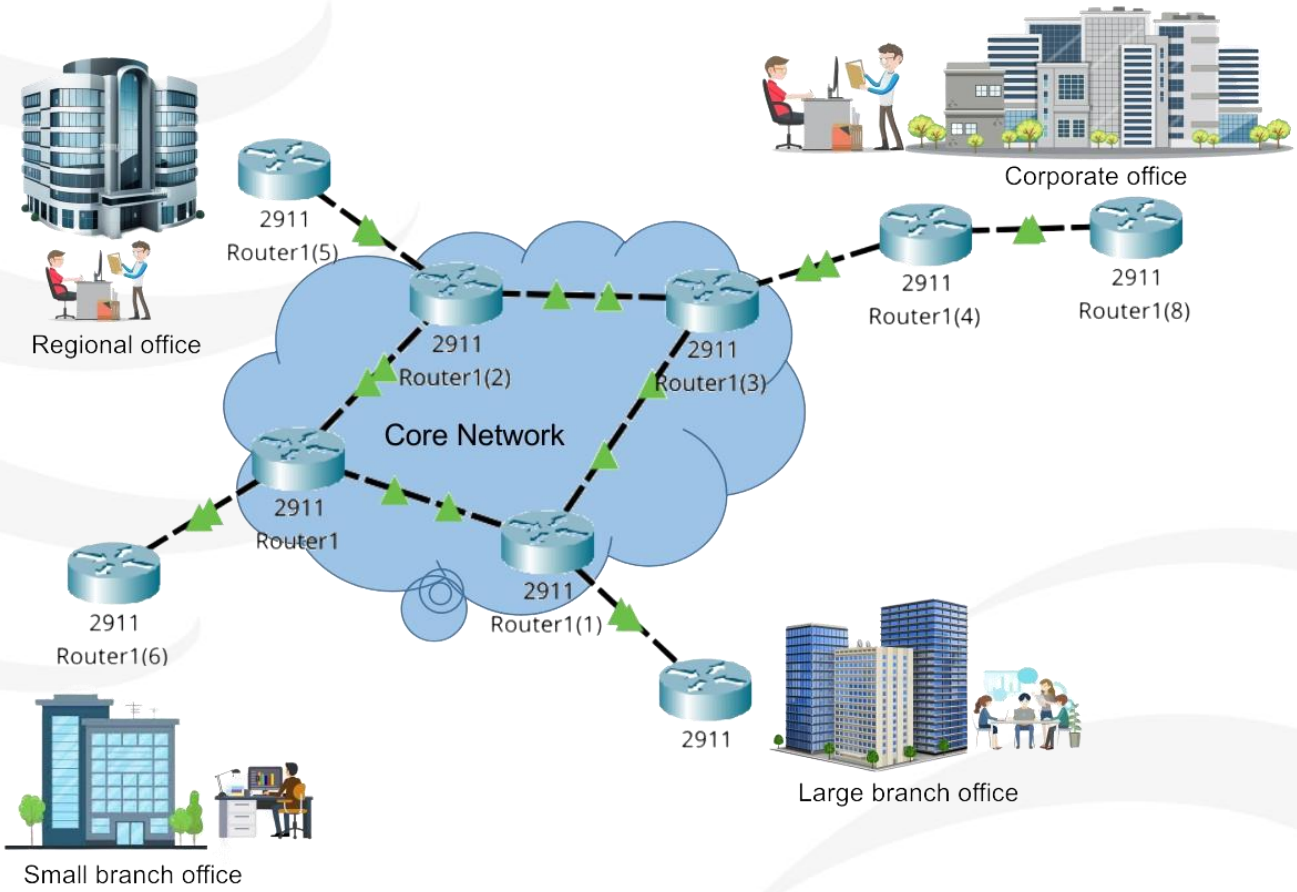
UNIVERSITAS TEKNOKRAT INDONESIA PRESS
2024



ROUTING & SWITCHING

Jupriyadi
Syaiful Ahdan
Adi Sucipto

Editor: Jupriyadi

ROUTING & SWITCHING

DITULIS OLEH

JUPRIYADI

SYAIFUL AHDAN

ADI SUCIPTO

2024

UNIVERSITAS TEKNOKRAT INDONESIA

KAMPUSNYA SANG JUARA

BUKU TEKS

ROUTING & SWITCHING

Penulis :

Jupriyadi

Syaiful Ahdan

Adi Sucipto

Editor/Cover, & Layout:

Jupriyadi

Cetakan Pertama :

Bandarlampung, Agustus 2024

ISBN: XXX-XXX-XXXXX-X-X

PENERBIT:

Universitas Teknokrat Indonesia Press

Jl. H. Zaenal Abidin, Pagaralam, No. 9-11 Labuhan Ratu, Bandarlampung

Kode Pos 35142. Telp (0721) 702022

Website : https://www.teknokrat.ac.id

PRAKATA

Puji Syukur penulis panjatkan kehadirat Allah, SWT, atas limpahan rahmat-Nya sehingga Buku Teks Routing & Switching dapat diselesaikan dengan baik. Buku Teks ini disusun berdasarkan pada standar proses pembelajaran yang lebih menempatkan mahasiswa sebagai pusat kegiatan belajar (*Student- Centered Learning*). Buku Teks ini juga dilengkapi dengan contoh kasus dan konfigurasi dalam membangun jaringan komputer agar komunikasi dapat dilakukan sesuai dengan kebutuhan jaringan dan layanan yang diinginkan.

Kami menyadari bahwa dalam penyusunan Buku Teks ini masih banyak kekurangan. Oleh karena itu, kami sangat mengharapkan kritik dan saran dari para pembaca demi perbaikan dan kesempurnaan Buku ini. Tak lupa, kami mengucapkan terima kasih kepada berbagai pihak yang telah membantu proses penyelesaian Buku Teks ini. Terutama kepada Ibu Pembina Yayasan dan Rektor Universitas Teknokrat Indonesia yang telah membimbing dalam penyelesaian Buku Teks ini. Semoga Buku Teks ini dapat bermanfaat bagi kita semua, khususnya bagi para mahasiswa.

Bandarlampung, Agustus 2024

Tim Penyusun

DAFTAR ISI

BAB 1

PENDAHULUAN JARINGAN KOMPUTER

1.1. Definisi

Pada bab ini akan membahas tentang konsep dasar dari jaringan komputer dan perangkatnya. Jaringan dipergunakan untuk menghubungkan dua atau lebih komputer. Jaringan Komputer adalah kumpulan dua komputer atau lebih. Ini membantu pengguna untuk berkomunikasi dengan lebih mudah. Melalui jaringan dan web, kedua komputer akan terhubung secara global. Saat ini, ada dua jenis modem yang tersedia: nirkabel, dan kabel, yang terhubung ke sistem komputer di dalamnya. Dalam bentuknya yang paling dasar, jaringan adalah penghubungan dua komputer atau lebih. Tujuan utama jaringan adalah untuk memfasilitasi pertukaran informasi di antara berbagai penggunanya.

Blok bangunan dasar jaringan komputer adalah node dan link. Node Jaringan dapat diilustrasikan sebagai Peralatan Komunikasi Data seperti Modem, Router, dll, atau Peralatan Terminal Data seperti menghubungkan dua komputer atau lebih. Tautan dalam jaringan komputer dapat didefinisikan sebagai kabel atau kabel atau ruang kosong dari jaringan nirkabel. Cara kerja jaringan komputer secara sederhana dapat didefinisikan sebagai aturan atau protokol yang membantu mengirim dan menerima data melalui tautan yang memungkinkan jaringan komputer berkomunikasi. Setiap perangkat memiliki Alamat IP yang membantu dalam mengidentifikasi suatu perangkat. Pada gambar 1.1 menunjukkan koneksi antar 2 komputer.

Gambar 1.1. Koneksi komputer dalam jaringan

Jaringan komputer terdiri dari berikut ini:

- ✓ Dua atau beberapa komputer yang dapat menjadi Server atau Klien.
- ✓ Kartu Antarmuka Jaringan (NIC).
- ✓ Media koneksi yang dapat memiliki kabel atau tanpa kabel.
- ✓ Sistem Operasi Jaringan seperti MS Windows, NT atau MS 2000, Novell NetWare, UNIX dan Linux.

Adapun beberapa kelebihan dari Jaringan Komputer antara lain: Berbagi sumber daya, Login jarak jauh (Akses ke basis data jarak jauh), E-Mailing (komunikasi orang ke orang), Hiburan, layanan internet, Konferensi video, Pertukaran pesan, Berbagi informasi dengan Biaya Rendah, Menyimpan File di server memungkinkan data dibagikan dengan mudah, Pencadangan File yang Cepat dan Cepat, Perangkat lunak dan sumber daya dapat dikelola dengan mudah., Perangkat lunak jaringan memiliki instalasi yang cepat, Perangkat dapat dibagikan dengan mudah, Mengakses file dari workstation mana pun.

1.2. Terminologi Dasar Jaringan Komputer

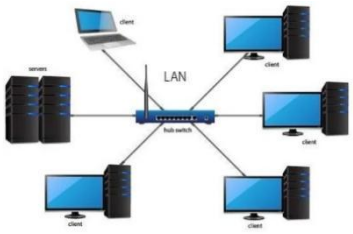
Ada beberapa hal yang perlu diketahui tentang terminologi jaringan komputer. Terminologi dari sebuah jaringan komputer antara lain.

- ✓ Jaringan: Jaringan adalah kumpulan komputer dan perangkat yang terhubung bersama untuk memungkinkan komunikasi dan pertukaran data.
- ✓ Node: Node adalah perangkat yang terhubung ke jaringan. Ini dapat mencakup komputer, Server, Printer, Router, Switch, dan perangkat lainnya.
- ✓ Protokol: Protokol adalah seperangkat aturan dan standar yang mengatur bagaimana data ditransmisikan melalui jaringan. Contoh protokol termasuk TCP/IP, HTTP, dan FTP.
- ✓ Topologi: Topologi jaringan mengacu pada susunan fisik dan logis dari node pada jaringan. Topologi jaringan yang umum meliputi bus, star, ring, mesh, dan tree.
- ✓ Jaringan Penyedia Layanan: Jaringan jenis ini memberikan izin untuk menyewa Kapasitas dan Fungsi Jaringan dari Penyedia. Jaringan Penyedia Layanan mencakup Komunikasi Nirkabel, Operator Data, dll.
- ✓ Alamat IP: Alamat IP adalah pengidentifikasi numerik unik yang ditetapkan untuk setiap perangkat di jaringan. Alamat IP digunakan untuk mengidentifikasi perangkat dan memungkinkan komunikasi di antara perangkat tersebut.
- ✓ DNS: Sistem Nama Domain (DNS) adalah protokol yang digunakan untuk menerjemahkan nama domain yang dapat dibaca manusia (seperti www.google.com) menjadi alamat IP yang dapat dipahami komputer.
- ✓ Firewall: Firewall adalah perangkat keamanan yang digunakan untuk memantau dan mengontrol lalu lintas jaringan masuk dan keluar. Firewall digunakan untuk melindungi jaringan dari akses tidak sah dan ancaman keamanan lainnya.

1.3. Jenis Jaringan Komputer

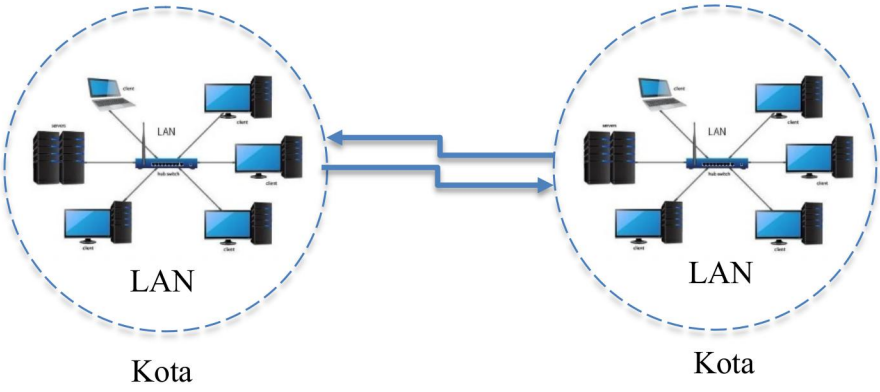
Ada beberapa tipe dalam jaringan komputer antara lain.

Local Area Network (LAN) adalah jaringan yang mencakup area kecil, seperti kantor atau rumah. LAN biasanya digunakan untuk menghubungkan komputer dan perangkat lain di dalam gedung atau kampus. Pada gambar 1.2 berikut adalah contoh bentuk dari LAN.



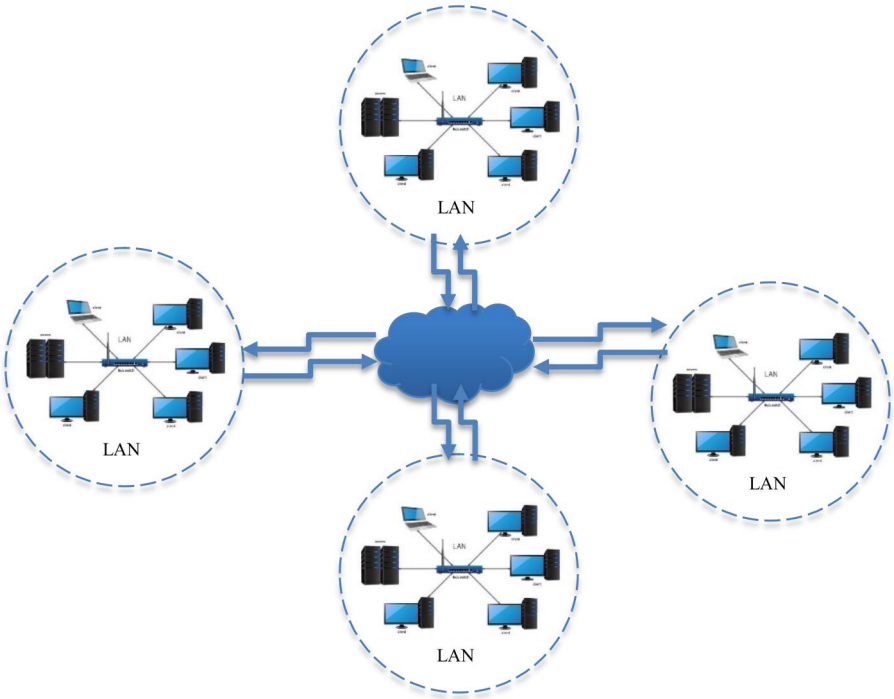
Gambar 1.2. Jenis jaringan LAN

Metropolitan Area Network (MAN) adalah suatu jaringan komputer yang dapat mencakup area yang lebih luas dan menggunakan teknologi yang lebih canggih dari LAN. Jaringan MAN merupakan gabungan beberapa jaringan LAN yang mana menjangkau hingga 10 s.d. 50 km. Jaringan MAN cocok dipakai untuk membangun jaringan antar perkantoran atau instansi yang masih dalam satu kota. Biasanya MAN dipakai untuk menghubungkan beberapa lokasi seperti perkantoran, kampus, pemerintahan, dan sebagainya. Pada gambar 1.3 berikut adalah contoh bentuk dari MAN.



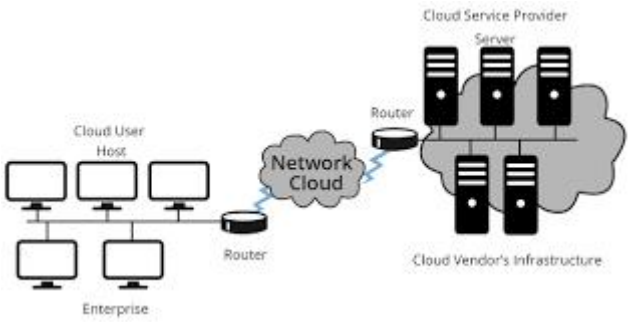
Gambar 1.3. Jenis jaringan MAN

Wide Area Network (WAN) adalah jaringan yang mencakup wilayah geografis yang luas, seperti kota, negara, atau bahkan seluruh dunia. WAN digunakan untuk menghubungkan LAN bersama-sama dan biasanya digunakan untuk komunikasi jarak jauh. Pada gambar 1.4 berikut adalah contoh bentuk dari WAN.



Gambar 1.4. Jenis jaringan WAN

Cloud Networks: Jaringan Cloud dapat divisualisasikan dengan Wide Area Network (WAN) karena dapat dihosting di penyedia layanan cloud publik atau swasta dan jaringan cloud tersedia jika ada permintaan. Jaringan Cloud terdiri dari Router Virtual, Firewall, dll. Pada gambar 1.5 berikut adalah contoh bentuk dari Cloud Networks.



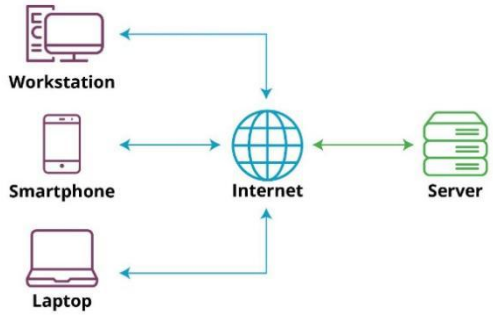
Gambar 1.5. Jenis jaringan Cloud Networks

Jaringan adalah bidang yang luas dan kompleks, dan masih banyak lagi konsep dan teknologi yang terlibat dalam membangun dan memelihara jaringan. Sekarang kita akan membahas beberapa konsep lagi tentang Jaringan Komputer.

- ✓ Sistem terbuka: Sistem yang terhubung ke jaringan dan siap untuk berkomunikasi.
- ✓ Sistem tertutup: Sistem yang tidak terhubung ke jaringan dan tidak dapat berkomunikasi.

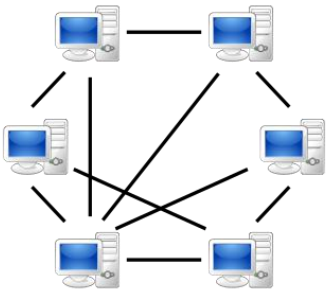
1.4.Jenis Arsitektur Jaringan Komputer

Jaringan Komputer termasuk dalam Kategori berikut:
Arsitektur Client-Server: Arsitektur Client-Server adalah jenis Arsitektur Jaringan Komputer dimana Node dapat menjadi Server atau Klien. Di sini, node server dapat mengelola Perilaku Node Klien. Pada gambar 1.6 berikut adalah contoh Arsitektur Client-Server.



