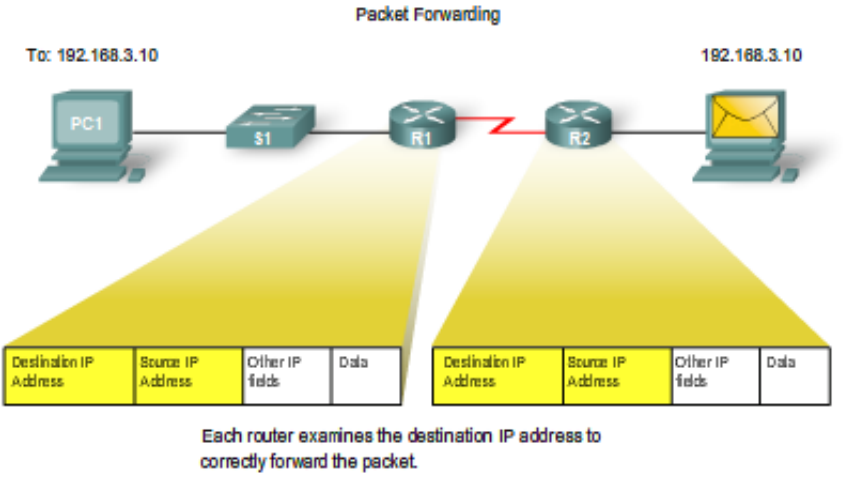
Seperti kebanyakan peralatan jaringan, router Cisco menggunakan indikator LED yang menyediakan informasi status. LED mengindikasikan kegiatan interface yang sesuai. Jika LED mati maka interface active dan interface terkoneksi dengan benar, Ini mungkin mengindikasikan suatu masalah dengan interface. Jika interface sangat sibuk, LED akan selalu hidup. Tergantung dari tipe router, kemungkinan terdapat LED yang lain. Untuk informasi lebih jauh tentang LED yang terdapat pada 1841, lihat link dibawah.

1.7 Router dan Network Layer

Tujuan utama dari router adalah menghubungkan multiple network dan mem-forward paket tujuan baik untuk network nya sendiri atau network lain. Sebuah router dianggap alat Layer 3 karena keputusan mem-forward utamanya didasarkan pada informasi IP Packet Layer 3, khususnya IP address tujuan. Proses ini disebut routing [4].

Ketika router menerima sebuah packet, router memeriksa IP address tujuan. Jika IP address tujuan bukan milik network yang terhubung langsung dengan router, router harus mem-forward paket ini ke router lain. Setelah mencari routing table, R1 mem-forward packet ke R2. Ketika R2 menerima paket, R2 juga memeriksa tujuan IP address paket. Setelah mencari routing table, R2 mem-forward paket keluar jaringan yang terhubung langsung ke Ethernetke PC2.

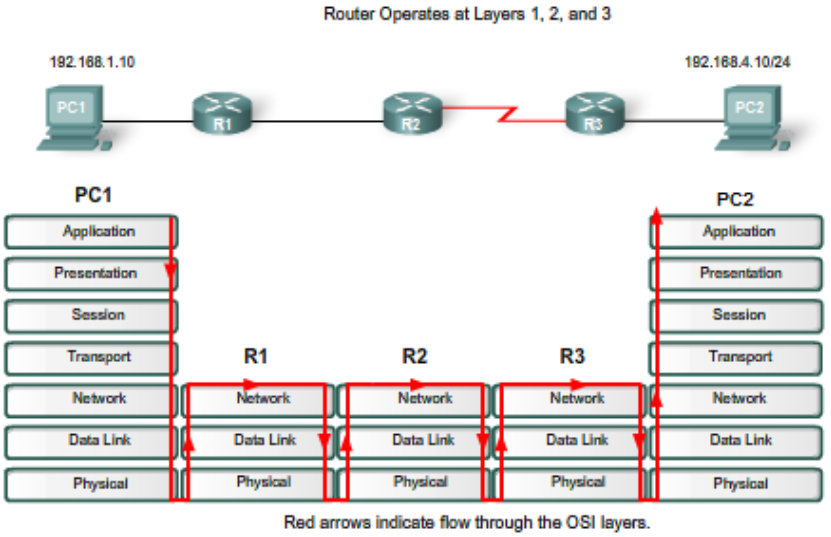
Ketika setiap router menerima paket, router mencari dalam routing table nya untuk menemukan yang paling sesuai antara IP address tujuan dengan network address. Ketika ditemukan kesamaan, paket dienkapsulasi di layer 2 data link frame untuk interface keluar. Tipe enkapsulasi data link tergantung pada tipe interface, seperti Ethernet atau HDLC.



Gambar 1.19. Packet forwarding

Pada akhirnya paket mencapai router yang merupakan bagian dari network yang sesuai dengan IP address tujuan paket. Pada contoh ini, router R2 menerima paket dari R1. R2 mem-forward paket keluar interface Ethernet, yang merupakan milik network yang sama dengan alat tujuan, PC2. Urutan kejadian ini dijelaskan secara rinci pada bab ini kemudian. Routers beroperasi pada Layers 1, 2, dan 3

Sebuah router membuat keputusan utama mem-forward pada Layer 3, tapi seperti kita lihat sebelumnya, router juga ikut pada proses Layer 1 dan Layer 2. Setelah sebuah router selesai memeriksa IP address tujuan dari paket dan berkonsultasi dengan routing table nya untuk membuat keputusan mem-forward, router dapat mem-forward paket keluar paket ke tujuan melalui interface yang sesuai. Router mengenkapsulasi IP paket Layer 3 ke dalam porsi data Layer 2 data link frame sesuai dengan interface keluar. Jenis frame dapat berupa Ethernet, HDLC, atau enkapsulasi Layer 2 lainnya – apapun enkapsulasi yang digunakan pada interface tertentu. Frame Layer 2 diterjemahkan ke sinyal fisik Layer 1 yang digunakan untuk mewakili bit melalui physical link.
Untuk mengerti proses ini lebih baik, lihat ke gambar. Perhatikan PC1 beroperasi pada ke tujuh layers, enkapsulasi data dan mengirim frame keluar sebagai rangkaian bit yang telah dienkode ke R1, default gatewaynya.



Gambar 1.20. operasi router pada layer 1,2,3

R1 menerima serangkaian bit yang di encode ke interfacenya. Bit diterjemahkan dan diteruskan sampai ke Layer 2, di mana R1 men-decapsulasi frame. Router memeriksa alamat tujuan dari data link frame untuk menentukan jika sesuai dengan interface yang menerima, termasuk broadcast atau multicast addres. Jika terdapat kesesuaian dengan porsi data dari frame, IP packet diteruskan ke Layer 3, dimana R1 membuat keputusan routing. R1 kemudian me-enkapsulasi ulang packet menjadi data link frame Layer 2 yang baru dan mem-forward keluar interface terluar sebagai serangkaian bit yang di enkode.

R2 menerima serangkaian bit, dan proses terulang dengan sendirinya. R2 men-dekapsulasi frame dan meneruskan porsi data dari frame, IP packet, ke Layer 3 dimana R2 membuat keputusan routing. R2 kemudian me-enkapsulasi ulang packet menjadi data link frame Layer 2 baru dan mem-forward keluar interface terluar sebagai serangkaian bit yang di encode. Proses ini diulang sekali lagi oleh router R3, yang mana mem-forward IP packet, me-enkapsulasi kedalam data link frame dan me-enkode sebagai bit, ke PC2.

Setiap router dalam jalur dari sumber ke tujuan melakukan proses yang sama dekapsulasi, mencari routing table, dan me-enkapsulasi ulang. Proses ini

penting untuk mengerti bagaimana kegiatan router dalam jaringan. Oleh karena itu, materi ini akan di diskusi ulang lebih dalam pada bagian berikutnya.

1.8 Konfigurasi CLI dan Pengalamatan

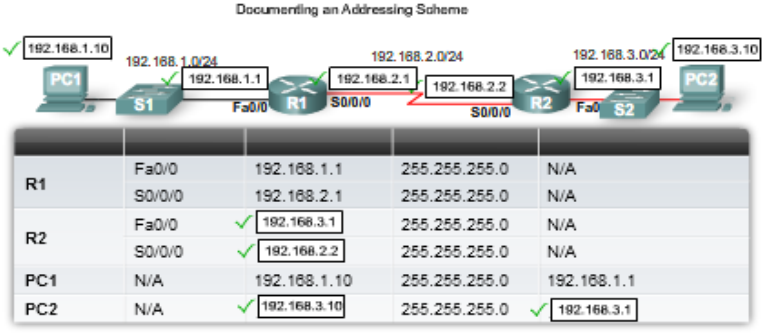
Penerapan Skema Pengalamatan Dasar

Ketika merancang jaringan baru atau mapping jaringan yang ada, dokumentasi kan jaringan. Paling sedikit, dokumentasi harus menyertakan topology diagram yang mengindikasikan hubungan secara fisik dan table pengalamatan yang berisi semua informasi dibawah ini:

- Nama Alat
- Interface yang digunakan dalam perancangan
- IP addresse dan subnet mask
- Default gateway addresses untuk end devices, seperti PCs

Mengisi sebuah Tabel Alamat

Gambar menunjukkan topologi jaringan dengan alat yang terinterkoneksi dan dikonfigurasi dengan IP address. Setelah topologi terdapat table yang digunakan untuk mendokumentasikan jaringan. Tabel secara terpisah di populasi dengan dokumentasi data jaringan (alat, IP address, subnet mask, dan interface).



R1	Fa0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0	192.168.2.1	255.255.255.0	N/A
R2	Fa0/0	192.168.3.1	255.255.255.0	N/A
	S0/0/0	192.168.2.2	255.255.255.0	N/A
PC1	N/A	192.168.1.10	255.255.255.0	192.168.1.1
PC2	N/A	192.168.3.10	255.255.255.0	192.168.3.1

Gambar 1.21. topologi jaringan

1.9 Konfigurasi Router Dasar

Saat mengkonfigurasi router, When configuring a router, tugas-tugas dasar tertentu yang dilakukan termasuk:

- Memberi nama router
- Setting password
- Konfigurasi interface
- Konfigurasi banner
- Menyimpan perubahan pada router
- Verifikasi konfigurasi dasar dan operasi router

Diasumsikan router tidak mempunyai startup-config file.

Prompt pertama muncul pada user mode. User mode memungkinkan melihat status dari router, tapi tidak untuk di konfigurasi. Jangan salah artikan istilah "user" yang digunakan di user mode dengan user di jaringan. User mode ditujukan untuk teknisi jaringan, operator, dan engineers yang memiliki tanggung jawab untuk mengkonfigurasi alat jaringan.

Router>

Perintah enable digunakan untuk masuk ke privileged EXEC mode. Mode ini memungkinkan user membuat perubahan konfigurasi pada router. Prompt router akan berubah dari “>” ke “#” pada mode ini.

Router>enable

Router#

Configuring Basic Router Parameters

Basic Router Configuration Command Syntax	
Naming the router	Router(config)#hostname *name*
Setting Passwords	Router(config)#enable secret *password*
	Router(config)#line console 0
	Router(config-line)#password *password*
	Router(config-line)#login
	Router(config)#line vty 0 4
	Router(config-line)#password *password*
	Router(config-line)#login
Configuring a message-of-the-day banner	Router(config)#banner motd # *message* #

Gambar 1.22. syntax perintah konfigurasi dasar

Nama Host dan Password

Router#config t	Pertama, masuk ke global configuration mode.
Router(config)#hostname R1 R1(config)#	Kemudian, masukkan nama host yang unik ke router.
Router(config)#enable secret class	konfigurasi password yang digunakan untuk masuk ke privileged EXEC mode Gunakan password class. Tetapi, dalam lingkungan produksi, router harus mempunyai password yang kuat.
R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit R1(config)#line vty 0 4 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit	console dan Telnet gunakan password cisco. Sekali lagi password cisco hanya digunakan untuk latihan. gunakanPerintah login enables password. Jika tidak digunakan pada console line, user akan diijinkan masuk tanpa harus memasukkan password

Konfigurasi Banner

R1(config)#banner motd # Enter TEXT message. End with the character '#'. ********** WARNING!! Unauthorized Access Prohibited!! ********** #	Dari global configuration mode, konfigurasi message-of-the-day (motd) banner. Pembatasan character, seperti "#" digunakan pada awal dan akhir pesan. Pembatasan memungkinkan mengkonfigurasi banner dengan banyak baris.

Mengkonfigurasi banner adalah bagian dari rencana pengamanan yang baik. Minimal,banner harus memperingatkan akses bagi yang tidak berhak. Jangan pernah mengkonfigurasi banner dengan kalimat "welcome" an unauthorized user.

Links

Untuk diskusikan penggunaan password yang kuat, lihat:

"Cisco Response to Dictionary Attacks on Cisco LEAP," at http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_bulletin09186a00801cc901.html#wp1002291

"Strong passwords: How to create and use them," at http://www.microsoft.com/athome/security/privacy/password.mspx

Konfigurasi Router Interface

Sekarang saatnya mengkonfigurasi router interface sendiri-sendiri dengan IP address dan informasi lainnya.

R1(config)#interface Serial0/0 R1(config-if)#ip address 192.168.2.1 255.255.255.0	Pertama, masuk interface configuration dengan menjabarkan tipe dan nomer interface. Selanjutnya, konfigurasi IP address dan subnet mask:
Router(config-if)#description Ciruit#VBN32696-123 (help desk:1-800-555-1234)	Jika interface terhubung dengan ISP atau service carrier, sangat membantu memasukan informasi koneksi dan informasi contact.
R1(config-if)#description Link to R2	Dalam lingkungan LAB, masukkan deskripsi sederhana yang akan membantu saat troubleshooting.
Router(config-if)#no shutdown	Interface harus diaktifkan dengan perintah no shutdown. Ini sama dengan memberi tenaga pada interface.
R1(config-if)#clock rate 64000	Router yang memiliki akhir DCE dari kabel yang terhubung dengan serial interface akan membutuhkan perintah tambahan clock rate Langkah ini hanya dibutuhkan di lingkungan lab.

R1(config)#interface FastEthernet0/0 R1(config-if)#ip address 192.168.1.1 255.255.255.0 R1(config-if)#description R1 LAN R1(config-if)#no shutdown	Mengulangi perintah konfigurasi interface pada interface yang lain yang butuh dikonfigurasi. Pada contoh topology, interface fastethernet butuh dikonfigurasi

Basic Router Configuration Command Syntax	
Configuring an interface	Router(config)#interface *type number*
	Router(config-if)#ip address *address mask*
	Router(config-if)#description *description*
	Router(config-if)#no shutdown
Saving changes on a router	Router#copy running-config startup-config
Examining the output of show commands	Router#show running-config
	Router#show ip route
	Router#show ip interface brief
	Router#show interfaces

Gambar 1.23. syntax perintah dasar konfigurasi router

Deskripsi dibatasi sampai 240 characters. Pada production networks deskripsi dapat membantu dalam menyediakan informasi untuk troubleshooting tentang tipe jaringan yang menghubungkan interface dan jika terdapat router lainnya pada suatu jaringan.

Setelah mengkonfigurasi IP address dan deskripsi. Interface juga harus dihubungkan ke alat lain (hub, switch, router yang lain) untuk mengaktifkan Physical Layer.

Catatan: Ketika menghubungkan dengan kabel point-to-point serial link saat di lingkungan lab, akhir satu kabel ditandai dengan DTE dan yang lainnya DCE.

Setiap interface kepunyaan jaringan yang berbeda

Perhatikan bahwa setiap interface harus terhubung ke jaringan yang berbeda. Walaupun IOS memungkinkan untuk mengkonfigurasi IP address dari jaringan yang sama pada dua interface yang berbeda, router tidak akan mengaktifkan interface kedua.

Contoh, bagaimana mengkonfigurasi interface FastEthernet 0/1 pada R1 dengan IP addres 192.168.1.0/24 pada jaringan? FastEthernet 0/0 telah terhubung dengan jaringan yang sama. Jika mencoba mengkonfigurasi interface yang lain, pesan ini akan tampil:

```
R1(config)#interface FastEthernet0/1
R1(config-if)#ip address 192.168.1.2 255.255.255.0
192.168.1.0 overlaps with FastEthernet0/0
```

Jika mencoba me-enable kan interface dengan perintah no shutdown, pesan berikut akan tampil:

```
R1(config-if)#no shutdown
192.168.1.0 overlaps with FastEthernet0/0
FastEthernet0/1: incorrect IP address assignment
```

Perhatikan output dari perintah show ip interface brief menunjukkan bahwa interface kedua dikonfigurasi untuk jaringan 192.168.1.0/24, Fasethernet 0/1 masih mati.

```
R1#show ip interface brief
<output omitted>
FastEthernet0/1 192.168.1.2 YES manual administratively down down
```

Memeriksa Konfigurasi Dasar Router

Semua perintah konfigurasi dasar router telah dimasukkan dan secepatnya disimpan di file running configuration milik R1. File Running-config disimpan dalam RAM dan file konfigurasi digunakan oleh IOS.

R1#show running-config	Langkah selanjutnya memeriksa perintah yang telah dimasukkan dengan menampilkan konfigurasi yang sedang berjalan dengan perintah berikut:
R1#copy running-config startup-config	Setelah konfigurasi router lengkap dan dicoba, sangat penting menyimpan running-config ke startup-config sebagai file konfigurasi yang permanen.
R1#show running-config	Perintah ini menampilkan konfigurasi yang sedang berjalan dan disimpan di RAM. Dengan beberapa pengecualian, semua perintah konfigurasi yang

	digunakan akan dimasukkan ke running-config dan diterapkan secepatnya oleh IOS.
R1#show ip route	Perintah ini menampilkan routing table yang sedang digunakan IOS untuk memilih jalur terbaik ke destination networks. Pada saat ini R1 hanya punya router yang terhubung langsung ke jaringan melalui interface nya sendiri.
R1#show interfaces	Perintah ini menampilkan semua konfigurasi parameter dan statistic dari interface.
R1#show ip interface brief	Perintah ini menampilkan informasi konfigurasi interface secara singkat, termasuk IP address dan status interface. Perintah ini merupakan tool yang berguna untuk troubleshooting dan cara cepat menentukan status dari semua router interface.

Setelah perintah konfigurasi dasar dimasukkan, sangat penting menyimpan running-config ke nonvolatile memory, NVRAM dari router. Dengan begitu, bila kehabisan daya, atau secara tidak sengaja di reload, router akan boot dengan konfigurasi yang sedang berjalan.

Bab 2

Static Routing

2.1 Pendahuluan

Routing adalah inti dari setiap data network, memindahkan informasi di sebuah internetwork dari sumber ke tujuan. Router adalah perangkat yang bertanggung jawab untuk malakukan transfer paket dari satu jaringan ke yang berikutnya [1].

Seperti yang kita pelajari dalam bab sebelumnya, router belajar tentang remote network baik secara dinamis menggunakan protokol routing atau secara manual dengan menggunakan rute statis. Dalam banyak kasus router menggunakan kombinasi dari kedua protokol routing dinamis dan rute statis. Bab ini berfokus pada routing statis.

Role of the Router

Router adalah komputer dengan tujuan khusus yang memainkan peran penting dalam pengoperasian setiap data network. Tugas utama dari router adalah bertanggung jawab untuk interkoneksi network dengan cara :

- Menentukan jalur terbaik untuk mengirim paket.
- Forwarding paket menuju network tujuan.

Router melakukan forwarding paket dengan belajar tentang remote network dan menjaga informasi routing. Router adalah persimpangan atau perempatan yang menghubungkan beberapa IP network. Keputusan forwarding router primer didasarkan pada Layer 3 informasi, alamat IP tujuan [5].

2.2 Static Routes With " Next Hop " Address

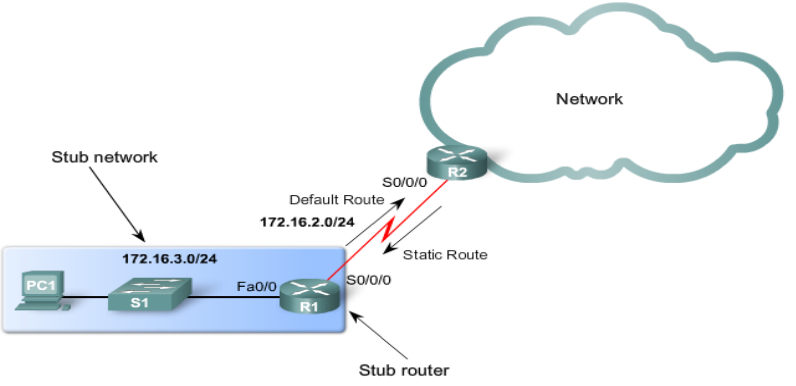
Purpose and Command Syntax of ip route

Sebagaimana telah kita bahas sebelumnya, router dapat belajar tentang remote network dengan dua cara, yaitu :

- Secara manual, dari rute statis dikonfigurasi
- Secara otomatis, dari protokol routing dinamis

Static routes

Static routes umumnya digunakan ketika routing dari sebuah network ke stub network. Sebuah stub network merupakan jaringan yang diakses oleh rute tunggal. Sebagai contoh, lihat gambar. Di sini kita melihat bahwa setiap jaringan terpasang ke R1 hanya akan memiliki satu cara untuk mencapai tujuan lain, baik ke jaringan melekat pada R2 atau ke tujuan luar R2. Oleh karena itu, jaringan 172.16.3.0 adalah jaringan stub dan R1 adalah stub router.



Menjalankan sebuah protokol routing antara R1 dan R2 adalah suatu pemborosan sumber daya karena R1 hanya memiliki satu jalan keluar untuk mengirimkan non-local traffic. Oleh karena itu, static route dikonfigurasi untuk konektivitas ke jaringan remote yang tidak langsung terhubung ke

router. Sekali lagi, mengacu pada gambar, kita akan mengkonfigurasi static route pada R2 ke LAN yang berada di R1. Kita juga akan melihat bagaimana mengkonfigurasi default static route dari R1 ke R2 sehingga R1 dapat mengirimkan traffic ke tujuan manapun di luar R2.

The ip route command

Perintah yang digunakan untuk mengkonfigurasi static route adalah **ip route**. Sintaks lengkap untuk mengkonfigurasi static route adalah:

```
Router(config)# ip route network-address subnet-mask
{ip-address | exit-interface }
```

Parameter	Description
network-address	Destination network address of the remote network to be added to the routing table.
subnet-mask	Subnet mask of the remote network to be added to the routing table. The subnet mask can be modified to summarize a group of networks.
ip-address	Commonly referred to as the next-hop router's IP address.
exit-interface	Outgoing interface that is used to forward packets to the destination network.

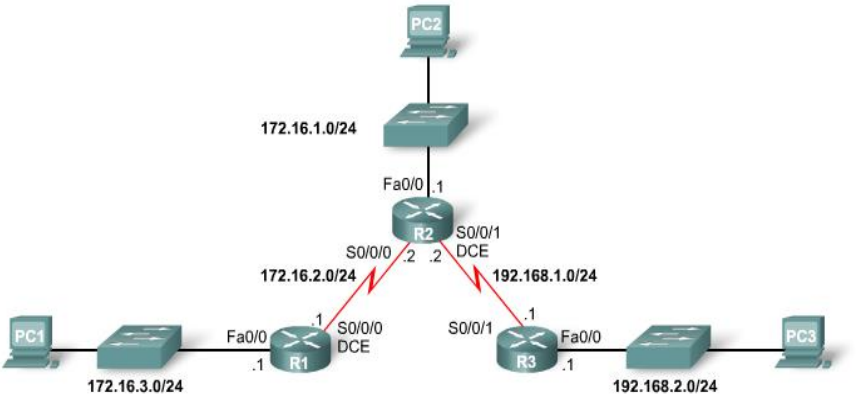
2.3 Configuring Static Routes

Ingat R1 tahu tentang directly connected networks . Ini adalah rute saat ini dalam tabel routing. Jaringan remote yang R1 tidak tahu tentang adalah:

172.16.1.0/124 - The LAN on R2

192.168.1.0/24 - The serial network between R2 and R3

192.168.2.0/24 - The LAN on R3



Pertama, aktifkan debug ip routing untuk menampilkan pesan ketika rute baru ditambahkan ke tabel routing. Kemudian, gunakan perintah ip route untuk mengkonfigurasi rute statis pada R1 untuk masing-masing jaringan. Angka tersebut menunjukkan rute pertama dikonfigurasi.

R1#debug ip routing

R1#conf t

R1(config)#ip route 172.16.1.0 255.255.255.0 172.16.2.2

Mari kita lihat setiap elemen dalam output ini:

- **ip route** - Static route command
- **172.16.1.0** - Network address of remote network
- **255.255.255.0** - Subnet mask of remote network
- **172.16.2.2** - Serial 0/0/0 interface IP address on R2, which is the "next-hop" to this network

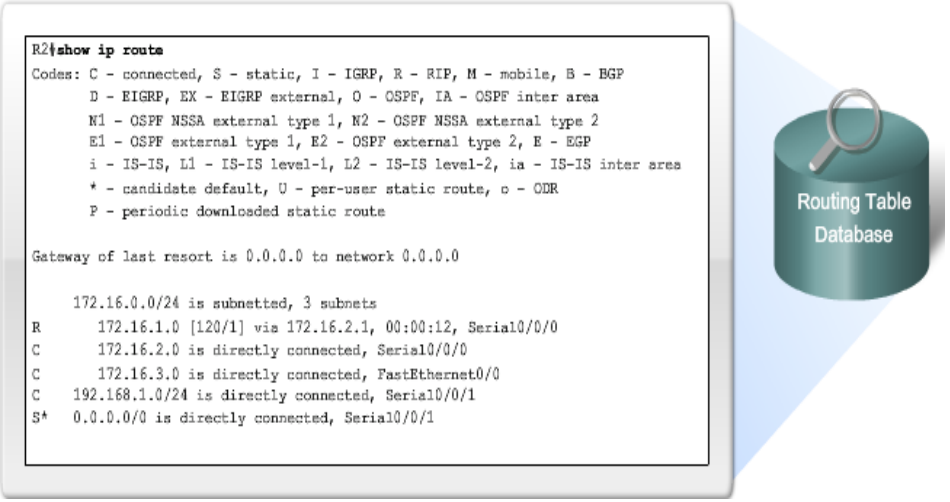
Bab 3

Tabel Routing

3.1 Pendahuluan

Sebagai administrator jaringan, sangatlah penting untuk mengetahui *routing table* secara mendalam,baik ketika terjadi troubleshooting masalah jaringan atau masalah lainya. Memahami struktur dan *lookup process* tabel routing akan membantu mendiagnosa masalah apapun yang ada dalam tabel routing - terlepas dari hubungan dengan protokol routing tertentu. Sebagai contoh, Anda mungkin menghadapi situasi di mana tabel routing memiliki semua rute yang diharapkan untuk memforward packet, tetapi paket forwarding tidak melakukan seperti yang diharapkan. Mengetahui bagaimana langkah melalui lookup process dari alamat IP tujuan untuk sebuah paket akan memberikan anda kemampuan untuk mendiagnosa apakah paket sedang diteruskan seperti yang diharapkan, jika dan mengapa paket sedang dikirim di tempat lain, atau jika paket telah dibuang.

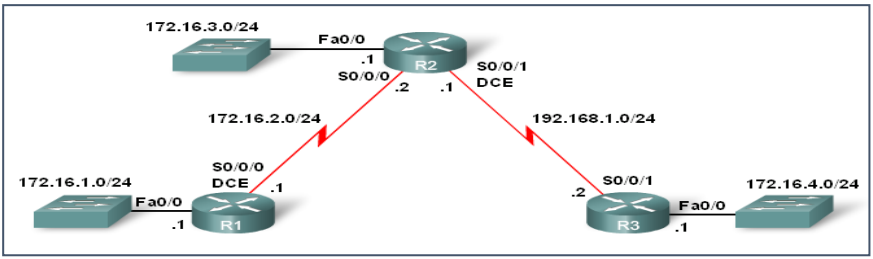
Dalam bab ini, kita akan melihat lebih dekat tentang *routing table*. Bagian pertama bab ini berfokus pada struktur Cisco's IP routing table Kami akan memeriksa format dari tabel routing dan belajar tentang tingkat 1 dan tingkat 2 rute. Bagian kedua bab ini menganalisis proses lookup dari tabel routing. Kita akan membahas perilaku routing yang classful, serta perilaku routing classless, dengan menggunakan perintah **no ip classless** dan perintah **ip classless** [6].



Gambar 8.1 Show ip route

3.2 Lab Topology

Dalam bab ini, kita akan menggunakan tiga buah router, seperti yang ditunjukkan pada gambar dibawah ini. R1 dan R2 menggunakan 172.16.0.0/16 umum dengan subnet 172.16.0.0/24. R2 dan R3 dihubungkan oleh jaringan 192.168.1.0/24. Perhatikan bahwa R3 juga memiliki subnet 172.16.4.0/24 yang terputus, atau tidak berhubungan, dari share network 172.16.0.0 yang R1 dan R2. Efek dari subnet yang tidak berhubungan akan dibahas kemudian dalam bab ini ketika kita melihat proses pencarian rute.