Gambar 1.6. Arsitektur Client-Server

Arsitektur Peer-to-Peer: Dalam Arsitektur P2P (Peer-to-Peer), tidak ada konsep Server Pusat. Setiap perangkat gratis untuk berfungsi sebagai klien atau server. Pada gambar 1.7 berikut adalah contoh Arsitektur Peer-to-Peer.



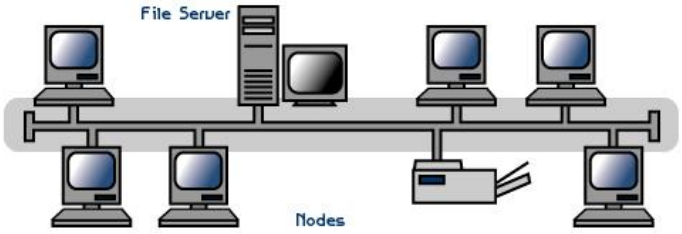
Gambar 1.7. Arsitektur Peer-to-Peer

1.5.Jenis Topologi

Topologi yang mendasari digunakan untuk membangun jaringan memberikan skema klasifikasi tambahan untuk jaringan komputer. Susunan geometris node dikenal sebagai topologi. Sumber daya komputer dan perangkat komunikasi yang berbeda disebut node. Topologi mendefinisikan struktur jaringan bagaimana semua komponen saling berhubungan satu sama lain. Ada dua jenis topologi: topologi fisik dan logis. Topologi fisik adalah representasi geometris dari semua node dalam jaringan. Ada enam jenis topologi jaringan yaitu Topologi Bus, Topologi Ring, Topologi Tree, Topologi Star, Topologi Mesh, dan Topologi Hybrid.

a. Topologi Bus

Pada jaringan Bus setiap node dalam jaringan bus dihubungkan ke satu rute bus. Bus ini juga dikenal sebagai bus berbagi waktu. Hanya sepasang node yang dapat menjalin komunikasi pada satu waktu melalui bus. Karakteristik ini membatasi jumlah total node yang dapat dihubungkan untuk menciptakan jaringan bus yang dapat diandalkan. Meskipun demikian, beberapa protokol diciptakan untuk bus agar komunikasi lebih andal dan efisien. Protokol bus token dan CSMA/CD adalah contoh yang masuk akal. Keuntungan dari jaringan bus adalah tidak memerlukan banyak perangkat keras untuk menghubungkan sejumlah node. Menghapus node dari bus juga mudah. Menjaga jaringan bus tetap terpelihara itu sederhana. Pada gambar 1.8 berikut adalah bentuk topologi Bus.



Gambar 1.8. Topologi Bus

Kelebihan Topologi Bus Linear

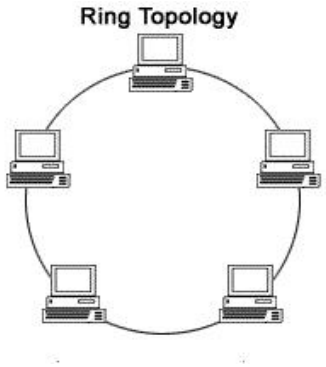
- ✓ Mudah untuk menghubungkan komputer atau periferal ke bus linier.
- ✓ Memerlukan panjang kabel yang lebih sedikit dibandingkan topologi star.
- ✓ Kekurangan Topologi Bus Linier
- ✓ Seluruh jaringan mati jika ada putusnya kabel utama.
- ✓ Terminator diperlukan di kedua ujung kabel tulang punggung.
- ✓ Sulit untuk mengidentifikasi masalah jika seluruh jaringan dimatikan.
- ✓ Tidak dimaksudkan untuk digunakan sebagai solusi yang berdiri sendiri di gedung besar.

b. Topologi Ring

Topologi ring adalah jenis pengaturan jaringan yang digunakan dalam jaringan komputer di mana setiap node terhubung ke dua node lainnya untuk menyediakan aliran sinyal tunggal yang berkelanjutan. Dalam jaringan area lokal (LAN), topologi ring sering digunakan. Setiap node dalam topologi ring memiliki dua tetangga, dan sinyal mengalir mengelilingi ring dalam arah yang berlawanan. Jaringan dapat menggunakan node lain sebagai jalur cadangan untuk mengalihkan sinyal di sekitar node yang gagal. Meskipun redundansi ini dapat meningkatkan toleransi kesalahan dan keandalan, hal ini juga membuat jaringan menjadi lebih kompleks.

Kabel serat optik atau twisted pair dapat digunakan untuk membangun topologi ring. Kecepatan transfer data yang diinginkan, jarak antar node, dan pertimbangan lainnya akan

menentukan jenis kabel yang akan digunakan. Pada gambar 1.9 berikut adalah bentuk topologi Ring.



Gambar 1.9. Topologi Ring

Kelebihan Topologi Ring

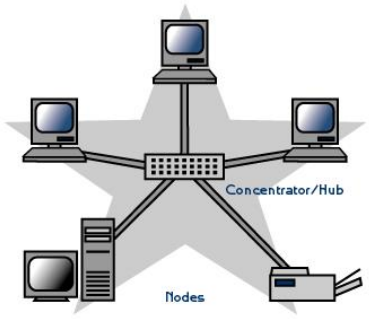
- ✓ Salah satu keuntungan utamanya adalah sangat sulit bagi pihak luar untuk memanfaatkan atau mengganggu jaringan yang menggunakan konfigurasi jenis ini.
- ✓ Selain itu, jika satu node di jaringan mati, node lainnya dapat terus berkomunikasi satu sama lain tanpa masalah. Hal ini dapat menjadi keuntungan besar dalam situasi kritis dimana waktu aktif adalah kuncinya.
- ✓ Terakhir, topologi ring cenderung sangat mudah untuk diperluas dan ditambahkan node baru sesuai kebutuhan.

Kekurangan Topologi Ring

- ✓ Ada beberapa kelemahan topologi ring.
- ✓ Pertama, jika satu node gagal, seluruh jaringan akan gagal.
- ✓ Kedua, menambah atau menghapus node dari jaringan bisa jadi sulit.
- ✓ Ketiga, topologi ring tidak cocok untuk jaringan besar.
- ✓ Terakhir, mereka rentan terhadap badai siaran.

c. Topologi Star

Arsitektur jaringan yang dikenal sebagai topologi star adalah arsitektur di mana setiap elemen jaringan terhubung secara fisik ke hub pusat, switch, atau router—hub pusat berfungsi sebagai server, dan node yang terhubung adalah klien dalam topologi star. Sebuah paket dapat dikirim ke node lain dalam jaringan melalui node pusat setelah diterima dari node penghubung. Jaringan bintang adalah nama lain dari topologi bintang. Pada gambar 1.10 berikut adalah bentuk topologi Star.



Gambar 1.10. Topologi Star

Kelebihan dari topologi jaringan star antara lain sebagai berikut:

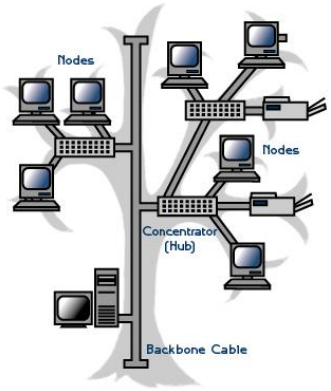
- ✓ Membatasi dampak dari satu titik kegagalan. Dalam jaringan bintang, setiap node penghubung diisolasi dari node penghubung lainnya. Jika salah satu node penghubung mati, maka tidak akan berdampak pada kinerja node penghubung lainnya dalam jaringan.
- ✓ Memfasilitasi penambahan atau penghapusan komponen individual ke dan dari jaringan. Jaringan bintang biasanya dibuat kecil karena kinerja jaringan dapat menurun ketika terlalu banyak perangkat bersaing untuk mendapatkan akses ke node pusat.

Kekurangan Topologi Star

- ✓ Membutuhkan lebih banyak panjang kabel dibandingkan topologi linier.
- ✓ Jika hub, switch, atau konsentrator gagal, node yang terpasang akan dinonaktifkan.
- ✓ Lebih mahal daripada topologi bus linier karena biaya hub, dll.

d. Topologi Tree

Topologi Pohon (tree), Topologi jenis ini menampilkan struktur pohon dengan koneksi antara semua komputer yang bertindak sebagai cabang pohon. Topologi pohon dalam jaringan komputer disebut sebagai hibrida dari topologi jaringan bus dan bintang. Manfaat utama topologi ini adalah skalabilitas dan fleksibilitasnya yang lebih besar. Dengan hanya satu jalur yang menghubungkan dua node jaringan, arsitektur jaringan pohon dianggap sebagai topologi paling mudah dari semuanya. Struktur koneksinya mirip dengan pohon, dimana semua cabangnya berasal dari akar yang sama (Topologi Pohon). Dari kelima topologi jaringan, topologi tree merupakan salah satu yang paling banyak digunakan. Pada gambar 1.11 berikut adalah bentuk topologi Tree.



Gambar 1.11. Topologi Tree

Kelebihan Topologi Tree :

- ✓ Topologi ini merupakan gabungan dari topologi bus dan star.
- ✓ Topologi ini menyediakan susunan data hierarkis dan sentral dari node.
- ✓ Karena node daun dapat menambahkan satu atau lebih node dalam rantai hierarki, topologi ini memberikan skalabilitas yang tinggi.
- ✓ Node lain dalam jaringan tidak terpengaruh jika salah satu nodenya rusak atau tidak berfungsi.
- ✓ Topologi pohon memberikan perawatan yang mudah dan identifikasi kesalahan yang mudah dapat dilakukan.
- ✓ Topologi yang dapat dipanggil. Node daun dapat menampung lebih banyak node.
- ✓ Didukung oleh beberapa vendor hardware dan software.
- ✓ Pengkabelan point-to-point untuk masing-masing segmen.
- ✓ Topologi Pohon sangat aman.
- ✓ Ini digunakan di WAN.
- ✓ Topologi Pohon dapat diandalkan.

Kekurangan Topologi Tree :

- ✓ Jaringan ini sangat sulit untuk dikonfigurasi dibandingkan dengan topologi jaringan lainnya.
- ✓ Panjang suatu segmen terbatas & batas segmen tergantung pada jenis kabel yang digunakan.
- ✓ Karena banyaknya node, kinerja jaringan topologi pohon menjadi agak lambat.
- ✓ Jika komputer pada level pertama bermasalah, komputer level berikutnya juga akan mengalami masalah.
- ✓ Membutuhkan jumlah kabel yang banyak dibandingkan topologi star dan ring.
- ✓ Karena data perlu dikirim dari kabel pusat, hal ini menciptakan lalu lintas jaringan yang padat.
- ✓ Backbone muncul sebagai titik kegagalan seluruh segmen jaringan.
- ✓ Perawatan topologinya cukup rumit.
- ✓ Biaya pendirian juga meningkat.

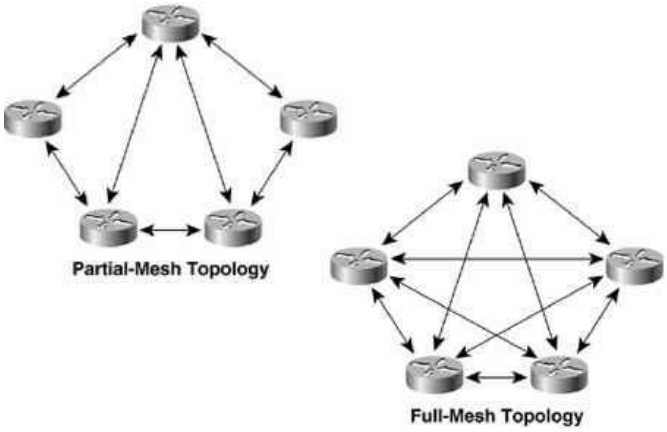
- ✓ Jika sebagian besar node ditambahkan ke jaringan ini, maka pemeliharaannya akan menjadi rumit.

e. Topologi Mesh

Topologi mesh mengacu pada konfigurasi jaringan di mana setiap komputer dan perangkat jaringan terhubung satu sama lain. Sebagian besar transmisi dapat disebarkan dengan arsitektur ini bahkan jika salah satu koneksi gagal. Ini adalah topologi yang sering digunakan jaringan nirkabel. Ilustrasi konfigurasi komputer dasar pada jaringan mesh ditunjukkan di bawah ini.

Ada dua bentuk topologi ini: mesh penuh dan mesh terhubung sebagian.

1. Pada topologi full mesh, setiap komputer dalam jaringan mempunyai koneksi ke masing-masing komputer lain dalam jaringan tersebut. Jumlah koneksi dalam jaringan ini dapat dihitung dengan menggunakan rumus berikut (n adalah jumlah komputer dalam jaringan): n(n-1)/2
2. Dalam topologi mesh yang terhubung sebagian (partial), setidaknya dua komputer di jaringan memiliki koneksi ke beberapa komputer lain di jaringan tersebut. Ini adalah cara yang murah untuk menerapkan redundansi dalam jaringan. Jika salah satu komputer utama atau koneksi dalam jaringan gagal, seluruh jaringan akan terus beroperasi secara normal.



Gambar 1.12. Topologi Mesh

Pada gambar 1.12 menunjukkan bentuk dari topologi mesh dalam jaringan komputer.

Kelebihan dari topologi mesh

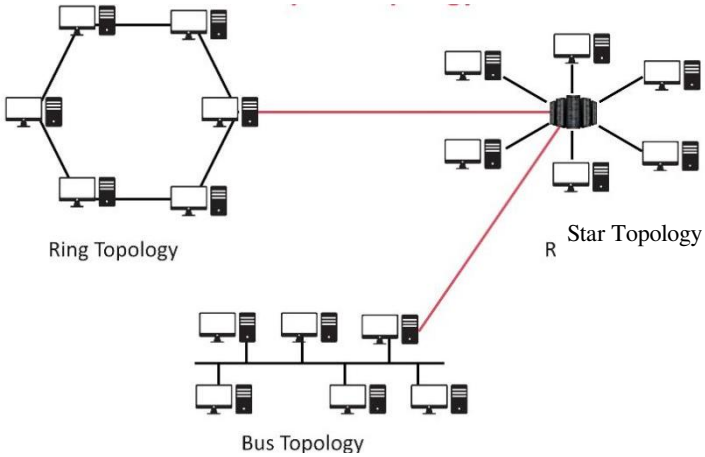
- ✓ Mengelola lalu lintas dalam jumlah besar, karena beberapa perangkat dapat mengirimkan data secara bersamaan.
- ✓ Kegagalan pada satu perangkat tidak menyebabkan putusnya jaringan atau transmisi data.
- ✓ Penambahan perangkat tambahan tidak mengganggu transmisi data antar perangkat lain.

Kekurangan topologi mesh

- ✓ Biaya penerapannya lebih tinggi dibandingkan topologi jaringan lainnya, sehingga pilihan ini kurang diminati.
- ✓ Membangun dan memelihara topologi itu sulit dan memakan waktu.
- ✓ Kemungkinan terjadinya redundant koneksi tinggi, sehingga menambah tingginya biaya dan potensi berkurangnya efisiensi.

f. Topologi Hybrid

Menggabungkan dua atau lebih topologi jaringan, seperti topologi mesh, bus, dan ring, menghasilkan topologi hybrid. Instalasi dan spesifikasinya—yang mencakup jumlah mesin, lokasinya, dan kinerja jaringan yang diperlukan—memiliki dampak pada penggunaan dan pemilihannya. Meskipun topologi hibrid menawarkan struktur yang rumit dan serangkaian teknologi diperlukan untuk pelaksanaan praktisnya, topologi hibrid memiliki manfaat berupa peningkatan fleksibilitas; ini dapat meningkatkan toleransi kesalahan dan mempermudah penambahan atau penghapusan topologi dasar yang berbeda. Ketika Anda perlu mencapai keragaman dalam jaringan komputer, topologi hybrid lebih praktis. Pada gambar 1.13 menunjukkan bentuk dari topologi hybrid dalam jaringan komputer.



Gambar 1.13. Topologi Hybrid

Kelebihan Topologi Hybrid

- ✓ Topologi jenis ini menggabungkan keunggulan berbagai jenis topologi dalam satu topologi.
- ✓ Dapat dimodifikasi sesuai kebutuhan.
- ✓ Ini sangat fleksibel.
- ✓ Hal ini sangat dapat diandalkan.
- ✓ Jaringan ini mudah diskalakan karena jaringan Hibrid dibangun dengan cara yang memungkinkan integrasi komponen perangkat keras baru dengan mudah.
- ✓ Deteksi kesalahan dan pemecahan masalah itu mudah.
- ✓ Menangani lalu lintas dalam jumlah besar.
- ✓ Ini digunakan untuk membuat jaringan besar.

- ✓ Kecepatan topologi menjadi cepat ketika dua topologi disatukan.

Kekurangan Topologi Hybrid

- ✓ Ini adalah jenis jaringan yang mahal.
- ✓ Desain jaringan hybrid sangat kompleks.
- ✓ Terjadi perubahan pada hardware untuk menghubungkan topologi yang satu dengan topologi yang lain.
- ✓ Biasanya arsitektur hybrid memiliki skala yang lebih besar sehingga membutuhkan banyak kabel dalam proses instalasinya.
- ✓ Hub yang digunakan untuk menghubungkan dua jaringan berbeda harganya sangat mahal. Dan hub berbeda dari hub biasa karena mereka harus cukup cerdas untuk bekerja dengan arsitektur yang berbeda.
- ✓ Instalasi adalah proses yang sulit.

1.6.Network Devices

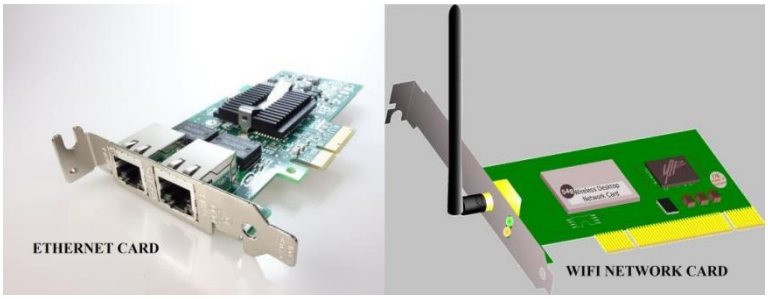
Interkoneksi beberapa perangkat, disebut juga host, yang terhubung menggunakan banyak jalur untuk tujuan mengirim/menerima data atau media. Jaringan komputer juga dapat mencakup beberapa perangkat/media yang membantu komunikasi antara dua perangkat berbeda; ini dikenal sebagai perangkat Jaringan dan mencakup hal-hal seperti router, switch, hub, dan bridge, serta lainnya.

a. Network Adaptor Cards/Network Interface Card Kabel and wireless

Perangkat fisik, biasanya berupa chip atau papan sirkuit, yang disebut kartu antarmuka jaringan (NIC), dipasang pada komputer untuk mengaktifkan konektivitas jaringan. Interupsi input/output, antarmuka akses memori langsung, transmisi data, rekayasa lalu lintas jaringan, dan partisi hanyalah beberapa fitur yang dimungkinkan oleh NIC modern untuk komputer.

Kartu antarmuka jaringan (NIC) memberi PC koneksi khusus dan berkelanjutan ke jaringan. Ini mempraktikkan sirkuit lapisan fisik yang diperlukan untuk membuat koneksi dengan standar lapisan data link, seperti Ethernet atau Wi-Fi. Setiap kartu berfungsi sebagai representasi perangkat dan memiliki kemampuan untuk menyiapkan, mengirim, dan mengatur aliran data melalui jaringan.

NIC berfungsi sebagai perantara komputer dan jaringan data. Misalnya, komputer meneruskan permintaan pengguna untuk halaman web ke kartu jaringan, yang mengubahnya menjadi impuls listrik. Pada gambar 1.14 berikut adalah contoh Network Adaptor Cards/Network Interface Card.



Gambar 1.14. Network Adaptor Cards/Network Interface Card

b. Bridge

Jembatan jaringan komputer adalah perangkat yang menggabungkan beberapa jaringan area lokal (LAN) menjadi satu LAN yang lebih luas. Bridging adalah nama proses agregasi jaringan. Bridge, juga disebut sebagai lapisan dua switch, adalah perangkat fisik atau perangkat keras yang berfungsi pada lapisan koneksi data model OSI.

Tugas utama switch adalah memeriksa lalu lintas masuk dan memutuskan apakah akan meneruskan atau memfilternya. Dalam jaringan komputer, jembatan pada dasarnya digunakan untuk membagi koneksi jaringan menjadi beberapa segmen; akibatnya, setiap segmen memiliki domain tabrakan dan bandwidthnya sendiri. Dalam hal ini, jembatan digunakan untuk meningkatkan fungsionalitas jaringan. Pada gambar 1.15 berikut adalah contoh Perangkat Bridge.

Gambar 1.15. Perangkat Bridge

c. Hubs

Hub adalah perangkat jaringan yang menghubungkan beberapa komputer dan perangkat lainnya. Hub adalah komponen inti dari jaringan area lokal (LAN), juga dikenal sebagai repeater atau konsentrator. Setiap perangkat yang terhubung ke hub berada di subnet yang sama dan menerima semua data yang ditransfer di sana. Setelah itu, hub mendistribusikan data ke setiap perangkat lain yang terhubung, sehingga membangun sistem produktif untuk berbagi data pengguna. Pada gambar 1.16 berikut adalah contoh Perangkat Bridge.

Gambar 1.16. Perangkat Bridge

d. Switches

Switch jaringan adalah perangkat keras yang memfasilitasi komunikasi antara dua atau lebih komputer atau perangkat TI lainnya. Jaringan komunikasi dihasilkan ketika beberapa perangkat IT terhubung. Berbagi jaringan dimungkinkan untuk server, penyimpanan file, pencetakan, komputasi, akses Internet, dan layanan TI lainnya. Perangkat TI bertukar data melalui jaringan dalam bentuk "paket". Meskipun tugas yang lebih kompleks (seperti menentukan apakah suatu paket dapat mencapai tujuan yang diinginkan) biasanya merupakan lingkup perangkat jaringan jenis lain, switch dasar meneruskan paket dari satu perangkat ke perangkat lainnya.

Switch dapat berupa perangkat yang berdiri sendiri atau bagian terintegrasi dari perangkat lain yang memproses paket data, termasuk router jaringan dan titik akses nirkabel (AP). Teknologi peralihan dasar yang berusia puluhan tahun adalah salah satu komponen penting dari semua jaringan TI kontemporer, termasuk Internet. Pada gambar 1.17 berikut adalah contoh Perangkat Switch.

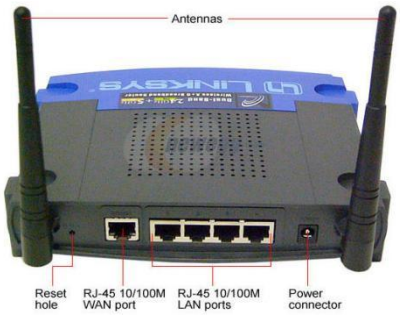
Gambar 1.17. Perangkat Switch

e. Routers

Peralatan yang menghubungkan dua atau lebih jaringan atau subjaringan packet-switched disebut router. Dengan meneruskan paket data ke alamat IP yang dituju, ia mengatur lalu lintas antara jaringan-jaringan ini dan memungkinkan banyak perangkat berbagi koneksi Internet. Inilah dua peran utamanya.

Meskipun ada banyak jenis router, sebagian besar router mentransfer data antara WAN (jaringan area luas) dan LAN (jaringan area lokal). LAN adalah kumpulan perangkat jaringan yang terbatas pada wilayah tertentu. Biasanya, LAN hanya membutuhkan satu router.

Wide area network (WAN) adalah jaringan yang tersebar di wilayah geografis yang luas. Misalnya, organisasi dan bisnis besar dengan beberapa lokasi di seluruh negara akan memerlukan LAN individual untuk setiap lokasi, yang terhubung ke LAN lain untuk membentuk WAN. WAN biasanya memerlukan beberapa router dan switch karena sifatnya yang tersebar. Pada gambar 1.18 berikut adalah contoh Perangkat Router.



Gambar 1.18. Perangkat Router

f. Access Points

Perangkat jaringan yang menghubungkan jaringan kabel dan nirkabel disebut titik akses (AP). Karena AP konsumen sering kali berfungsi ganda sebagai firewall dan router internet, mereka sering disebut sebagai "router nirkabel". Firewall jarang ditemukan pada AP komersial dan industri, yang biasanya memiliki kemampuan perutean jaringan yang sederhana.

Standar Wi-Fi digunakan oleh sebagian besar AP untuk menghubungkan jaringan nirkabel, meskipun semakin banyak AP komersial dan industri kontemporer yang mendukung teknologi nirkabel Bluetooth dan Thread. Hal ini memungkinkan perangkat Internet of Things (IoT) dan perangkat yang berpusat pada manusia didukung oleh AP komersial dan industri. Pada gambar 1.19 berikut adalah contoh Perangkat Access Point (AP).

Gambar 1.19. Perangkat Access Point (AP)

g. Repeater

Perangkat jaringan yang disebut repeater digunakan untuk membuat dan memperbesar sinyal masuk. Repeater berfungsi pada lapisan fisik model OSI. Tujuan utama penggunaan repeater adalah untuk memperluas jangkauan jaringan dengan meningkatkan kekuatan dan kualitas sinyal. Repeater untuk Wide Area Network (WAN) dan Local Area Network (LAN) digunakan untuk mengukur kinerjanya. Penggunaan repeater memungkinkan data dikirim ke area tertentu secara eksklusif dan mengurangi kesalahan dan kehilangan data. Keuntungan utama menggunakan repeater adalah memungkinkan data ditransfer dalam jarak yang jauh dan dengan keamanan yang lebih baik. Pada gambar 1.20 berikut adalah contoh Perangkat repeater.

Gambar 1.20. Perangkat repeater

1.7.Kriteria Jaringan

Kriteria jaringan yang paling penting adalah kinerja, keandalan, keamanan, dan bentuk topologi. Kinerja tergantung pada faktor-faktor seperti jumlah pengguna dan kecepatan transmisi. Keandalan diukur dengan frekuensi kegagalan dan waktu pemulihan. Kriteria yang harus dipenuhi oleh suatu jaringan komputer adalah:

1. Performansi : Ini diukur dalam hal waktu transit dan waktu respons.

- ✓ Waktu transit adalah waktu yang dibutuhkan pesan untuk berpindah dari satu perangkat ke perangkat lainnya
- ✓ Waktu respons adalah waktu yang berlalu antara penyelidikan dan respons.
- ✓ Kinerja bergantung pada faktor-faktor berikut:
- ✓ Jumlah pengguna
- ✓ Jenis media transmisi
- ✓ Kemampuan jaringan yang terhubung
- ✓ Efisiensi perangkat lunak
- ✓ Bandwidth
- ✓ Topologi jaringan
- ✓ Protokol jaringan
- ✓ Jarak
- ✓ Kemacetan jaringan
- ✓ Perangkat keras jaringan

2. Keandalan – Diukur dalam bentuk:

- ✓ Frekuensi kegagalan
- ✓ Pemulihan dari kegagalan
- ✓ Ketahanan saat terjadi bencana
- ✓ Kualitas layanan (Quality of service -QoS)
- ✓ Mengurangi satu titik kegagalan
- ✓ Perencanaan kapasitas
- ✓ Arsitektur jaringan

3. Keamanan – Ini berarti melindungi data dari akses tidak sah.
4. Topologi jaringan

Topologi jaringan ini adalah faktor penting lainnya yang perlu dipertimbangkan ketika merancang jaringan komputer. Ini mengacu pada cara komputer, perangkat, dan tautan diatur dalam jaringan. Topologi umum meliputi bus, star, ring, mesh, dan hybrid, masing-masing memiliki kelebihan dan kekurangan dalam hal biaya, skalabilitas, keandalan, dan kinerja. Pilihan topologi tergantung pada kebutuhan spesifik dan batasan jaringan. Kriteria penting lainnya yang harus dipenuhi oleh jaringan komputer antara lain kinerja, keandalan, dan keamanan.

1.8. Tujuan dibangunnya Jaringan Komputer

Ada beberapa tujuan dibangunnya jaringan komputer antara lain:

1. Berbagi Sumber Daya – Banyak organisasi memiliki sejumlah besar komputer dalam operasinya, yang lokasinya terpisah. Mantan. Sekelompok pekerja kantoran dapat berbagi printer, faks, modem, pemindai, dll.
2. Keandalan Tinggi – Jika ada sumber pasokan alternatif, semua file dapat direplikasi pada dua mesin atau lebih. Jika salah satunya tidak tersedia karena kegagalan perangkat keras, salinan lainnya dapat digunakan.
3. Komunikasi Antar-proses – Pengguna jaringan, yang letaknya terpisah secara geografis, dapat berkomunikasi dalam sesi interaktif melalui jaringan. Untuk memungkinkan hal ini, jaringan harus menyediakan komunikasi yang hampir bebas dari kesalahan.
4. Akses fleksibel – File dapat diakses dari komputer mana pun di jaringan. Proyek dapat dimulai di satu komputer dan diselesaikan di komputer lain.
5. Keamanan – Jaringan komputer harus aman untuk melindungi dari akses tidak sah, pelanggaran data, dan ancaman keamanan lainnya. Hal ini mencakup penerapan langkah-langkah seperti firewall, perangkat lunak antivirus, dan enkripsi untuk memastikan kerahasiaan, integritas, dan ketersediaan data.
6. Kinerja – Jaringan komputer harus memberikan kinerja tinggi dan latensi rendah untuk memastikan bahwa aplikasi dan layanan responsif dan tersedia saat dibutuhkan. Hal ini memerlukan optimalisasi infrastruktur jaringan, pemanfaatan bandwidth, dan manajemen lalu lintas.
7. Skalabilitas- Jaringan komputer harus dirancang untuk ditingkatkan atau diturunkan skalanya sesuai kebutuhan untuk mengakomodasi perubahan jumlah pengguna, perangkat, dan lalu lintas data. Hal ini memerlukan perencanaan dan pengelolaan yang cermat untuk memastikan jaringan dapat memenuhi kebutuhan saat ini dan masa depan.
8. Tujuan lainnya termasuk Distribusi fungsi pemrosesan, Manajemen terpusat, dan alokasi sumber daya jaringan, Kompatibilitas peralatan dan perangkat lunak yang

berbeda, Kinerja jaringan yang baik, Skalabilitas, Penghematan uang, Akses ke informasi jarak jauh, Komunikasi orang ke orang, dll.

1.9. Layer OSI pada Jaringan Komputer

The open systems interconnection (OSI) adalah model konseptual yang dibuat oleh Organisasi Internasional untuk Standardisasi yang memungkinkan beragam sistem komunikasi untuk berkomunikasi menggunakan protokol standar. Dalam bahasa Inggris sederhananya, OSI memberikan standar bagi sistem komputer yang berbeda untuk dapat berkomunikasi satu sama lain.

Model OSI dapat dilihat sebagai bahasa universal untuk jaringan komputer. Hal ini didasarkan pada konsep pemisahan sistem komunikasi menjadi tujuh lapisan abstrak, yang masing-masing ditumpuk di atas lapisan terakhir. Ada 7 lapisan pada OSI antara lain; Physical, Datalink, Network, Transport, Session, Presentation, dan Application. Pembahasan tentang layer OSI ada pada bab selanjutnya.

1.10. Rangkuman

1. Jaringan komputer adalah kumpulan dua atau lebih komputer yang terhubung untuk berkomunikasi dan berbagi sumber daya, seperti file, printer, dan koneksi internet. Tujuan utama jaringan adalah untuk memfasilitasi pertukaran informasi di antara pengguna.
2. Node: Perangkat yang terhubung dalam jaringan, seperti komputer, printer, atau server.
3. Bandwidth: Kapasitas maksimum dari jalur komunikasi untuk mentransfer data dalam waktu tertentu.
4. Latency: Waktu yang dibutuhkan untuk mengirimkan data dari sumber ke tujuan.
5. LAN (Local Area Network): Jaringan yang terbatas pada area geografis kecil, seperti rumah atau kantor.
6. WAN (Wide Area Network): Jaringan yang mencakup area yang lebih luas, seperti antar kota atau negara.
7. MAN (Metropolitan Area Network): Jaringan yang mencakup area yang lebih besar dari LAN tetapi lebih kecil dari WAN, biasanya dalam satu kota.
8. Client-Server: Model di mana satu atau lebih komputer (server) menyediakan layanan kepada komputer lain (client).
9. Peer-to-Peer: Model di mana setiap komputer dalam jaringan memiliki kemampuan untuk bertindak sebagai server dan client.
10. Jenis Topologi : Topologi Bus: Semua perangkat terhubung ke satu kabel utama. Topologi Star: Semua perangkat terhubung ke satu titik pusat (hub atau switch). Topologi Ring: Setiap perangkat terhubung ke dua perangkat lainnya, membentuk

lingkaran. Topologi Tree: Kombinasi dari topologi star dan bus, dengan struktur hierarkis. Topologi Hybrid: Kombinasi dari berbagai topologi yang ada.

11. Network Devices terdiri atas: Router: Perangkat yang menghubungkan beberapa jaringan dan mengarahkan lalu lintas data. Switch: Perangkat yang menghubungkan perangkat dalam jaringan lokal dan mengelola lalu lintas data di dalamnya. Hub: Perangkat yang menghubungkan beberapa perangkat dalam jaringan, tetapi tidak mengelola lalu lintas data. Modem: Perangkat yang mengubah sinyal digital menjadi sinyal analog dan sebaliknya untuk koneksi internet.
12. Kriteria Jaringan terdiri atas: Kecepatan: Kecepatan transfer data dalam jaringan. Keamanan: Perlindungan data dari akses tidak sah. Skalabilitas: Kemampuan jaringan untuk berkembang dan menampung lebih banyak perangkat.
13. Layer OSI terdiri atas 7 Lapisan yaitu: Physical Layer: Mengatur pengiriman data fisik. Data Link Layer: Menyediakan pengalamatan dan pengendalian akses ke media. Network Layer: Mengatur pengalamatan dan routing data. Transport Layer: Menjamin pengiriman data yang andal. Session Layer: Mengelola sesi komunikasi antar aplikasi. Presentation Layer: Mengatur format data dan enkripsi. Application Layer: Menyediakan antarmuka untuk aplikasi pengguna.