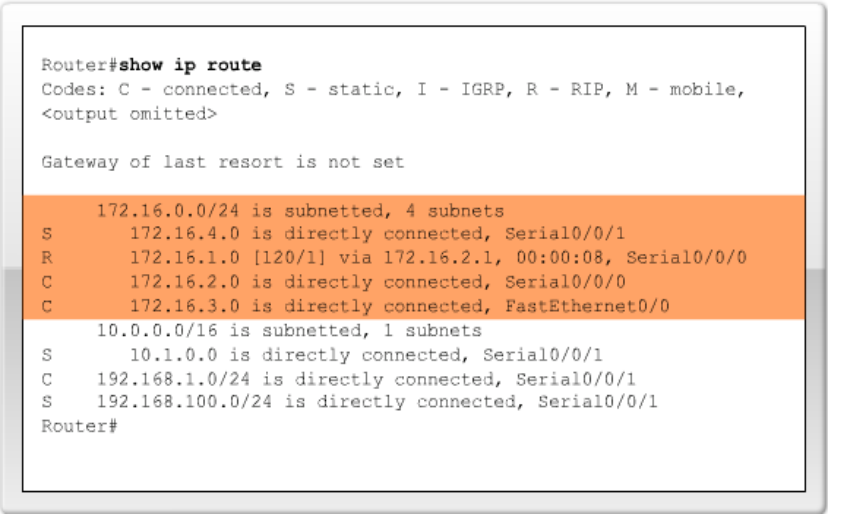
Gambar 8.1 Lab Topology

3.3 Routing Table Entries

Contoh tabel routing pada gambar terdiri dari entri rute dari sumber-sumber berikut:

- Directly connected networks
- Static routes
- Dynamic routing protocols

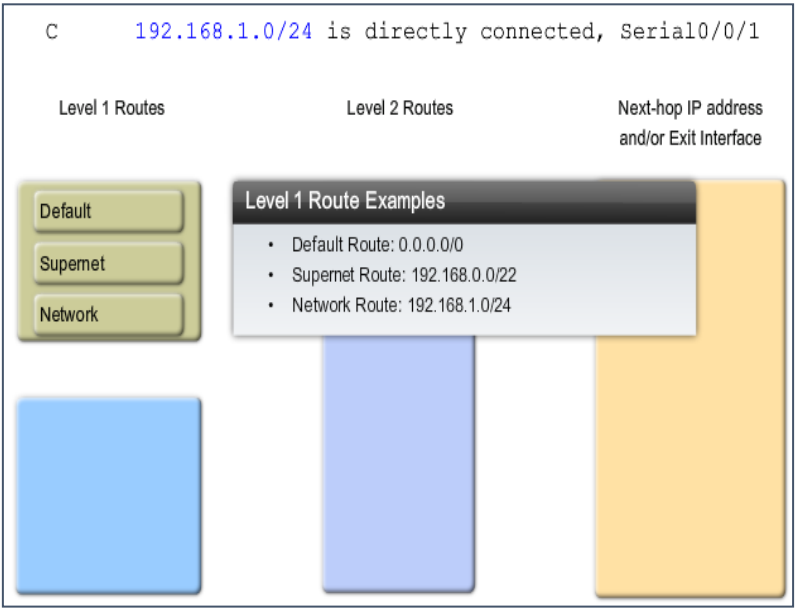
Sumber rute tidak mempengaruhi struktur dari tabel routing. Angka ini menunjukkan tabel contoh routing dengan directly connected, static, and dynamic routes.. Perhatikan bahwa subnet 172.16.0.0/24 memiliki kombinasi dari semua tiga jenis sumber routing.



Gambar 8.2 Sample Routing Table

Level 1 rute rute dengan subnet mask sama dengan atau kurang dari classful mask dari alamat network. 192.168.1.0/24 adalah level 1 rute network, karena subnet masknya sama untuk menutupi classful jaringan. / 24 adalah classful mask untuk network kelas C, seperti jaringan 192.168.1.0.
level 1 rute dapat berfungsi sebagai :

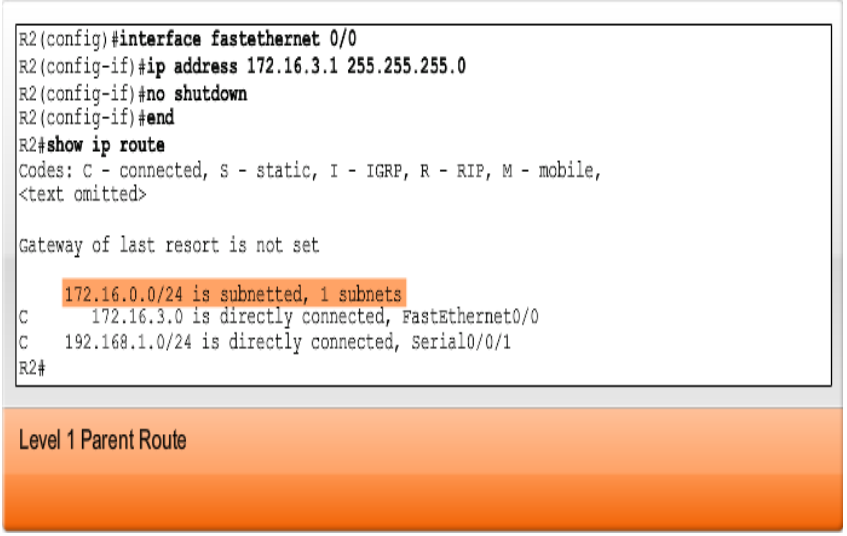
- Default route adalah Sebuah rute default adalah rute statis dengan alamat 0.0.0.0 / 0.
- Supernet route adalah alamat jaringan dengan mask kurang dari classful mask.
- Network route adalah rute yang memiliki subnet mask yang sama dengan yang classful mask. Sebuah rute jaringan juga dapat menjadi parent route. Parent routes akan dibahas pada bagian berikutnya.



Gambar 8.3 Routing Table : level 1 Route

3.4 Parent and Child Routes

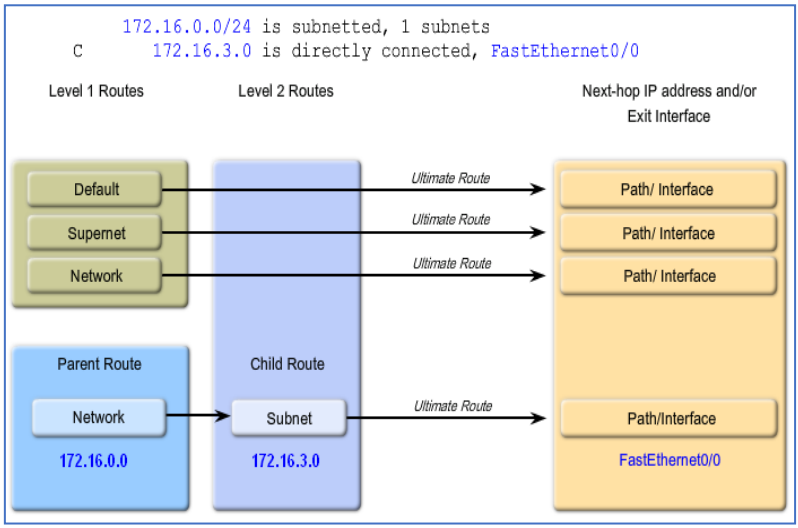
Pada topik sebelumnya, kita melihat level 1 rute network yang juga merupakan rute utama. Sekarang mari kita lihat jenis lain dari level 1 rute network, parent route. Angka ini menunjukkan konfigurasi dari interface 172.16.3.1/24 pada R2 dan output dari perintah show ip route. Perhatikan bahwa sebenarnya ada dua entri tambahan dalam tabel routing. Satu entri adalah parent route dan entri lain adalah child route. Mengapa ada dua entri bukan satu?



Gambar 8.4 Parent and Child Route

Ketika subnet 172.16.3.0 ditambahkan ke tabel routing, rute yang lain, 172.16.0.0, juga ditambahkan. Entri pertama, 172.16.0.0/24, tidak berisi hop berikutnya alamat IP atau informasi yang exit interface. Rute ini dikenal sebagai level 1 parent route.

- Level 1 parent route adalah rute jaringan yang tidak mengandung next-hop IP address atau exit interface untuk network apapun.
- level 2 route adalah rute yang merupakan subnet dari alamat classful network.



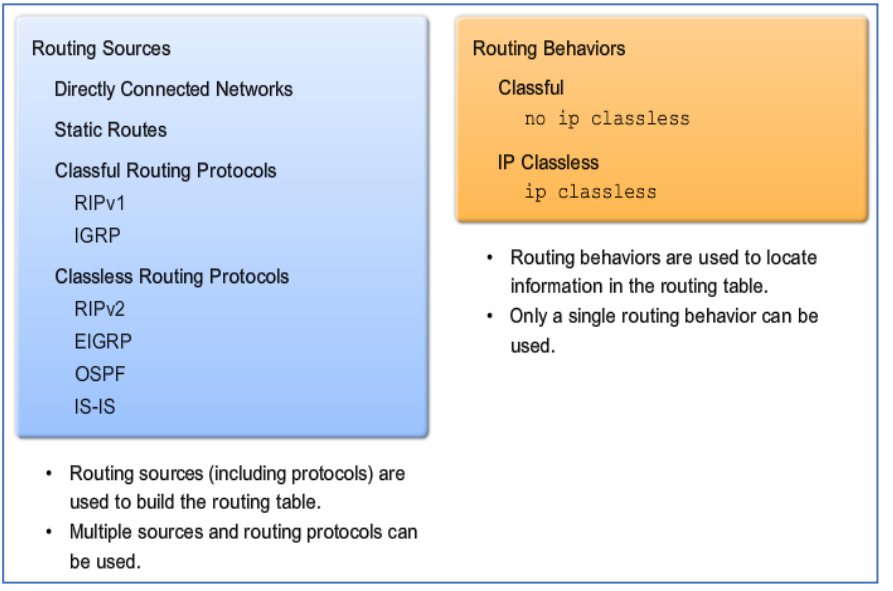
Gambar 8.5 Routing Table: Parent/Child Relationship

Dibawah ini adalah tabel yang menunjukkan perbedaan classful dan classless routing protocol level 1 parents route.

Network Type	**Parent route's Classful mask is Displayed**	**Term variably subnetted is seen in parent route in routing table**	**Includes the # of different masks of child routes**	**Subnet mask included with each child route entry**
Class-ful	No	No	No	No
Class-less	Yes	Yes	Yes	Yes

3.5 Classful And Classless Routing Behavior

Perilaku Classless and classful routing tidak sama dengan classless and classful routing protocols. Classful and classless routing protocols mempengaruhi bagaimana tabel routing diisi. Perilaku Classful and classless routing menentukan bagaimana tabel routing dicari setelah diisi. Dalam gambar, sumber routing (termasuk classful and classless routing protocols) adalah input yang digunakan untuk mengisi tabel routing. Perilaku routing, ditentukan dengan perintah **ip classless or no ip classless**, menentukan bagaimana proses pencarian rute akan dilanjutkan pada Langkah 3 [6].



Gambar 8.6 Routing Protocols vs Routing Behaviors

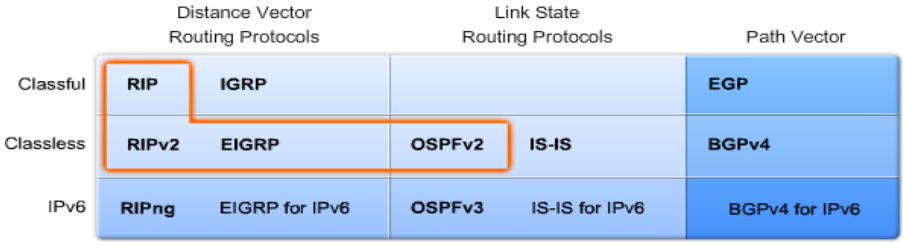
Seperti yang Anda lihat, perilaku routing protokol dan routing benar-benar independen satu sama lain. Tabel routing bisa diisi dengan rute dari sebuah classless routing protocol RIPv2 dan tidak seperti pada classful routing protocol karena tidak ada perintah no ip classless yang dikonfigurasi.

Bab 4

Distance Vector Routing Protocol

4.1 Pendahuluan

Bab-bab routing dinamis ini tentu saja fokus pada Interior Gateway Protokol (IGPs). Seperti dibahas dalam Bab 3, IGPs diklasifikasikan sebagai distance vector atau link-state routing protokol. Bab ini menjelaskan karakteristik, operasi, dan fungsi dari protokol routing distance vector. Ada keuntungan dan kerugian untuk menggunakan semua jenis protokol routing. Oleh karena itu, kondisi yang mempengaruhi operasi protokol distance vector dan perangkap operasi distance vector protokol - bersama dengan obat untuk mengatasi jebakan tersebut. Memahami operasi distance vector routing adalah hal yang sangat peting, memverifikasi, dan pemecahan masalah protokol ini [8].



Gambar 4.1 Distance vector routing protocols

Dynamic routing protokol membantu administrator jaringan mengatasi proses routing yang memakan waktu dan menuntut mengkonfigurasi yang panjang dari pada mempertahankan rute statis. Sebagai contoh, dapat Anda bayangkan mempertahankan konfigurasi routing statis dari 28 router. Apa yang terjadi ketika link down? Bagaimana Anda memastikan bahwa ada jalur ganda yang tersedia? Dynamic routing adalah pilihan yang paling umum untuk jaringan besar. Distance vector routing protocols termasuk RIP, IGRP, dan EIGRP.

4.2 Distance Vector Routing Protocols

RIP

Routing Information Protocol (RIP) pada awalnya ditentukan dalam RFC 1058. Ini memiliki karakteristik utama sebagai berikut [7]:

- Hop count digunakan sebagai metrik untuk pemilihan path.
- Jika jumlah hop untuk jaringan lebih besar dari 15, RIP tidak dapat menyediakan rute ke jaringan tersebut.
- Routing update broadcast atau multicast setiap 30 detik, secara default.

IGRP

Interior Gateway Routing Protocol (IGRP) adalah sebuah protokol proprietary yang dikembangkan oleh Cisco. IGRP memiliki karakteristik desain utama berikut:

- Bandwidth, delay, load and reliability adalah komponen yang digunakan untuk membuat komposit metrik.
- Update routing disiarkan setiap 90 detik, secara default.
- IGRP adalah pendahulu EIGRP.

EIGRP

Enhanced IGRP (EIGRP) adalah Cisco proprietary distance vector routing protocol. EIGRP memiliki karakteristik sebagai berikut :

- EIGRP dapat load balancing dengan biaya beban yang tidak setara.

- Algoritma yang digunakan adalah Diffusing Update Algorithm (DUAL) untuk menghitung jalur terpendek.
- Tidak ada update periodik sepetti RIP dan IGRP. Routing update dikirim hanya jika ada perubahan dalam topologi.

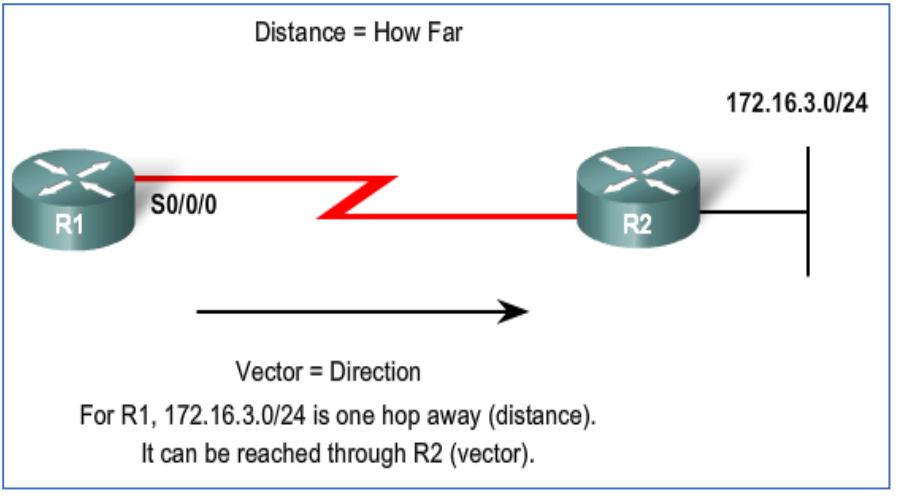
4.3 Distance Vector Technology

Seperti namanya, distance vector berarti bahwa rute yang hitung adalah vektor jarak dan arah. Jarak didefinisikan dalam hal metrik seperti jumlah hop dan arah hanyalah arah hop berikutnya-router atau exit interface.

Sebuah router yang menggunakan distance vector routing protocol tidak memiliki pengetahuan tentang seluruh jalan ke network tujuan. Sebaliknya router hanya tahu:

- Arah atau interface yang mana paket harus diteruskan
- Jarak atau seberapa jauh ke network tujuan

Sebagai contoh, dalam gambar, R1 tahu bahwa jarak untuk mencapai jaringan 172.16.3.0/24 adalah 1 hop dan bahwa arahny keluar interface S0/0/0 ke R2.



Gambar 4.1 The meaning of distance vector

4.4 Operation of Distance Vector Routing Protocols

Beberapa protokol routing distance disebut router yang secara berkala menyiarkan informasi update routing ke seluruh tabel routing untuk setiap tetangganya. Metode ini tidak efisien karena update tidak hanya mengkonsumsi bandwidth tetapi juga mengkonsumsi sumber daya CPU router untuk proses update.

Distance routing protokol memiliki karakteristik tertentu [8].

Periodic Updates

Pengiriman update routing secara berkala (30 detik untuk RIP dan 90 detik untuk IGRP). Bahkan jika topologi tidak berubah dalam beberapa hari, update periodik terus dikirim ke semua tetangga.

Neighbors

Router tetangga yang berbagi link dan dikonfigurasi untuk menggunakan protokol routing yang sama. Router hanya mengetahui alamat interface network sendiri dan alamat network remote yang dapat dicapai melalui tetangganya. Ini tidak memiliki pengetahuan yang lebih luas dari topologi network. Router menggunakan routing distance vector dan tidak mengetahui topologi jaringan.

Broadcast Updates

Update broadcast dikirim ke 255.255.255.255. Router tetangga yang dikonfigurasi dengan protokol routing yang sama akan mendapatkan proses update. Semua perangkat lain juga akan mendapatkan proses update sampai ke Layer 3 sebelum membuang packet broadcast. Beberapa protokol routing distance vector menggunakan alamat multicast bukan alamat broadcast.

Entire Routing Table Updates

Update Tabel Routing keseluruh network, dengan beberapa pengecualian yang akan dibicarakan nanti, secara berkala ke semua tetangga. Semua tetangga menerima update ini secara keseluruhan untuk menemukan informasi terkait dan membuang sisanya. Beberapa routing distance vector protokol seperti EIGRP tidak mengirimkan update routing tabel secara periodik.

Routing Protocols Characteristics

Routing protocols dapat dibandingkan berdasarkan karakteristik sebagai berikut :

Time to Convergence

Waktu untuk konvergensi mendefinisikan seberapa cepat router dalam topologi network berbagi informasi routing dan mencapai keadaan pengetahuan yang konsisten. Semakin cepat konvergensi, semakin disukai protokol tersebut. Routing loop dapat terjadi bila tabel routing tidak konsisten dan tidak diperbarui karena akan memperlambat konvergensi dalam sebuah network.

Scalability

Skalabilitas mendefinisikan seberapa besar jaringan dapat menjadi dasar pada protokol routing yang digunakan. Semakin besar jaringan, protokol yang lebih scalable untuk routing yang sangaty diperlukan.

Classless (Use of VLSM) or Classful

Classless routing protocols termasuk update subnet mask. Fitur ini mendukung penggunaan Variable Length Subnet Masking (VLSM) dan summarization rute yang lebih baik. Protokol routing classful tidak termasuk subnet mask update dan tidak dapat mendukung VLSM.

Resource Usage

Penggunaan sumber daya salah satu persyaratan dari sebuah routing protocol, seperti ruang memori, penggunaan CPU, dan pemanfaatan link bandwidth. Kebutuhan sumber daya yang lebih tinggi memerlukan hardware yang lebih kuat untuk mendukung operasi protokol routing di samping paket forwarding.

Implementation and Maintenance

Implementasi dan pemeliharaan menggambarkan tingkat pengetahuan yang diperlukan untuk administrator jaringan untuk menerapkan dan memelihara jaringan berbasis pada protokol routing yang digunakan.

Advantages:	Disadvantages:
Simple implementation and maintenance. The level of knowledge required to deploy and later maintain a network with distance vector protocol is not high.	**Slow convergence.** The use of periodic updates can cause slower convergence. Even if some advanced techniques are used, like triggered updates which are discussed later, the overall convergence is still slower compared to link state routing protocols.
Low resource requirements. Distance vector protocols typically do not need large amounts of memory to store the information. Nor do they require a powerful CPU. Depending of the network size and the IP addressing implemented they also typically do not require a high level of link bandwidth to send routing updates. However, this can become an issue if you deploy a distance vector protocol in a large network.	**Limited scalability.** Slow convergence may limit the size of the network because larger networks require more time to propagate routing information.
	Routing loops. Routing loops can occur when inconsistent routing tables are not updated due to slow convergence in a changing network.

Gambar 4.2

Bab 5

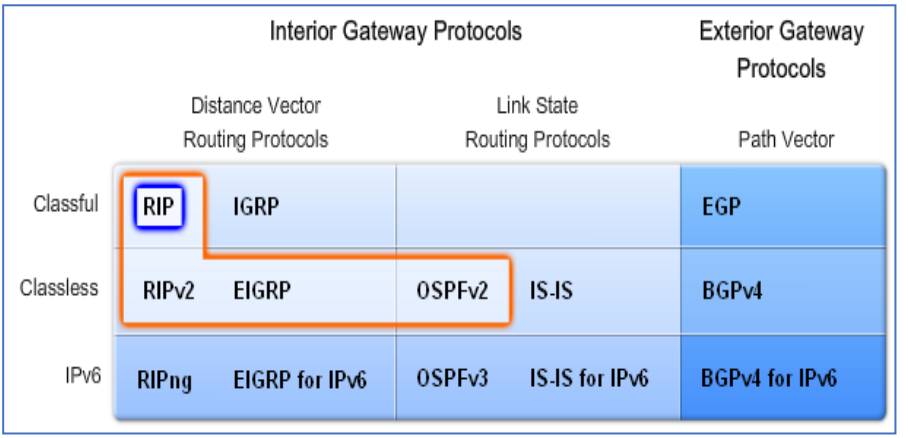
Routing Information Protocol Versi 1 (RIP v1)

5.1 Pendahuluan

Selama bertahun-tahun, protokol routing telah berevolusi untuk memenuhi tuntutan peningkatan jaringan yang kompleks. Protokol pertama digunakan adalah Routing Information Protocol (RIP). RIP masih menikmati popularitas karena kesederhanaan dan dukungan luas.

Memahami RIP penting untuk studi jaringan Anda untuk dua alasan. Pertama, RIP masih digunakan sampai sekarang. Anda mungkin menghadapi implementasi jaringan yang cukup besar membutuhkan sebuah routing protocol, tapi cukup sederhana untuk digunakan RIP efektif. Kedua, keakraban dengan banyak konsep dasar RIP akan membantu Anda untuk membandingkan RIP dengan protokol lain. Memahami bagaimana RIP beroperasi dan pelaksanaannya akan membuat belajar lebih mudah protokol routing lain.

Bab ini mencakup rincian versi pertama RIP, termasuk sedikit sejarah, RIPv1 karakteristik, operasi, konfigurasi, verifikasi, dan pemecahan masalah. Sepanjang bab, Anda dapat menggunakan Packet Tracer untuk mempraktekkan apa yang Anda pelajari. Pada akhir bab, three hands-on labs dan Packet Tracer Skills Integrasi ini disediakan untuk membantu Anda mengintegrasikan RIPv1 ke pengetahuan dan keterampilan network.



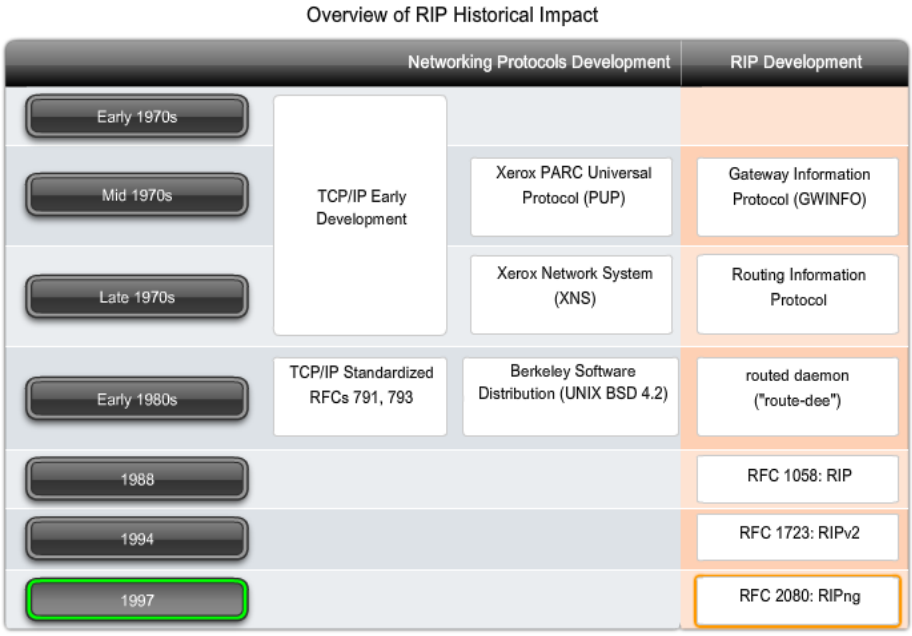
Gambar 5.1 RIP Version 1

5.2 Background and Perspective

RIP Historical Impact

RIP adalah protocol routing yang tertua dari distance vector routing protocols. Meskipun RIP tidak memiliki kecanggihan yang lebih dari protokol routing yang lebih canggih, kesederhanaan dan terus digunakan secara luas adalah bukti umur panjang. RIP bukan protokol "on the way out". Bahkan, bentuk IPv6 RIP disebut RIPng (generasi berikutnya) sekarang tersedia [9].

RIP berevolusi dari protokol sebelumnya dikembangkan di Xerox, yang disebut Gateway Information Protocol (GWINFO). Dengan perkembangan Sistem Jaringan Xerox (XNS), GWINFO berkembang menjadi RIP. Ini kemudian mendapatkan popularitas karena dilaksanakan dalam Berkeley Software Distribution (BSD) sebagai daemon bernama routed (pronounced "route-dee", not "rout-ed"). Berbagai vendor lainnya membuat mereka sendiri, implementasi RIP sedikit berbeda. Menyadari perlunya standarisasi protokol, Charles Hedrick menulis RFC 1058 pada tahun 1988, di mana ia mendokumentasikan protokol yang ada dan ditetapkan beberapa perbaikan. Sejak itu, RIP telah diperbaiki dengan RIPv2 pada tahun 1994 dan dengan RIPng pada tahun 1997.

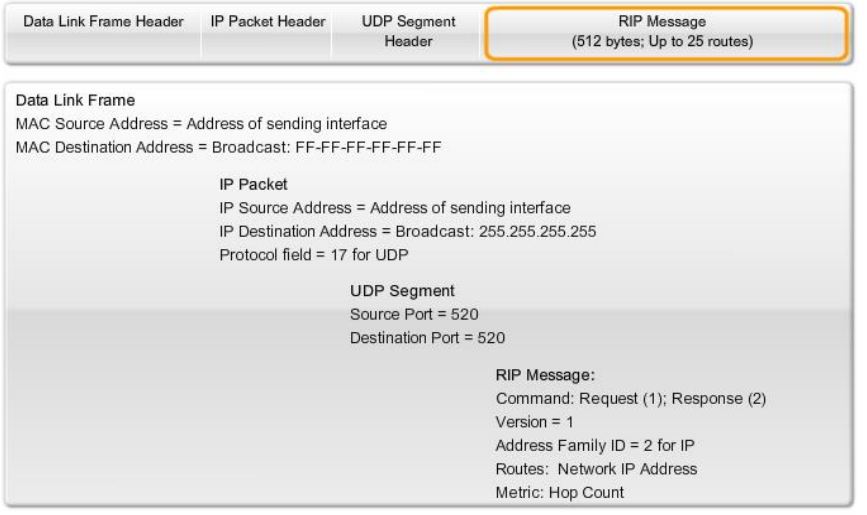


Gambar 5.2 Rip Historical Impact

RIP Characteristics

Seperti dibahas dalam Bab 4, "Distance Vector Routing Protokol," RIP mempunyai karakteristik utama sebagai berikut:

- RIP adalah protokol routing vektor jarak.
- RIP menggunakan hop count hanya sebagai metrik untuk pemilihan path.
- Rute dengan jumlah hop diiklankan lebih besar dari 15 yang terjangkau.
- Pesan disiarkan setiap 30 detik.



Gambar 5.3 Encapsulated RIPv1 Message

Bagian data dari pesan RIP dienkapsulasi menjadi segmen UDP, dengan kedua sumber dan nomor port tujuan diatur ke 520. Header IP dan header data link menambahkan alamat broadcast tujuan sebelum pesan dikirim ke semua interface dikonfigurasi RIP.