1.11. Latihan Soal

1. Apa yang dimaksud dengan jaringan komputer?

a) Sekumpulan perangkat yang terhubung untuk berbagi informasi
b) Hanya komputer yang terhubung ke internet
c) Hanya perangkat keras yang digunakan untuk komunikasi
d) Sistem operasi yang digunakan pada komputer
e) Sekumpulan perangkat lunak yang saling berinteraksi

2. Jenis jaringan yang mencakup area geografis yang luas seperti kota atau negara adalah:

a) LAN
b) WAN
c) MAN
d) PAN
e) WLAN

3. Topologi jaringan yang paling mudah dikelola dan tahan terhadap kerusakan adalah:

a) Bus
b) Star
c) Ring
d) Mesh
e) Hybrid

4. Perangkat yang berfungsi untuk menghubungkan beberapa jaringan dan mengarahkan lalu lintas data adalah:
a) Hub
b) Switch
c) Router
d) Modem
e) Repeater

5. Apa tujuan utama dari membangun jaringan komputer?
a) Meningkatkan biaya operasional
b) Mempercepat akses informasi dan berbagi sumber daya
c) Mengurangi jumlah perangkat yang digunakan
d) Meningkatkan kompleksitas sistem
e) Meningkatkan keamanan data

6. Lapisan OSI yang bertanggung jawab untuk pengalamatan dan pengiriman data adalah:
a) Application
b) Transport
c) Network
d) Data Link
e) Session

7. Istilah yang digunakan untuk menggambarkan kecepatan dan efisiensi dalam jaringan adalah:
a) Keandalan
b) Bandwidth
c) Latensi
d) Keamanan
e) Throughput

8. Jenis arsitektur jaringan yang memungkinkan setiap perangkat untuk berfungsi sebagai server dan client adalah:
a) Client-server
b) Peer-to-peer
c) Hybrid
d) Distributed
e) Centralized

9. Topologi jaringan yang menghubungkan setiap perangkat satu sama lain disebut:
a) Star

b) Bus
c) Ring
d) Mesh
e) Tree

10. Kriteria penting yang harus dipenuhi oleh jaringan komputer meliputi:
a) Kecepatan, keandalan, dan keamanan
b) Hanya kecepatan dan biaya
c) Hanya keandalan dan keamanan
d) Hanya biaya dan efisiensi
e) Kecepatan, biaya, dan fleksibilitas

Soal Esai

11. Jelaskan perbedaan antara LAN, WAN, dan MAN serta berikan contoh penggunaan masing-masing jenis jaringan.
12. Diskusikan kelebihan dan kekurangan dari berbagai topologi jaringan yang umum digunakan, seperti bus, star, dan ring.
13. Apa saja perangkat jaringan yang umum digunakan dan fungsi masing-masing dalam mengelola lalu lintas data?
14. Uraikan tujuan dibangunnya jaringan komputer dan bagaimana jaringan dapat meningkatkan efisiensi dalam organisasi.
15. Deskripsikan model OSI dan jelaskan peran masing-masing lapisan dalam proses pengiriman data melalui jaringan.

1.12. Daftar Pustaka

Haryanto, B. (2023). *Jaringan Komputer untuk Pemula: Routing dan Switching.* Jakarta: Salemba Empat.

Putra, M. (2021). *Pengantar Jaringan Komputer: Fokus pada Routing dan Switching.* Yogyakarta: Graha Ilmu.

Rudiantoro, A. (2021). *Routing dan Switching dalam Jaringan Komputer: Panduan Lengkap*. Bandung: Informatika.

Syamsul, I. (2020). *Teknik Routing dan Switching untuk Jaringan Skala Kecil dan Menengah*. Yogyakarta: Andi.

Santoso, H. (2022). *Jaringan Komputer: Teori dan Praktik Routing serta Switching*. Jakarta: Erlangga.

BAB 2

OSI MODEL

2.1. Definisi

Open System Interconnection atau OSI adalah model referensi yang diciptakan dari sebuah kerangka yang bersifat konseptual. Namun, saat ini telah berkembang dan menjadi sebuah standarisasi khusus berkaitan dengan koneksi komputer. Tujuan dari pembuatan OSI Layer adalah menjadi model rujukan bagi setiap vendor atau developer, sehingga produk atau perangkat lunak yang dibuat memiliki sifat interpolate. Yang berarti, user dapat melakukan kerja sama dengan produk atau sistem tanpa perlu melakukan penanganan secara khusus atau special.

2.2. Protokol Jaringan

Protokol adalah sebuah aturan yang mendefinisikan beberapa fungsi yang ada dalam sebuah jaringan komputer, misalnya mengirim pesan, data, informasi dan fungsi lain yang harus dipenuhi oleh sisi pengirim (*transmitter*) dan sisi penerima (*receiver*) agar komunikasi berlangsung dengan benar. Selain itu protokol juga berfungsi untuk memungkinkan dua atau lebih komputer dapat berkomunikasi dengan bahasa yang sama.

Fungsi Protokol adalah sebagai berikut:

1. *Fragmentasi dan Reassembly*, Membagi informasi yang dikirim menjadi beberapa paket data pada saat sisi pengirim mengirimkan informasi tadi dan setelah diterima maka sisi penerima akan menggabungkan lagi menjadi paket berita yang lengkap.
2. *Encaptulation*, Fungsi dari encaptulation adalah melengkapi berita yang dikirimkan dengan address, kode-kode koreksi dan lain-lain *Connection Control*, Fungsi dari *connection control* adalah membangun hubungan komunikasi dari *transmitter* dan *receiver*.
3. *Flow Control*, Fungsi dari *flow control* adalah mengatur perjalanan data dari *transmitter* ke *receiver.*
4. *Error Control,* Fungsi dari *error control* adalah mengontrol terjadinya kesalahan yang terjadi pada waktu data dikirimkan.
5. *Transmission Service,* Fungsi dari *transmission service* adalah memberi pelayanan komunikasi data khususnya yang berkaitan dengan prioritas dan keamanan serta perlindungan data.

Beberapa perusahaan yang berperan dalam usaha komunikasi, antara lain :

1. Electronic Industries Association (EIA)

2. Committee Consultative Internationale de Telegrapque et Telephonique (CCITT)
3. International Standards Organization (ISO)
4. American National Standard Institute (ANSI)
5. Institute of Electrical and Electronic Engineers (IEEE)

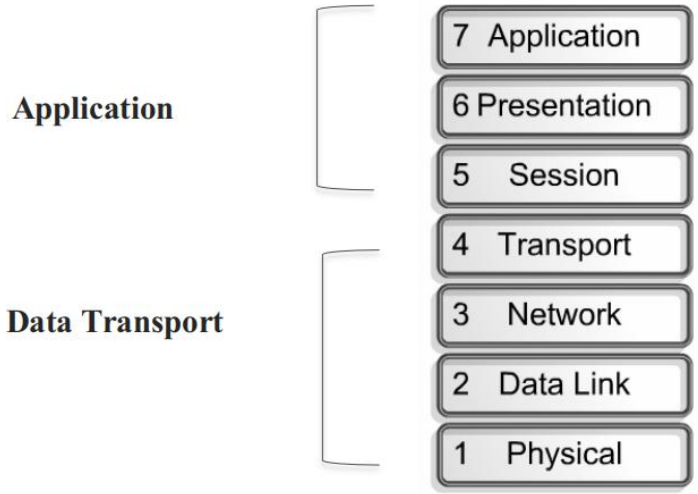
Alasan diperlukan standarisasi dalam komunikasi data pada suatu jaringan komputer:

1. Standarisasi memberikan jaminan kepada produsen hardware dan software bahwa produknya akan banyak digunakan oleh pemakai dengan kata lain potensi pasar menjadi lebih besar.
2. Standarisasi menjadikan produk dari para produsen komputer dapat saling berkomunikasi, sehingga pembeli menjadi lebih leluasa dalam memilih peralatan dan menggunakanya.
3. Dengan standarisasi maka produsen tidak dapat melakukan monopoli pasar sehingga harga produk menjadi lebih murah karena terjadi persaingan sehat antar para produsen dalam menjual produknya.

2.3.Layer OSI Model

Model Referensi OSI merupakan salah satu arsitektur jaringan komputer yang dibuat oleh ISO (International for standardization Organization) untuk memecahkan masalah kompatibilitas device antar vendor, dengan menyediakan standarisasi yang dapat digunakan oleh para vendor dalam membuat device. Model referensi OSI mengidentifikasikan semua proses yang dibutuhkan untuk melakukan komunikasi dan membaginya ke dalam kelompok secara logika yang disebut layer. OSI menjelaskan bagaimana data dan informasi dari sebuah aplikasi pada sebuah komputer melewati media jaringan berkomunikasi ke aplikasi yang berada di komputer lain. Model referensi *OSI* merupakan petunjuk bagi para developer aplikasi dalam membuat dan mengimplementasikan aplikasinya berjalan pada sebuah jaringan. *OSI* juga merupakan sebuah framework dalam pembuatan dan mengimplementasikan standar jaringan.

OSI terdiri dari tujuh *layer*, yang secara umum terbagi dalam dua kelompok, yakni *Upper layer (Application Layer)* dan *lower layer* (*data transport layer*). *Layer* yang tergolong dalam *upper layer* mendefinisikan bagaimana aplikasi pada sebuah *host* akan berkomunikasi dengan user dan host lainnya. Sedangkan *lower layer* mendefinisikan bagaimana data terkirim dari satu *host* ke *host* lainnya. Model referensi *OSI* terdiri dari tujuh *layer*, antara lain : *Application Layer, Presentation Layer, Session Layer, Transport Layer, Network Layer, Data Link Layer, Physical Layer.*



Gambar 2.1. Dua Kelompok di dalam *OSI Layer*

2.3.1. Application Layer

Application layer berfungsi sebagai *interface* antara user dan komputer. *Layer* ini bertanggung jawab untuk mengidentifikasi ketersediaan dari *partner* komunikasi, menentukan ketersediaan *resources* dan melakukan proses sinkronisasi komunikasi. *Application layer* menentukan identitas dan ketersediaan dari *partner* komunikasi untuk sebuah aplikasi dengan data yang dikirim Beberapa contoh aplikasi yang bekerja di *application layer* antara lain:

1. ***Telnet* (*Telecommunication Network*)**
   Telnet merupakan program yang menyediakan kemampuan bagi user untuk dapat mengakses resource sebuah mesin (telnet server) dari mesin lain (telnet client) secara remote, seolah-olah user berada dekat dengan mesin dimana resource tersimpan.
2. ***FTP (File Transfer Protocol)***
   FTP merupakan sebuah program yang berfungsi mengirimkan *file* dari suatu *host* ke *host* lain melalui jaringan.
3. ***DNS (Domain Name system)***
   Mekanisme pemetaan antara *FQDN (Fully Qualified Domain Names)* dengan alamat *IP*. *FQDM* merupakan sebuah hirarki yang secara logika menempatkan sistem berbasis pada domain pengenal.
4. ***SMTP (Simple Mail Transfer Protocol)***
   SMTP merupakan sebuah protokol (program yang dieksekusi oleh program lain) yang berfungsi untuk mengatur pengiriman e-mail
5. ***SNMP (Simple Network Management Protocol)***
   SNMP merupakan salah satu jenis protokol yang memberikan kemampuan untuk mengawasi dan mengatur peralatan-peralatan dalam jaringan komputer.

2.3.2. Presentation Layer

Presentation *Layer* berfungsi untuk menyediakan sistem penyajian data ke *application layer,* Menyediakan sistem pembentuk kode (*format coding*), misalnya format ASCII yang digunakan komputer IBM, *compatible* dan format EBDIC digunakan oleh mesin IBM, Menyediakan proses konversi antar format *coding* yang berbeda, Menyediakan layanan translation. *Presentation layer* menjamin data yang dikirimkan dari *application layer* suatu sistem dapat dibaca oleh *layer* aplikasi di sistem yang lain, Menyediakan sarana untuk melakukan *compression*, *decompression*, *encryption,* dan *decryption*. Beberapa contoh aplikasi yang bekerja di *presentation layer* antara lain:

1. *PICT, TIFF, JPEG*, merupakan format data untuk aplikasi berupa gambar (image).
2. *MIDI*, *MPEG* dan quicktime, merupakan format data untuk aplikasi sound & movie.
3. *EBDIC* dan *ASCII*, Apllication Layer merupakan format data untuk informasi dalam bentuk *teks*.

2.3.3. Session Layer

Session Layer berfungsi dan bertanggung jawab :

1. Mengkoordinasi jalannya komunikasi antar sistem
2. Melakukan proses pembentukan, pengelolaan dan pemutusan *session* antar sistem aplikasi
3. Mengendalikan dialog antar *device*

Berikut ini *adalah* beberapa contoh protokol yang bekerja di *session layer*:

1. ***Remote Procedure Call (RPC).*** Merupakan protokol yang menyediakan mekanisme *client/server* pada sistem operasi *windows NT.*
2. ***Structure Query Language (SQL)***, dibangun oleh IBM untuk menyediakan kemudahan bagi user dalam mendefinisikan kebutuhan informasi yang terdapat di sistem lokal atau *remote sistem*.
3. ***Network File System* (*NFS*),** dibangun oleh *Sun Microsystem* dan digunakan oleh *workstation* TCP/IP dan Unix agar dapat mengakses *remote resource*.
4. ***X Windows***, merupakan protokol yang menyediakan mekanisme *client*/*server* pada sistem operasi Unix
5. ***Appletalk Session Protocol (ASP),*** merupakan protokol yang menyediakan mekanisme *client*,/*server* pada mesin-mesin apple.

2.3.4. Transport Layer

Transport Layer bertanggung jawab dalam proses :

1. Pengemasan data *upper layer* ke dalam bentuk *segment*.
2. Pengiriman *segment* antar *host*.
3. Penetapan hubungan secara logika antar host pengirim dan penerima dengan membentuk *virtual circuit*.
4. Secara opsional, menjamin proses pengiriman data yang dapat diandalkan.

5. Proses pengiriman pada transport layer ini dapat dilakukan dengan 2 mekanisme:

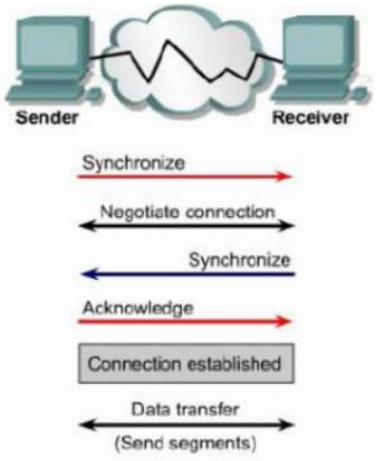
Connection oriented

Proses pengiriman yang menggunakan *Connection oriented* dapat diilustrasikan pemberian pesan kepada seseorang yang dipisahkan oleh jarak yang jauh. Memberikan pesan tersebut dilakukan melalui telepon. Proses pemberian pesan akan dilakukan jika lawan bicara adalah orang yang dituju sehingga dapat dipastikan bahwa pesan diterima oleh orang membentuk virtual circuit. yang dimaksudkan. Dari ilustrasi tersebut dapat kita simpulkan bahwa data yang dikirimkan dengan menggunakan mekanisme *connection oriented* dapat diandalkan. TCP (Transmission Control Protocol) merupakan jenis protokol yang mampu mengirimkan data yang reliable.

Connection Less

Mekanisme *connectionless* diilustrasikan dengan proses memberikan pesan yang dilakukan melalui surat. Pengiriman surat mengkin sampai ke tempat tujuan tetapi penerima di tempat tujuan belum tentu orang yang dimaksudkan sehingga pesan belum tentu sampai ke orang yang dimaksud. Dari ilustrasi tersebut dapat kita simpulkan bahwa data yang dikirimkan dengan menggunakan mekanisme Connectionless kurang dapat diandalkan. UDP *(User Datagram Protocol)* mengirimkan data unreliable, Pengiriman data dengan menggunakan TCP tidak berarti selalu tanpa kesalahan. Kesalahan dapat terjadi tetapi kesalahan tersebut dapat dideteksi dan dapat dilakukan proses pengiriman ulang atas segmen yang salah. Proses pembentukan hubungan connection-oriented dilakukan melalui beberapa langkah yakni :

1. Pengiriman segment *synchronization* untuk menetapkan *connection agreement*.
2. Segment kedua dan ketiga adalah *acknowledge* yang meminta dan menetapkan parameter-parameter antar host.
3. Segment terakhir merupakan sebuah *acknowledgement*, *segment* ini memberitahu host tujuan bahwa *connection agreement* telah diterima dan hubungan telah ditetapkan, sehingga dan sudah mulai dikirimkan.



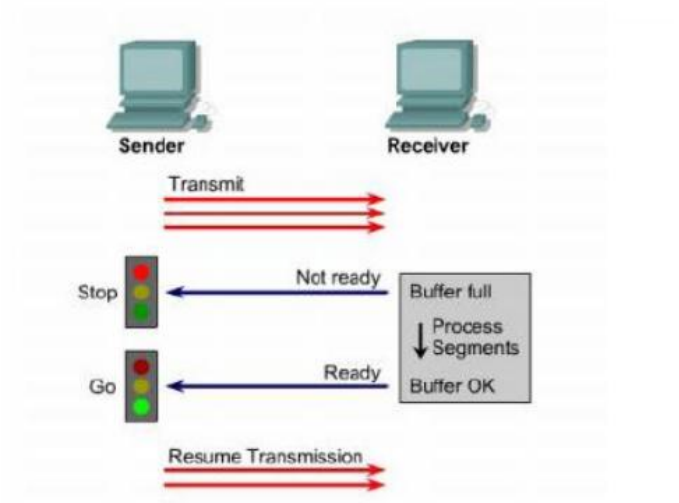
Gambar 2.2. Pembentukan Hubungan dengan mekanisme *connection oriented*

Connection oriented memiliki karakteristik sebagai berikut :

1. Setelah menerima *segment* dari pengirim, station penerima akan mengirimkan *segment acknowledge back* ke *station* pengirim.
2. Station pengirim akan mengulang pengiriman segment ketika menerima *acknowledge* dari penerima
3. S*egment-segment* akan disusun kembali oleh penerima ke dalam susunan yang tepat.
4. Dapat mengelola aliran data sehingga tidak terjadi *congestion*, *overload* dan kehilangan data.

Ketika menerima data dari komputer lain, sebuah komputer akan menyimpan dalam sebuah memori yang disebut *buffer*. Teknik *buffering* merupakan salah satu teknik untuk mengatasi *congestion*. Teknik *buffering* terbatas untuk penerimaan data dalam jumlah tertentu karena kapasitas *buffer* sangat terbatas. Untuk menangani keterbatasan ukuran *buffer*, *layer transport* menyediakan mekanisme *flow control*. *Flow* control mencegah host pengirim melakukan pengiriman data yang menyebabkan terjadinya overflow dan kehilangan data pada sisi host penerima.

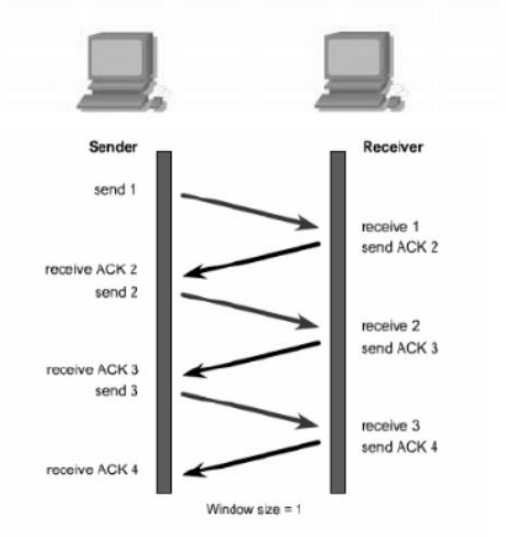
Pencegahan dilakukan dengan mengirimkan sinyal not ready pada pengirim ketika kapasitas *buffer* sudah penuh pada sisi penerima, sehingga host pengirim menghentikan sementara proses pengiriman data sampai menerima sinyal go. Proses di atas diilustrasikan pada gambar dibawah ini.



Gambar 2.3. Pengiriman segment dengan menggunakan *Flow Control*

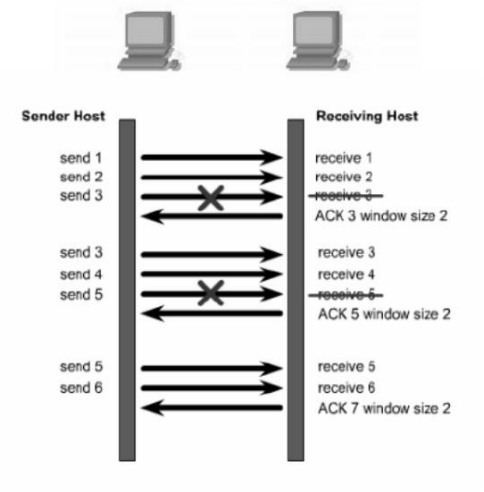
Pengiriman data akan berjalan lambat jika *host* pengirim selalu menunggu *acknowledgment* setelah mengirimkan tiap *segment*-nya. Banyak waktu terbuang karena *host* pengirim hanya bisa melakukan pengiriman *segment* berikutnya setelah selesai menerima acknowledgment dari *host* penerima. Masalah banyaknya waktu yang terbuang dapat diatasi dengan

mekanisme *windowing*. Sejumlah *segmen* yang diperbolehkan untuk dikirimkan tanpa menunggu *acknowledgment* disebut *window*. Windowing mengontrol berapa banyak informasi yang dikirimkan dari satu *host* ke *host* lainnya. Gambar dibawah ini menampilkan proses pengiriman dengan ukuran window watu dan untuk meningkatkan *performance* ukuran *window* diubah menjadi tiga.



Gambar 2.4. Mekanisme Windowing

Dengan memperbesar ukuran window menjadi tiga, maka acknowledgment hanya akan dikirimkan oleh penerima ketika telah menjadi tiga segment. Sesuai dengan ukuran window. Host pengirim akan mencatat setiap segmen yang dikirim dan menunggu *acknowledgement* dari *host* penerima sebelum mengirimkan *segment* berikutnya. Jika dalam jangka waktu tertentu tidak menerima *acknowledgement* maka host pengirim akan melakukan pengiriman ulang. Dalam dibawah ini diperlihatkan bahwa sebuah *host* mengirimkan *segment* 1,2, 3 . host penerima memberitahu host pengirim bahwa *segment-segment* tersebut telah diterima dan meminta segment ke 4. karena menerima *acknowledgment* 4 maka host pengirim akan mengirimkan segment ke 4, 5 dan 6. segment 5 mengalami masalah dalam proses pengirimannya dan mengakibatkan *host* penerima memberitahu kejadian tersebut pada *host* pengirim dan meminta p pengiriman ulang terhadap segment 5. ketika *host* penerima telah menerima segment ke 5, *acknowledgment* yang diberikan kepada *host* pengirim adalah *acknowledge* untuk meminta *segment* 7.



Gambar 2.5. *Positive acknowledgement* dengan pengiriman ulang

Beberapa *protokol* yang bekerja di layer ini adalah sebagai berikut :

1. *ATP (Appletalk Transaction Protocol)* dan NBP *(Name Binding Protocol),* merupakan protokol-protokol di jaringan apple yang bertugas membentuk hubungan antar host.
2. NetBios/NetBEUI, menetapkan dan mengelola komunikasi antar komputer sedangkan NetBEUI menyediakan layanan *transport* data untuk melakukan komunikasi.
3. *SPX(sequenced Packet Exchange)* dan *NWLink protocol connection oriented* pada jaringan *Netware* yang digunakan untuk menjamin pengiriman data.
4. *TCP (Transmission Control Protocol),*bagian dari protokol TCP/IP yang bertanggung jawab untuk mengirimkan data.

2.3.5. Network Layer

Network Layer bertanggung jawab untuk:

1. Melakukan mekanisme *routing* melalui *internetwork*, *router* merupakan *device* yang berfungsi membawa trafik antar *host* yang terletak dalam *network* yang berbeda.
2. Mengelola sistem pengalamatan logika terhadap jaringan komputer.
3. Data berupa segmen yang diterima dari transport layer akan dikemas ke dalam bentuk packet. Ketika packet diterima oleh interface sebuah router, maka alamat tujuan akan diperiksa jika alamat tujuan tidak ditemukan maka packet tersebut akan dibuang. Tetapi jika alamat tujuan ditemukan dalam routing table (sebuah tabel yang terdapat di dalam router berisi informasi tentang alamat network yang dapat dijangkau oleh router) maka paket akan dikeluarkan melalui outbound interface menuju ke alamat tujuan.

Pada network layer terdapat dua jenis packet yaitu

1. *Packet* Data, digunakan untuk membawa data milik user dikirimkan melalui jaringan dan protokol yang digunakan untuk mengelola *packet* data disebut *Routed Protocol*. Contoh *protokol* yang tergolong ke dalam *routed protocol* antara liain IP dan IPX.
2. *Route Update Packet*, digunakan untuk mengupdate informasi yang terdapat dalam *routing table* milik *router* yang terhubung dengan *router* lainnya. Protokol yang mengelola *routing table* disebut dengan *routing protocol*. Contoh protokol yang tergolong dalam *routing* protokol antara lain *RIP*, *IGRP*, *OSPF* dan sebagainya.

Beberapa contoh protokol yang bekerja di *network layer* adalah sebagai berikut :
1. DDP (*delivery* datagram *protocol*), merupakan protokol *transport* yang biasa digunakan oleh jaringan komputer apple.
2. IP (*internet Protocol*), bagian dari *Protokol TCP/IP* yang menyediakan informasi *routing* dan sistem pengalamatan logika.
3. IPX *(Internet packet Exchange)* dan NWLink merupakan protokol yang disediakan oleh sistem operasi *netware* yang dibuat oleh *novell*, digunakan untuk *routing* paket.
4. *NETBEUI* dibangun oleh IBM dan *Microsoft*, menyediakan layanan transport untuk *NetBIOS*.

2.3.6. Data Link Layer

Paket yang diperoleh dari *network layer* dibungkus (dienkapsulasi oleh *data link layer* ke dalam sebuah *frame*. Data link *layer* bertugas menjamin pesan yang dikirimkan ke media yang tepat dan menerjemahkan pesan dari *network layer* ke dalam bentuk bit di *physical layer* untuk dikirimkan ke *host* lain. Data link *layer* akan membentuk *packet* ke dalam bentuk *frame* dan menambahkan sebuah header yang berisi alamat *hardware* (*physical*/hardware *addressing*), Data Link terbagi dalam dua sublayer :
1. *Logical* Link Control (LLC) 802.2, bertanggung jawab mengidentifikasikan protokol *network layer* dan kemudian melakukan enkapsulasi protokol-protokol tersebut. Isi LLC akan menentukan langkah selanjutnya yang harus dilakukan ketika merima frame dari host lain (LLC bertindak sebagai service access point). Sebagai contoh, ketika host menerima frame, LLC akan mengerti bahwa *packet* ditujukan untuk protokol IP di *Network Layer*.
2. *Media Acces* Control (MAC) 802.3, mendefinisikan bagaimana packet ditempatkan pada sebuah media dalam sublayer ini sistem pengalamatan hardware didefinisikan.

2.3.7. Physical Layer

Tanggung jawab dari *layer* ini adalah melakukan pengiriman dan penerimaan bit. *Physical layer* secara langsung menghubungkan media komunikasi yang berbeda-beda. *Physical layer* menetapkan kebutuhan-kebutuhannya secara *electrical*, *mechanical* prosedur untuk mengaktifkan, memelihara dan memutuskan jalur antar sistem secara fisik

2.4. Rangkuman

1. *Open System Interconnection* atau OSI adalah model referensi yang diciptakan dari sebuah kerangka yang bersifat konseptual. Tujuan dari pembuatan OSI Layer adalah menjadi model rujukan bagi setiap vendor atau developer, sehingga produk atau perangkat lunak yang dibuat memiliki sifat interpolate.
2. Fungsi Protokol berfungsi sebagai *Fragmentasi* dan *Reassembly*, Encapsulation, *Flow Control*, *Error Control, Transmission Service.*
3. Alasan diperlukan standarisasi dalam komunikasi data pada suatu jaringan komputer adalah sebagai Standarisasi memberikan jaminan kepada produsen hardware dan software, Standarisasi menjadikan produk dari para produsen komputer dapat saling berkomunikasi, sehingga pembeli menjadi lebih leluasa dalam memilih peralatan dan menggunakanya.
4. *OSI* terdiri dari tujuh *layer*, yang secara umum terbagi dalam dua kelompok, yakni *Upper layer (Application Layer)* dan *lower layer* (*data transport layer*). *Layer* yang tergolong dalam *upper layer* mendefinisikan bagaimana aplikasi pada sebuah *host* akan berkomunikasi dengan user dan host lainnya. L*ower layer* mendefinisikan bagaimana data terkirim dari satu *host* ke *host* lainnya.
5. Model referensi *OSI* terdiri dari tujuh *layer*, antara lain : *Application Layer, Presentation Layer, Session Layer, Transport Layer, Network Layer, Data Link Layer, Physical Layer.*
6. *Application layer* berfungsi sebagai *interface* antara user dan komputer. *Layer* ini bertanggung jawab untuk mengidentifikasi ketersediaan dari *partner* komunikasi, menentukan *ketersediaan resources* dan melakukan proses sinkronisasi komunikasi.
7. *Presentation Layer* berfungsi untuk : Menyediakan sistem penyajian data ke *application layer,* Menyediakan sistem pembentuk kode (*format coding*), misalnya format ASCII yang digunakan komputer IBM, *compatible* dan format EBDIC digunakan oleh mesin IBM, Menyediakan proses konversi antar format *coding* yang berbeda.
8. *Session Layer* berfungsi dan bertanggung jawab Mengkoordinasi jalannya komunikasi antar sistem, Melakukan proses pembentukan, pengelolaan dan pemutusan *session* antar sistem aplikasi, Mengendalikan dialog antar *device.*
9. Transport Layer bertanggung jawab dalam proses : Pengemasan data *upper layer* ke dalam bentuk *segment*, Pengiriman *segment* antar *host*, Penetapan hubungan secara logika antar host pengirim dan penerima dengan membentuk *virtual circuit*, Secara opsional, menjamin proses pengiriman data yang dapat diandalkan.
10. *Network Layer* bertanggung jawab Melakukan mekanisme *routing* melalui *internetwork*, *router* merupakan *device* yang berfungsi membawa trafik antar *host* yang terletak dalam *network* yang berbeda, mengelola sistem pengalamatan logika terhadap jaringan komputer.
11. Data link *layer* bertugas menjamin pesan yang dikirimkan ke media yang tepat dan menerjemahkan pesan dari *network layer* ke dalam bentuk bit di *physical layer* untuk dikirimkan ke *host* lain.

12. *Physical layer* bertanggung jawab melakukan pengiriman dan penerimaan bit. *Physical layer* secara langsung menghubungkan media komunikasi yang berbeda- beda.

2.5.Latihan Soal

1. MAC atau Media Access Control di OSI Layer ada pada layer ....
   A. Phisical C. Data Link E. Session
   B. Network D. Transport
2. Protokol pada layer transport yang connection oriented dan reliable tapi delay transfer datanya tinggi adalah ….
   A. TCP C. FTP E. HTTP
   B. IRC D. UDP
3. Protokol pada layer network yang berguna mendapatkan informasi ethernet address dari nomor IP adalah :
   A. RIP C. HTTP E. UDP
   B. RARP D. ARP
4. SMB atau Server Message Block adalah protokol untuk transfer file di lingkungan Windows, pada TCP/IP ada pada layer ....
   A. Presentasi C. Transport E. Internet
   B. Network D. Aplikasi
5. Protokol pada layer aplikasi yang berguna mentransfer file html dan web adalah :
   A.XTP C. TCP E. HTTP
   B. IRC D. UDP
6. Protokol Telnet digunakan untuk mengakses jarak jauh, adalah berada pada layer :
   A. Presentasi C. Transport E. Internet
   B. Network D. Aplikasi
7. Protokol untuk koneksi point to point (PPP) berada pada layer :
   A. network C. transport E. Data Link LLC
   B. internet D. Data Link MAC
8. Protokol pada layer network yang berguna mendapatkan informasi nomor IP dari ethernet address adalah :
   A. RIP C. HTTP E. UDP
   B. RARP D. ARP
9. Berikut ini adalah protokol-protokol yang bekerja di layer aplikasi adalah kecuali :
   A. HTTP C. TELNET E. FTP
   B. SMB D. DNS
10. Protokol untuk pertukaran mail yaitu :
   A. SMTP C. TFTP E. NETBIOS
   B. SNMP D. MIME

Soal Esai

11. Jelaskan apa yang dimaksud dengan model OSI dan mengapa model ini penting dalam jaringan komputer.
12. Uraikan tujuh lapisan dalam model OSI dan sebutkan fungsi utama dari masing-masing lapisan tersebut.
13. Diskusikan perbedaan antara protokol jaringan yang beroperasi pada lapisan transport dan lapisan network dalam model OSI.
14. Bagaimana proses pengiriman data melalui model OSI? Jelaskan langkah-langkah yang dilalui data dari pengirim ke penerima.
15. Apa yang dimaksud dengan encapsulation dalam konteks model OSI? Berikan contoh bagaimana data dikemas di setiap lapisan.

2.6. Daftar Pustaka

Academy, Cisco Networking Cisco Networking. (2020). *Switching, Routing, and Wireless Essentials Companion Guide (CCNAv7)*. London: Pearson Education.

Damanik, Hillman Akhyar, Merry Anggraeni, dan Farida Ayu Avisena Nusantar. (2023). *Konsep dan Penerapan Switching dan Routing Implementasi Jaringan Komputer Berbasis Cisco*. Jawa Barat: Mega Press Nusantara.

Januari, R. (2022). *Cisco Networking: Panduan Lengkap Routing dan Switching*. Yogyakarta: Graha Ilmu.

Lestari, N. (2022). *Pengenalan dan Implementasi Routing serta Switching pada Jaringan Cisco.* Jakarta: Elex Media Komputindo.

Haryanto, B. (2023). *Jaringan Komputer untuk Pemula: Routing dan Switching.* Jakarta: Salemba Empat.

BAB 3

TCP/IP

3.1.Sejarah TCP/IP

Transmission Contorl Protocol (TCP)/*Internet Protocol* (IP) merupakan protokol komunikasi yang digunakan untuk menghubungkan perangkat jaringan baik yang bersifat LAN, WAN maupun internet. Teknologi TCP/IP dimulai dari lahirnya ARPANET pada tahu 1969 yang merupakan jaringan paket switching digital yang didanai oleh DARPA (Defence Advanced Research Projects Agency). Protokol jaringan yang digunakan oleh ARPANET tidak dapat menghandle jumlah node jaringan yang semakin besar sehingga dibutuhkan perbaikan protokol yang digunakan. Protokol yang dikembangkan dibuat lebih umum agar perangkat yang lain dapat berkomunikasi dengan perangkat yang sudah ada. Protokol tersebut adalah protokol TCP/IP dan diadopsi sebagai standar ARPANET pada tahun 1983. Protokol ini juga dikembangkan dan diimplementasikan kedalam sistem UNIX.
Perkembangan TCP/IP (Transmission Control Protocol/Internet Protocol) mencerminkan evolusi teknologi jaringan, pengembangan internet, dan kebutuhan komunikasi yang semakin kompleks. Berikut adalah beberapa tonggak perkembangan utama TCP/IP:

1. Pembentukan Konsep dan Pengembangan Awal (1970-an): Pada awal 1970-an, TCP/IP dikembangkan sebagai respons terhadap kebutuhan untuk menghubungkan jaringan komputer yang berbeda di DARPA. Model referensi ini menjadi dasar bagi protokol yang diperlukan untuk komunikasi antarjaringan.
2. Pengenalan TCP dan IP (1974-1978): Pada tahun 1974, Vinton Cerf dan Bob Kahn mengusulkan protokol TCP dalam dokumen "A Protocol for Packet Network Intercommunication." Kemudian, pada tahun 1978, versi pertama dari protokol IP (IPv4) dijelaskan.
3. Adopsi oleh ARPANET (1983): Pada 1 Januari 1983, ARPANET secara resmi beralih sepenuhnya ke TCP/IP, menandai perubahan besar dalam arsitektur internet. Hal ini memungkinkan kompatibilitas dan komunikasi yang lebih baik antarjaringan.
4. Pembentukan Internet Society (1984): Pada tahun 1984, Vinton Cerf dan Robert Kahn mendirikan Internet Society (ISOC) untuk mendukung pengembangan internet secara global dan mempromosikan standar terbuka.
5. Pengembangan IPv6 (1990-an): Dengan peningkatan jumlah perangkat yang terhubung ke internet, alamat IPv4 mulai terbatas. Ini mendorong pengembangan IPv6 pada tahun 1990-an, yang menyediakan alamat IP yang lebih banyak untuk mendukung pertumbuhan internet yang pesat.

6. Proliferasi Internet dan Standarisasi (1990-an hingga 2000-an): Internet menjadi semakin umum di kalangan masyarakat umum, bisnis, dan pemerintahan. Standarisasi dan adopsi TCP/IP sebagai model protokol utama menjadi kunci untuk interoperabilitas global.
7. Migrasi ke IPv6 (2000-an hingga Sekarang): Meskipun pengenalan IPv6 telah terjadi sejak tahun 1990-an, migrasi dari IPv4 ke IPv6 masih berlangsung. Hal ini dilakukan untuk mengatasi kekurangan alamat IPv4 dan memastikan kelangsungan pertumbuhan internet.
8. Internet of Things (IoT) dan Kompleksitas Modern (2010-an hingga Sekarang): Pertumbuhan fenomena Internet of Things (IoT) membawa tantangan baru dalam skala, keamanan, dan efisiensi komunikasi. TCP/IP terus beradaptasi untuk memenuhi tuntutan lingkungan jaringan yang semakin kompleks ini.