RIP Operation

RIP menggunakan dua jenis pesan tertentu yaitu **Request message** and **Response message**. Setiap interface RIP-dikonfigurasi mengirimkan sebuah pesan permintaan pada startup, meminta agar semua tetangga RIP mengirimkan tabel routing mereka lengkap. Sebuah pesan respon yang dikirim kembali oleh RIP-enabled tetangga. Ketika router menerima tanggapan meminta, ia akan mengevaluasi setiap entri rute. Jika entri rute baru, router menerima menginstal route di routing table. Jika rute tersebut sudah dalam tabel, entri yang ada diganti jika entri baru memiliki hop count yang lebih baik. Startup router kemudian mengirimkan update ke semua infterce RIP-enabled yang mengandung tabel routing sendiri sehingga tetangga RIP dapat diinformasikan dari setiap rute baru [9].

Anda mungkin ingat dari penelitian sebelumnya bahwa IP address yang ditentukan sebagai host address pada awalnya dibagi menjadi 3 kelas: kelas A, kelas B, dan kelas C. Setiap kelas memiliki subnet mask default. Mengetahui

subnet mask standar untuk setiap kelas adalah penting untuk memahami bagaimana RIP beroperasi.

RIP adalah protokol routing classful. Seperti Anda mungkin telah menyadari dari diskusi format pesan sebelumnya, RIPv1 tidak mengirimkan informasi subnet mask di update. Oleh karena itu, router yang menggunakan subnet mask dikonfigurasi pada interface lokal, atau menerapkan subnet mask standar berdasarkan kelas alamat. Karena keterbatasan ini, network RIPv1 tidak dapat berhubungan dan tidak dapat mengimplementasikan VLSM. IP Addressing dibahas lebih lanjut dalam Bab 6, "VLSM dan CIDR."

Administrative Distance

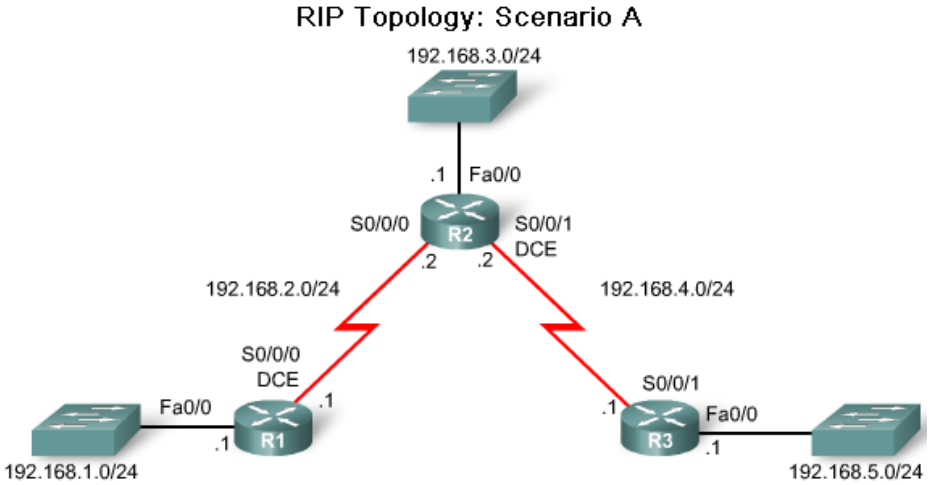
Seperti yang Anda ketahui dari Bab 3, "Pengantar Protokol Routing Dinamis," administrative distance (AD) adalah kepercayaan (atau preferensi) dari sumber rute. RIP memiliki jarak standar administratif 120. Bila dibandingkan dengan protokol gateway interior, RIP adalah protocol yang paling-tinggi administrative distance (AD). IS-IS, OSPF, IGRP, dan EIGRP semua memiliki nilai default AD lebih rendah. Ingat, Anda dapat memeriksa administrative distance dengan menggunakan perintah **show ip route** or **show ip protocols.**

```
R3#show ip protocols
Routing Protocol is "rip"
  <output omitted>
  Redistributing: rip
  Default version control: send version 1, receive any version
    Interface             Send  Recv  Triggered RIP  Key-chain
    FastEthernet0/0       1     1 2
    Serial0/0/0           1     1 2
    Serial0/0/1           1     1 2
  Automatic network summarization is in effect
  Routing for Networks:
    192.168.4.0
    192.168.5.0
    192.168.6.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.6.2          120      00:00:10
    192.168.4.2          120      00:00:18
  Distance: (default is 120)
```

Gambar 5.4 Verifying administrative distance

5.3 Basic RIP Configuration

Angka ini menunjukkan topologi dengan tiga router yang kita digunakan dalam Bab 2, "Routing statis". Secara fisik, topologi adalah sama kecuali bahwa kita tidak perlu PC melekat pada LAN. Logikanya, bagaimanapun, skema pengalamatan yang digunakan berbeda. Kami menggunakan lima kelas alamat network C.



Gambar 5.5 RIP Topology

Tabel 5.1 Addressing table

Device	Interface	IP Address	Subnet Mask
R1	Fa0/0	192.168.1.1	255.255.255.0
	S0/0/0	192.168.2.1	255.255.255.0
R2	Fa0/0	192.168.3.1	255.255.255.0
	S0/0/0	192.168.2.2	255.255.255.0
	S0/0/1	192.168.4.2	255.255.255.0
R3	Fa0/0	192.168.5.1	255.255.255.0
	S0/0/1	192.168.4.1	255.255.255.0

Untuk mengaktifkan protokol routing dinamis, masukkan ke global configuration mode dan gunakan perintah **router**. Seperti ditunjukkan dalam gambar, jika Anda mengetik space diikuti dengan tanda tanya, daftar dari semua protokol routing yang tersedia akan tampil beserta IOS.

Untuk masuk ke dalam configuration mode pada router dengan protocol RIP, ketikkan perintah **router rip** pada global configuration prompt. Perhatikan bahwa prompt berubah dari global configuration prompt menjadi seperti dibawah ini :

R1(config-router)#

Perintah ini tidak langsung memulai proses RIP. Sebaliknya, ia menyediakan akses untuk mengkonfigurasi pengaturan rute protokol. Tidak ada routing update dikirim. Jika Anda perlu untuk menghapus proses routing RIP dari perangkat, gunakan perintah **no router rip**. Perintah ini menghentikan proses RIP dan menghapus semua konfigurasi RIP yang ada.

Dengan masuk kedalam configuration mode router RIP, router diinstruksikan untuk menjalankan RIP. Tetapi router masih perlu tahu interface lokal yang digunakan untuk komunikasi dengan router lainnya, serta yang terhubung ke network lokal untuk menginformasikan kepada router tetangga. Untuk mengaktifkan RIP routing pada sebuah network, gunakan perintah **network** dalam router configuration mode dan masukkan alamat network classful untuk setiap jaringan yang terhubung langsung.

Router(config-router)#network directly-connected-classful-network-address

Perintah **network** berfungsi untuk:

- Mengaktifkan RIP pada semua interface dengan network tertentu. Interface yang telah dikonfigurasi akan mengirim dan menerima update RIP.
- Menyebarkan setiap informasi routing pada semua router yang terkoneksi dengan mengirim routing update setiap 30 detik.

The network Command	
Purpose	▪ Enables the sending and receiving of RIP updates for interfaces that belong to the specified network ▪ Advertises the specified network in RIP updates
Syntax	`Router(config-router)#network directly-connected-classful-address`

Gambar 5.6 Network command syntax and purpose

Konfigurasi RIPv1 pada R1, R2 dan R3

R1(config)#router rip

R1(config-router)#network 192.168.1.0

R1(config-router)#network 192.168.2.0

R2(config)#router rip

R2(config-router)#network 192.168.2.0

R2(config-router)#network 192.168.3.0

R2(config-router)#network 192.168.4.0

R3(config)#router rip

R3(config-router)#network 192.168.4.0

R3(config-router)#network 192.168.5.1

5.4 Verifying RIP : Show ip route

Untuk memverifikasi dan memecahkan masalah routing, pertama kali gunakan peritah **show ip route** atau **show ip protocols**. Jika Anda tidak dapat mengisolasi masalah dengan menggunakan kedua perintah, kemudian gunakan **debug ip rip** untuk melihat apa yang terjadi. Ketiga perintah digunakan dalam melakukan verifikasi untuk melihat kemunkinan masalah yang terjadi dalam routing dan memecahkan masalah konfigurasi protokol routing. Ingat, sebelum

Anda mengkonfigurasi Routing apapun - apakah statis atau dinamis - pastikan semua interface yang diperlukan adalah "up" dan "up" dengan perintah show ip interface brief.

Perintah Show ip route memverifikasi bahwa rute yang diterima oleh tetangga RIP telah diinstal dalam tabel routing. **R** pada output menunjukkan rute yang digunakan adalah protocol RIP. Karena perintah ini menampilkan tabel routing secara keseluruhan, termasuk directly connected dan static routes , biasanya ini juga digunakan untuk memeriksa konvergensi. Rute mungkin tidak segera muncul saat Anda menjalankan perintah karena network membutuhkan waktu untuk melakukan konvergensi. Namun, setelah routing dikonfigurasi dengan benar pada semua router, perintah **show ip route** akan mencerminkan bahwa setiap router memiliki tabel routing penuh, dengan rute ke setiap network dalam topologi.

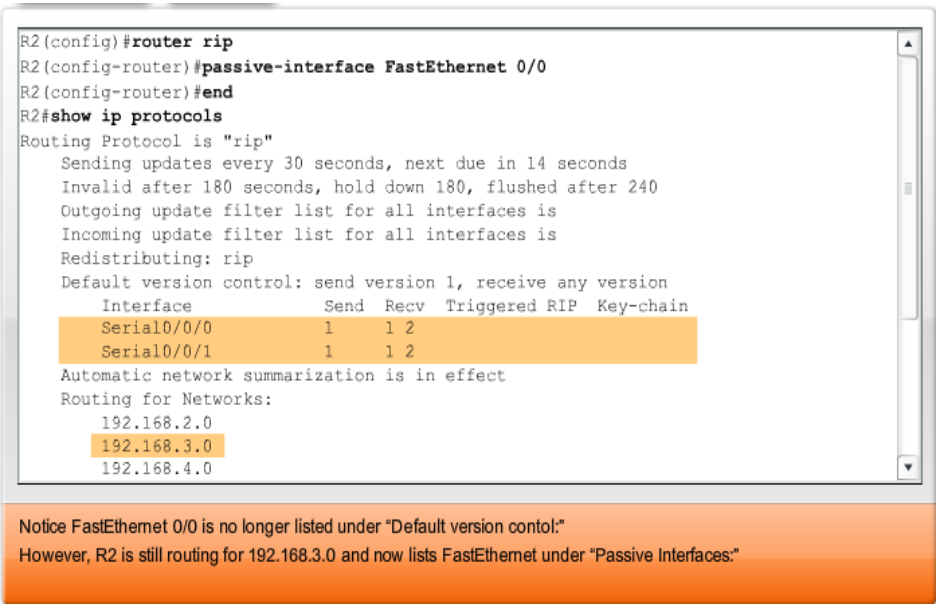
5.5 Passive Interface

Passive interfae digunakan untuk menonaktifkan pengirimin routing update ke router – router tetangga. Ada tiga alasan mengapa router tidak membutuhkan pengiriman update ke local area network atau router tetangga :

1. Mengoptimalkan penggunaan bandwidth karena bandwith digunakan untuk mengangkut update ke semua router. Karena update RIP selalu diforward, switch akan meneruskan update semua port.
2. Semua perangkat pada LAN harus proses update sampai ke lapisan Transport, di mana perangkat penerima akan membuang update.
3. Iklan update pada jaringan broadcast adalah risiko keamanan. Update RIP dapat disadap dengan software sniffing paket. Update routing dapat diubah dan dikirim kembali ke router, tabel routing merusak dengan metrik palsu yang menyesatkan lalu lintas.

Perintah yang digunakan untuk mengkonfigurasi router dengan passive interface adalah :

Router(config-router)#passive-interface interface-type interface-number



Gambar 5.7 Disabling updates with the passive-interface command

5.6 Automatic Summarization

Advantages of Automatic Summarization

Seperti yang kita lihat dengan R2 pada gambar sebelumnya, RIP update otomatis merangkum antara jaringan classful. Karena update 172.30.0.0 dikirim keluar sebuah interface (Serial 0/0/1) pada network classful berbeda (192.168.4.0), RIP mengirimkan hanya update tunggal untuk jaringan seluruh classful bukan satu untuk masing-masing yang berbeda subnet. Proses ini mirip dengan apa yang kita lakukan ketika dirangkum beberapa rute statis menjadi sebuah rute statis tunggal. Mengapa summarization otomatis menguntungkan ?

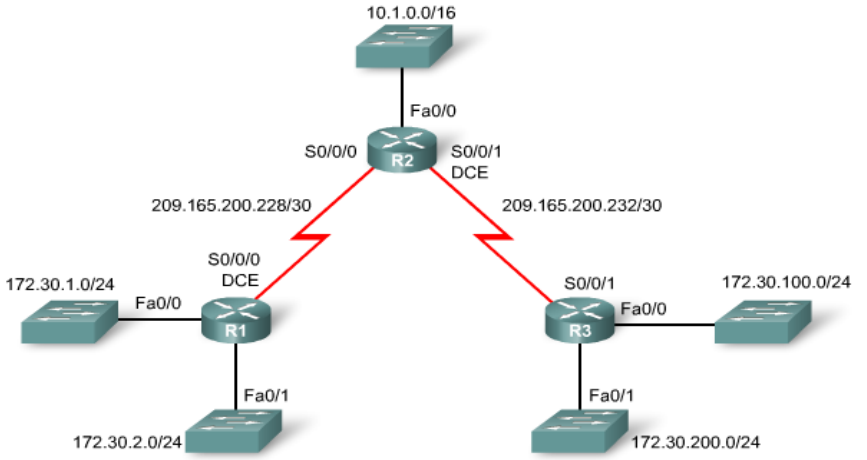
- Update routing yang lebih kecil yang dikirim dan diterima akan menggunakan bandwidth yang lebih sedikit untuk routing update antara R2 dan R3.
- R3 memiliki rute tunggal untuk jaringan 172.30.0.0/16, terlepas dari berapa banyak subnet ada atau bagaimana subnet.

Menggunakan rute tunggal dalam proses ini akan lebih cepat untuk melakukan lookup di tabel routing untuk R3.

Disadvantage of Automatic Summarization

Apakah ada kerugian untuk summarization otomatis? Ya, ketika ada jaringan yang tidak berhubungan dikonfigurasi dalam topologi network.

Protokol routing classful tidak menyertakan subnet mask dalam routing update. Jaringan secara otomatis diringkas melintasi batas-batas jaringan utama karena router akan menerima dan tidak dapat menentukan rute mask. Hal ini karena interface yang menerima harus memiliki mask yang berbeda dari rute subnet.



Gambar 5.8 Disadvantages to automatic summarization

Perhatikan bahwa R1 dan R3 keduanya memiliki subnet dari jaringan utama 172.30.0.0/16, sedangkan R2 tidak. Pada dasarnya, R1 dan R3 adalah batas router untuk 172.30.0.0/16 karena mereka dipisahkan oleh jaringan lain utama, 209.165.200.0/24. Pemisahan ini menciptakan jaringan tidak berhubungan, sebagai dua kelompok subnet 172.30.0.0/24 dipisahkan oleh setidaknya satu jaringan besar lainnya. 172.30.0.0/16 adalah jaringan tidak akan terkoneksi.

Bab 6

VLSM dan CIDR

6.1 Pendahuluan

Sebelum tahun 1981, alamat IP yang digunakan hanya 8 bit pertama untuk menentukan bagian network dari alamat, membatasi Internet - kemudian dikenal sebagai ARPANET - dengan 256 network. Awalnya sudah jelas bahwa ini tidak akan cukup untuk ruang alamat yang tersedia. Pada tahun 1981, RFC 791 diubah IPv4 32-bit alamat untuk memungkinkan tiga kelas yang berbeda atau ukuran dari network: kelas A, kelas B, dan kelas C. Kelas A alamat yang digunakan 8 bit untuk bagian network dari alamat, kelas B digunakan 16 bit, dan kelas C digunakan 24 bit. Format ini kemudian dikenal sebagai classful IP addressing.

Pengembangan awal dari classful dapat memecahkan masalah pembatasan 256 network - untuk sementara waktu. Satu dekade kemudian, menjadi jelas bahwa ruang alamat IP menipis dengan cepat. Sebagai tanggapan, Internet Engineering Task Force (IETF) memperkenalkan Classless Inter-Domain Routing (CIDR), yang digunakan Variable Length Subnet Masking (VLSM) untuk membantu menghemat ruang alamat [10].

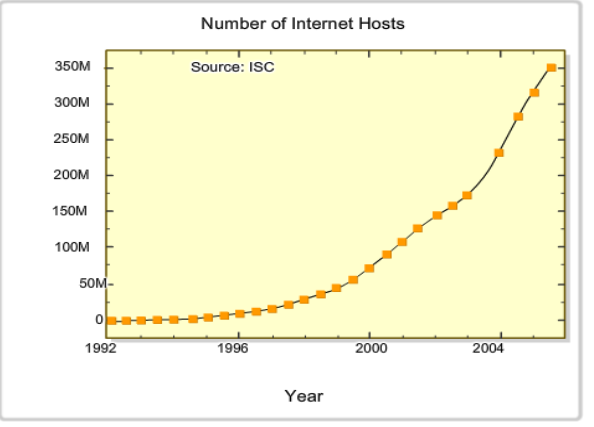
Dengan diperkenalkannya CIDR dan VLSM, ISP sekarang bisa menetapkan satu bagian dari jaringan classful untuk satu pelanggan dan bagian yang berbeda untuk pelanggan lain. Discontiguous address yang menjadi masalah dengan ISP disejajarkan dengan pengembangan classless routing protocols. Untuk membandingkan: classful routing protocols selalu meringkas pada batas classful dan tidak menyertakan subnet mask dalam routing update. Classless

routing protocols selalu menyertakan subnet mask dalam routing update dan tidak diharuskan untuk melakukan summarization. classless routing protocols yang dibahas dalam kursus ini adalah RIPv2, EIGRP dan OSPF.

Dengan diperkenalkannya VLSM dan CIDR, administrator jaringan harus menggunakan subnetting sebagai keterampilan tambahan. VLSM subnetting hanyalah subnet. Subnet dapat lebih dari satu subnet dalam beberapa tingkat, karena Anda akan belajar dalam bab ini. Selain subnetting, menjadi mungkin untuk melakukan summarize terhadap jaringan besar dengan classful network menjadi rute agregat, atau supernet. Dalam bab ini, Anda juga akan meninjau keterampilan rute summarization.

6.2 Classful IP Addressing

Ketika ARPANET dibentuk pada tahun 1969, tidak ada yang mengantisipasi bahwa Internet akan meledak dari awal yang sederhana dari proyek penelitian ini. Pada tahun 1989, ARPANET telah berubah menjadi apa yang sekarang kita sebut internet. Selama dekade berikutnya, jumlah host di Internet tumbuh secara eksponensial, dari 159.000 pada bulan Oktober 1989, lebih dari 72 juta pada akhir milenium. Pada Januari 2007, ada lebih dari 433 juta host di Internet [10].



Gambar 6.1 Pertumbuhan Eksponensial Host Pada Internet

Alamat IPv4 awalnya dialokasikan berdasarkan kelas. Dalam spesifikasi asli dari IPv4 (RFC 791) dirilis pada tahun 1981, penulis mendirikan kelas untuk

menyediakan tiga ukuran yang berbeda untuk jaringan besar, organisasi menengah dan kecil. Akibatnya, kelas A, B dan C alamat didefinisikan dengan format khusus untuk bit urutan tinggi. Urutan bit tinggi adalah paling kiri bit-bit pada alamat 32-bit.

Class	High Order Bits	Start	End
Class A	0	0.0.0.0	127.255.255.255
Class B	10	128.0.0.0	191.255.255.255
Class C	110	192.0.0.0	223.255.255.255
Multicast	1110	224.0.0.0	239.255.255.255
Experimental	1111	240.0.0.0	255.255.255.255

Gambar 6.2 High Order Bits

Seperti ditunjukkan pada gambar:

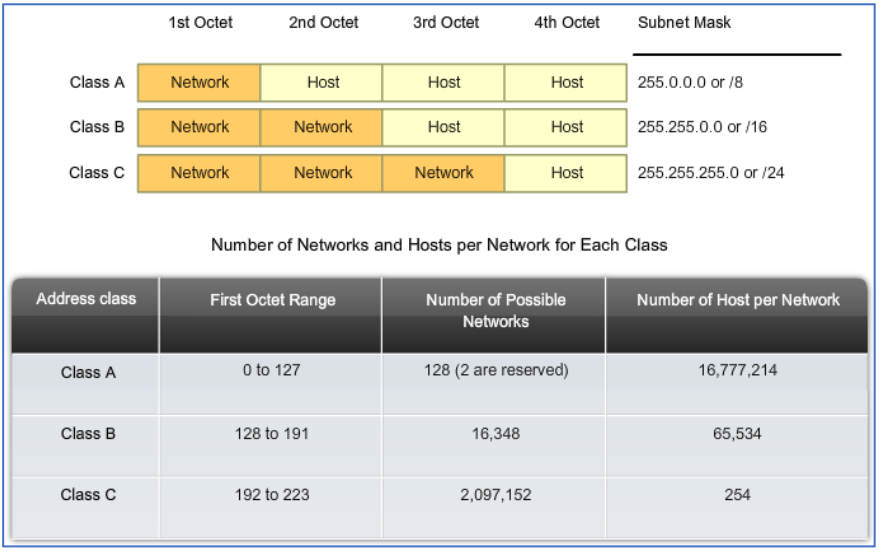
- Kelas A alamat dimulai dengan bit 0. Oleh karena itu, semua alamat dari 0.0.0.0 ke 127.255.255.255 milik kelas A. Alamat 0.0.0.0 dicadangkan untuk routing default dan alamat 127.0.0.0 dicadangkan untuk pengujian loopback.
- Alamat Kelas B dimulai dengan sedikit 1 dan 0 bit. Oleh karena itu, semua alamat dari 128.0.0.0 ke 191.255.255.255 milik kelas B.
- Kelas C alamat dimulai dengan dua bit 1 dan 0 bit. Kelas C berkisar dari 192.0.0.0 alamat ke 223.255.255.255.

Alamat sisanya dicadangkan untuk skema multicast dan penggunaan IP masa depan. Alamat multicast dimulai dengan tiga 1s dan sedikit 0. Alamat multicast yang digunakan untuk mengidentifikasi sekelompok host yang merupakan bagian dari kelompok multicast. Ini membantu mengurangi jumlah pengolahan paket yang dilakukan oleh host, terutama pada media penyiaran. Dalam kursus ini, Anda akan melihat bahwa routing protokol RIPv2, EIGRP, dan OSPF menggunakan alamat multicast yang ditunjuk.

The IPv4 Classful Addressing Structure

Penentuan bit network dan bit host ditetapkan dalam RFC 790 (dirilis dengan RFC 791). Seperti ditunjukkan dalam gambar, jaringan kelas A oktet pertama digunakan untuk tugas network, yang diterjemahkan ke

subnet mask 255.0.0.0 classful. Karena hanya 7 bit yang tersisa dalam oktet pertama (ingat, bit pertama selalu 0), ini membuat 2 pangkat 7 atau 128 jaringan.



	1st Octet	2nd Octet	3rd Octet	4th Octet	Subnet Mask
Class A	Network	Host	Host	Host	255.0.0.0 or /8
Class B	Network	Network	Host	Host	255.255.0.0 or /16
Class C	Network	Network	Network	Host	255.255.255.0 or /24

Number of Networks and Hosts per Network for Each Class

Address class	First Octet Range	Number of Possible Networks	Number of Host per Network
Class A	0 to 127	128 (2 are reserved)	16,777,214
Class B	128 to 191	16,348	65,534
Class C	192 to 223	2,097,152	254

Gambar 6.3 Subnet Mask Based On Class

Dengan 24 bit di bagian host, masing-masing kelas alamat A memiliki potensi untuk lebih dari 16 juta alamat host individu. Sebelum CIDR dan VLSM dibuat, penggunaan alamat network selalu classful network. Apakah satu organisasi akan menggunakan 16 juta alamat ? Sekarang Anda dapat memahami limbah yang luar biasa dari ruang alamat yang terjadi pada hari-hari awal Internet, ketika perusahaan menerima kelas A alamat. Beberapa perusahaan dan organisasi pemerintah masih memiliki kelas alamat A. Sebagai contoh, General Electric memiliki 3.0.0.0 / 8, Apple Computer memiliki 17.0.0.0 / 8, dan US Postal Service memiliki 56.0.0.0 / 8.

Kelas B tidak jauh lebih baik dari kelas A. RFC 790 menententukan dua oktet pertama sebagai network. Dengan dua bit pertama telah ditetapkan sebagai 1 dan 0, 14 bit tetap dalam dua oktet pertama untuk tugas network, yang mengakibatkan 16.384 alamat network kelas B. Karena setiap kelas B yang terkandung alamat jaringan 16 bit di bagian host, itu dikendalikan 65.534 alamat. (Ingat, 2 alamat yang dicadangkan untuk alamat network dan broadcast.) Hanya organisasi terbesar dan pemerintah pernah bisa berharap

untuk menggunakan semua 65.000 alamat. Seperti kelas A, kelas B address space banyak juga yang akan terbuang.

Kelas C alamat sering kali terlalu kecil. RFC 790 menetapkan tiga oktet pertama sebagai network. Dengan tiga bit pertama 1 dan ditetapkan sebagai 1 dan 0, 21 bit tetap untuk menetapkan network selama lebih dari 2 juta jaringan kelas C. Tapi, masing-masing kelas C jaringan hanya memiliki 8 bit di bagian host, atau 254 alamat host mungkin untuk digunakan.

6.3 Classless IP Addressing

Pada tahun 1992, anggota IETF (Internet Engineering Task Force) telah memiliki keprihatinan yang serius tentang pertumbuhan eksponensial dari internet dan skalabilitas terbatas tabel routing internet. Mereka juga khawatir dengan kelelahan akhirnya 32-bit address space IPv4. Menipisnya ruang alamat kelas B itu terjadi begitu cepat sehingga dalam waktu dua tahun di sana akan ada lagi kelas B alamat yang tersedia (RFC 1519). Deplesi ini terjadi karena setiap organisasi yang diminta dan memperoleh persetujuan untuk ruang alamat IP menerima alamat seluruh jaringan classful - baik kelas B dengan 65.534 alamat host atau kelas C dengan 254 alamat host. Salah satu penyebab mendasar dari masalah ini adalah kurangnya fleksibilitas. Tidak ada kelas alamat untuk melayani sebuah organisasi menengah yang membutuhkan ribuan alamat IP tetapi tidak 65.000.

Pada tahun 1993, IETF memperkenalkan Classless Inter-Domain Routing, CIDR atau (RFC 1517). CIDR dibuat untuk:

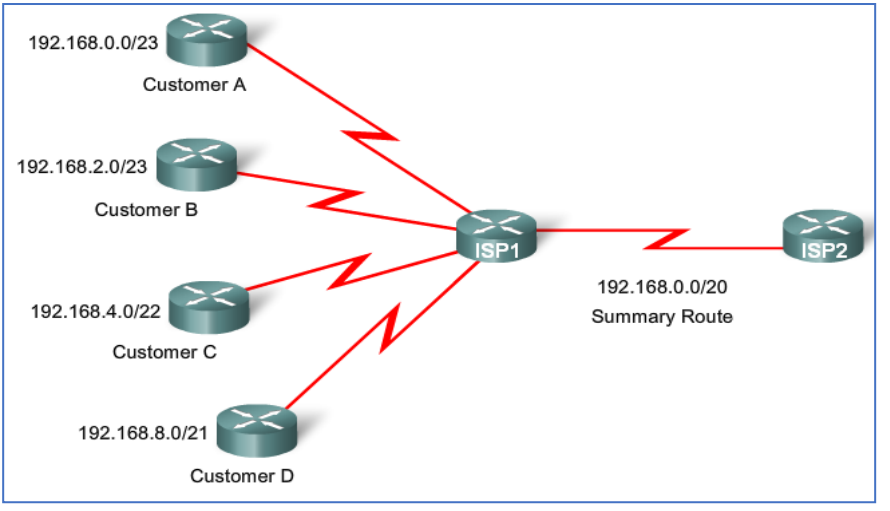
- Lebih efisien menggunakan ruang alamat IPv4
- Awalan agregasi, yang mengurangi ukuran tabel routing

Untuk CIDR-compliant router, alamat kelas tidak berarti. Bagian jaringan dari alamat yang ditentukan oleh subnet mask jaringan, juga dikenal sebagai network prefix, atau prefix length (/ 8, / 19, dll). Alamat network tidak lagi ditentukan oleh kelas dari alamat.

ISP sekarang bisa lebih efisien mengalokasikan ruang alamat menggunakan prefix length, dimulai dengan / 8 dan lebih besar (/ 8, / 9, / 10, dll). ISP tidak lagi terbatas pada, / 8 / 16, atau / 24 subnet mask. Blok alamat IP dapat diberikan ke network berdasarkan kebutuhan pelanggan, mulai dari beberapa host ke ratusan atau ribuan host.

CIDR menggunakan Variable Length Subnet Mask (VLSM) untuk mengalokasikan alamat IP untuk subnet sesuai dengan kebutuhan individu. Jenis alokasi memungkinkan batas network atau host untuk terjadi pada setiap bit dalam alamat. Jaringan dapat dibagi lagi ke dalam subnet subnet atau lebih kecil dan lebih kecil.