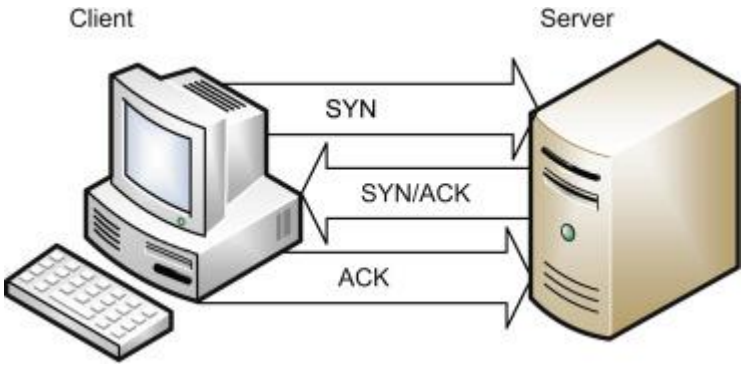
   Perkembangan TCP/IP terus berlanjut seiring berjalannya waktu, dengan pembaruan dan penyesuaian yang dilakukan untuk memenuhi kebutuhan jaringan modern dan teknologi terkini.

3.2. Cara Kerja TCP/IP

Dalam membangun komunikasi dan pertukaran data antar node dalam jaringan, TCP/IP memiliki meknaisme yang handal untuk menjamin komunikasi berjalan dengan baik. Secara umum komunikasi dibangun dalam 3 tahap yaitu pembentukan koneksi TCP/IP, transfer data, dan pelepasan koneksi TCP IP.

a) Pembentukan koneksi TCP/IP

   Pembentukkan koneksi TCP/IP merupakan proses awal yang dilakukan sebelum pengiriman data. Pembentukkan koneksi ini dikenal dengan "*Three-Way-Handshake"* yang melibatkan serangkaian langkah berikut ini.



Gambar 3.1. Proses *three way handshake*

1. Permintaan (SYN) dari komputer pengirim (client) ke komputer penerima (server)
2. Penerima (server) menerima pesan SYN, kemudian mengirimkan pesan SYN-ACK (Synchronize-Acknowledgment) sebagai tanggapan.

3. Pengirim menerima pesan SYN-ACK dan mengirimkan pesan ACK (Acknowledgment) sebagai konfirmasi kepada server.

Setelah langkah ini selesai, koneksi dianggap sudah terbentuk dan siap untuk mentransfer data.

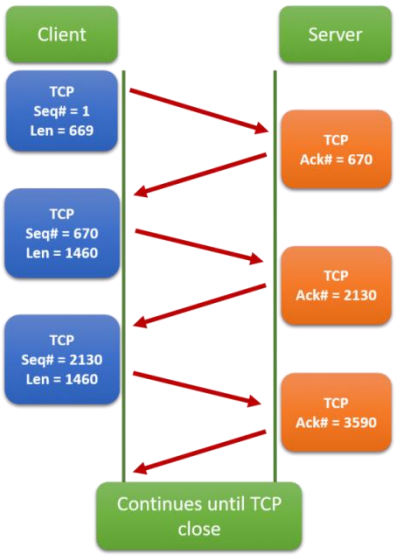
b) Transfer data pada TCP/IP

Setelah terbentuknya koneksi TCP melalui proses three-way handshake yang telah dijelaskan sebelumnya, maka data dapat ditransfer antara pengirim (client) dan penerima (server) melalui serangkaian langkah-langkah. Berikut adalah ringkasan dari proses transfer data pada TCP/IP:

4. Segmentasi Data: Data yang akan dikirim dari aplikasi pengirim dibagi menjadi segmen-segmen yang lebih kecil. Setiap segmen diberi nomor urutan untuk membantu dalam pengaturan ulang dan rekonstruksi data di penerima.
5. Pengiriman Segmen: Setiap segmen data dikirimkan ke lapisan transport (TCP). TCP menambahkan informasi header, termasuk nomor urutan dan nomor akhir (sequence number dan acknowledgment number).
6. Penerimaan dan Konfirmasi: Penerima menerima segmen-segmen tersebut. Penerima mengirimkan kembali pesan ACK (Acknowledgment) kepada pengirim untuk mengkonfirmasi bahwa segmen telah diterima.
7. Reassembling Segmen: Penerima mengumpulkan segmen-segmen yang diterima dan me-reassemble (menggabungkan) data untuk membentuk pesan lengkap.
8. Acknowledgment: Pengirim menerima pesan ACK dan menandai segmen-segmen yang telah berhasil dikirim. Jika pengirim tidak menerima ACK dalam batas waktu tertentu, maka segmen tersebut dianggap hilang, dan akan dikirimkan kembali.
9. Flow Control: TCP menggunakan mekanisme flow control untuk mengontrol laju pengiriman data dan mencegah penumpukan di penerima. Penerima memberikan indikasi berapa banyak data yang dapat diterima melalui penggunaan mekanisme window size.
10. Retransmisi: Jika terjadi hilangnya segmen atau jika pengirim tidak menerima ACK dalam waktu yang ditentukan, pengirim akan mengirimkan kembali segmen tersebut (retransmission).

Proses di atas diulang hingga seluruh data berhasil ditransfer. TCP memastikan kehandalan dan urutan pengiriman data. Jika ada kesalahan atau kehilangan data, TCP akan mengatasi masalah tersebut dengan melakukan retransmisi dan pengaturan ulang nomor urutan.

Berikut ini adalah gambaran proses transfer data pada TCP/IP



Gambar 3.2. Proses transfer data pada TCP IP

c) Pelepasan koneksi TCP/IP

Setelah koneksi dan pertukaran data selesai dilakukan dan koneksi tidak diperlukan lagi, maka dapat dilakukan pelepasan koneksi. Berikut ini adalah tahapan dalam pelepasan koneksi TCP/IP.

1. Inisiasi Pelepasan (FIN) dari Pengirim
   Pengirim mengirimkan pesan FIN ke penerima untuk mengindikasikan bahwa pengirim telah selesai mentransfer data dan ingin menutup koneksi.
2. Konfirmasi Pelepasan (ACK) dari Penerima
   Penerima menerima pesan FIN dan mengirimkan pesan ACK (Acknowledgment) untuk mengkonfirmasi bahwa pesan FIN telah diterima. Penerima dapat melanjutkan proses penutupan sendiri atau melanjutkan mentransfer data yang tersisa sebelum menutup koneksi.
3. Inisiasi Pelepasan (FIN) dari Penerima
   Penerima, setelah menyelesaikan pengiriman data yang tersisa atau memutuskan untuk menutup koneksi, mengirimkan pesan FIN ke pengirim.
4. Konfirmasi Pelepasan (ACK) dari Pengirim
   Pengirim menerima pesan FIN dari penerima dan mengirimkan pesan ACK sebagai konfirmasi.

Jika tahap diatas sudah selesai, maka koneksi dianggap ditutup.

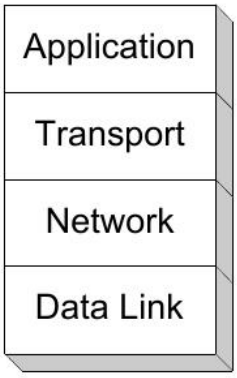
3.3. TCP/IP Layer

Protokol TCP/IP terdiri dari beberapa lapisan atau layer yang bekerja bersama-sama untuk komunikasi yang efisien antara perangkat atau node didalam jaringan. Setiap lapisan memiliki

fungsi dan tanggung jawabnya sendiri-sendiri, dan kolaborasi antara lapisan-lapisan ini memungkinkan pengiriman dan penerimaan data dengan efisien di seluruh jaringan. Berikut ini adalah layer dalam TCP/IP:

1. Link Layer (Lapisan Tautan)
   Lapisan ini bertanggung jawab untuk mengelola fisik pengiriman data di antara perangkat di jaringan yang berdekatan mencakup semua aspek fisik dan elektrik dari transmisi data, serta protokol yang digunakan untuk mengirim dan menerima data di tingkat fisik. Contoh protokol yang bekerja pada layer ini adalah ethernet dan PPP. Ethernet: Protokol yang digunakan untuk menghubungkan perangkat di jaringan lokal (LAN). PPP (Point-to-Point Protocol): Protokol untuk menghubungkan dua perangkat langsung melalui saluran poin-ke-poin seperti modem.
2. Internet Layer (Lapisan Internet)
   Lapisan ini menangani pengalamatan dan routing di seluruh jaringan. Protokol utama di lapisan ini adalah Internet Protocol (IP), yang memberikan alamat unik kepada setiap perangkat dalam jaringan dan memastikan data mencapai tujuannya dengan mengatur rute terbaik melalui jaringan. Conoth protokol yang berkerja pada layer ini adalah IP dan ICMP. IP (Internet Protocol): Protokol yang memberikan alamat unik (IPv4 atau IPv6) untuk perangkat di jaringan. ICMP (Internet Control Message Protocol): Digunakan untuk mengirim pesan kontrol dan kesalahan, seperti pesan "ping" untuk menguji ketersediaan perangkat.
3. Transport Layer (Lapisan Transport)
   Lapisan transport bertanggung jawab untuk mengatur pengiriman data end-to-end antara perangkat sumber dan tujuan. Dua protokol utama di lapisan ini adalah Transmission Control Protocol (TCP), yang menyediakan pengiriman data yang handal dan terurut, serta User Datagram Protocol (UDP), yang menyediakan pengiriman data yang lebih cepat dan lebih ringan, tetapi kurang dapat diandalkan. Contoh protokol yang berkerja pada layer ini TCP dan UDP. TCP (Transmission Control Protocol): Protokol yang menjamin pengiriman data yang handal, terurut, dan bebas kesalahan. UDP (User Datagram Protocol): Protokol yang memberikan pengiriman data yang lebih cepat tanpa jaminan handal atau urutan.
4. Application Layer (Lapisan Aplikasi)
   Lapisan ini menyediakan antarmuka untuk aplikasi dan layanan jaringan. Ini adalah lapisan di mana aplikasi seperti web browsers, email clients, dan protokol seperti HTTP, FTP, dan SMTP beroperasi. Lapisan aplikasi memungkinkan pengguna untuk berinteraksi dengan jaringan dan menggunakan berbagai layanan yang disediakan oleh protokol di lapisan di bawahnya.

Protokol TCP/IP terdiri atas 4 (empat) layer seperti tampak pada gambar 3.3.



Gambar 3.3. Empat layer protokol TCP/IP

3.4. Kelebihan dan Kekurangan TCP/IP

TCP/IP dapat diterima secara luas karena memiliki beberapa keunggulan sebagai berikut:

a. TCP/IP menggunakan standar protokol terbuka sehingga tersedia secara luas dan dapat diadopsi oleh siapa pun. Semua orang dapat mengembangkan perangkat lunak dengan protokol ini. Kelebihan inilah yang membuat TCP/IP cepat berkembang dan diadopsi oleh berbagai sistem operasi.
b. TCP/IP tidak bergantung pada perangkat keras dan perangkat lunak tertentu sehingga cocok digunakan untuk menghubungkan berbagai macam jaringan seperti ethernet, token ring dan lainnya.
c. TCP/IP menggunakan sistem pengalamatan yang unik sehingga dapat mengidentifikasi secara unik perangkat yang terhubung kedalam jaringan yang sangat luas.
d. TCP/IP menyediakan fitur routing sehingga memungkinkan antar jaringan dapat terhubung.

Kekurangan atau keterbatasan dari protokol TCP/IP adalah sebagai berikut:

a. Keterbatasan Alamat IPv4: Salah satu tantangan utama adalah ketersediaan alamat IPv4 yang terbatas. Dengan semakin banyaknya perangkat yang terhubung ke internet, alamat IPv4 mulai habis. Meskipun sudah ada solusi yaitu IPv6 dengan alamat yang lebih banyak, migrasi masih memerlukan waktu dan sumber daya.
b. Keamanan Terbatas: Protokol awal TCP/IP dirancang tanpa mempertimbangkan keamanan sebagai prioritas utama. Seiring dengan meningkatnya ancaman keamanan seperti serangan phishing, malware, dan DDoS, tantangan keamanan semakin kompleks. Meskipun telah ada peningkatan melalui protokol keamanan tambahan seperti SSL/TLS, tantangan keamanan tetap relevan.
c. Kompleksitas Konfigurasi: Konfigurasi TCP/IP, terutama pada tingkat administratif dan manajemen, dapat menjadi kompleks terutama dalam lingkungan jaringan yang besar. Administrasi, pemeliharaan, dan pemecahan masalah dapat memerlukan keahlian teknis yang tinggi.

d. Ketergantungan pada Koneksi: Meskipun TCP/IP menyediakan mekanisme handshaking dan pemulihan kesalahan, ketergantungan pada koneksi yang andal membuat aplikasi rentan terhadap latensi atau gangguan koneksi.
e. Overhead Protokol: Protokol TCP/IP memperkenalkan overhead, terutama dalam hal header, yang dapat mengurangi efisiensi penggunaan bandwidth. Ini bisa menjadi masalah, terutama dalam situasi di mana efisiensi penggunaan bandwidth sangat penting.
f. Ketergantungan pada Infrastruktur Sentral: Sistem TCP/IP memerlukan infrastruktur yang dapat diandalkan. Jika ada kegagalan pada infrastruktur sentral atau titik-titik pusat lainnya, dapat menyebabkan gangguan komunikasi di seluruh jaringan.
g. Perkembangan IoT: Pertumbuhan Internet of Things (IoT) menambahkan tantangan baru dalam skala, keamanan, dan manajemen jaringan. Jumlah perangkat yang terhubung secara eksponensial meningkat, dan pengelolaan serta keamanannya menjadi fokus utama.
h. Pertumbuhan Global Jaringan: Dengan pertumbuhan global jaringan, terutama di wilayah-wilayah dengan tingkat pertumbuhan yang tinggi, tantangan dalam mempertahankan koneksi yang andal, serta kebutuhan untuk mendukung ragam infrastruktur, menjadi semakin kompleks.

3.5. Rangkuman

1. TCP/IP merupakan protokol komunikasi utama yang digunakan untuk menghubungkan perangkat dalam jaringan, baik itu LAN, WAN, maupun internet.
2. Sejarah TCP/IP dimulai dari pengembangan ARPANET pada tahun 1969, yang membutuhkan protokol yang lebih umum untuk mengatasi pertumbuhan jumlah node jaringan.
3. Protokol TCP/IP menjadi standar komunikasi untuk internet pada tahun 1983, menggantikan protokol sebelumnya seperti NCP (Network Control Protocol). Seiring perkembangan teknologi, TCP/IP terus diperbarui untuk mendukung kebutuhan komunikasi yang semakin kompleks.
4. TCP/IP terdiri dari dua protokol utama: TCP (Transmission Control Protocol) untuk pengiriman data yang andal dan IP (Internet Protocol) untuk pengalamatan dan pengiriman paket data.
5. Three-Way Handshake: Proses pembentukan koneksi TCP dimulai dengan three-way handshake, di mana pengirim dan penerima saling bertukar sinyal untuk memastikan koneksi yang stabil.
6. Pengiriman Data: Setelah koneksi terbentuk, data dibagi menjadi segmen-segmen yang lebih kecil untuk dikirim melalui jaringan, dan setiap segmen dilengkapi dengan informasi pengalamatan.
7. TCP/IP Layer terdiri atas 4 layer
8. Layer Aplikasi: Menyediakan antarmuka untuk aplikasi pengguna, seperti HTTP, FTP, dan SMTP.

9. Layer Transport: Mengelola pengiriman data antara aplikasi, memastikan data sampai dengan benar dan dalam urutan yang tepat (TCP) atau tanpa jaminan (UDP).
10. Layer Internet: Bertanggung jawab untuk pengalamatan dan routing paket data melalui jaringan (IP).
11. Layer Akses Jaringan: Mengatur pengiriman data fisik melalui media jaringan, termasuk protokol Ethernet dan Wi-Fi.
12. TCP/IP memiliki kelebihan Interoperabilitas, Skalabilitas, Fleksibilitas. Sedangkan kekurangannya adalah Kompleksitas, Keamanan dan Overhead.

3.6. Latihan Soal

1. Apa kepanjangan dari TCP dalam model TCP/IP?
a) Transmission Control Protocol
b) Transfer Control Protocol
c) Transport Control Protocol
d) Transmission Communication Protocol
e) Transport Communication Protocol

2. Protokol yang digunakan untuk mengirimkan data tanpa menjamin pengiriman adalah:
a) TCP
b) UDP
c) ICMP
d) FTP
e) HTTP

3. Layer mana dalam model TCP/IP yang setara dengan lapisan transport dalam model OSI?
a) Application
b) Internet
c) Transport
d) Network Access
e) Session

4. Apa fungsi utama dari protokol IP dalam model TCP/IP?
a) Mengatur sesi komunikasi
b) Mengirimkan data dengan kecepatan tinggi
c) Mengatur pengalamatan dan pengiriman paket data
d) Menyediakan antarmuka pengguna
e) Mengelola koneksi antara aplikasi

5. Protokol mana yang digunakan untuk mengirim email?
a) HTTP

b) FTP
c) SMTP
d) SNMP
e) DHCP

6. Apa yang dimaksud dengan subnetting dalam konteks TCP/IP?
a) Menghubungkan beberapa jaringan
b) Membagi jaringan menjadi beberapa subnet yang lebih kecil
c) Mengubah alamat IP menjadi format yang lebih sederhana
d) Mengatur kecepatan transfer data
e) Mengamankan data yang dikirim

7. Protokol yang digunakan untuk mendapatkan alamat IP secara otomatis adalah:
a) DHCP
b) DNS
c) ARP
d) ICMP
e) FTP

8. Apa yang dimaksud dengan NAT dalam konteks TCP/IP?
a) Network Address Translation
b) Network Access Technology
c) Network Application Transfer
d) Network Address Transfer
e) Network Access Translation

9. Layer mana dalam model TCP/IP yang bertanggung jawab untuk pengalamatan logis?
a) Application
b) Transport
c) Internet
d) Network Access
e) Session

10. Apa keuntungan utama dari menggunakan TCP dibandingkan dengan UDP?
a) Kecepatan pengiriman
b) Pengiriman data yang lebih aman
c) Jaminan pengiriman data dan urutan yang benar
d) Penggunaan bandwidth yang lebih rendah
e) Kemudahan dalam konfigurasi

Soal Esai

11. Jelaskan sejarah perkembangan protokol TCP/IP dan bagaimana protokol ini menjadi standar komunikasi di internet.
12. Uraikan cara kerja TCP dalam menjamin pengiriman data yang andal dan bagaimana mekanisme pengendalian aliran diterapkan.
13. Diskusikan perbedaan antara TCP dan UDP, serta situasi di mana masing-masing protokol lebih cocok digunakan.
14. Jelaskan konsep pengalamatan IP dan bagaimana pengalamatan ini berfungsi dalam jaringan TCP/IP. Sertakan penjelasan tentang IPv4 dan IPv6.
15. Deskripsikan bagaimana model TCP/IP berfungsi dalam pengiriman data dari satu perangkat ke perangkat lain, termasuk peran setiap layer dalam proses tersebut

3.7. Daftar Pustaka

Haryanto, B. (2023). *Jaringan Komputer untuk Pemula: Routing dan Switching.* Jakarta: Salemba Empat.

Putra, M. (2021). *Pengantar Jaringan Komputer: Fokus pada Routing dan Switching.* Yogyakarta: Graha Ilmu.

Rudiantoro, A. (2021). *Routing dan Switching dalam Jaringan Komputer: Panduan Lengkap*. Bandung: Informatika.

Syamsul, I. (2020). *Teknik Routing dan Switching untuk Jaringan Skala Kecil dan Menengah*. Yogyakarta: Andi.

BAB 4

IP ADDRESSING

4.1. Pendahuluan Pengalamatan IP

IP addressing atau pengalamatan IP merupakan singkatan dari *Internet Protocol addressing,* merupakan sistem penotomran unik yang digunakan untuk mengidentifikasi dan lokalisasi perangkat atau device didalam jaringan komputer menggunakan protokol IP. Pengalamatan IP memiliki peran yang sangat penting dalam pengiriman data melalui jaringan, memastikan bahwa paket data dapat diarahkan dengan tepat ke perangkat yang dituju. Setiap perangkat yang terhubung ke internet atau jaringan lokal harus memiliki alamat yang unik. Alamat IP dapat dilihat sebagai "alamat rumah" perangkat tersebut dalam dunia maya, memungkinkan perangkat untuk dikenali dan mampu berkomunikasi dengan perangkat lain diseluruh dunia.

Ada dua versi utama dari protokol IP yang digunakan saat ini yaitu internet protocol version 4 (IPv4) dan internet protocol version 6 (IPv6). IPv4 menggunakan alamat 32 bit sedangkan IPv6 menggunakan alamat 128 bit. IPv4 saat ini semakin habis karena jumlah alamat IPv4 yang terbatas sehingga muncul IPv6 dengan jumlah alamat yang jauh lebih banyak. Sebuah alamat IP memiliki dua bagian utama yaitu bagian jaringan (*network portion*) dan bagian host (*host portion*). Pada umumnya alamat IP dibagi menjadi beberapa kelas seperti kelas A, B, atau C yang menentukan seberapa besar bagian jaringan dan bagian host dari alamat tersebut.

Sebuah jaringan dapat dibagi dalam beberapa sub jaringan atau subnet. Dalam pengalamatan IP terdapat teknik untuk membagi sebuah jaringan menjadi beberapa subnet yang lebih kecil yang dikenal dengan istilah *subnetting.* Dengan teknik subnetting akan membantu dalam manajemen jaringan dan keamanan, memungkinkan administrator untuk mengatur lalu lintas dan mengelola sumber daya jaringan dengan lebih efisien. Pengalamatan IP dapat dilakukan secara manual maupun otomatis. Untuk pengalamtan IP secara otomatis adalah dengan menggunakan protokol *dynamic host configuration protocol* (DHCP). DHCP adalah protokol jaringan yang memungkinkan perangkat jaringan mendapatkan alamat IP secara dinamis dari server DHCP. Hal ini sangat berguna dalam lingkungan dimana perangkat sering bergabung atau meninggalkan jaringan.

Alamat IP dibagi menjadi dua ketegori yaitu private dan public. IP private digunakan dalam jaringan lokal dan tidak dapat diakses secara langsung dari jaringan internet. Sedangkan IP publik adalah IP yang digunakan untuk mengidentifikasi perangkat yang terhubung langsung ke internet dan perangkat tersebut dapat diakses dari jaringan internet. IP address merupakan dasar dari komunikasi di internet. Dengan alamat IP, perangkat dapat mengirim dan menerima

data dengan akurat dan efisien. Dengan berkembangnya teknologi dan pertumbuhan internet, pemahaman yang baik tetang pengalamatan IP menjadi kunci untuk merancang dan mengelola jaringan yang andal dan aman.

4.2. Dasar Pengalamatan IP

Alamat IPv4 merupakan identitas unik dari sebuah perangkat dalam jaringan. IPv4 memiliki panjang 32 bit dan dinotasikan dalam format dot desimal dan memiliki karakteristik berikut:

1. Terbagi menjadi dua bagian yaitu bagian network (*network portion*) dan bagian host (*host portion*)
2. Dipecah menjadi 4 bagian atau oktet (1 oktet = 8 bit)
3. Setiap oktet dapat dikonversikan kedalam biner ke desimal dan sebaliknya.

Contoh alamat IP adalah 192.168.15.1 maka alamat tersebut dipecah menjadi 4 oktet sebagai berikut:

- ✓ 192
- ✓ 168
- ✓ 15
- ✓ 1

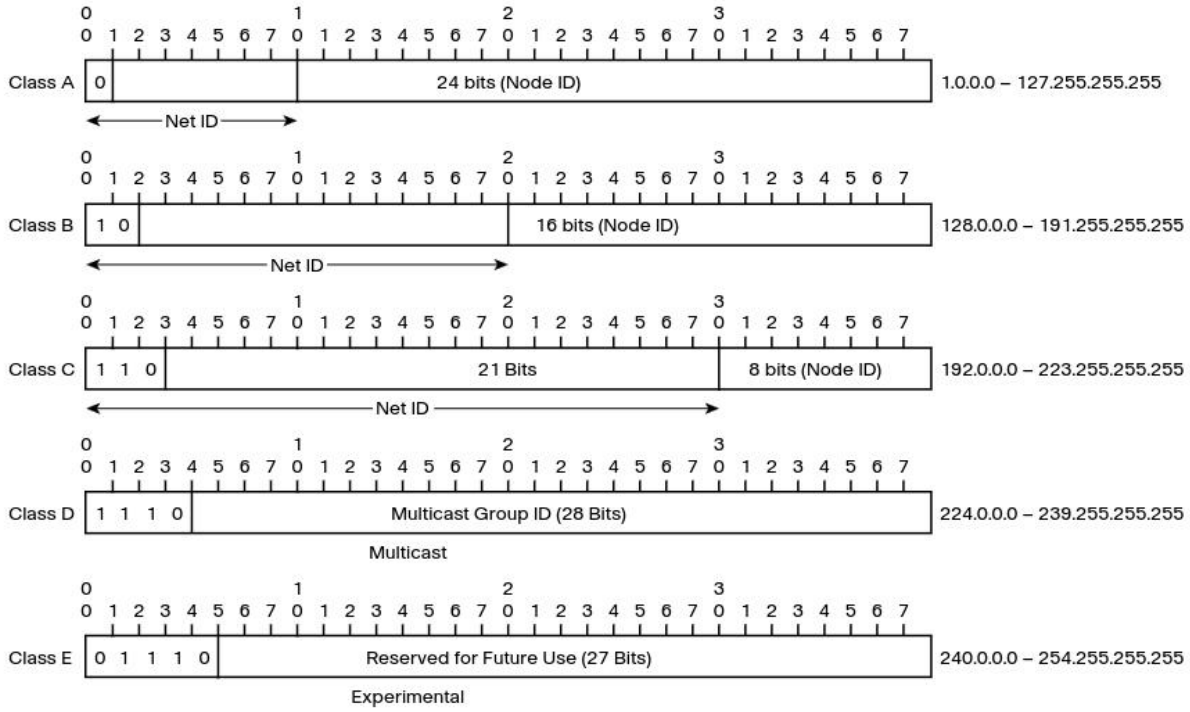
Dimana nilai setiap oktet antara 0 sampai 255, atau dalam notasi biner 00000000 - 11111111. Untuk alamat 192.168.15.1 jika direpresentasikan dalam notasi biner 32 bit menjadi 11000000.10101000.00001111.00000001.

Kelas alamat IP

Alamat IP dibagi menjadi beberapa kelas yaitu kelas A, B, C, D (multicast) dan kelas E (khusus). Pembagian kelas ini didefinisikan berdasarkan jumlah bit yang digunakan untuk porsi network dari sebuah alamat dan sisanya adalah menentukan jumlah host.

- ✓ Untuk alamat kelas A, oktet pertama sebagai porsi network dan 3 oktet terakhir sebagai porsi host.
- ✓ Untuk alamat kelas B, oktet pertama dan kedua sebagai porsi network dan 2 oktet terakhir sebagai porsi host.
- ✓ Untuk alamat kelas C, 3 (tiga) oktet pertama sebagai porsi network dan 1 oktet terakhir sebagai porsi host.

Semakin besar porsi host maka semakin semakin kecil porsi host, sebaliknya semakin sedikit porsi network maka akan semakin banyak porsi hostnya. Porsi network menggambarkan seberapa banyak jaringan atau subnet yang dapat terbentuk. Sedangkan porsi host menggambarkan seberapa banyak jumlah host dalam sebuah jaringan atau subnet. Gambar berikut ini menunjukkan kelas alamat IP.



Gambar 4.1. Pembagian kelas alamat IP

Kelas A:

- ✓ Range: 1.0.0.0 hingga 126.255.255.255
- ✓ Subnet Mask Default: 255.0.0.0
- ✓ Jumlah Host per Jaringan: 16,777,214

Kelas B:

- ✓ Range: 128.0.0.0 hingga 191.255.255.255
- ✓ Subnet Mask Default: 255.255.0.0
- ✓ Jumlah Host per Jaringan: 65,534

Kelas C:

- ✓ Range: 192.0.0.0 hingga 223.255.255.255
- ✓ Subnet Mask Default: 255.255.255.0
- ✓ Jumlah Host per Jaringan: 254

Kelas D:

- ✓ Range: 224.0.0.0 hingga 239.255.255.255
- ✓ Digunakan untuk multicast (transmisi ke sekelompok penerima).

Kelas E:

- ✓ Range: 240.0.0.0 hingga 255.255.255.255
- ✓ Digunakan untuk keperluan eksperimen dan pengembangan, dan tidak dapat diakses secara umum di internet.

IP Privat dan IP Publik

Alamat IP privat adalah alamat IP yang digunakan dalam jaringan lokal atau lingkup pribadi. Alamat ini tidak dapat diakses secara langsung dari jaringan internet. Alamat IP privat biasanya digunakan dalam jaringan rumah, perusahaan, atau organisasi untuk mengidentifikasi dan berkomunikasi antar perangkat dalam jaringan tersebut. Sebuah badan yang berfungsi sebagai pemberi dan pengelola alamat IP telah menetapkan alamat IPv4 privat yang didefinisikan dalam RFC 1918. Range alamat IP privat dapat digunakan oleh organisasi yang ingin membangun jaringan internal berbasis TCP/IP tanpa menggunakan alamat IP publik. Berikut ini adalah alamat IP privat berdasarkan RFC 1918:

- ✓ 10.0.0.0 - 10.255.255.255 (10.0.0.0/8)
- ✓ 172.16.0.0 - 172.31.255.255 (172.16.0.0/12)
- ✓ 192.168.0.0 - 192.168.255.255 (192.168.0.0/16)

Alamat IP privat diatas tidak dapat dirutekan kedalam jaringan internet namun dapat digunakan oleh organisasi tanpa mengganggu alamat yang digunakan di internet. Selain alamat IP diatas merupakan alamat IP publik. Untuk meneruskan paket dari alamat IP private menuju jaringan internet digunakan alamat IP publik dengan teknologi *network address translation* (NAT). Teknologi NAT memungkinkan alamat IP privat dapat mengakses alamat IP publik diinternet.

Alamat IP publik adalah alamat utama yang menghubungkan perangkat didalam jaringan internet. Perangkat jaringan yang memiliki alamat IP publik akan dapat diakses secara langsung melalui jaringan internet. Biasanya IP publik diperoleh dari internet service provider (ISP) yaitu perusahaan yang menyediakan layanan jaringan internet. ISP memiliki banyak alamat IP publik yang didistribusikan ke pelanggannya.

4.3. Mengelola Pengalamatan IP

Mengelola alamat IP merupakan hal yang harus dikuasai oleh admin jaringan sehingga dapat membantu meningkatkan efisiensi penggunaan alamat IP dan mengoptimalkan kinerja jaringan. Menglola alamat IP umumnya dilakukan untuk memenuhi kebutuhan organisasi yang memeiliki beberapa departemen atau lokasi yang memerlukan jaringan yang terpisah. Untuk mengelola alamat IP dapat menggunakan teknik subnetting klasik dan *variabel length subnetting masking* (VLSM). Berikut ini adalah langkah-langkah umum yang dilakukan dalam mengelola alamat IP dengan teknik subnetting:

1. Perlu memahami teknik subnetting
2. Menentukan jumlah subnet yang dibutuhkan
3. Menentukan jumlah host per subnet
4. Menentukan subnet mask

5. Menghitung jumlah alamat IP per subnet
6. Memberikan alama IP yang dapat digunakan untuk host
7. Melakukan dokumentasi alamat IP
8. Implementasi alamat IP dalam jaringan
9. Monitoring dan melakukan pemeliharaan.

Subnetting Klasik

Subnetting merupakan teknik yang digunakan untuk membagi jaringan kedalam sub jaringan yang lebih kecil. Dengan subnetting memungkinkan kita untuk membuat multiple jaringan logikal dari satu kelas A, B, atau C. Jika tidak ada subnet, kita hanya dapat mengunakan satu jaringan dari kelas yang tersedia, A,B, atau C. Dalam sebuah jaringan harus memiliki alamat jaringan yang unik. Untuk membuat subnet dalam sebuah jaringan, kita dapat menggunakan beberapa bit pada porsi host yang nantinya akan menambah subnet ID. Misalnya jaringan kelas C dengan alamat 192.168.1.0/24, jaringan ini memiliki subnet mask 255.255.255.0, maka kita dapat membuat subnet seperti berikut ini.

Dalam hal ini kita memiliki 254 alamat IP yang dapat digunakan untuk perangkat dalam subnet (2^8 - 2 = 256 - 2 = 254). Misalnya kita akan membuat 4 subnet maka kita perlu memodifikasi subnet mask yang ada agar dapat menampung jumlah subnet yang diinginkan. Jika kita ingin membuat 4 subnet, maka kita perlu menambahkan 2 bit pada porsi network dengan meminjam 2 bit pada porsi host. Mengapa menambahkan 2 bit karen 2^2 = 4, 4 subnet yang akan dibuat.

```
192.168.1.0          - 11000000.10101000.00000001.00000000
255.255.255.192      - 11111111.11111111.11111111.11000000
-------------------------------------------------------------------------------[sub]------
```

Dengan subnet baru, kita memiliki 4 subnet dengan masing-masing subnet terdiri atas 62 alamat IP yang bisa digunakan (2^6 = 64). Angka 6 adalah sisa porsi host yang tersedia atau jumlah angka 0 pada subnet. Subnet yang terbentuk adalah:

1. Subnet 1 : 192.168.1.0 - 192.168.1.63
2. Subnet 2 : 192.168.1.64 - 192.168.1.127
3. Subnet 3 : 192.168.1.128 - 192.168.1.191
4. Subnet 4 : 192.168.1.192 - 192.168.1.255

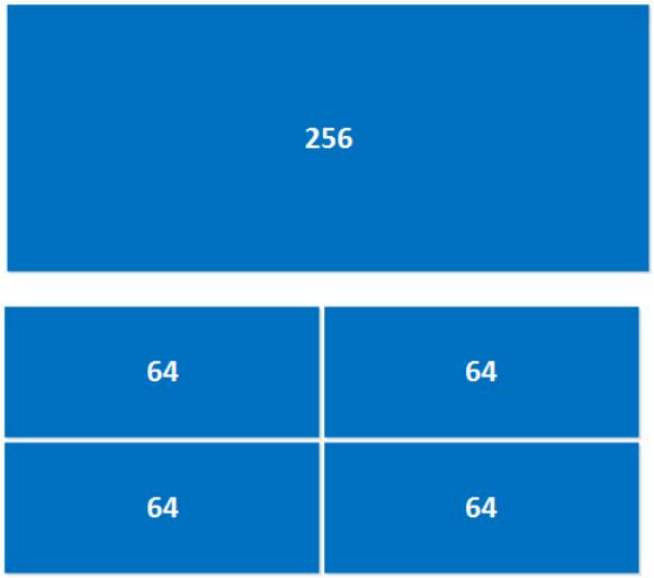
Untuk membuat subnet yang lebih fleksibel sesuai dengan jumlah perangkat yang ada didalam jaringan, maka kita dapat menggunakan teknik yang disebut dengan *variable length subnet masking* (VLSM) dan menggunakan classless inter-domain routing (CIDR).