Sama seperti Internet telah tumbuh pada tingkat eksponensial pada awal 1990-an, begitu pula ukuran tabel routing yang dikelola oleh router internet dengan pengalamatan IP classful. CIDR diperbolehkan untuk awalan agregasi, yang anda sudah tahu sebagai rute summarization. Ingat kembali dari Bab 2, "Routing statis" bahwa Anda dapat membuat satu rute statis untuk beberapa jaringan. Internet tabel routing kini bisa mendapatkan keuntungan dari jenis yang sama untukagregasi rute. Kemampuan untuk rute yang akan diringkas sebagai rute tunggal membantu mengurangi ukuran tabel routing Internet.



Gambar 6.4 Summary Route

Dalam gambar, perhatikan bahwa ISP1 memiliki empat pelanggan, masing-masing dengan sejumlah variabel ruang alamat IP. Namun, semua ruang alamat pelanggan dapat diringkas ke dalam satu iklan ke ISP2. Diringkas 192.168.0.0/20 atau rute dikumpulkan mencakup semua jaringan milik Pelanggan A, B, C, dan D. Jenis rute ini dikenal sebagai rute supernet. Sebuah supernet merangkum beberapa alamat jaringan dengan mask kurang dari mask classful.

Menyebarkan VLSM dan rute supernet membutuhkan classless routing protocol, karena subnet mask tidak bisa lagi ditentukan oleh nilai oktet pertama. Subnet mask sekarang perlu disertakan dengan alamat network. Classless routing protocol termasuk subnet mask dengan alamat nework di update ke tabel routing.

6.4 VLSM And IP Address

Perhitungan IP Address menggunakan metode VLSM adalah metode yang berbeda dengan memberikan suatu Network Address lebih dari satu subnet mask, jika menggunakan CIDR dimana suatu Network ID hanya memiliki satu subnet mask saja perbedaan yang mendasar disini juga adalah terletak pada pembagian blok, pembagian blok VLSM bebas dan hanya dilakukan oleh si pemilik Network Address yang telah diberikan kepadanya atau dengan kata lain sebagai IP address local dan IP Address ini tidak dikenal dalam jaringan internet, namun tetap dapat melakukan koneksi kedalam jaringan internet, hal ini terjadi dikarenakan jaringan internet hanya mengenal IP Address berkelas.

Metode VLSM ataupun CIDR pada prinsipnya sama yaitu untuk mengatasi kekurangan IP Address dan dilakukannya pemecahan Network ID guna mengatasi kekerungan IP Address tersebut. Network Address yang telah diberikan oleh lembaga IANA jumlahnya sangat terbatas, biasanya suatu perusahaan baik instansi pemerintah, swasta maupun institusi pendidikan yang terkoneksi ke jaringan internet hanya memilik Network ID tidak lebih dari 5 – 7 Network ID (IP Public).

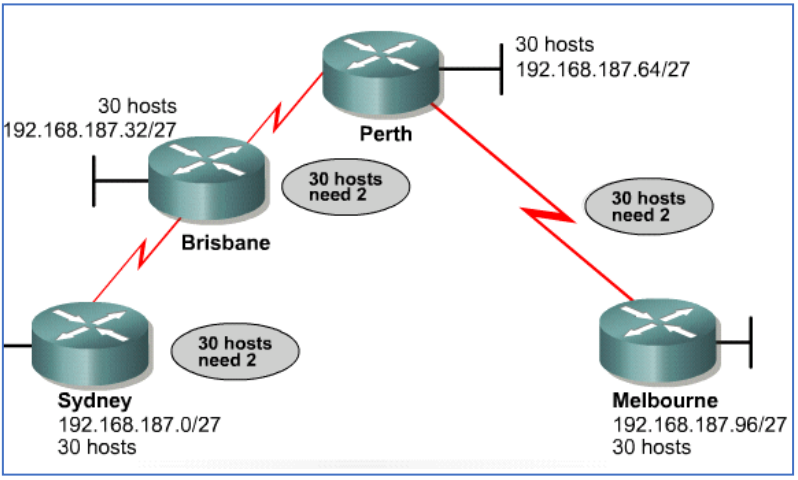
Dalam penerapan IP Address menggunakan metode VLSM agar tetap dapat berkomunikasi kedalam jaringan internet sebaiknya pengelolaan network-nya dapat memenuhi persyaratan. Routing protocol yang digunakan harus mampu membawa informasi mengenai notasi prefix untuk setiap rute broadcastnya (routing protocol : RIP, IGRP, EIGRP, OSPF dan lainnya, bahan bacaan lanjut protocol routing : CNAP 1-2), semua perangkat router yang digunakan dalam jaringan harus mendukung metode VLSM yang menggunakan algoritma penerus packet informasi. Tahapan perihitungan menggunakan VLSM IP Address yang ada dihitung menggunakan CIDR selanjutnya baru dipecah kembali menggunakan VLSM.

VLSM dapat digunakan routing protocol seperti OSPF, Integrated IS-IS, EIGRP, RIP v2,dan routing static. Beikut ini ilustrasi digunakan :

Tabel 6.1 Tabel IP address

No	ID	Range
0	192.168.187.0	192.168.187.1 - 192.168.187.30
1	192.168.187.32	192.168.187.33 - 192.168.187.62
2	192.168.187.64	192.168.187.65 - 192.168.187.94
3	192.168.187.96	192.168.187.97 - 192.168.187.126
4	192.168.187.128	192.168.187.129 - 192.168.187.158
5	192.168.187.160	192.168.187.161 - 192.168.187.190
6	192.168.187.192	192.168.187.193 - 192.168.187.222
7	192.168.187.224	192.168.187.225 - 192.168.187.254

Terdapat subnetting dengan network id 192.168.187.0/27 seperti pada tabel diatas yang sudah terdapat pengelompokannya .



Gambar 6.5 Implementasi VLSM

Pada gambar diatas, untuk menghubungkan antara router (point to point) diperlukan 2 IP, jika digunakan pada network diatas dengan subnet /27, host yang dimiliki 30 IP, sehingga terjadi pemborosan IP. Untuk mengatasinya, kita dapat memilih salah satu network misalkan no 6 : 192.168.187.192/27 akan di sub subnet kembali.

Hasilnya :

Tabel 6.2 Hasil Perhitungan VLSM

Subnet Number	Subnet Address	
sub-subnet 0	192.168.187.192	/30
sub-subnet 1	192.168.187.196	/30
sub-subnet 2	192.168.187.200	/30
sub-subnet 3	192.168.187.204	/30
sub-subnet 4	192.168.187.208	/30
sub-subnet 5	192.168.187.212	/30
sub-subnet 6	192.168.187.216	/30
sub-subnet 7	192.168.187.220	/30

Lalu bagaimana cara menghitungnya ????
Solusi :Network 192.168.187.192 /27 akan disubnet kembali menjadi 192.168.187.192/30 hanya memiliki 2 host dari 30 host .
Jika dirubah ke binary :
3 oktet pertama dari network tidak berubah, jadi dibiarkan dalam bentuk desimal
192.168.187.11 000000
255.255.255.11 100000 = /27

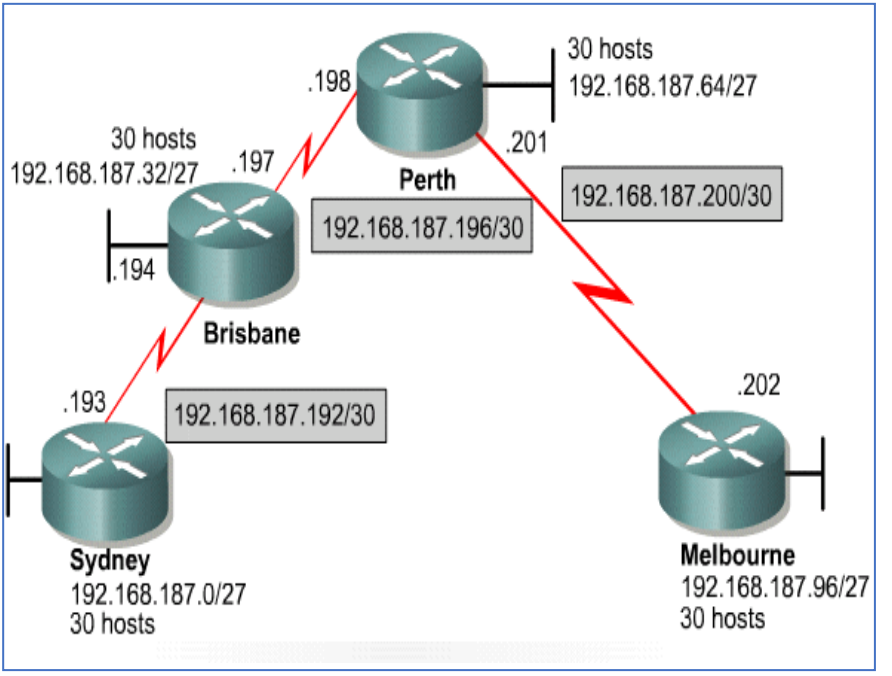
Kemudian host diperkecil menjadi 2 dimana subnet /30
Sehingga
192.168.187.11 000000
255.255.255.11 111100 =/30

Dan terjadi network baru dimana range dimulai dari:
192.168.187.11 000000
255.255.255.11 111100 =/30

Dan network 192.168.187.192/30
Range nya adalah

1. 192.168.187.11 000000 - 192..168.187.11 011100 atau jika didesimalkan menjadi 192.168.187.192 – 192.168.187.220
2. Dan karena subnet nya /30, ingat bit 0 sisanya hanya 2, sehingga host menjadi kelipata $2^2 = 4$
3. Subentting selesai hasilnya adalah :

Gambar router akan menjadi :

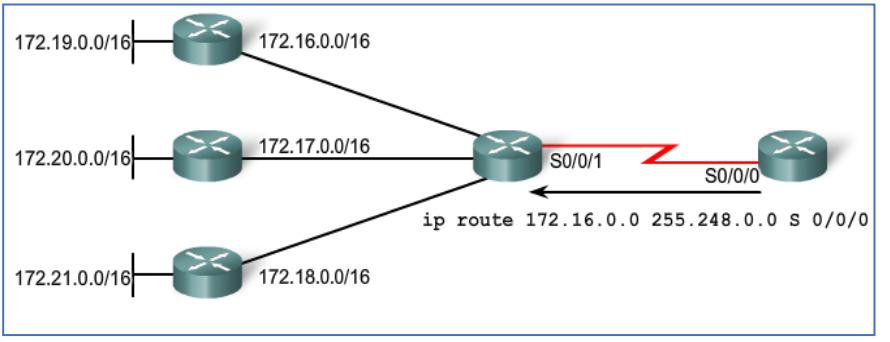


Gambar 6.6 Hasil Implementasi VLSM

6.5 Route Summarization

Seperti yang Anda pelajari sebelumnya, rute summarization juga dikenal sebagai rute agregasi, adalah proses dari advertising satu set bersebelahan alamat sebagai alamat tunggal dengan less-specific, shorter subnet mask. Ingat bahwa CIDR adalah bentuk summarization rute dan ini identik dengan istilah supernetting.

Anda sudah harus akrab dengan rute summarization yang dilakukan oleh protokol routing classful seperti RIPv1. RIPv1 merangkum ke alamat subnet jaringan tunggal utama classful saat mengirim update RIPv1 keluar interface yang dimiliki jaringan lain yang lebih besar. Sebagai contoh, RIPv1 akan meringkas 10.0.0.0/24 subnet (10.0.0.0/24 melalui 10.255.255.0/24) sebagai 10.0.0.0 / 8.



Gambar 6.7 Route Sumarization

CIDR mengabaikan pembatasan batas classful, dan memungkinkan summarization dengan mask yang kurang dibandingkan dengan default classful mask. Jenis summarization membantu mengurangi jumlah entri dalam routing update dan menurunkan jumlah entri dalam tabel routing lokal. Hal ini juga membantu mengurangi penggunaan bandwidth untuk routing update dan hasil pencarian lebih cepat tabel routing.

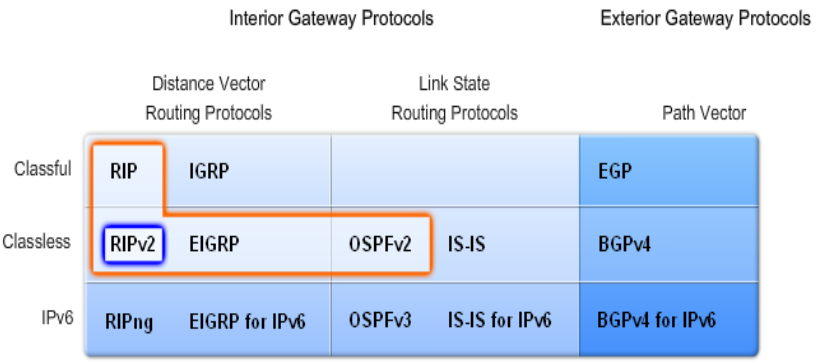
Angka ini menunjukkan rute statis tunggal dengan alamat 172.16.0.0 dan 255.248.0.0 mask merangkum semua 172.23.0.0/16 172.16.0.0/16 untuk jaringan classful. Meskipun 172.22.0.0/16 dan 172.23.0.0/16 tidak ditampilkan dalam grafik, ini juga termasuk dalam rute ringkasan. Perhatikan bahwa / 13 mask (255.248.0.0) kurang dari default classful mask/ 16 (255.255.0.0).

Bab 7

Routing Information Protocol Versi 2 (RIP v2)

7.1 Pendahuluan

Routing Information Protocol (RIP) adalah sebuah protokol routing dinamis yang digunakan dalam jaringan LAN (Local Area Network) dan WAN (Wide Area Network). Karena itu protokol ini diklasifikasikan sebagai Interior Gateway Protocol (IGP). Protokol ini menggunakan algoritma Distance-Vector Routing. Pertama kali didefinisikan dalam RFC 1058 (1988). Protokol ini telah dikembangkan beberapa kali, sehingga terciptalah RIP Versi 2 (RFC 2453). Kedua versi ini masih digunakan sampai sekarang, meskipun begitu secara teknis mereka telah dianggap usang oleh teknik-teknik yang lebih maju, seperti Open Shortest Path First (OSPF) dan protokol OSI IS-IS. RIP juga telah diadaptasi untuk digunakan dalam jaringan IPv6, yang dikenal sebagai standar *RIPng* (RIP *Next Generation* / RIP generasi berikutnya), yang diterbitkan dalam RFC 2080 (1997) [11].



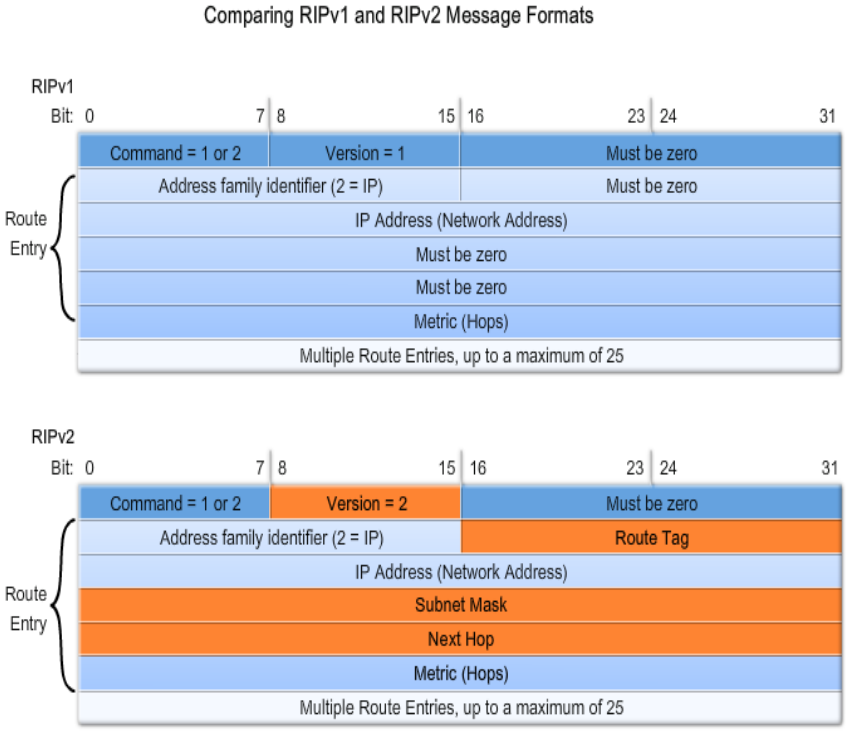
Gambar 7.1 Routing protocol

Algoritma routing yang digunakan dalam RIP, algoritma Bellman-Ford, pertama kali digunakan dalam jaringan komputer pada tahun 1968, sebagai awal dari algoritma routing ARPANET. Versi paling awal protokol khusus yang menjadi RIP adalah Gateway Information Protocol, sebagai bagian dari PARC Universal Packet internetworking protocol suite, yang dikembangkan di Xerox Parc. Sebuah versi yang bernama *Routing Information Protocol*, adalah bagian dari Xerox Network Services. Sebuah versi dari RIP yang mendukung Internet Protocol (IP) kemudian dimasukkan dalam Berkeley Software Distribution (BSD) dari sistem operasi Unix. Ini dikenal sebagai daemon routed. Berbagai vendor lainnya membuat protokol routing yang diimplementasikan sendiri. Akhirnya, RFC 1058 menyatukan berbagai implementasi di bawah satu standar [11].

Routing Information Protocol (RIP) adalah sebuah routing protocol jenis distance vector yang sejati. RIP mengirimkan routing tabel yang lengkap ke semua interface yang aktif setiap 30 detik. RIP hanya menggunakan jumlah hop untuk menentukancara terbaik ke sebuah network remote, tetapi RIP secara default memiliki sebuah nilai jumlah hop maksimum yang diizinkan yaitu 15 hop, yang

berarti nilai 16 dianggap tidak terjangkau (*unreacbable*). RIP bekerja dengan baik di network – network yang kecil, tetapi RIP tidak efisien pada network – network besar dengan link WAN yang lambat atau pada network yang memiliki sejumlah besar router terpasang.

RIP versi 1 menggunakan hanya *classful routing*, yang berarti semua alat di network harus menggunakan subnet mask default. Ini karena RIP versi 1 tidak mengirimkan update dengan informasi subnet mask di dalamnya. RIP versi 2 menyediakan sesuatu yang disebut *prefix routing* dan bisa mengirimkan informasi subnet mask bersama dengan update – update dari route. Ini disebut *classless routing*.



Gambar 7.2 Perbandingan message formats RIPv1 dengan RIPv2

RIP versi 1 adalah protokol routing classful. Seperti yang dapat dilihat dalam *message format* RIPv1, RIP versi 1 tidak mengirimkan update dengan informasi subnet mask di dalamnya. Oleh karena itu, RIPv1 tidak dapat mendukung *discontiguous networks*, VLSM, atau *Classless Inter-Domain Routing* (CIDR) *supernets*.

7.2 RIP Timers

RIP menggunakan tiga jenis timer yang berbeda untuk mengatur kinerjanya [11] :

Route update timer **:** timer ini menset interval (biasanya 30 detik) antara update routing yang periodic, dimana router mengirimkan sebuah copy yang lengkap dari routing tabel nya ke semua router tetangga.
Route invalid timer : timer ini menentukan jangaka waktu yang harus lewat (180 detik) sebelum sebuah router menentukan bahwa sebuah route menjadi tidak valid. Kesimpulan bahwa sebuah route tidak valid akan dibuat jika router tidak mendengar update apapun tentang sebuah route tertentu selama periode waktu itu. Ketika itu terjadi, router akan mengirimkan update ke semua router tetangga untuk memberitahu bahwa route itu sudah tidak valid.

Holddown timer **:** timer ini menset lamanya waktu dimana informasi routing ditahan. Router akan masuk ke status yang disebut holddown state jika sebuah paket update yang diterima menunjukkan bahwa route tidak terjangkau. Ini akan berlanjut sampai sebuah packet update diterima dengan sebuah metric yang lebih baik atu sampai holddown timer habis (*expired*). Default nya adalah 180 detik.

Route flash timer **:** timer ini menset waktu antara sebuah route menjadi tidak valid dan penghapusannya dari routing tabel (240 detik). Sebelum route dihapus dari tabel, router memberitahu router tetangganya tentang route yang akan mati itu. Nilai dari route invalid timer harus lebih kecil daripada nilai dan route flash timer. Hal ini akan member cukup waktu pada router untuk memberitahu router tetangganya tantang router yang tidak valid sebelum routing tabel local di-update.

7.3 Mengkonfigurasi RIP version 2

Perintah untuk menjalankan RIP versi 2 sebagai routing protokol adalah **router rip**. Setelah itu ketik **version 2** untuk menggunak RIP versi 2. Perintah **network** kemudian digunakan untuk menjelaskan interface mana yang digunakan oleh RIP. Proses routing memasangkan interface yang bersangkutan dengan alamat jaringan dan mulai mengirimkan dan menerima update RIP ke interface tersebut.

RIP mengirim pesan routing-update pada interval yang tetap. Ketika router menerima routing-update yang berisi perubahan tabel routing, ia mengupdate tabel routingnya ke route yang baru. Dalam hal ini metric yang diterima bertambah nilainya 1, dan interface asal dari update menunjukkan hop berikutnya dalam tabel routing. Router-router RIP memperbaiki hanya route yang terbaik saja ke tujuan tapi juga memperbaiki route ke tujuan yang nilainya sama.

RIP merupakan time-driven, tapi implementasi Cisco, RIP mengirim triggered update kapanpun kalau perubahan dideteksi. Topologi mengalami perubahan juga akan dikirim triggered update langsung. Tanpa trigger, RIP dan IGRP tidak akan bagus unjuk kerjanya. Setelah proses update dalam tabel routing terjadi, maka konfigurasipun mengalami perubahan, kemudian router secara langsung mulai transmit update routing untuk menginformasikan ke router-router lainnya tentang perubahan yang terjadi. Triggered update ini, dikirim secara regular dan terjadwal. Dibawah ini adalah cara mengkonfigurasi RIP versi 2 kedalam beberapa router.

R1(config)#**router rip** – memilih RIP sebagai routing protokol

R1(config-router)#**version 2 –** menggunakan RIP versi 2

R1(config-router)#**network 172.30.1.0** – spesifikasi alamat yang terhubung langsung

R1(config-router)#**network 172.30.2.0 –** spesifikasi alamat yang terhubung langsung

R1(config-router)#**network 209.165.200.228 –** spesifikasi alamat yang terhubung langsung

R2(config)#**router rip** – memilih RIP sebagai routing protokol

R2(config-router)#**version 2 –** menggunakan RIP versi 2

R2(config-router)#**network 10.1.0.0** – spesifikasi alamat yang terhubung langsung

R2(config-router)#**network 209.165.200.228 –** spesifikasi alamat yang terhubung langsung

R2(config-router)#**network 209.165.200.228 –** spesifikasi alamat yang terhubung langsung

R2(config-router)#**network 209.165.200.232 –** spesifikasi alamat yang terhubung langsung

R3(config)#**router rip** – memilih RIP sebagai routing protokol

R3(config-router)#**version 2 –** menggunakan RIP versi 2

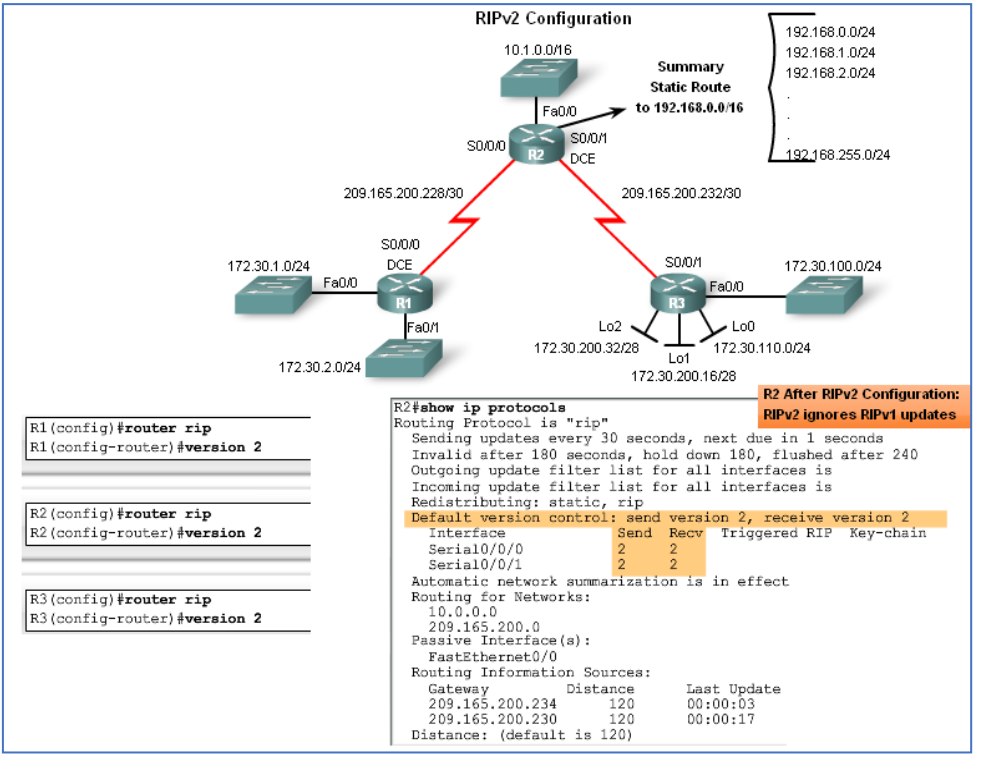
R3(config-router)#**network 172.30.100.0** – spesifikasi alamat yang terhubung langsung

R3(config-router)#**network 172.30.110.0 –** spesifikasi alamat yang terhubung langsung

R3(config-router)#**network 172.30.200.16 –** spesifikasi alamat yang terhubung langsung

R3(config-router)#**network 172.30.200.32 –** spesifikasi alamat yang terhubung langsung

R3(config-router)#**network 209.165.200.232 –** spesifikasi alamat yang terhubung langsung

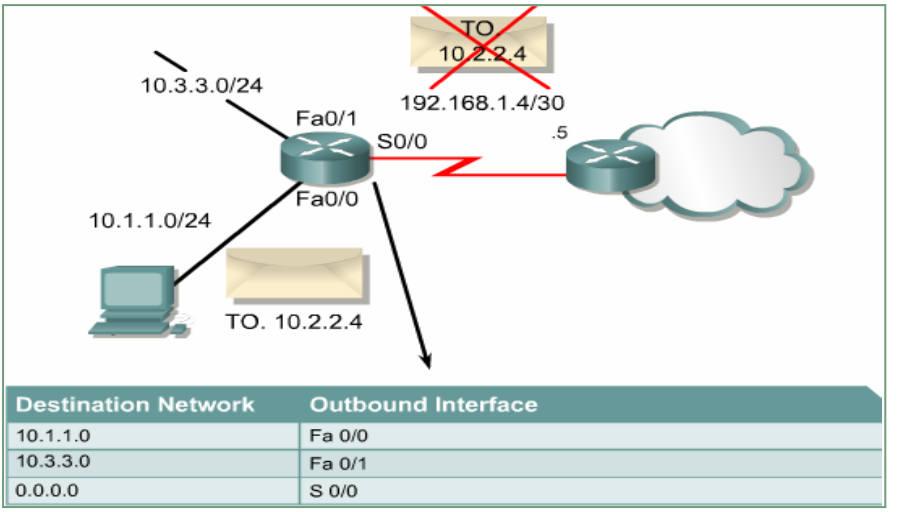


Gambar 7.3 Konfigurasi RIPv2

7.4 Penggunaan Perintah Ip Classless

Kadang-kadang router menerima paket-paket yang ditujukan untuk subnet yang tidak diketahui dari jaringan yang terhubung langsung. Gunakan perintah ip classless untuk keperluan itu. Sebagai contoh, jika menggunakan enterprise dalam subnet 10.10.0.0/24 menjadi 10.10.0.0/16. Perintah ip classless di-enable.

R1#config terminal
R1(config)#ip classless



Destination Network	Outbound Interface
10.1.1.0	Fa 0/0
10.3.3.0	Fa 0/1
0.0.0.0	S 0/0

Gambar 7.5 Routing dengan ip classless

7.5 Seting Holddown Timer

Untuk mengurangi routing loop dan counting to infinity, RIP menggunakan beberapa teknik seperti:

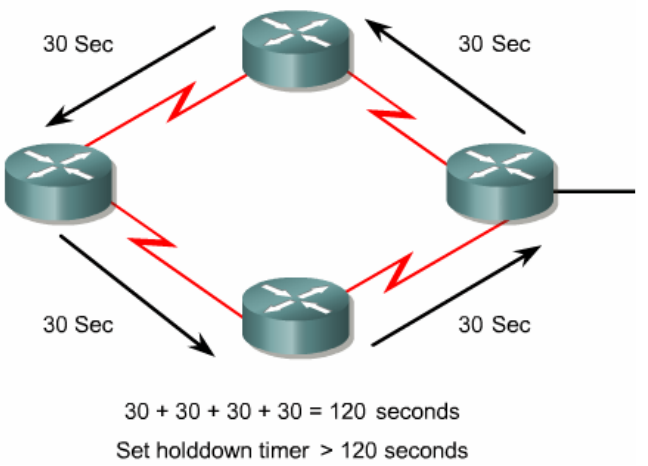
- Split Horizon
- Poison reverse
- Holddown counter
- Triggered update

RIP mengijinkan maksimum hop count 15. Untuk tujuan ke jaringan mana saja, jika hop count lebih besar dari 15, maka jaringan dianggap unreachable.

Split horizon menggunakan teori dimana ketidakbergunaan untuk mengirim informasi tentang rute balik dari asal informasi itu datang. Dalam beberapa konfigurasi jaringan, mungkin lebih baik men-disable split horizon. Perintah yang digunakan untuk disable split horizon:

R1(config-if)#**no ip split-horizon**

Holddown timer mekanisme lain untuk menurunkan routing loop. Holddown timer membantu mencegah counting to infinity tapi juga menaikkan waktu konvergen. Default holddown timer RIP adalah 180 detik. Hal ini mencegah rute salah diupdate tapi juga memungkinkan alternative routing. Holddown timer dapat diturunkan untuk menaikkan konvergen tapi harus dilakukan dengan peringatan. Secara ideal, timer seharusnya di set lebih lama daripada kemungkinan waktu update terlama.



Gambar 7.6 Seting holddown timer

Pada gambar di atas, loop terjadi di 4 router, jika tiap-tiap router mempunyai waktu update 30 detik, loop terlama seharusnya 120 detik. Karena itu holddown timer harus di-set lebih dari 120 detik. Gunakan perintah berikut ini:

Router(config-router)#**timers basic** *update invalid holddown fluch [sleeptime]*

Pada saat perintah **network** diberikan, RIP secara langsung akan mulai mengirim advertisement ke semua interface dengan range alamat yang terspesifikasi. Admin jaringan dapat menggunakan perintah passive-interface untuk men-disable routing update.

Gambar 7.7 Perintah passive-interface

Command	Purpose
`GAD(config-router)#` **`passive-interface Fa0/0`**	Configures an interface to keep it from sending RIP packets

Karena RIP menggunakan protokol broadcast, admin jaringan mungkin mengkonfigurasi RIP untuk pertukaran informasi routing dalam jaringan non-broadcast seperti Frame Relay. Dalam jaringan jenis ini, RIP harus diinformasikan ke router-router tetangganya. Untuk itu dapat dilakukan dengan perintah **neighbor**.

Command	Purpose
GAD(config-router)# **neighbor** *ip address*	Defines a neighboring router with which to exchange routing information

Gambar 7.8 Perintah neighbor

Command	Purpose
GAD(config-router)#**version {1|2}**	Configures the software to receive and send RIP Version 1 or Version 2 packets
GAD(config-if)#**ip rip send version 1**	Configures an interface to accept only RIP Version 1 packets
GAD(config-if)#**ip rip send version 2**	Configures an interface to send only RIP Version 2 packets
GAD(config-if)#**ip rip send version 1 2**	Configure an interface to send only RIP Version 1 or 2 packets

Gambar 7.9 Konfigurasi router untuk mengirim dan menerima paket

Secara default, software IOS Cicso menerima paket-paket RIP versi 1 dan versi 2, tapi mengirimkan paket hanya untuk versi 1. Admin jaringan dapat mengkonfigurasi router hanya menerima dan mengirim paket versi 1 atau admin dapat mengkonfigurasi router untuk hanya mengirim paket versi 2. untuk mengkonfigurasinya dapat dilakukan seperti perintah yang ada di gambar di atas.

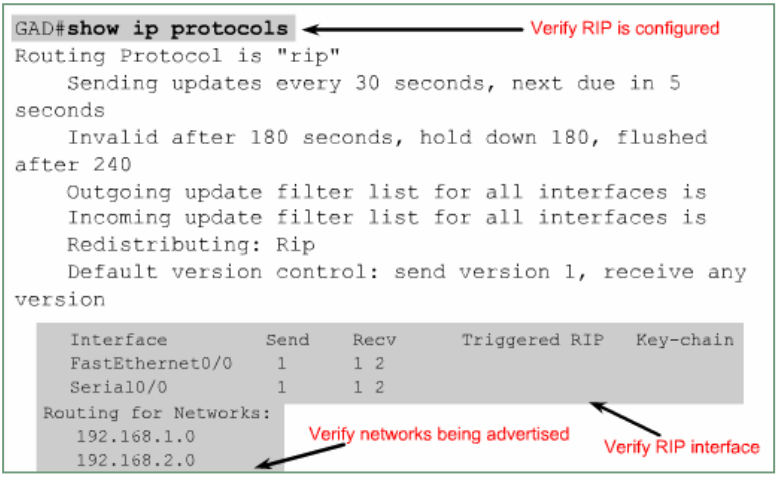
Command	Purpose
GAD(config-if)#ip rip receive version 1	Configures an interface to accept only RIP Version 1 packets
GAD(config-if)#ip rip receive version 2	Configures an interface to accept only RIP Version 2 packets
GAD(config-if)#ip rip receive version 1 2	Configures an interface to accept either RIP Version 1 or 2 packets

Gambar 7.10 Mengatur bagaimana paket diterima dari suatu interface

7.6 Perintah Show Ip Protocols

Perintah **show ip protocols** digunakan untuk menampilkan routing protokol yang membawa trafik IP dalam router. Output dari perintah itu dapat digunakan untuk memverifikasi konfigurasi RIP. Beberapa konfigurasi umum untuk verifikasi:

- Routing RIP yang dikonfigurasi
- Interface yang digunakan untuk mengirim dan menerima update RIP
- Router memberi informasi tentang jaringan yang benar



Gambar 7.11 Show ip protocol

Perintah show ip protocols dapat digunakan untuk mem-verifikasi bahwa rute yang diterima RIP tetangga ada dalam table routing.

```
GAD#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP,
M - mobile, B - BGP
            D - EIGRP, EX - EIGRP external, O - OSPF,
IA - OSPF inter area
            N1 - OSPF NSSA external type 1, N2 - OSPF
NSSA external type2
            E1 - OSPF external type 1, E2 - OSPF
external type 2, E - EGP
            i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS
level-2, ia - IS-IS inter
                area
            * - candidate default, U - per-user
static route, o - ODR
            P - periodic download static route

Gateway of last resort is not set
```

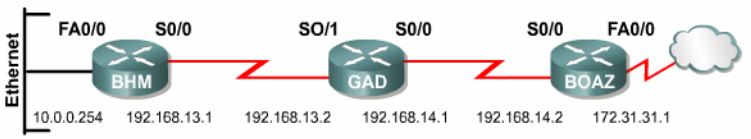
Gambar 7.12 Show ip route

Output dari perintah show ip route dapat memberi informasi tentang penggunaan routing protokol RIP yang ditandai dengan "R". Sedangkan perintah tambahan untuk meng-cek konfigurasi RIP adalah:

- **show interface** *interface*
- **show ip interface** *interface*
- **show running-config**

7.7 Perintah Debug Ip Rip

Sebagian besar error konfigurasi RIP disebabkan karena penulisan jaringan yang salah, penulisan subnet yang salah, atau split horizon. Perintah yang efektif yang digunakan untuk menemukan update RIP adalah **debug ip rip**. Perintah debug ip rip menampilkan update routing RIP seperti yang mereka kirim dan terima. Contoh pada gambar berikut menunjukkan tampilan output dari perintah **debug ip rip**.

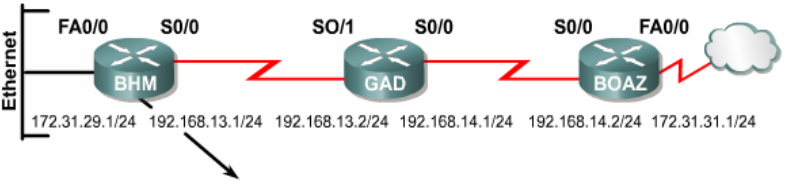



```
BHM#debug ip rip
RIP event debugging is on
BHM#
00:45:33: RIP: received v1 update from 192.168.13.2
on Serial0/0
00:45:33:        192.168.14.0 in 1 hop
00:45:33:        172.31.0.0 in 2 hop
00:45:33:        172.29.0.0 15 hops
00:45:36: RIP: sending v1 update to 255.255.255.255
via Serial0/0 (192.168.13.1)
```

Gambar 7.13 Perintah debug ip rip

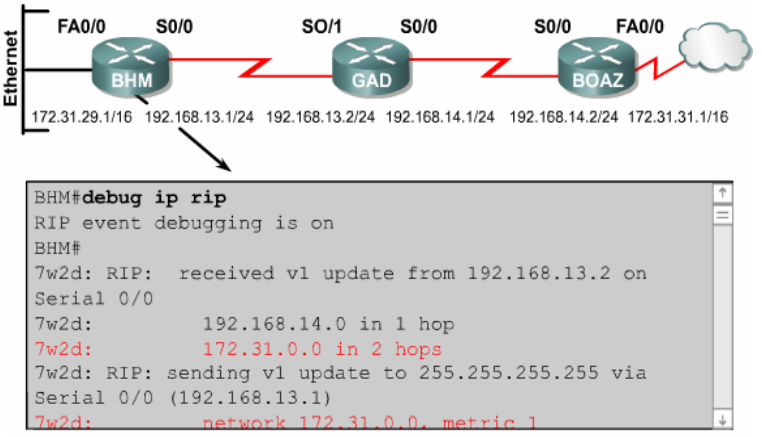
Setelah router menerima dan memproses update, ia mengirim informasi update keluar dua interface RIP. Output menampilkan router menggunakan RIPv1 dan broadcast update dengan alamat 255.255.255.255.

Ada beberapa petunjuk untuk melihat tampilan perintah **debug ip rip**. Masalah pendefinisian subnetwork atau duplikat jaringan dapat di-diagnosa dengan perintah ini.




```
BHM#debug ip rip
RIP event debugging is on
BHM#
7w2d: RIP:  received v1 update from 192.168.13.2 on
Serial 0/0
7w2d:         192.168.14.0 in 1 hop
7w2d:         172.31.0.0 in 2 hops
7w2d: RIP: sending v1 update to 255.255.255.255 via
Serial 0/0 (192.168.13.1)
7w2d:         network 172.31.0.0, metric 1
```

Gambar 7.13 Discontiguous subnetwork



Gambar 7.14 Duplikat subnetwork

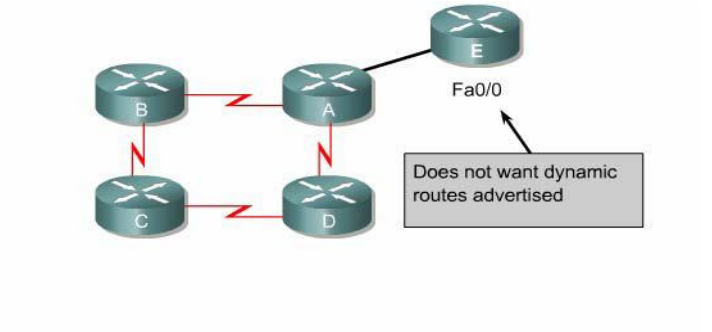
Perintah-perintah di bawah ini untuk troubleshooting RIP:

- **show ip rip databases**
- **show ip protocols** {summary}
- **show ip route**
- **debug ip rip** {events}
- **show ip interface brief**

7.8 Perintah Passive-interface

Perintah passive-interface digunakan untuk mencegah transmisi routing update melalui suatu interface router. Pada saat update pesan tidak dikirim lewat interface router, sistem yang lain tidak dapat mempelajari tentang rute dinamis.

Untuk RIP dan IGRP perintah passive-interface menghentikan router dari pengiriman update ke router tetangga, tapi router meneruskan mendengarkan dan menggunakan routing update dari tetangga tersebut

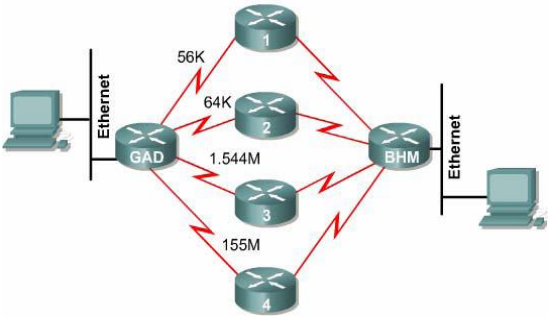


Gambar 7.15 Perintah passive-interface

7.9 RIP Load Balancing

Load Balancing adalah sebuah konsep dimana router mengambil keuntungan dari beberapa jalur terbaik untuk diberikan ke tujuan. Jalur ini dapat didefinisikan oleh admin jaringan atau dihitung oleh routing protokol dinamis seperti RIP.

RIP mempunyai kemampuan untuk load balancing sebanyak 6 jalur. Defaultnya sebanyak 4 jalur. Untuk fungsi load balancing ini RIP menggunakan teknik "round robin", artinya RIP mengambil paket forward melalui jalur parallel.



Gambar 7.16 RIP load Balancing

Gambar di atas adalah contoh routing dengan RIP dengan cost 4 jalur. Router akan mulai dengan interface pointer ke interface yang terhubung ke router1. kemudian interface pointer melalui interface dan rute dalam pola 1-2-3-4-1-2-3-4-1 dan seterusnya.

Perintah **show ip route** dapat digunakan untuk mencari rute dengan cost yang sama. Contoh, gambar di bawah ini menampilkan output dari perintah **show ip route** ke subnet tertentu dengan rute-rute yang beragam.

```
Router#show ip route 10.0.0.0
  Routing entry for 10.0.0.0/8
  Known via "rip", distance 120, metric 1
  Redistributing via rip
  Advertised by rip (self originated)
  Last update from 192.168.75.7 on Serial1,
00:00:00 ago
  Routing Descriptor Blocks:
  * 192.168.57.7, from 192.168.57.7, 00:00:18 ago,
via Serial0
      Route metric is 1, traffic share count is 1
    192.168.75.7, from 192.168.75.7, 00:00:00 ago,
via Serial1
      Route metric is 1, traffic share count is 1
```

Gambar 7.17 Output perintah show ip route

Load Balancing melalui banyak jalur. Ketika router mempelajari beberapa jalur ke suatu jaringan tertentu, jalur dengan administrative disntace terkecil yang dipilih. Seperti yang dijelaskan oleh gambar berikut ini.

Administrative Distance Route Source	Default Distance
Connected interface	0
Static route	1
EIGRP summary route	5
External BGP	20
EIGRP internal route	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP external route	170
Internal BGP	200
Unknown	255

Gambr 7.18 Cisco IOS administrative distance

Kadang-kadang router harus memilih jalur dari beberapa jalur, mempelajari melalui proses routing yang sama dengan administrative distance. Dalam hal ini, router memilih jalur dengan cost terkecil atau metric ke tujuan. Masing-masing proses routing menghitung costnya dan cost mungkin membutuhkan konfigurasi secara manul agar mencapai keadaan load balancing.

Jika router menerima dan memasang jalur banyak dengan administrative distance dan cost yang sama ke suatu tujuan, load balancing dapat terjadi. Secara default kebanyakan routing protokol IP memasang maksimum 4 jalur parallel dalam table routing. Routing statis selalu memasang 6 jalur. Kecuali BGP, defaultnya hanya mengijinkan satu jalur ke tujuan.

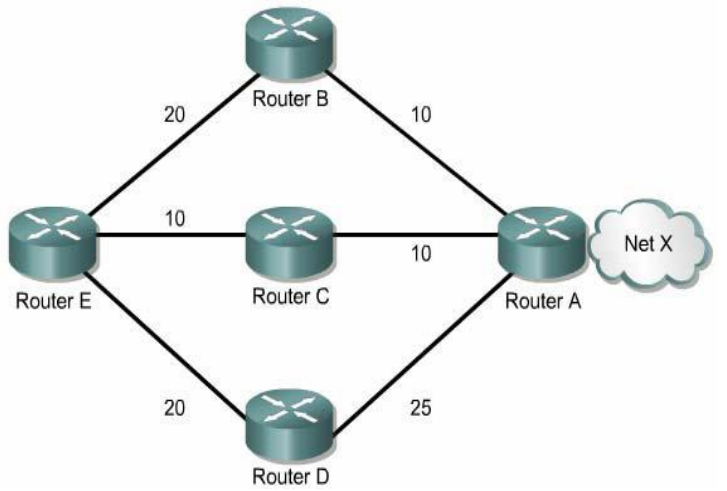
Range maksimum jalur adalah satu sampai 6 jalur. Untuk merubah jumlah maksimum dari jalur parallel yang diijinkan, menggunakan perintah:

Router(config-router)#**maximum-paths** [*number*]

IGRP dapat melakukan load balancing sampai dengan 6 jalur. Jaringan RIP harus memiliki hop count yang sama untuk load balance, dimana IGRP menggunakan bandwidth untuk menentukan bagaimana load balanbe.

Pada gambar berikut, terdapat 3 cara untuk mencapai jaringan X;

- E ke B ke A dengan metric 30
- E ke C ke A dengan metric 20
- E ke D ke A dengan metric 45



Gambar 7.19 Tiga cara untuk mencapai jaringan X

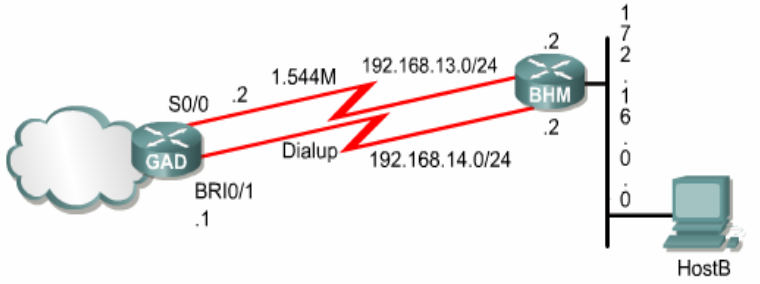
Router E memilih jalur kedua, E ke C ke A dengan metric 20 karena metricnya lebih kecil dari 30 dan 45.

Cisco IOS mendukung dua metode load balancing untuk paket-paket IP per paket dan per tujuan. Jika proses switching di-enable, router akan mengambil jalur berdasarkan per paket. Jika fast switching di-enable, router mengambil per alamat tujuan.

Secara default router menggunakan per tujuan untuk load balancing dan dikenal dengan fast switching. Cache dari jalur mengijinkan paket keluar di-laod balance per tujuan daripada per paketnya. Untuk melakukan disable fast switching dengan menggunakan perintah **no ip route-cache** dengan tujuan supaya trafik yang akan di-load balancing berdasar per paket.

7.10 Integrasi Routing statis dengan RIP

Router yang menjalankan RIP dapat menerima default rute melalui update dari router yang lain yang menjalankan RIP. Dengan menggunakan perintah **no ip route** dalam global config untuk menghapus rute statis. Admin jaringan dapat mengganti routing statis dengan dinamis dengan melakukan seting nilai administrative distance. Setiap routing dinamis mempunyai default administrative distance (AD). Routing statis dapat didefinisikan nilai AD lebih kecil dari routing dinamis.




```
GAD#configure terminal
GAD(config)#ip route 172.16.0.0 255.255.0.0
192.168.14.2 130
GAD#show ip route
Codes: C - connected, s - static, I - IGRP, R - RIP,
M - mobile, B - BGP
           D - EIGRP, EX - EIGRP external, O -
OSPF, IA - OSPF inter area
           N1 - OSPF NSSA external type 1, N2 -
```

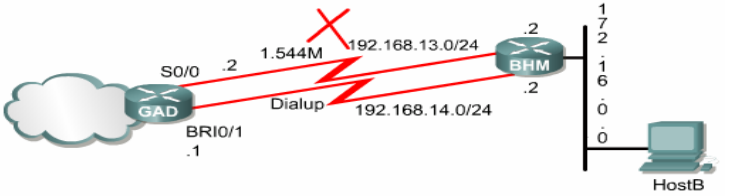
Gambar 7.20 RIP dengan floating static

Setelah routing statis ke jaringan 172.16.0.0 melalui 192.168.14.2 dimasukkan, dalam table routing tidak akan kelihatan. Hanya routing dinamis yang mempelajari melalui RIP, hal ini karena AD 130 lebih besar dari routing statis jika tidak jalur RIP akan melalui S0/0 putus, routing statis tidak akan dipasang dalam table routing.

Rute statis pada titik dimana interface akan di-advertise oleh router RIP yang memiliki rute statis itu dan dipropagasi ke internetwork. Hal ini karena rute

statis pada titik itu dihubungkan dan mereka kehilangan rute statis. Jika rute statis didefinisikan ke interface dengan perintah **network**, perintah **redistribute static** harus di-spesifikasikan dalam proses RIP sebelum RIP akan advertise rute.

Pada saat interface down, semua rute statis dihapus dari table routing IP. Pada gambar berikut rute statis dikonfigurasi dalam router GAD yang diletakkan pada rute RIP pada saat proses routing RIP gagal. Hal ini disebut dengan floating static route. Untuk mengkonfigurasi rute statis, AD 130 didefinisikan dalam rute statis. Hal ini lebih besar dari default AD 120. router BHM akan membutuhkan dikonfigurasi dengan default route.




```
GAD#show ip route
Codes: C - connected, s - static, I - IGRP, R - RIP,
M - mobile, B - BGP
             D - EIGRP, EX - EIGRP external, O -
OSPF, IA - OSPF inter area
             N1 - OSPF NSSA external type 1, N2 -
OSPF NSSA external type 2
             E1 - OSPF external type 1, E2 - OSPF
external type 2, E - EGP
             i - IS-IS, L1 - IS-IS level - 1, L2 -
```

Gambar 7.21 Floating static dengan rute RIP yang gagal

Untuk mengkonfigurasi rute statis, menggunakan perintah yang ditunjukkan gambar berikut.

Command	Purpose
ip route destination mask {interface/nexthop}	Establish a static route

Gambar 7.22 Konfigurasi static route

7.11 Perintah Perintah Yang Digunakan

Daftar berikut mengandung sebuah rangkuman dari semua perintah yang digunakan pada bab ini.

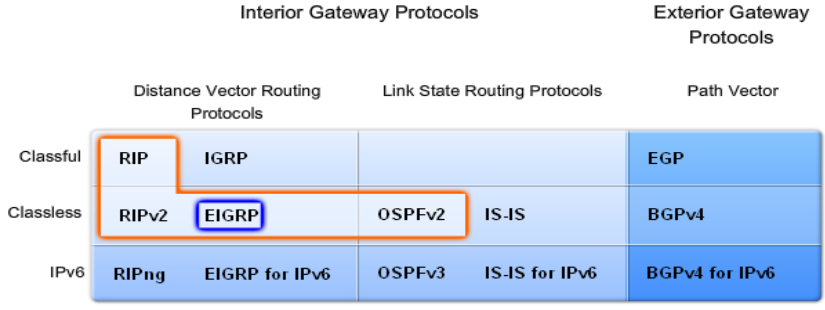
Perintah	Keterangan
Show ip router	Menampilkan routing table
Ip route	Menciptakan route statis dan route default pada sebuah router
Ip classless	Merupakan perintah global configuration yang digunakan untuk memberitahu router agar meneruskan (forward) paket ke sebuah route yang default ketika network tujuan ada di routing tbale
Router rip	Menghidupkan routing IP RIP di sebuah router
Network	Memberitahu routing protocol tentang network apa yang akan diumumkan
No ip route	Menghapus sebuah route statis atau route default
Show protocols	Menunjukkan routed protocol dan alamat network yang dikonfigurasi pada setiap interface
Show ip protocols	Menunjukkan routing protocol dan timer – timer yang berkaitan dengan setiap routing protocol yang dikonfigurasi
Debug ip rip	Mengirimkan pesan konsol yang menampilkan informasi tentang paket RIP yang dikirim dan diterima pada sebuah interface router

Bab 8

Enhanced Interior Gateway Protocol (EIGRP)

8.1 Pendahuluan

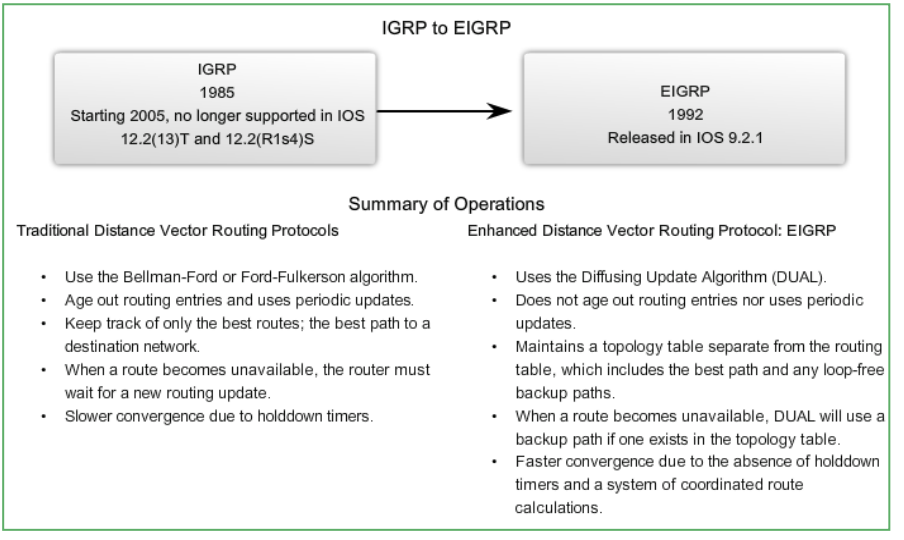
Enhanced Interior Gateway Routing Protocol (EIGRP) adalah sebuah protocol proprietary Cisco yang bekerja pada router Cisco dan pada prosesor - prosesor route internal yang terdapat pada switch layer core dan switch layer distributor Cisco. EIGRP adalah sebuah distance vector routing protocol yang mendukung classless routing protocol. EIGRP dirilis pada tahun 1992 dengan IOS 9.21. Seperti namanya, EIGRP merupakan pengembangan dari IGRP Cisco (Interior Gateway Routing Protocol). Keduanya adalah protokol proprietary Cisco dan hanya beroperasi pada router Cisco [12].



Gambari 9.1 Routing Protocol EIGRP

Enhanced Interior Gateway Routing Protocol (EIGRP) adalah sebuah protocol distance-vector yang classless dan yang sudah ditingkatkan

(enhanced), yang memberikan kita keunggulan yang nyata dibandingkan protocol propriertary Cisco lainnya, yaitu Interior Gateway Routing Protocol (IGRP). Inilah pada dasarnya mengapa ia disebut Enhanced IGRP. Seperti IGRP, EIGRP menggunakan konsep dari sebuah autonomous system untuk menggambarkan kumpulan dari router-router yang contiguous (berentetan ,sebelah-menyebelah)yang menjalankan routing protocol yang sama dan berbagi informasi routing. Tetapi tidak seperti IGRP, EIGRP memasukan subnet mask ke dalam update route-nya. Dan seperti yang anda ketahui sekarang, pengumuman (advertisement)dari informasi subnet memungkinkan kita menggunakan VLSM dan melakukan summarization (perangkuman) ketika merancang network-network kita [12].



Gambar 9.2 Perbedaan IGRP dengan EIGRP

EIGRP kadang-kadang disebut sebagai routing protocol protocol hybrid karena ia mempunyai karakteristik-karakteristik baik dari protocol distance-vector maupun dari protocol link-state.sebagai contih, EIGRP tidak mengirimkan paket-paket link-state seperti dilakukan OSPF; melainkan ia mengirimkan update distance-vector yang tradisional yang berisi informasi

tentang network-network ditambah dengan cost(biaya) untuk mencapai mereka dari prespektif router yang melakukan pengumuman tersebut.

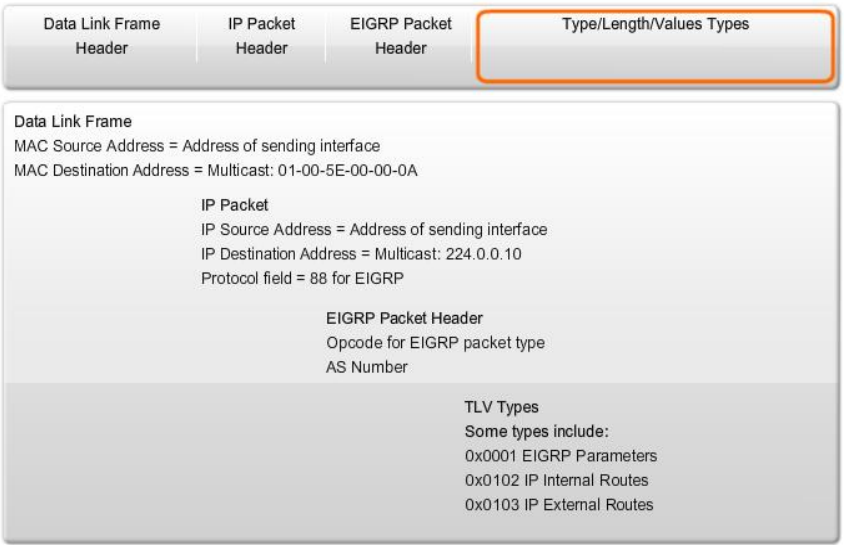
Sebuah EIGRP memiliki karakteristik-karakteristik link-state juga-ia mensinkronisasikan routing table antara router-router tetangga pada saat dimulai dijalankan (startup), dan kemudian mengirimkan update-update yang spesifik hanya jika topologi network berubah. Ini membuat EIGRP sesuai untuk network-network yang sangat besar. EIGRP mempunyai sebuah jumlah hop maksimum.

Ada sejumlah fitur yang kuat dan membuat EIGRP jauh lebih baik dibandingkan IGRP dan protocol-protocol lainnya. Yang utamanya adalah sebagai berikut :

- Mendukung IP, IPX,dan AppleTalk melalui modul-modul yang bersifat protocol-dependent (bergantung pada protocol)
- Pencarian network tetangga (neighbor discovery) yang dilakukan dengan efisien
- Komunikasi melalui Reliable Transport Protocol (RTP)
- Pemilihan jalur terbaik melalui Diffussing Upadsate Algorithm (DUAL)

8.2 EIGRP Message Format

Bagian data dari message EIGRP akan diencapsulasi dalam sebuah paket. Di dalam paket tersebut terdapat beberapa field data yang disebut Type/Length/Value or TLV. Header paket EIGRP disertakan dengan setiap paket EIGRP, terlepas dari jenis. EIGRP paket header dan TLV kemudian diencapsulasi menjadi paket IP. Dalam header paket IP, field protokol diatur ke 88 menunjukkan EIGRP, dan alamat tujuan diatur ke multicast 224.0.0.10. Jika paket EIGRP dirumuskan dalam sebuah frame Ethernet, alamat tujuan MAC juga merupakan alamat multicast: 01-00-5E-00-00-0A



Gambar 9.2 Encapsulated EIGRP message

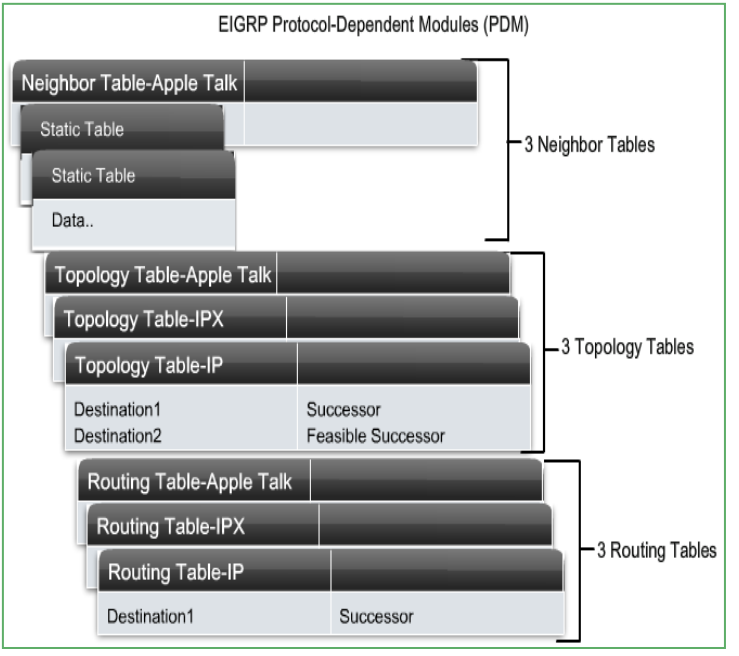
8.3 Protocol Dependent Modules (PDM)

Satu dari Fitur paling menarik EIGRP adalah ia menyediakan dukungan routing untuk berbagai protokol layer network : IP, IPX dan AppleTalk. Satu-satunya routing protocol lain yang hampir menyamai EIGRP dan mendukung banyak protokol layer network adalah Intermediate System to Intermediate System (IS-IS) tetapi protocol ini hanya mendukung IP dan Connectionless Network Service (CLNS).

EIGRP mendukung protocol-protocol layer Network yang berbeda melalui penggunaan modul-modul yang disebut protocol-dependent modules (PDMs). Setiap PDM dari EIGRP akan memelihara serangkaian tabel yang terpisah yang mengandung informasi routing yang berlaku untuk sebuah protocol yang spesifik. Ini artinya akan ada table-tabel IP/EIGRP, table-tabel IPX/EIGRP, dan table-tabel AppleTalk/EIGRP.

Sebagai contoh :

- Modul IP-EIGRP bertanggung jawab untuk mengirim dan menerima paket EIGRP yang dikemas dalam IP dan untuk menggunakan DUAL untuk membangun dan memelihara tabel routing IP. Seperti yang dapat dilihat pada gambar, EIGRP menggunakan paket EIGRP yang berbeda dan melakukan separate neighbor terpisah, topologi, dan tabel routing untuk setiap protokol network layer.
- Modul IPX EIGRP bertanggung jawab untuk bertukar informasi routing tentang jaringan IPX dengan router lainnya yang mengunakan IPXEIGRP



Gambar 9.3 EIGRP Protocol-dependent Modules (PDM)

8.4 RTP and EIGRP Packet Types

EIGRP menggunakan sebuah protocol proprierty, yang disebut Reliable Transport Protocol (RTP), untuk mengelola komunikasi dari pesan-pesan diantara router-router yang menggunakan EIGRP. Dan seperti yang terlihat dari namanya, reliabilitas adalah perhatian utama dari protocol ini. Cisco telah merancang sebuah mekanisme yang memanfaatkan multicast dan unicast untuk mengirimkan update secara cepat , dan untuk melacak penerimaan data.

Ketika EIGRP mengirimkan lalu-lintas multicast, ia menggunakan alamat Class D 224.0.0.10 . Setiap router EIGRP menyadari tentang siapa router-router tetangganya, dan untuk setiap multicast yang dikirimkan keluar, router EIGRP akan memelihara sebuah daftar dari tetangga-tetangga yang telah menjawab.Jika EIGRP tidak mendapatkan jawaban dari satu tetangganya, ia akan beralih menggunakan unicast untuk mengirimkan kembali data yang sama.

Jika masih tidak mendapatkan jawaban sebuah jawaban sampai dengan 16 kali percobaan unicast, maka tetangga tersebut dinyatakan mati. Orang sering menyebut proses ini sebagai Reliable multicast.

Router menyimpan setiap informasi yang mereka kirimkan dengan memberikan sebuah nomor urut (sequence number) pada setiap paket. Dengan tekni ini, adalah mungkin bagi router untuk mendeteksi datangnya informasi yang sudah lama, informasi yang redundant, atau yang tidak urut (out-of-sequence).

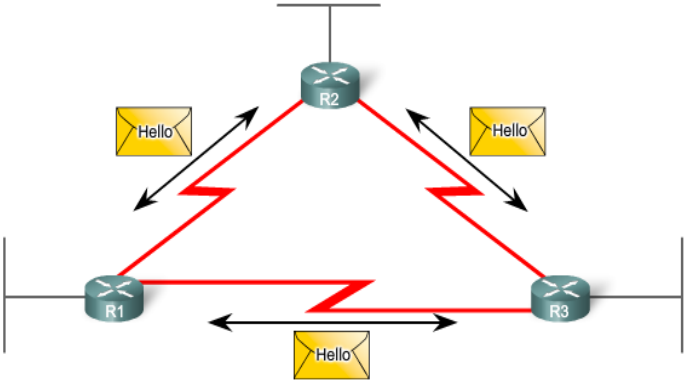
Kemampuan melakukan hal-hal ini adalah sangat penting karena EIGRP merupakan sebuah protokol yang diam (quiet). EIGRP bergantung pada kemampuannya melakukan sinkronisasi database-database routing pada saat mulai bekerja (startup) dan kemudian memelihara konsistensi database-nya terhadap waktu dengan cara mengkomunikasikan hanya perubahan-perubahannya saja. Jadi, hilangnya paket-paket secara permanen, atau paket

yang dieksekusi dengan tidak urut, dapat mengakibatkan rusaknya database routing tersebut.

8.5 EIGRP Packet Types

EIGRP saling berkomunikasi dengan tetangga (neighbor) nya secara multicast (224.0.0.10) dan menggunakan 5 jenis pesan (message) dalam berhubungan dengan neighbornya:

- **Hello:** Router-Router menggunakan paket Hello untuk menjalin hubungan neighbor. Paket-paket dikirimkan secara multicast dan tidak membutuhkan.
- **Update:** Untuk mengirimkan update informasi routing. Tidak seperti RIP yang selalu mengirimkan keseluruhan tabel routing dalam pesan Update, EIGRP menggunakan triggered update yang berarti hanya mengirimkan update jika terjadi perubahan pada network (mis: ada network yang down). Paket update berisi informasi perubahan jalur/route. Update-update ini dapat berupa unicast untuk router tertentu atau multicast untuk beberapa router yang terhubung.
- **Query:** Untuk menanyakan suatu route kepada tetangga. Biasanya digunakan saat setelah terjadi kegagalan/down pada salah satu route network, dan tidak terdapat feasible successor untuk route/jalur tersebut. router akan mengirimkan pesan Query untuk memperoleh informasi route alternatif untuk mencapai network tersebut, biasanya dalam bentuk multicast tapi bisa juga dalam bentuk unicast untuk beberapa kasus tertentu.
- **Reply:** Respon dari pesan **Query**.
- **ACK:** Untuk memberikan acknow ledgement (pengakuan/konfirmasi) atas pesan Update, Query, dan Reply.



Bandwidth	Example Link	Default Hello Interval	Default Hold Time
1.544 Mbps	Multipoint Frame Relay	60 seconds	180 seconds
Greater than 1.544 Mbps	T1, Ethernet	5 seconds	15 seconds

Gambar 9.4 Default hello interval dan hold times EIGRP

Administrative Distance

Seperti yang kita ketahui dari Bab 3, " "Introduction to Dynamic Routing Protocols," administrative distance (AD) adalah kepercayaan (atau preferensi) dari sumber rute. EIGRP memiliki default administrative distance 90 untuk internal routes dan 170 untuk imported from an external source, seperti rute default. Bila dibandingkan dengan lain protokol gateway interior (iGPS), EIGRP adalah yang paling disukai oleh Cisco IOS karena memiliki administrative distanc terendah ,Perhatikan pada gambar bahwa EIGRP memiliki nilai AD ketiga, dari 5, untuk summary routes .

Route Source	Administrative Distance
Connected	0
Static	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
External EIGRP	170
Internal BGP	200

Gambar 9.5 Default administrative distance

8.6 Basig EIGRP Configuration

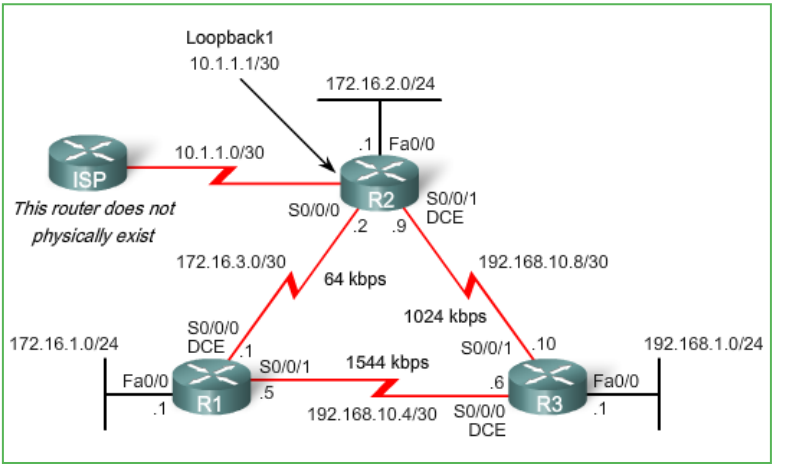
The router EIGRP command

router eigrp autonomous-system adalah command global yang digunakan untuk mengaktifkan EIGRP. autonomous system parameter nomor yang dipilih oleh administrator jaringan antara 1 dan 65535. Nomor yang dipilih adalah nomor proses ID dan ini penting karena semua router dalam domain routing EIGRP harus menggunakan ID proses nomor yang sama. Dibawah ini adalah configturasi EIGRP pada sebuah router cisco:

```
router eigrp autonomous-system
Router(config-router)#network network-address
Router(config-router)#network network-address[wildcard-mask]
```

wildcard mask adalah sebagai invers dari subnet mask. Kebalikan dari subnet mask 255.255.255.252 adalah 0.0.0.3. Untuk menghitung invers dari subnet mask, kurangi subnet mask dari 255.255.255.255:

255.255.255.255
- 255.255.255.252
Subtract the subnet mask
---
0. 0. 0. 3
Wildcard mask



Gambar 9.6 EIGP Topology configurasi

Konfigurasi R1

```
R1 (config)#router eigrp 100
R1(config-router)#network 192.168.10.4 0.0.0.3
R1(config-router)#network 172.16.3.0 0.0.0.3
R1(config-router)#network 172.16.1.0 0.0.0.255
```

Konfigurasi R2

```
R2 (config)#router eigrp 100
R2(config-router)#network 192.168.10.8 0.0.0.3
R2(config-router)#network 172.16.3.0 0.0.0.3
R2(config-router)#network 172.16.1.0 0.0.0.255
```

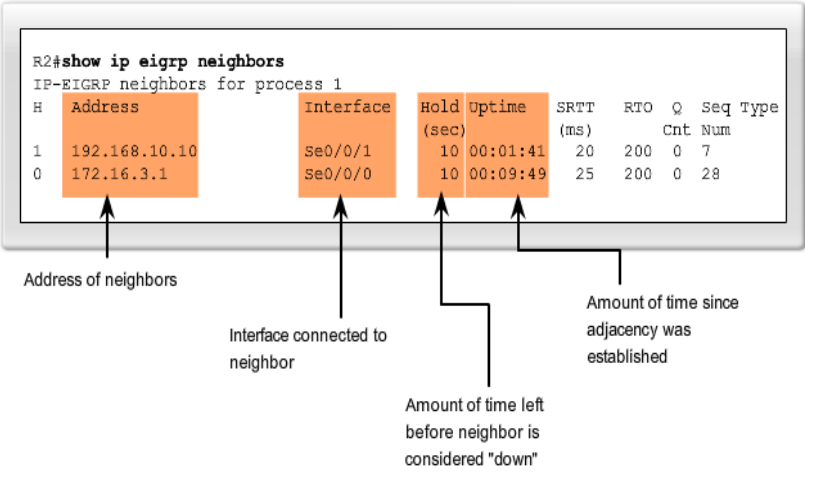
Konfigurasi R3

```
R3 (config)#router eigrp 100
R3(config-router)#network 192.168.10.8 0.0.0.3
R3(config-router)#network 192.168.4.0 0.0.0.3
R3(config-router)#network 192.168.1.0 0.0.0.255
```

8.7 Verifying EIGRP

Sebelum update dapat dikirim atau diterima oleh EIGRP, router harus membangun adjacencies dengan router tetangga mereka. EIGRP akan membangun adjacencies dengan router tetangga dengan bertukar hello paket EIGRP.

Gunakan perintah **show ip eigrp neighbors** untuk melihat tabel tetangga dan memverifikasi bahwa EIGRP telah membentuk adjacency dengan tetangganya. Untuk setiap router, Anda harus dapat melihat alamat IP dari router yang berdekatan dan interface yang digunakan router ini untuk mencapai EIGRP tetangga. Pada gambar, kita dapat memverifikasi bahwa semua router telah menetapkan adjacencies yang diperlukan. Setiap router memiliki dua tetangga yang tercantum dalam tabel tetangga.



Gambar 9.7 The neighbors table

Perintah **show ip eigrp neighbors** sangat berguna untuk memverifikasi dan memecahkan masalah pada EIGRP. Jika tetangga tidak terdaftar setelah adjacencies telah didirikan dengan tetangga router, periksa antarmuka lokal untuk memastikan itu diaktifkan dengan perintah **show ip interface brief**. Jika interface telah aktif, coba ping alamat IP dari tetangga. Jika ping gagal, itu

berarti bahwa interface tetangga down dan perlu diaktifkan. Jika ping berhasil dan EIGRP masih tidak melihat router tetangga, periksa konfigurasi berikut :

- Apakah kedua router dikonfigurasi dengan EIGRP proses ID yang sama?
- Apakah *directly connected network* dimasukkan dalam laporan jaringan EIGRP?
- Apakah perintah **passive-interface** dikonfigurasi untuk mencegah paket Halo EIGRP pada interface?

8.8 EIGRP Composite Metric and The K Values

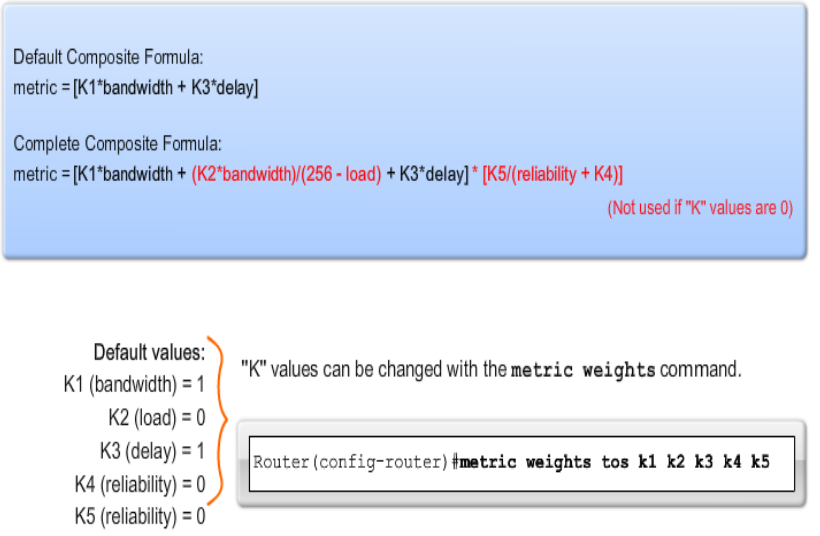
EIGRP menggunakan nilai berikut dalam metrik komposit untuk menghitung jalur pilihan ke network :

- Bandwidth
- Delay
- Reliability
- Load

The Composite Metric

Angka ini menunjukkan rumus metrik komposit yang digunakan oleh EIGRP. Formula terdiri dari nilai-nilai K1 sampai K5, yang dikenal sebagai bobot metrik EIGRP. Secara default, K1 dan K3 di set ke 1, dan K2, K4, K5 dan diatur ke 0. Hasilnya adalah bahwa hanya bandwidth dan nilai-nilai delay yang digunakan dalam perhitungan metrik standar komposit. Nilai default K dapat diubah dengan perintah router EIGRP:

Router(config-router)#metric weights tos k1 k2 k3 k4 k5



Gambar 9.8 EIGRP Composite metric

8.9 Dual Concepts

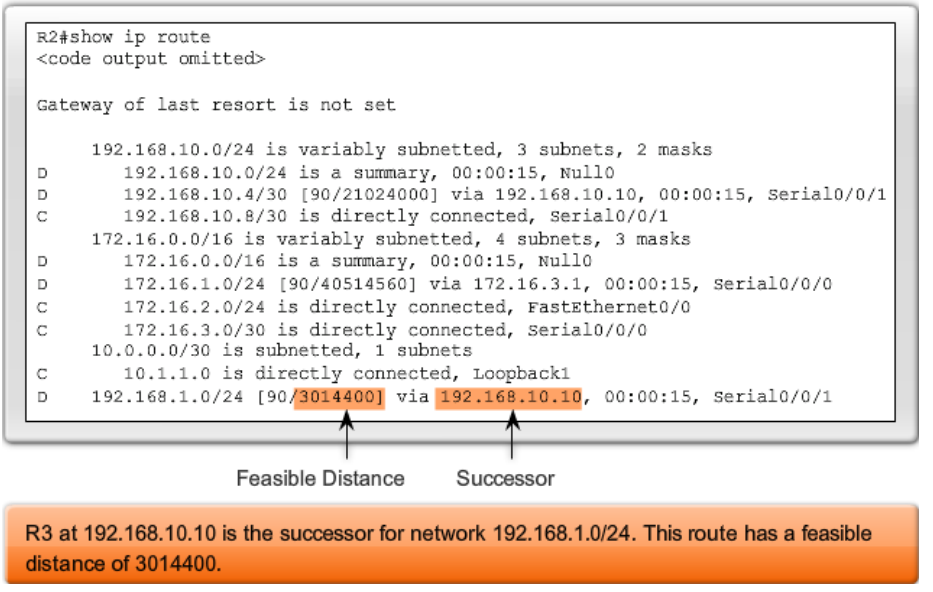
Sebagaimana dinyatakan dalam bagian sebelumnya, DUAL (Diffusing update Algoritma) adalah algoritma yang digunakan oleh EIGRP. Bagian ini akan membahas bagaimana menentukan DUAL best loop-free dan loop-free cadangan. DUAL menggunakan beberapa istilah yang akan dibahas secara lebih rinci pada seluruh bagian ini:

- Successor
- Feasible Distance (FD)
- Feasible Successor (FS)
- Reported Distance (RD) or Advertised Distance (AD)
- Feasible Condition or Feasibility Condition (FC)

Successor and Feasible Distance (FD)

Successor adalah router tetangga yang digunakan untuk meneruskan paket dan rute dengan biaya terendah ke jaringan tujuan. Alamat IP penggantinya akan ditampilkan di entri tabel routing tepat setelah kata **via.**

Feasible distance (FD) adalah adalah metrik terendah untuk mencapai network tujuan. FD adalah metrik yang tercantum dalam entri tabel routing sebagai nomor kedua di dalam tanda kurung. Seperti dengan protokol routing lain ini juga dikenal sebagai metrik untuk rute.



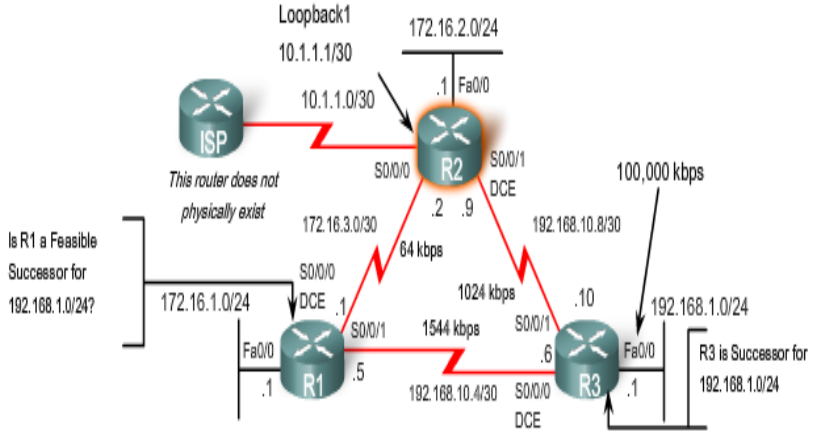
Gambar 9.9 Successor and Feasible Distance (FD)

Feasible Successor ,Reported Distance ,Feasible Condition

Feasible successor (FS) adalah router tetangga yang memiliki jalur loop-free backup untuk network yang sama *successor*-nya dengan kondisi jalur yang layak.

Reported Distance adalah total metric sepanjang jalur ke network tujuan sebagai advertised dari router tatangga dalam EIGRP.

Feasibility condition (FC) terpenuhi ketika *reported distance (RD)* ke network kurang dari *feasible distance* router lokal ke network tujuan yang sama.




```
R2#show ip route
<code output omitted>

Gateway of last resort is not set

     192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D       192.168.10.0/24 is a summary, 00:00:15, Null0
D       192.168.10.4/30 [90/21024000] via 192.168.10.10, 00:00:15, Serial0/0/1
C       192.168.10.8/30 is directly connected, Serial0/0/1
```

Gambar 9.10 Feasible Successor

8.10 Perintah Perintah Yang Digunakan

Perintah	Keterangan
Router eigrp as	Melalui proses – proses EIGRP pada sebuah router menggunakan sebuah nomor autonomous system tertentu
Network *ip-address*	Mengaktifkan EIGRP pada interface – interface local yang berada pada network yang ditentukan. EIGRP dikonfigurasi dengan sebuah alamat classful
Passive-interface *interface-type interface number*	Mengidentifikasi interface – interface yang tidak berpartisipasi dalam update – update EIGRP
No auto – summary	Mematikan summarization otomatis dari route – route pada batas – batas classful
Show ip eigrp neighbors	Menunjukkan semua tetangga EIGRP
Show ip route eigrp	Menunjukkan semua route EIGRP
Show ip eigrp topology	Menunjukkan entri – entri dalam topology tabel EIGRP
Show ip eigrp traffic	Menunjukkan packet yang dihitung sebagai packet EIGRP yang dikirim dan diterima

Bab 9

Link-State Protocol

9.1 Pendahuluan

Dalam bab 3. "Introduction to Dynamic Routing Protocols" mengilustrasikan kepada kita perbedaan antara link-state dan distance vector beserta analoginya. Analogi distance vector routing protocols menyatakan bahwa distance vector layaknya seperti menggunakan tanda – tanda di jalan sebagai petunjuk untuk sampai ke tempat tujuan. Distance vector hanya memberikan informasi tentang jarak dan arah untuk sampai ke tujuan. Namun berbeda dengan link-state routing protocol, pada link-state routing protocol kita seakan menggunakan peta untuk sampai ke tujuan. Dengan peta kita dapat melihat semua potesial jalur terbaik dan link-state routing protocol menentukan sendiri pilihannya untuk sampai ke tempat tujuan.

Distance vector routing protocols layaknya seperti tanda – tanda dijalan, karena router harus membuat keputusan *best path* berdasarkan distance dan metric ke tujuan. Router yang menggunakan distance vector percaya bahwa router lain pasti memberikan informasi **best path** yang benar untuk sampai ke tujuan hanya dengan mengunakan jalur terpendek [13].

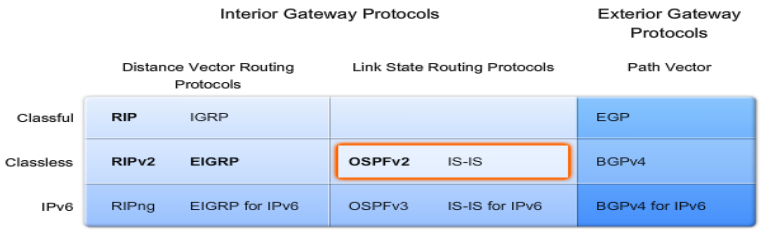
Berbeda dengan link-state routing protocols, link-state sama halnya seperti peta sebuah jalan. Dimana link-state membuat peta jalan sendiri yang dipejari dari topologi jaringan yang ada dan setiap router menggunakan peta ini untuk menentukan the best path ke setiap network tujuan dengan melakukan perhitungan jalur mana yang paling baik untuk melewatkan packet data. Jalur yang terpendek belum tentu jalur yang terbaik bagi link-state routing protocols.

Router menjalankan link-state routing protocols dengan mengirimkan semua informasi tentang keadaan link (jalur) ke router lain dalam domain routing yang sama. Link-sate tersebut akan berisi informasi network yang

berhubungan secara langsung melalui sebauh interface, informasi tetang type network, dan router – router tetangga yang ada didalam network tersebut. Tujuan utamanya adalah setiap router akan menerima semua informasi link-state tentang semua router lain di daerah domain routing. Dengan informasi link-state ini, setiap router akan dapat membuat sendiri peta topologi jaringannya dan akan secara independen menghitung jalur terpendek ke setiap network.

9.2 Link-state Routing Protocols

Link-state routing protocols yang dikenal juga sebagai *shortest path first* dibangun dengan menggunakan Edsger Dijkstra's shortest path first (SPF) algorithm. Link-state routing protocols memiliki reputasi yang jauh lebih kompleks daripada routing protocols lain yaitu distance vector. Namun, fungsi dasar dan konfigurasi protokol link-state routing tidak rumit sama sekali. Bahkan algoritma itu sendiri dapat dengan mudah dipahami. Operasi dasar OSPF dapat dikonfigurasi dengan menggunakan perintah **router ospf process-id** dan diikuti dengan perintah **network**, mirip dengan routing protokol lain seperti RIP dan EIGRP [13].

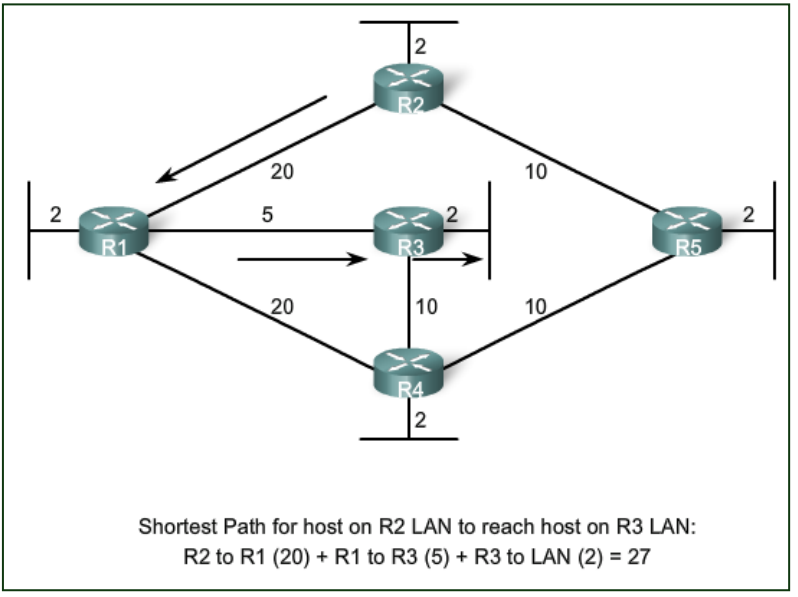


Gambar 10.1 Clasification of routing protocols

9.3 Introduction To The OSPF Algorithm

Algoritma Dijkstra sering disebut sebagai algoritma *shortest path first* (SPF). Algoritma ini menggunakan cost pada setiap path untuk menghitung jalur terbaik untuk mengirim sebuah packet dari suatu sumber ke tujan. Pada gambar dibawah ini, setiap jalur telah diberi label

dengan nilai cost untuk mencapai network yang dituju. Cost dengan jalan terpendek dari R2 ke R3 adalah 27. Setiap router menentukan biaya sendiri untuk setiap tujuan dalam topologi. Dengan kata lain, setiap router menghitung algoritma SPF dan menentukan biaya dari perspektif sendiri.



Gambar 10.2 Dijkstra's shortest path first algorithm

9.4 Link-state Routing Process

cara kerja link-state routing protocol :

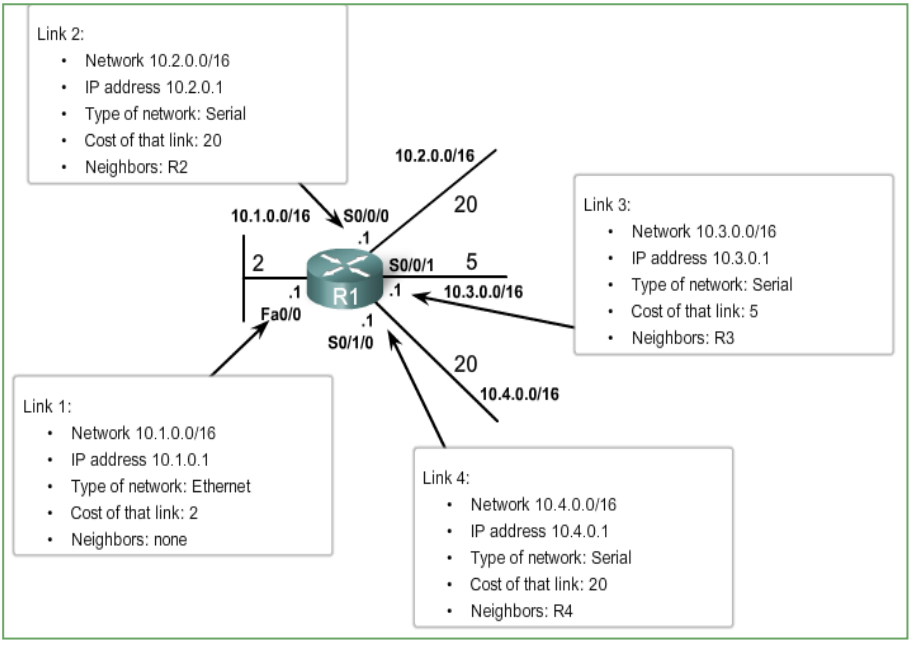
1. Setiap router belajar tentang link sendiri, directly connected (interface yang terhubung langsung ke router).
2. Setiap router bertanggung jawab untuk menghubungi tetangganya dengan dengan mengirimkan **hello packet**.
3. Setiap router membangun paket Link-state (LSP) yang berisi keadaan setiap link yang terhubung langsung.
4. Setiap router menyebarkan LSP ke semua router tetangga, dan kemudian menyimpan semua LSP yang diterima dalam database.

5. Setiap router menggunakan database untuk membangun peta lengkap dari topologi dan menghitung jalur terbaik ke setiap network tujuan.

Learning About Derectly Connected Networks

Pada link-state routing protocols, link (interface) perlu didefenisikan dan dikonfirasi. Sama hal pada distance vector routing protocols dan static route. Interface harus benar – benar dikonfigurasi dengan alamat dan subnet mask. Dan harus dipastikan bahwa link tersebut dalam keadaan **up**.

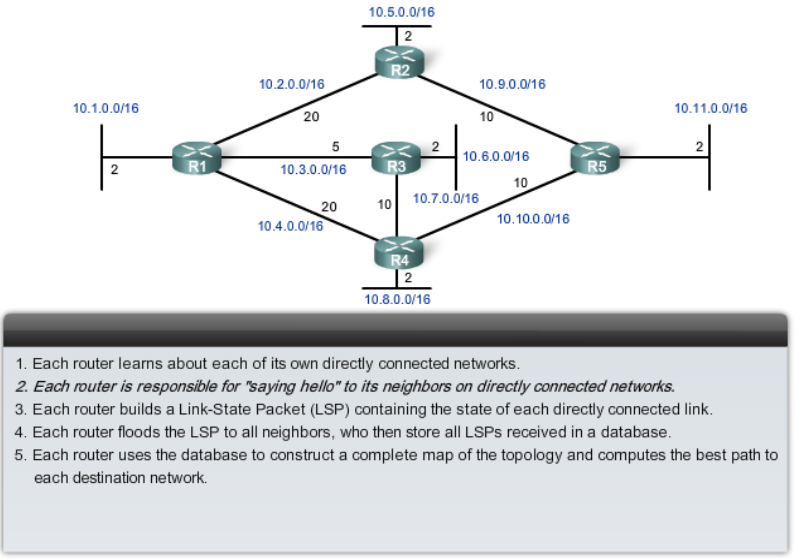
Gambar dibawah ini menunjukkan R1 memiliki 4 link (interface) yang sifatnya *directly connected*.



Gambar 10.3 link-state information pada R1

Sending hello packets to neighbors

Router yang mengunakan link-state routing protokol menggunakan **Hello protocol** untuk menemukan setiap tetangga di link nya. Semua router tetangga yang menggunakan link-state routing protocol akan mendapatkan hello packet dari sebuah router.

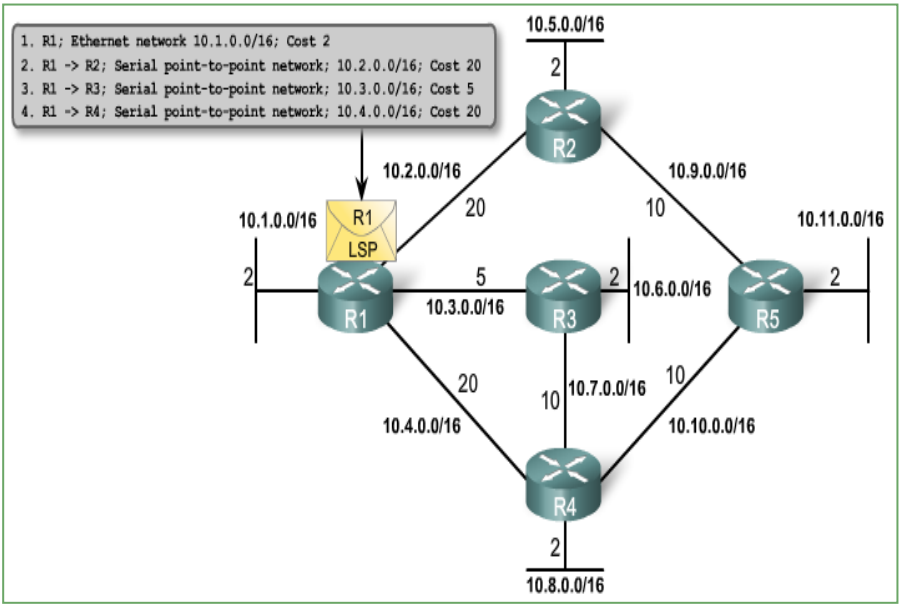


Gambar 10.4 Link-state routing process

Building Link-State Packet

Setelah router telah melakukan adjacencies, router akan membangun link-state paket (LSP) yang berisi informasi link-state tentang link nya. Sebuah versi sederhana dari LSP dari R1:

1. R1; Ethernet network 10.1.0.0/16; Cost 2
2. R1 -> R2; Serial point-to-point network; 10.2.0.0/16; Cost 20
3. R1 -> R3; Serial point-to-point network; 10.3.0.0/16; Cost 5
4. R1 -> R4; Serial point-to-point network; 10.4.0.0/16; Cost 20

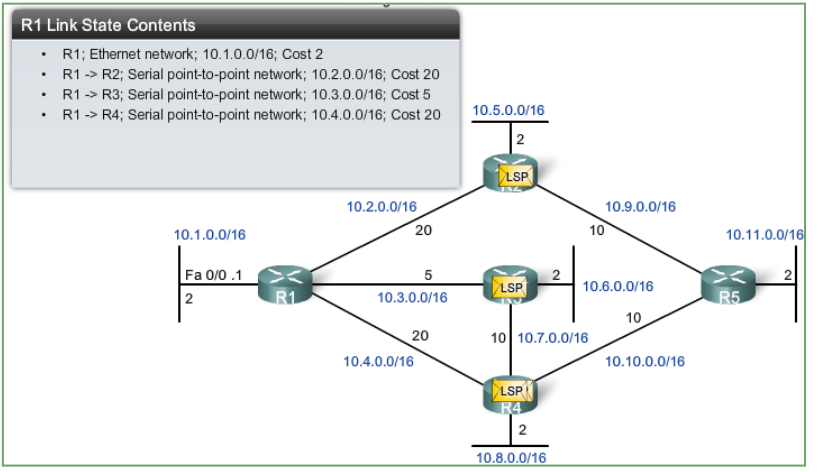


Gambar 10.5 Link-State Packet (LSP) pada R1

Flooding Link-state Packets To Neighbors

Link-State Packet tidak perlu dikirim secara berkala. LSP hanya perlu dikirim pada :

- Selama startup awal dari router atau proses routing protokol pada router
- Setiap kali ada perubahan dalam topologi, termasuk link **down** atau **up**, atau terjadi adjacency dengan router tetangga.

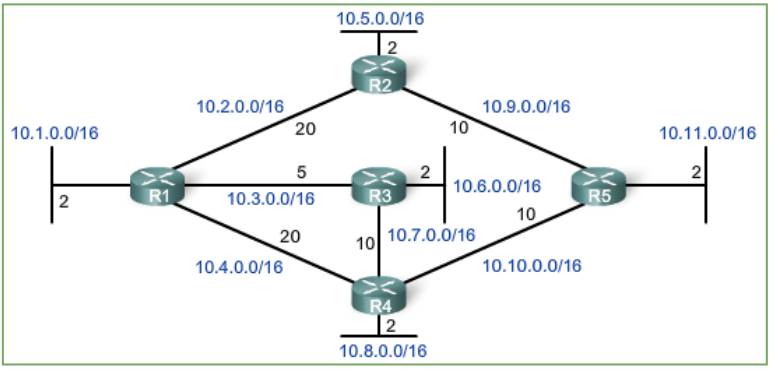


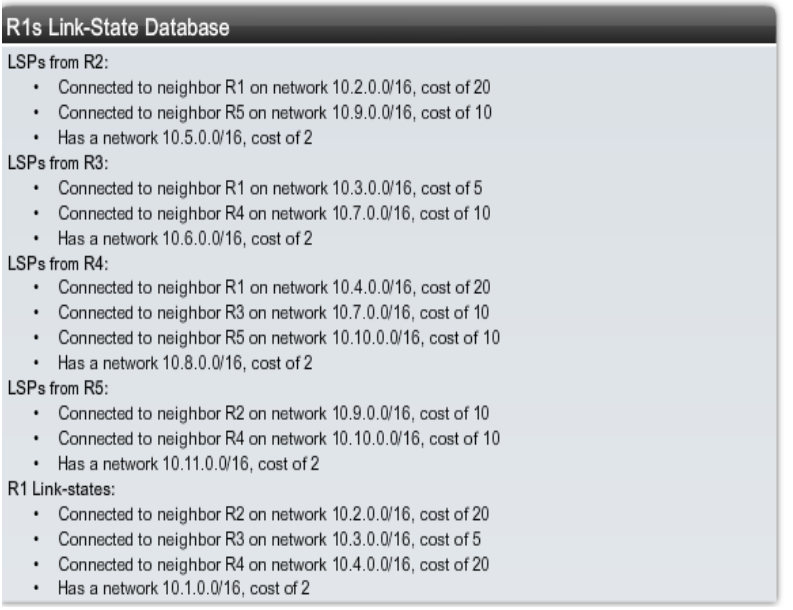
Gambar 10.6 Flooding of R1 LSP

Constructing a Link-state Database

Step terakhir dari link-state routing proses adalah :

Setiap router menggunakan database untuk membangun peta lengkap yang diambil dari topologi dan menghitung jalur terbaik ke setiap network tujuan. Setelah setiap router menyebarkan LSP-nya menggunakan proses flooding link-state, setiap router akan memiliki LSP dari setiap router link-state di area routing. LSP ini disimpan dalam database link-state. Setiap router dalam area routing yang sama dapat menggunakan algoritma SPF untuk membangun SPF trees yang telah dibahas sebelumnya.





Gambar 10.7 Links-state database

Advantage of a Link-state Routing Protocol

Ada beberapa keuntungan dari link-state routing protokol dibandingkan dengan protokol distance vector routing.

Builds a Topological Map

Link-state routing protokol membuat peta topologi jaringan sendiri, atau SPF tree. Karena link-state routing protokol melakukan pertukaran link-state, setiap router secara independen dapat menentukan jalur terpendek ke setiap network. Sedangkan distance vector routing protocols tidak memiliki peta topologi jaringan. Router yang mengimplementasikan distance vector routing protokol hanya menggunakan network yang telah terdaftar saja sebagai pilihan route yang dihitung berdarsarkan cost (distance) and next-hop routers (direction).

Fast Convergence

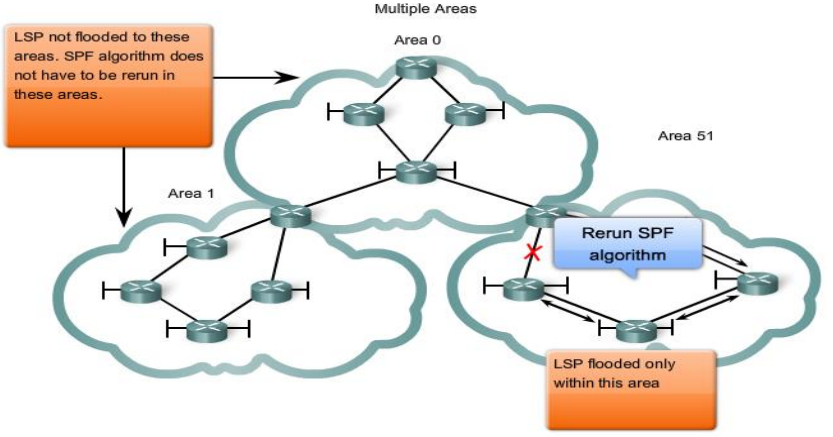
Ketika menerima Link-state Packet (LSP), link-state routing protokol membanjiri semua interface dengan Link-state Packet (LSP), kecuali untuk interface sumber LSP. Sedangkan router yang menggunakan distance vector routing protocols membutuhkan proses untuk update route dan update tabel routing sebelum membanjirinya ke semua interface. Dari proses kerja kedua protocol routing ini, konvergensi yang lebih cepat dicapai adalah dengan menggunakan link-stete routing protocols.

Event-driven Updates

Setelah membanjiri semua interface dengan Link-state Packet (LSP), link-state routing protokol hanya mengirimkan LSP kembali ketika ada perubahan dalam topologi network. LSP hanya berisi informasi tentang interface atau link yang berubah saja. Tidak seperti distance vector routing protocols, link-state routing protocol tidak menginrim update secara periodic.

Hierarchical Design

Link-state routing protocols seperti OSPF and IS-IS menggunakan suatu konsep yang disebut *areas*. Multiple areas secara langsung akan membuat hierarchical design to networks, memungkinkan untuk agregasi (summarization). dan mengisolasi (membatasi) masalah routing dalam suatu *areas*.



Gambar 10.8 Multipel areas pada link-state routing protocol

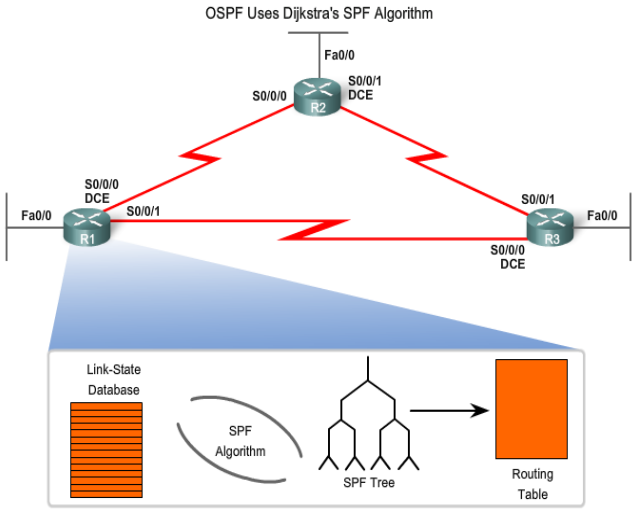
Bab 10

Open Shortest Path First (OSPF)

10.1 Pendahuluan

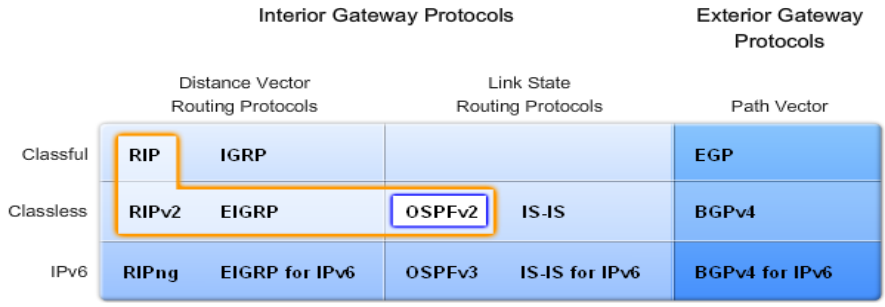
OSPF (Open Shortest Path First) ini merupakan protocol link-state. Teknologi link-state dikembangkan dalam ARPAnet untuk menghasilkan protokol yang terdistribusi yang jauh lebih baik daripada protokol distance-vector. Alih-alih saling bertukar jarak (distance) ke tujuan, setiap router dalam jaringan memiliki peta jaringan yang dapat diperbarui dengan cepat setelah setiap perubahan topologi. Peta ini digunakan untuk menghitung route yang lebih akurat daripada menggunakan protokol distance-vector. Perkembangan teknologi ini akhirnya menghasilkan protokol Open Shortest Path First (OSPF) yang dikembangkan oleh IETF untuk digunakan di Internet. Bahkan sekarang Internet Architecture Board (IAB) telah merekomendasikan OSPF sebagai pengganti RIP [14].

OSPF bekerja dengan sebuah algoritma yang disebut *Dijkstra*. Pertama, sebuah pohon jalur terpendek (*shortest path tree*) akan dibangun, dan kemudian *routing table* akan diisi dengan jalur terbaik yang dihasilkan dari pohon tersebut. OSPF melakukan *converge* dengan cepat, meskipun tidak secepat EIGRP, dan OSPF mendukung *multiple route* dengan biaya (cost) yang sama ke tutujuan yang sama [14].



Gambar 11.1 Dijkstra's SPF algorithn

Prinsip link-state routing sangat sederhana. Sebagai pengganti menghitung route "terbaik" dengan cara terdistribusi, semua router mempunyai peta jaringan dan menghitung semua route yang terbaik dari peta ini. Peta jaringan tersebut disimpan dalam sebuah basis data dan setiap record dalam basis data tersebut menyatakan sebuah link dalam jaringan. Record-record tersebut dikirimkan oleh router yang terhubung langsung dengan masing-masing link



Gambar 11.2 Routing protocol

Karena setiap router perlu memiliki peta jaringan yang menggambarkan kondisi terakhir topologi jaringan yang lengkap, setiap perubahan dalam jaringan harus diikuti oleh perubahan dalam basis data link-state yang terletak di setiap router. Perubahan status link yang dideteksi router akan mengubah basis data link-state router tersebut, kemudian router mengirimkan perubahan tersebut ke router-router lain.

Protokol yang digunakan untuk mengirimkan perubahan ini harus cepat dan dapat diandalkan. Ini dapat dicapai oleh protokol flooding. Dalam protokol flooding, pesan yang dikirim adalah perubahan dari basis data serta nomor urut pesan tersebut. Dengan hanya mengirimkan perubahan basis data, waktu yang diperlukan untuk pengiriman dan pemrosesan pesan tersebut lebih sedikit dibandingdengan mengirim seluruh isi basis data tersebut. Nomor urut pesan diperlukan untuk mengetahui apakah pesan yang diterima lebih baru daripada yang terdapat dalam basis data. Nomor urut ini berguna pada kasus link yang putus menjadi tersambung kembali.

Pada saat terdapat link putus dan jaringan menjadi terpisah, basis data kedua bagian jaringan tersebut menjadi berbeda. Ketika link yang putus tersebut hidup kembali, basis data di semua router harus disamakan. Basis data ini tidak akan kembali sama dengan mengirimkan satu pesan link-state saja. Proses penyamaan basis data pada router yang bertetangga disebut sebagai menghidupkan adjacency. Dua buah router bertetangga disebut sebagai adjacent bila basis data link-state keduanya telah sama. Dalam proses ini kedua router tersebut tidak saling bertukar basis data karena akan membutuhkan waktu yang lama.

Proses menghidupkan adjacency terdiri dari dua fasa.Fasa pertama, kedua router saling bertukar deskripsi basis data yang merupakan ringkasan dari basis data yang dimiliki setiap router. Setiap router kemudian membandingkan deskripsi basis data yang diterima dengan basis data yang dimilikinya. Pada fasa kedua, setiap router meminta tetangganya untuk mengirimkan record-record basis data yang berbeda, yaitu bila router tidak memiliki record tersebut, atau nomor urut record yang dimiliki lebih kecil daripada yang dikirimkan oleh deskripsi basis data. Setelah proses ini, router memperbarui beberapa record dan ini kemudian dikirimkan ke router-router lain melalui protokol flooding.

Protokol link-state lebih baik daripada protokol distance-vector disebabkan oleh beberapa hal: waktu yang diperlukan untuk konvergen lebih cepat, dan lebih penting lagi protokol ini tidak menghasilkan routing loop. Protokol ini mendukung penggunaan beberapa metrik sekaligus. Throughput, delay, biaya, dan keandalan adalah metrik-metrik yang umum digunakan dalam jaringan. Di samping itu protokol ini juga dapat menghasilkan banyak jalur ke sebuah tujuan. Misalkan router A memiliki dua buah jalur dengan metrik yang sama ke host B. Protokol dapat memasukkan kedua jalur tersebut ke dalam forwarding table sehingga router mampu membagi beban di antara kedua jalur tersebut.

Rancangan OSPF menggunakan protokol link-state dengan beberapa penambahan fungsi. Fungsi-fungsi yang ditambahkan antara lain mendukung jaringan multi-akses, seperti X.25 dan Ethernet, dan membagi jaringan yang besar mejadi beberapa area [14].

Telah dijelaskan di atas bahwa setiap router dalam protokol link-state perlu membentuk adjacency dengan router tetangganya. Pada jaringan multi-akses, tetangga setiap router dapat lebih dari satu. Dalam situasi seperti ini, setiap router dalam jaringan perlu membentuk adjacency dengan semua router yang lain, dan ini tidak efisien. OSPF mengefisienkan adjacency ini dengan memperkenalkan konsep designated router dan designated router cadangan. Semua router hanya perlu adjacent dengan designated router tersebut, sehingga hanya designated router yang adjacent dengan semua router yang lain. Designated router cadangan akan mengambil alih fungsi designated router yang gagal berfungsi.

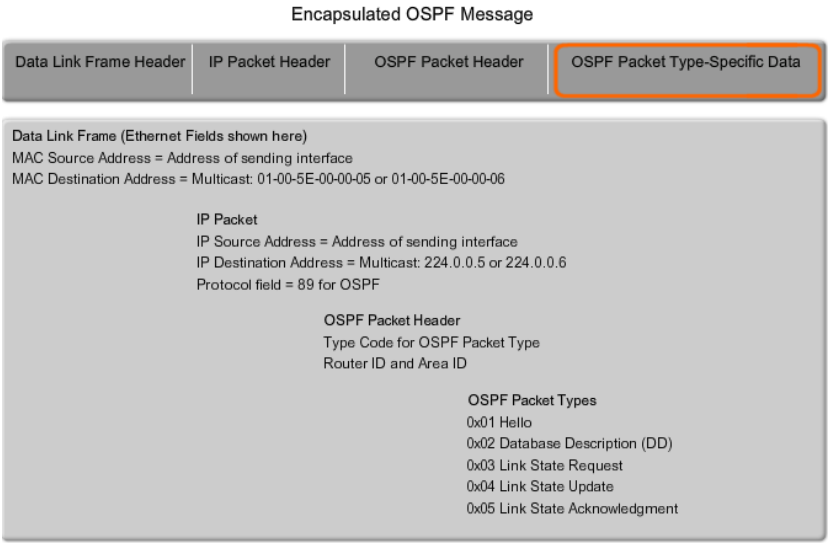
Langkah pertama dalam jaringan multi-akses adalah memilih designated router dan cadangannya. Pemilihan ini dimasukkan ke dalam protokol Hello, protokol dalam OSPF untuk mengetahui tetangga-tetangga router dalam setiap link. Setelah pemilihan, baru kemudian router-router membentuk adjacency dengan designated router dan cadangannya. Setiap terjadi perubahan jaringan, router mengirimkan pesan menggunakan protokol flooding ke designated router, dan designated router yang mengirimkan pesan tersebut ke router-router lain dalam link.

Designated router cadangan juga mendengarkan pesan-pesan yang dikirim ke designated router. Jika designated router gagal, cadangannya kemudian menjadi designated router yang baru serta dipilih designated router cadangan yang baru. Karena designated router yang baru telah adjacent dengan router-router lain, tidak perlu dilakukan lagi proses penyamaan basis data yang membutuhkan waktu yang lama tersebut.

Dalam jaringan yang besar tentu dibutuhkan basis data yang besar pula untuk menyimpan topologi jaringan. Ini mengarah kepada kebutuhan memori router yang lebih besar serta waktu perhitungan route yang lebih lama. Untuk mengantisipasi hal ini, OSPF menggunakan konsep area dan backbone. Jaringan dibagi menjadi beberapa area yang terhubung ke backbone. Setiap area dianggap sebagai jaringan tersendiri dan router-router di dalamnya hanya perlu memiliki peta topologi jaringan dalam area tersebut. Router-router yang terletak di perbatasan antar area hanya mengirimkan ringkasan dari link-link yang terdapat dalam area dan tidak mengirimkan topologi area satu ke area lain. Dengan demikian, perhitungan route menjadi lebih sederhana.

10.2 OSPF Message Encapsulation

OSPF Message Encapsulation terjadi pada lapisan data-link dengan nomor protocol 89. Data field ini dapat berisi salah satu dari lima tipe paket OSPF. Pada IP packet header, alamat tujuannya mempunyai dua alamat multicast yaitu 224.0.0.5 dan 224.0.0.6



Gambar 11.3 OSPF Message encapsulation

10.3 OSPF Packet types

Ada 5 tipe paket yang digunakan OSPF, yaitu :

1. Hello packet ¦ untuk menemukan serta membangun hubungan antar tetangga router OSPF.
2. Database Description (DBD) ¦ untuk mengecek singkronisasi database antar router.
3. Link-State Request (LSR) ¦ meminta spesifikasi link-state records antara router satu dengan
   yang lain.
4. Link-State Update (LSU) ¦ mengirimkan permintaan spesifikasi link-state records.
5. Link-State Acknowledgement (LSAck) ¦ menerima paket link-state.

Type	Packet Name	Description
1	Hello	Discovers neighbors and builds adjacencies between them
2	Database Description (DBD)	Checks for database synchronization between routers
3	Link-State Request (LSR)	Requests specific link-state records from router to router
4	Link-State Update (LSU)	Sends specifically requested link-state records
5	Link-State Acknowledgement (LSAck)	Acknowledges the other packet types

Gambar 11.4 Tipe paket OSPF

Hello Packet

Hello Packet digunakan untuk menemukan serta membentuk suatu hubungan tetangga antara router OSPF. Untuk membentuk hubungan ini router OSPF akan mengirimkan paket berukuran kecil secara berkala ke jaringan. Paket inilah yang disebut dengan Hello packet. Paket ini juga mengadpertensikan router mana saja yang akan menjadi tetangganya. Pada jaringan multi-access Hello Packet digunakan untuk memilih Designated Router (DR) dan Back-up Designated Router (BDR). DR dan BDR akan menjadi pusat komunikasi seputar informasi OSPF dalam jaringan tersebut.

Database Description (DBD)

DBD digunakan selama pertukaran database. Paket DBD pertama digunakan untuk memilih hubungan master dan slave serta menetapkan urutan yang dipilih oleh master. Pemilihan master dan slave berdasarkan router ID tertinggi dari salah satu router. Router dengan router ID tertinggi akan menjadi master dan memulai sinkronisasi database. Router yang menjadi master akan melakukan pengiriman lebih dulu ke router slave. Peristiwa ini di istilahkan fase Exstart State. Setelah fase Exstart State lewat, selanjutnya adalah fase Exchange. Pada fase ini kedua router akan saling mengirimkan Database Description Packet. Bila si penerima belum memiliki informasi yang terdapat dalam paket tersebut, maka router pengirim akan memasuki fase Loading State. Dimana fase ini router akan mengirimkan informasi state secara lengkap ke router

tetangganya. Setelah selesai router-router OSPF akan memiliki informasi state yang lengkap dalam databasenya, ini disebut fase Full State.

Link-State Request (LSR)
LSR akan dikirim jika bagian dari database hilang atau out of date. LSR juga digunakan setelah pertukaran DBD selesai untuk meminta LSAs yang telah terjadi selama pertukaran DBD.

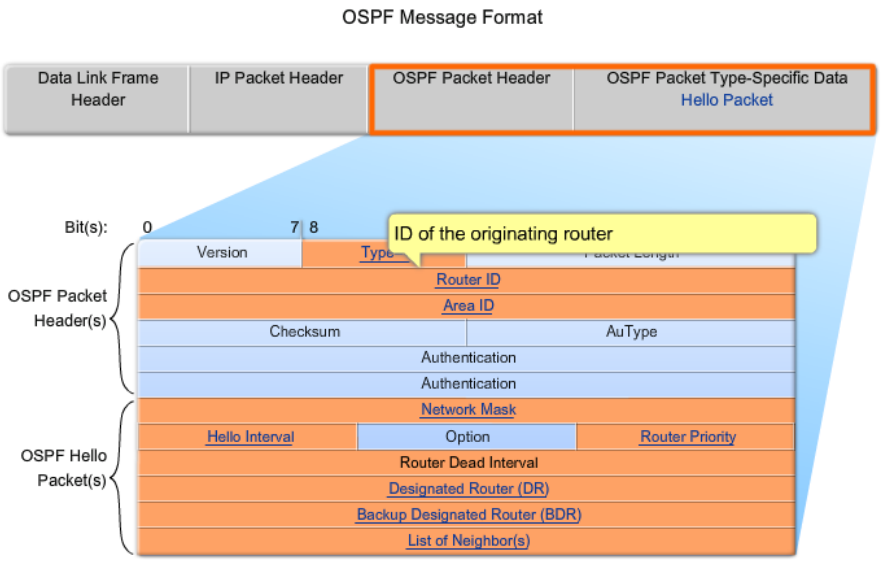
Link-State Update (LSU)
LSU mengimplementasikan flooding dari LSAs yang berisi routing dan informasi metric. LSU dikirim sebagai tanggapan dari LSR.

Link-State Acknowledgement (LSAck)
OSPF membutuhkan pengakuan untuk menerima setiap LSA. Beberapa LSA dapat diakui dalam sebuah paket single link-state acknowledgement. Paket ini dikirim sebagai jawaban dari packet update link state serta memverifikasi bahwa paket update telah diterima dengan sukses. LSAck akan dikirim sebagai multicast. Jika router dalam keadaan DR atau BDR maka pengakukan dikirim ke alamat multicast router OSPF dari 224.0.0.5 sedangkan bila router dalam keadaan tidak DR atau BDR pengakuan akan dikirim kesemua alamat multicast router DR dari 224.0.0.6

Hello Protocol

Paket OSPF yang pertama adalah Hello packet. Hello packet digunakan untuk :

- Menentukan tetangga OSPF dan membangun adjacencies dengan tetangga
- Memberitahu kepada router lain untuk setuju menjadi tetangga
- Menentukan Designated Router (DR) and Backup Designated Router (BDR)



Gambar 11.5 OSPF Message format

Gambar diatas meliputi

- Type: OSPF Packet Type: Hello (1), DD (2), LS Request (3), LS Update (4), LS ACK (5)
- Router ID: ID dari router
- Area ID: area dari mana packet berasal
- Network Mask: subnet mask dari interface pengirim
- Hello Interval: waktu pengiriman packet hello dari router
- Router Priority: digunakan untuk menentukan DR dan BDR
- Designated Router (DR): Router ID dari DR, jika ada
- Backup Designated Router (BDR): Router ID dari BDR, jika ada
- List of Neighbors: daftar ID Router OSPF dari router tetangga

Neighbor Establishment

Sebelum sebuah router OSPF menyebarkan link-state ke router lain, hal yang pertama kali harus ditentukan adalah apakah ada tetangga OSPF lain pada setiap link nya. Dalam gambar dibawah, router OSPF akan

mengirimkan paket Hello ke semua OSPF yang aktif pada setiap interfece untuk menentukan apakah ada tetangga di link tersebut. Informasi dalam Hello OSPF termasuk ID Router OSPF dari router mengirimkan paket Hello. Menerima paket Hello OSPF pada sebuah interface untuk setiap router menegaskan bahwa ada router lain dengan menggunakan OSPF pada link ini. OSPF adjacency untuk menetapkan router tetangga yang terhubung. Sebagai contoh, dalam gambar, R1 akan membangun adjacencies dengan R2 dan R3.

OSPF Hello and Dead Intervals

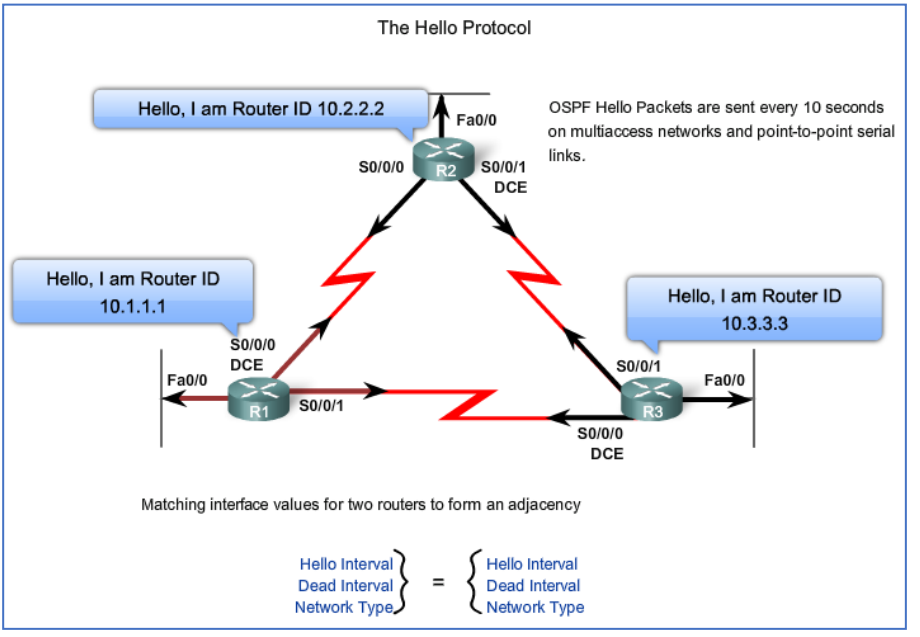
Sebelum dua router dapat melakukan OSPF adjacency dengan tetanggannya, router harus terlebih dahulu menyepakati nilai dari : Hello interval, Dead interval, and network type. OSPF hello interval menunjukkan intensitas OSPF mengirimkan hello packet. Secara default OSPF hello packet dikirim setiap 10 detik pada multiaccess dan point-to-point segmen dan setiap 30 detik pada non-broadcast multi-access (NBMA) segmen (Frame Relay, X.25, ATM).

Dalam kebanyakan kasus, OSPF Halo paket dikirim sebagai multicast (224.0.0.5). Menggunakan alamat multicast memungkinkan sebuah perangkat untuk mengabaikan paket jika interface tidak diaktifkan untuk menerima paket OSPF. Ini menghemat waktu pemrosesan pada CPU yang menggunakan non-OSPF device.

Periode dead interval, dinyatakan dalam satuan detik. Selama ini router akan menunggu untuk menerima packet hello sebelum menyatakan tetangga nya dalam keadaan down. Cisco menggunakan default dead interval selama 4 kali hello interval. Periode untuk multi-access dan point-to- point adalah 40 detik. Dan untuk NBMA, dead intervalnya salama 120 detik.
Jika dead interval expired sebelum router menerima hello packet, OSPF akan menghapus informasi tetangga dari link-state database. Dan router akan membanjiri informasi link-state dengan informasi tetangga dalam keadaan “down” disemua interface yang aktif.

Electing a DR and BDR

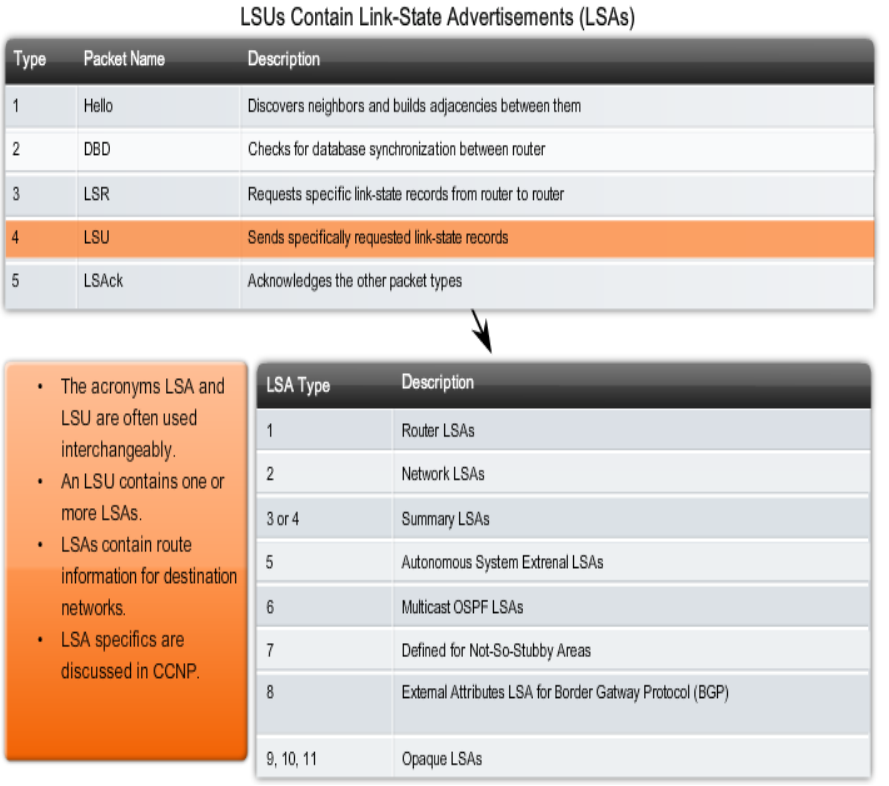
Untuk mengurangi jumlah lalu lintas jaringan OSPF multiaccess, OSPF memilih satu Designated Router (DR) dan Backup Designated Router (BDR). DR bertanggung jawab untuk memperbarui semua router OSPF yang lain. ketika perubahan terjadi dalam jaringan multiaccess. BDR memantau DR dan mengambil alih sebagai DR jika DR saat ini gagal.



Gambar 11.6 Electing a DR and BDR

OSPF Link-State Update

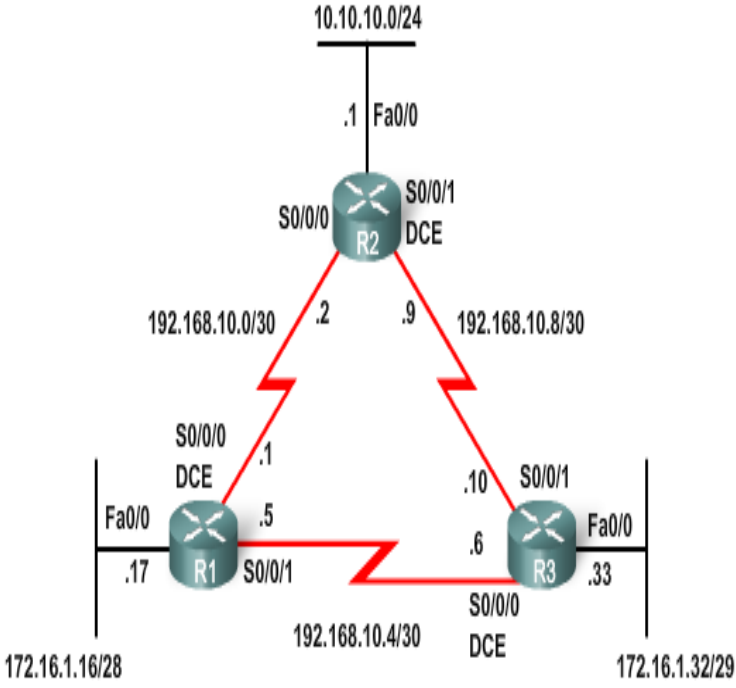
Update link-state (LSUs) adalah paket digunakan untuk update routing OSPF. Sebuah paket LSU dapat berisi sepuluh jenis Link-State Advertisements (LSAs)



Gambar 11.7 LSUs contain link-state advertisements (LSAs)

10.4 Basic OSPF Configuration

Gambar dibawah ini menunjukkan topologi untuk bab ini. Perhatikan bahwa skema pengalamatan tidak berhubungan. OSPF adalah sebuah classless routing protocol. Oleh karena itu, kita akan mengkonfigurasi mask sebagai bagian dari konfigurasi OSPF. Juga perhatikan dalam topologi ini ada tiga link serial dengan bandwidth yang telah ditentukan. Dan router masing-masing memiliki beberapa jalur untuk setiap jaringan remote.



Gambar 11.8 OSPF Topology

Device	Interface	IP Address	Subnet Mask
R1	Fa0/0	172.16.1.17	255.255.255.240
	S0/0/0	192.168.10.1	255.255.255.252
	S0/0/1	192.168.10.5	255.255.255.252
R2	Fa0/0	10.10.10.1	255.255.255.0
	S0/0/0	192.168.10.2	255.255.255.252
	S0/0/1	192.168.10.9	255.255.255.252
R3	Fa0/0	172.16.1.33	255.255.255.248
	S0/0/0	192.168.10.6	255.255.255.252
	S0/0/1	192.168.10.10	255.255.255.252

Gambar 11.9 IP Address OSPF Topology

OSPF diaktifkan dengan perintah **router ospf process-id**. Proses-id adalah nomor antara 1 dan 65535 dan dipilih oleh administrator jaringan. Proses-id lokal yang signifikan, yang berarti bahwa ia tidak harus sesuai dengan OSPF router lainnya untuk membangun adjacencies dengan router – router tetangga. Ini berbeda dari EIGRP. ID proses EIGRP atau nomor sistem otonomi tidak perlu untuk mencocokkan dua tetangga EIGRP menjadi berdekatan. Dalam topologi kami, kami akan mengaktifkan OSPF pada tiga router menggunakan proses ID yang sama 1. Kami menggunakan ID proses yang sama hanya untuk konsistensi.

R1(config)#router ospf 1
R1(config-router)#

Router(config-router)#network network-address wildcard-mask area area-id

Perintah jaringan OSPF menggunakan kombinasi network-address dan wildcard-mask sama dengan yang dapat digunakan oleh EIGRP. Tidak seperti EIGRP, OSPF membutuhkan wildcard mask. Network address dan wildcard mask digunakan untuk menentukan interface atau range interfaces yang akan diaktifkan ketika menggunakan routing protocol OSPF.

Seperti dengan EIGRP, wildcard mask dapat dikonfigurasi sebagai invers dari subnet mask. Misalnya, FastEthernet 0 / 0 interface R1 adalah pada jaringan 172.16.1.16/28. Subnet mask untuk interface ini adalah / 28 atau 255.255.255.240. Kebalikan dari subnet mask hasil di wildcard mask

```
R1(config)#router ospf 1
R1(config-router)#network 172.16.1.16 0.0.0.15 area 0
R1(config-router)#network 192.168.10.0 0.0.0.3 area 0
R1(config-router)#network 192.168.10.4 0.0.0.3 area 0

R2(config)#router ospf 1
R2(config-router)#network 10.10.10.0 0.0.0.255 area 0
R2(config-router)#network 192.168.10.0 0.0.0.3 area 0
R2(config-router)#network 192.168.10.8 0.0.0.3 area 0

R3(config)#router ospf 1
R3(config-router)#network 172.16.1.32 0.0.0.7 area 0
R3(config-router)#network 192.168.10.4 0.0.0.3 area 0
R3(config-router)#network 192.168.10.8 0.0.0.3 area 0
```

Gambar 11.10 Konfigurasi OSPF

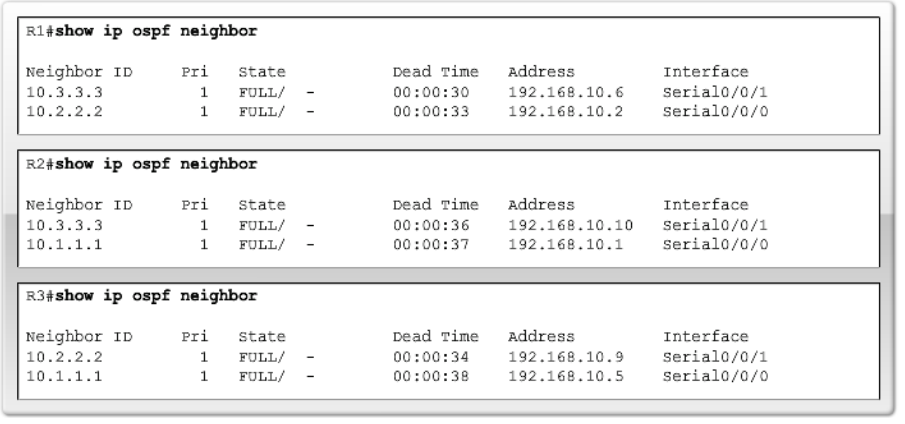
OSPF Router ID

Router ID OSPF digunakan untuk secara unik mengidentifikasi setiap router dalam domain routing OSPF. Sebuah Router ID hanya sebuah alamat IP. Router Cisco memperoleh Router ID berdasarkan tiga kriteria dan dengan prioritas berikut :

1. Gunakan Alamat IP yang telah dikonfigurasi dengan menggunakan perintah pada OSPF **router-id**.
2. jika router-id tidak dikonfigurasi, router akan memilih alamat IP tertinggi dari setiap interface loopback tersebut.
3. Jika tidak ada interface loopback yang dikonfigurasi, router memilih alamat IP aktif tertinggi dari setiap interface fisiknya.

Verifying OSPF

show ip ospf neighbor adalah perintah yang dapat digunakan untuk memverifikasi dan memecahkan masalah hubungan router tetangga OSPF. Untuk setiap router tetangga, perintah ini menampilkan output sebagai berikut:



Gambar 11.11 Verifikasi OSPF

Ketika masalah pada network dengan menggunakan OSPF terjadi, perintah **show ip ospf neighbor** dapat digunakan untuk memverifikasi bahwa router telah membentuk adjacency dengan router tetangganya. Jika Router ID dari router tetangga tidak ditampilkan, atau jika router tidak menunjukkan dalam keadaan FULL, kedua router tidak membentuk adjacency OSPF. Jika dua router tidak membangun adjacency, link-state informasi tidak akan dipertukarkan. Selain itu command yang dapat digunakan untuk melakukan verifikasi pada router antara lain : **show ip protocols, show ip ospf, show ip ospf interface**

Dua router tidak dapat membentuk adjacency OSPF jika:

- Subnet mask tidak cocok, menyebabkan router berada pada network yang terpisah.
- OSPF Hello atau Dead Timers tidak cocok.
- Type network OSPF tidak cocok
- ada command OSPF network yang hilang atau salah

Examining The Routing Table

Perintah **Show IP route** dapat digunakan untuk melakukan verifikasi bahwa OSPF dapat mengirim dan menerima informasi route dari router melalui OSPF. Huruf **O** pada awal informasi route menunjukkan bahwa router menggunakan OSPF sebagai protocol routingnya. Tabel routing dan OSPF akan diperiksa lebih erat dalam bagian berikut. Namun, Anda harus segera memperhatikan dua perbedaan yang terdapat dalam tabel routing OSPF dibandingkan dengan tabel routing pada bab sebelumnya.. Pertama, perhatikan bahwa setiap router memiliki empat network yang terhubung langsung karena jumlah interface loopback dalam network ada empat. interface loopback ini tidak advertised di OSPF. Oleh karena itu, setiap router terdapat tujuh network yang dikenal. Kedua, tidak seperti RIPv2 dan EIGRP, OSPF tidak secara otomatis melakukan summarize. OSPF adalah jenis routing protocol inherently classless.

```
R1#show ip route

Codes: <some code output omitted>
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

Gateway of last resort is not set

     192.168.10.0/30 is subnetted, 3 subnets
C       192.168.10.0 is directly connected, Serial0/0/0
C       192.168.10.4 is directly connected, Serial0/0/1
O       192.168.10.8 [110/128] via 192.168.10.2, 14:27:57, Serial0/0/0
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
O       172.16.1.32/29 [110/65] via 192.168.10.6, 14:27:57, Serial0/0/1
C       172.16.1.16/28 is directly connected, FastEthernet0/0
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
O       10.10.10.0/24 [110/65] via 192.168.10.2, 14:27:57, Serial0/0/0
C       10.1.1.1/32 is directly connected, Loopback0
```

Gambar 11.11 Perintah Show ip route

10.5 OSPF Metric

Metrik OSPF disebut cost. RFC 2328 menyatakan bahwa: *"A cost is associated with the output side of each router interface. This cost is configurable by the system administrator. The lower the cost, the more likely the interface is to be used to forward data traffic."*

Interface Type	10^8/bps = Cost
Fast Ethernet and faster	10^8/100,000,000 bps = 1
Ethernet	10^8/10,000,000 bps = 10
E1	10^8/2,048,000 bps = 48
T1	10^8/1,544,000 bps = 64
128 kbps	10^8/128,000 bps = 781
64 kbps	10^8/64,000 bps = 1562
56 kbps	10^8/56,000 bps = 1785

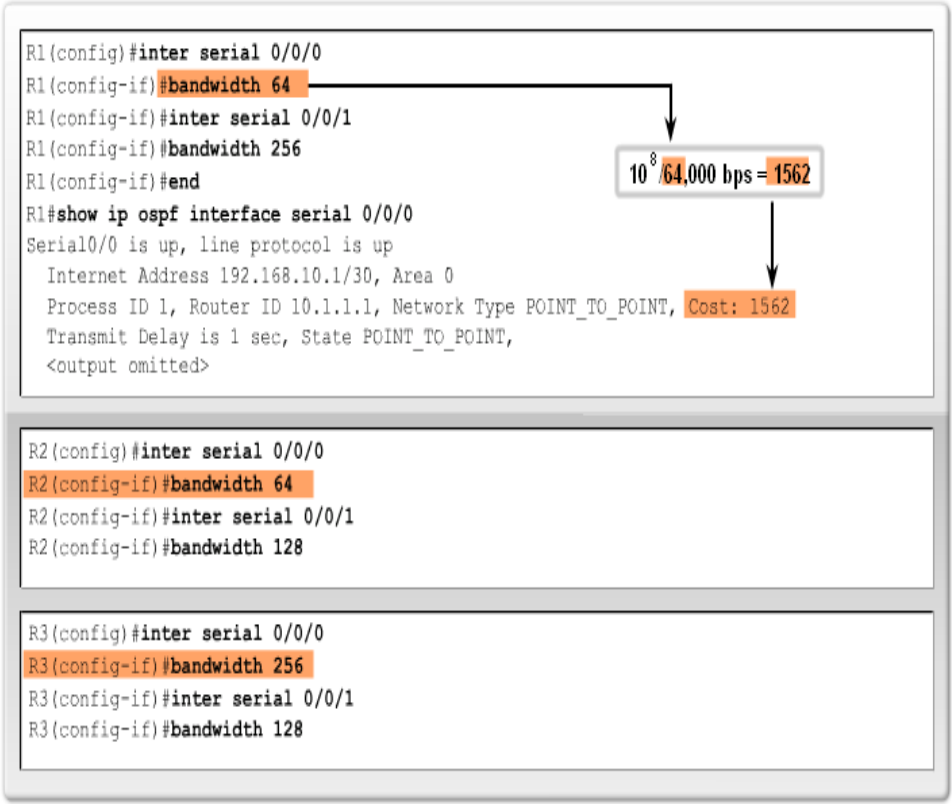
Gambar 11.12 CISCO OSPF cost value

Modifying The Cost Of The Link

Ketika sebuah l interface tidak benar-benar beroperasi pada kecepatan T1 default ,interface tersebuat memerlukan modifikasi secara manual. Kedua sisi dari link harus dikonfigurasi untuk memiliki nilai yang sama. Gunak perintah **Bandwith** pada kedua interface atau perintah **ip ospf cost** untuk mencapai tujuan ini - nilai yang akurat untuk digunakan oleh OSPF dalam menentukan rute terbaik.

Perintah **bandwidth** digunakan untuk memodifikasi nilai bandwidth yang digunakan oleh IOS dalam menghitung biaya OSPF metrik.

Router(config-if)#bandwidth bandwidth-kbps



Gambar 11.13 Modifikasi Bandwith

Angka ini menunjukkan perintah bandwidth digunakan untuk memodifikasi biaya semua interface serial di topologi. Untuk R1, perintah **show ip ospf interface** menunjukkan bahwa biaya dari link Serial 0/0/0 sekarang 1562, hasil perhitungan biaya OSPF Cisco 100.000.000 / 64.000.

10.6 Perintah Perintah Yang Digunakan

Perintah	Keterangan
Router ospf *proses-id*	Mengaktifasi proses routing OSPF dan mengidentifikasi proses-id dimana ia akan bekerja. Proses-id ada di range 1 – 65535
Network *network-number wild-card area area-id*	Mengaktifkan OSPF pada sebuah interface tertentu atau sekumpulan interface yang berada di network yang disebutkan. Interface – interface ini akan berada pada area yang disebutkan
Show ip ospf	Merangkum semua informasi yang berhubungan dengan OSPF, seperti proses – proses OSPF, Router ID, pemilihan area, autentikasi, dan statistic SPF
Show ip ospf proses-id	Menunjukkan informasi yang sama seperti perintah show ip ospf, tetapi hanya untuk proses yang disebutkan
Show ip ospf database	Menunjukkan topology database untuk link-state
Show ip ospf interface	Menunjukkan parameter – parameter interface OSPF dan informasi OSPF lain yang spesifik pada interface tersebut
Show ip ospf neighbor	Menunjukkan setiap tetangga OSPF dan status adjacency
Show ip protocol	Menunjukkan status dan ringkasan konfigurasi untuk semua routing protocol yang aktif

Daftar Pustaka

[1] Kaunang, F.J., Karim, A., Simarmata, J., Iskandar, A., Ardiana, D.P.Y., Septarini, R.S., Negara, E.S., Hazriani, H. and Widyastuti, R.D., 2021. Konsep Teknologi Informasi. Yayasan Kita Menulis.

[2] Simarmata, J., Manuhutu, M.A., Yendrianof, D., Iskandar, A., Amin, M., Sinlae, A.A.J., Siregar, M.N.H., Hazriani, H., Herlinah, H., Sinambela, M. and Negara, E.S., 2021. Pengantar Teknologi Informasi. Yayasan Kita Menulis.

[3] Negara, E.S., 2019. Jaringan Komputer Routing dan Switching Essentials.

[4] Mukmin, C., Antoni, D. and Surya Negara, E., 2016. Comparison Route Redistribution on Dynamic Routing Protocol (EIGRP into OSPF and EIGRP into IS-IS).

[5] Aan Restu, M. and Edi, S.N., 2016, December. Studi Performa Migrasi Ipv4 Ke Ipv6 pada Metode Dual Stack. In Annual Research Seminar. Universitas Sriwijaya.

[6] Testart, C., Richter, P., King, A., Dainotti, A. and Clark, D., 2019, October. Profiling BGP serial hijackers: capturing persistent misbehavior in the global routing table. In Proceedings of the Internet Measurement Conference (pp. 420-434).

[7] Robinson, Y.H., Balaji, S. and Julie, E.G., 2019. Design of a buffer enabled ad hoc on-demand multipath distance vector routing protocol for improving throughput in mobile ad hoc networks. Wireless Personal Communications, 106(4), pp.2053-2078.

[8] Savage, D., Ng, J., Moore, S., Slice, D., Paluch, P. and White, R., 2016. Cisco's enhanced interior gateway routing protocol (eigrp). Request for Comments, 7868.

[9] Baggan, V., Sahoo, A.K., Sarangi, P.K. and Chaturvedi, S.P., 2020. A comprehensive analysis and experimental evaluation

of routing information protocol: An elucidation. Materials Today: Proceedings.

[10] Zhang, W., Gong, X., Tian, Y. and Tang, J., 2020, October. High Speed Route Lookup for Variable-Length IP Address. In 2020 IEEE 28th International Conference on Network Protocols (ICNP) (pp. 1-6). IEEE.

[11] MAHMOOD, A., 2020. Performance Analysis of Routing Protocols RIP, EIGRP, OSPF and IGRP using Networks connector.

[12] Macfarlane, J., 2007. Network routing basics: Understanding IP routing in Cisco systems. John Wiley & Sons.

[13] Wang, L., Lehman, V., Hoque, A.M., Zhang, B., Yu, Y. and Zhang, L., 2018. A secure link state routing protocol for NDN. IEEE Access, 6, pp.10470-10482.

[14] Esha, R.A. and Tahura, S., 2018. Simulation based EIGRP over OSPF performance analysis (Doctoral dissertation, East West University).

Routing merupakan sebuah mekanisme pada jaringan komputer dalam melakukan pengiriman paket data dari satu network ke network yang lain. Pada router, biasanya memiliki satu atau beberapa tabel routing yang menyimpan informasi jalur routing yang digunakan saat mentransfer data melalui router. Proses perutean terjadi pada lapisan 3 pada Open Sistem Interconection layer (OSI). Buku ini akan menyajikan pengenalan protokol routing yang sering digunakan dalam dunia jaringan komputer.

Buku ini terdiri dari 10 bab, yaitu:

Penerbit :
PPP-UBD Press

ISBN 978-979-3877-44-0

PENGENALAN PROTOKOL ROUTING

Edi Surya Negara