***Variable Length Subnet Masking* (VLSM)**

VLSM (Variable Length Subnet Masking) adalah teknik subnetting yang memungkinkan penggunaan subnet mask dengan panjang yang bervariasi untuk mengoptimalkan penggunaan alamat IP. Dalam VLSM, subnetting tidak dibatasi oleh batasan kelas (Class A, B, atau C), dan subnet mask dapat disesuaikan untuk setiap subnet sesuai dengan kebutuhan spesifiknya. Hal ini memungkinkan penggunaan alamat IP dengan lebih efisien dan fleksibel. Sebagai contoh, musalkan kita memiliki blok alamat IP 192.168.1.0/24 (kelas C) dan kita ingin membuat beberapa subnet sesuai dengan kebutuhan dimana jumlah host yang ada pada tiap subnet yang kita miliki berbeda-beda sebagai berikut:

1. Satu subnet memiliki 12 host.
2. Satu subnet memiliki 44 host.
3. Satu subnet memiliki 2 host.
4. Satu subnet memiliki 24 host.

Jika menggunakan subnetting klasik, maka kita akan peroleh gambaran subnet dari 256 alamat dibagi menjadi 4 sama rata seperti gambar berikut ini.



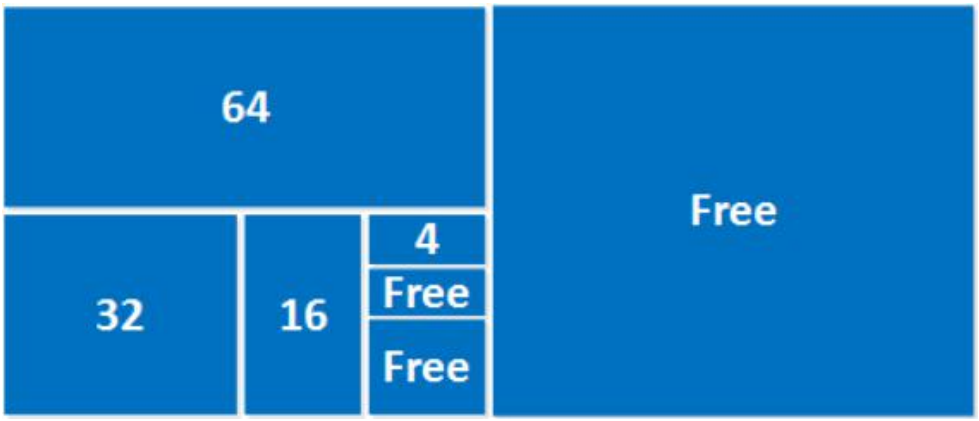
Gambar 4.2. Contoh subnetting klasik

Namun dapat tilihat bahwa jika kita membagi seperti gambar diatas, maka akan banyak alamat IP yang tidak terpakai dalam 1 subnet. Sebagai contoh untuk subnet yang memiliki 2 host, alamat yang tersedia 64 - 2 = 62, artinya ada 60 alamat yang akan tidak terpakai. Dengan kebutuhan subnet yang berbeda-beda seperti diatas, maka kita membutuhkan:

- ✓ 12 host, untuk subnet terkecil yang dapat digunakan adalah subnet dengan jumlah blok 16
- ✓ 44 host, untuk subnet terkecil yang dapat digunakan adalah subnet dengan jumlah blok 64

- ✓ 2 host, untuk subnet terkecil yang dapat digunakan adalah subnet dengan jumlah blok 4.
- ✓ 24 host, untuk subnet terkecil yang dapat digunakan adalah subnet dengan jumlah blok 32.

Maka 1 subnet dengan 256 alamat yang tersedia dapat dipecah menjadi berikut ini.



Gambar 4.3. Contoh pembagian IP menggunakan VLSM

Untuk menemukan alamat yang dapat digunakan dalam subnet yang tersedia, kita perlu menjawab beberapa pertanyaan berikut.

- ✓ Berapa alamat network dari subnet?
- ✓ Berapa alamat broadcast dari subnet?
- ✓ Berapa subnet mask yang digunakan?
- ✓ Berapa alamat IP yang dapat digunakan untuk tiap host?

Alamat network (network address) adalah alamat pertama dalam sebuah subnet yang terbentuk. Alamat network masing subnet adalah:

1. Subnet 1 (ukuran 64) alamat networknya adalah 192.168.1.0
2. Subnet 2 (ukuran 32) alamat networknya adalah 192.168.1.64
3. Subnet 3 (ukuran 16) alamat networknya adalah 192.168.1.96
4. Subnet 4 (ukuran 4) alamat networknya adalah 192.168.1.112
5. Subnet 5 (sisa alamat yang tersedia) alamat networknya adalah 192.168.1.116

Alamat broadcast (broadcast address) adalah alamat terakhir dalam sebuah subnet yang terbentuk. Alamat broadcast dari masing-masing subnet adalah:

1. Subnet 1 (ukuran 64) alamat networknya 192.168.1.0 dan alamat broadcast 192.168.1.63.
2. Subnet 2 (ukuran 32) alamat networknya 192.168.1.64 dan alamat broadcast 192.168.1.95
3. Subnet 3 (ukuran 16) alamat networknya 192.168.1.96 dan alamat broadcast 192.168.1.111.
4. Subnet 4 (ukuran 4) alamat networknya 192.168.1.112 dan alamat broadcast 192.168.1.115.

Karena setiap subnet memiliki ukuran yang berbeda-beda, maka subnet mask nya pun berbeda-beda untuk setiap subnet. Untuk mencari subnet mask kita dapat menggunakan persamaatn berikut:

```
256 - ukuran subnet = subnet mask.
```

- ✓ Subnet 1 : 256 - 64 = 192, maka subnet masknya adalah 255.255.255.192
- ✓ Subnet 2 : 256 - 32 = 224, maka subnet masknya adalah 255.255.255.224
- ✓ Subnet 3 : 256 - 16 = 240, maka subnet masknya adalah 255.255.255.240
- ✓ Subnet 4 : 256 - 4 = 252, maka subnet masknya adalah 255.255.255.252.

Berikutnya adalah menentukan alamat IP yang dapat digunakan pada host untuk masing-masing subnet.

- ✓ Subnet 1 (ukuran 64)
  - Alamat network 192.168.1.0
  - Alamat host pertama 192.168.1.1
  - Alamat host terakhir 192.168.1.62
  - Alamat broadcast 192.168.1.162
- ✓ Subnet 2 (ukuran 32)
  - Alamat network 192.168.1.64
  - Alamat host pertama 192.168.1.65
  - Alamat host terakhir 192.168.1.94
  - Alamat broadcast 192.168.1.95
- ✓ Subnet 3 (ukuran 16)
  - Alamat network 192.168.1.96
  - Alamat host pertama 192.168.1.97
  - Alamat host terakhir 192.168.1.110
  - Alamat broadcast 192.168.1.111
- ✓ Subnet 4 (ukuran 4)
  - Alamat network 192.168.1.112
  - Alamat host pertama 192.168.1.113
  - Alamat host terakhir 192.168.1.114
  - Alamat broadcast 192.168.1.115

4.4. Rangkuman

1. IP Address atau alamat IP adalah identifikasi numerik yang diberikan kepada setiap perangkat yang terhubung ke jaringan komputer, memungkinkan perangkat untuk saling berkomunikasi. IP address berfungsi untuk mengidentifikasi perangkat dalam jaringan dan mengarahkan data ke tujuan yang tepat.

2. Terdapat dua versi alamat IP, yaitu IPv4 (32-bit) dan IPv6 (128-bit). IPv4 ditulis dalam format desimal bertitik (contoh: 192.168.1.1), sedangkan IPv6 ditulis dalam format heksadesimal.
3. Alamat IPv4, memiliki panjang 32 bit, dibagi menjadi dua bagian: network dan host, serta dinyatakan dalam format dot desimal yang terdiri dari empat oktet. Pengalamatan ini terbagi menjadi beberapa kelas (A, B, C, D, dan E) berdasarkan ukuran jaringan dan jumlah host yang dapat diakomodasi, dengan kelas A mendukung jumlah host yang sangat besar dan kelas C lebih cocok untuk jaringan kecil.
4. Teknik subnetting seperti Variable Length Subnet Masking (VLSM) dan Classless Inter-Domain Routing (CIDR) digunakan untuk mengelola pengalamatan IP secara efisien.
5. IPv6 dengan panjang alamat 128 bit mengatasi keterbatasan jumlah alamat di IPv4.
6. Pengelolaan alamat IP yang baik sangat penting untuk meningkatkan efisiensi, keamanan, dan kinerja jaringan, serta memungkinkan administrator untuk merancang jaringan yang scalable dan sesuai dengan kebutuhan organisasi.
7. Subnetting: Proses membagi jaringan besar menjadi subnet yang lebih kecil untuk efisiensi dan pengelolaan yang lebih baik. Subnetting membantu mengurangi kemacetan dan meningkatkan keamanan.
8. CIDR (Classless Inter-Domain Routing): Metode pengalamatan yang memungkinkan penggunaan alamat IP tanpa batasan kelas, menggunakan notasi slash (contoh: 192.168.1.0/24) untuk menunjukkan jumlah bit yang digunakan untuk subnet mask.
9. DHCP (Dynamic Host Configuration Protocol): Protokol yang secara otomatis memberikan alamat IP kepada perangkat yang terhubung ke jaringan, mengurangi kebutuhan konfigurasi manual.
10. Alamat IP Publik: Alamat yang dapat diakses dari internet, digunakan untuk mengidentifikasi perangkat di jaringan global.
11. Alamat IP Privat: Alamat yang digunakan dalam jaringan lokal dan tidak dapat diakses langsung dari internet. Contoh: 192.168.x.x, 10.x.x.x, dan 172.16.x.x hingga 172.31.x.x.
12. Alamat IP Statis dan Dinamis: Alamat statis ditetapkan secara permanen untuk perangkat, sedangkan alamat dinamis diberikan oleh DHCP dan dapat berubah seiring waktu.

4.5. Latihan Soal

1. Apa yang dimaksud dengan pengalamatan IP?
a) Sistem penomoran untuk perangkat dalam jaringan
b) Proses pengiriman data antar jaringan
c) Metode enkripsi data
d) Protokol komunikasi antar perangkat
e) Sistem pengelolaan bandwidth

2. Alamat IPv4 terdiri dari berapa bit?
a) 16 bit

b) 24 bit
c) 32 bit
d) 64 bit
e) 128 bit

3. Dalam format dot-decimal, berapa banyak oktet yang terdapat dalam alamat IP?
a) 2
b) 3
c) 4
d) 5
e) 6

4. Kelas alamat IP yang memiliki jumlah host terbanyak per jaringan adalah:
a) Kelas A
b) Kelas B
c) Kelas C
d) Kelas D
e) Kelas E

5. Apa fungsi dari subnet mask dalam pengalamatan IP?
a) Mengidentifikasi alamat perangkat
b) Menentukan bagian network dan host dari alamat IP
c) Mengatur kecepatan transfer data
d) Mengamankan data yang dikirim
e) Mengelola koneksi internet

6. Alamat IP yang digunakan untuk multicast adalah:
a) Kelas A
b) Kelas B
c) Kelas C
d) Kelas D
e) Kelas E

7. Apa yang dimaksud dengan subnetting?
a) Menghubungkan beberapa jaringan
b) Membagi jaringan menjadi sub-jaringan yang lebih kecil
c) Mengubah alamat IP menjadi format yang lebih sederhana
d) Mengatur kecepatan transfer data
e) Mengamankan data yang dikirim

8. Alamat IP 192.168.1.1 termasuk dalam kelas:
a) Kelas A
b) Kelas B
c) Kelas C
d) Kelas D
e) Kelas E

9. Apa yang dimaksud dengan VLSM (Variable Length Subnet Mask)?
a) Teknik untuk mengubah alamat IP
b) Metode untuk membagi jaringan dengan subnet mask yang berbeda
c) Protokol untuk mengelola alamat IP
d) Sistem untuk mengamankan data
e) Teknik untuk meningkatkan kecepatan transfer data

10. Apa yang menjadi tujuan utama dari pengelolaan pengalamatan IP dalam sebuah organisasi?
a) Mengurangi biaya operasional
b) Meningkatkan efisiensi penggunaan alamat IP dan kinerja jaringan
c) Mengurangi jumlah perangkat yang digunakan
d) Meningkatkan kompleksitas sistem
e) Meningkatkan keamanan data

Soal Esai

11. Jelaskan konsep dasar pengalamatan IP dan peran pentingnya dalam jaringan komputer.
12. Uraikan perbedaan antara alamat IP kelas A, B, dan C, serta berikan contoh penggunaan masing-masing kelas.
13. Diskusikan proses subnetting dan bagaimana teknik ini dapat meningkatkan efisiensi penggunaan alamat IP dalam jaringan.
14. Jelaskan apa itu subnet mask dan bagaimana cara kerjanya dalam membedakan bagian network dan host dari alamat IP.
15. Deskripsikan teknik VLSM (Variable Length Subnet Mask) dan bagaimana teknik ini dapat digunakan untuk mengoptimalkan pengalamatan IP dalam organisasi

4.6. Daftar Pustaka

Santoso, H. (2022). *Jaringan Komputer: Teori dan Praktik Routing serta Switching*. Jakarta: Erlangga.

Tukino. (2020). *Network Design and Management CISCO CCNA Routing and Switching (Network Simulation with Packet Tracer)*. Batam: Batam Publisher.

BAB 5

KONSEP ROUTING

5.1. Definisi

Protokol routing adalah protokol yang termasuk dalam routing dinamis *(dynamic routing)*. Protokol routing bertanggung jawab untuk menentukan jalur terbaik untuk data dan memperbarui informasi tabel routing ketika terjadi perubahan jaringan. Ada berbagai protokol routing yang bisa kita gunakan untuk melakukan routing dinamis. Setiap protokol memiliki kelebihan dan kekurangannya masing-masing. Beberapa protokol routing juga menggunakan algoritma yang tugasnya melakukan perhitungan untuk menentukan jalur terbaik *(Best Path)*. Oleh karena itu, protokol routing dinamis dibagi menjadi dua bagian, yaitu *Interior Gateway Protocol (IGP)* dan *Exterior Gateway Protocol (EGP)*.

Routing IP adalah Proses pemindahan paket dari satu network ke network lain dengan menggunakan router-router. Pada dasarnya sebuah routing protocol menentukan jalur (path) yang dilalui oleh sebuah paket melalui sebuah internetwork. Contoh dari routing protocol adalah.

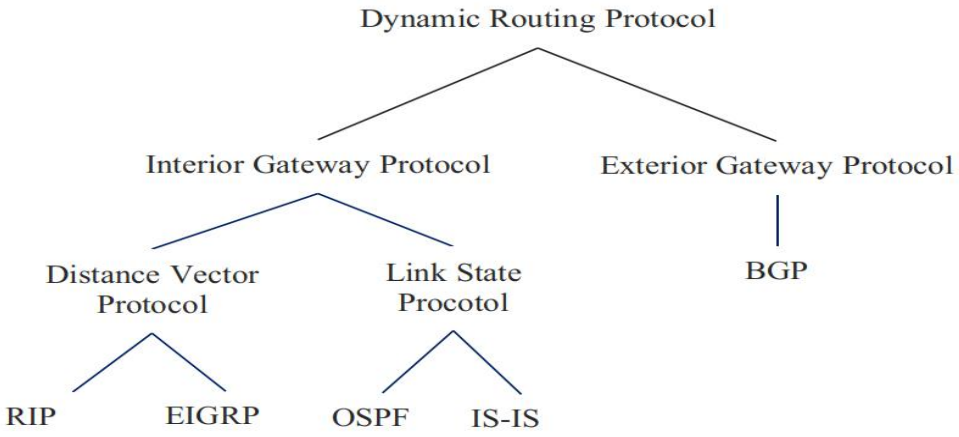
1. RIP (Routing Internet Protocol)
2. IGRP (Interior Gateway Routing Protocol)
3. EIGRP (Enhanced Gateway Routing Protocol)
4. OSPF (Open Short Path Firts)

Istilah routing digunakan untuk proses pengambilan sebuah paket dari sebuah alat dan mengirimkannya melalui network ke perangkat lain di sebuah network yang berbeda. Apabila dalam sebuah network tidak memiliki router, maka tidak akan dapat melakukan routing. Routing melakukan pengiriman paket ke lalu lintas data ke semua network di internetwork anda. Agar kita dapat melakukan routing paket, sebuah router harus mengetahui, hal-hal sebagai berikut :

- ✓ Alamat tujuan (Destination Address)
- ✓ Router-router yang bersebelahan (neighbor router)
- ✓ Route terbaik untuk setiap network remote.

5.2. Klasifikasi Routing Protocol

Ada berbagai protokol routing yang bisa kita gunakan untuk melakukan routing dinamis. Setiap protokol memiliki kelebihan dan kekurangannya masing-masing. Sebelum membahas masing-masing routing protocol, terlebih dahulu harus mengetahui tentang klasifikasi dari routing protocol.



Gambar 5.0. Klasifikasi Routing Protocol

Berdasarkan gambar klasifikasi routing protocol diatas, bahwa dynamic routing protocol itu terbagi menjadi 2, yakni Interior Gateway Protocol (IGP) dan Exterior Gateway Protocol (EGP). penjelasan jenis jenis routing adalah sebagai berikut.

5.2.1. Interior Gateway Protocol (IGP)

IGP adalah protokol perutean yang digunakan oleh jaringan dalam AS yang sama (sistem otonom). Sistem otonom itu sendiri adalah kumpulan jaringan yang dikelola dan dikendalikan oleh satu otoritas administratif yang menggunakan kebijakan perutean internal yang sama. Contoh sistem otonom dapat ditemukan di jaringan ISP, jaringan kampus, dan jaringan tempat kerja dengan banyak cabang. Sedangkan contoh IGP adalah : RIP, EIGRP, OSPF, dan IS-IS. IGP masih dibagi menjadi dua kategori, yaitu distance vector dan link state. Jalur perutean dipilih menggunakan protokol perutean yang disebut "vektor jarak" berdasarkan jumlah lompatan antara perute dan tujuan (Hop Count). Contoh protokol routing distance vector adalah : RIP dan EIGRP. Sementara Link state adalah jenis routing protocol yang melakukan pemilihan jalur berdasarkan kondisi link. Contoh link state protocol adalah : OSPF dan IS-IS.

5.2.2. Exterior Gateway Protocol (EGP)

EGP adalah protokol routing yang digunakan untuk menghubungkan jaringan (routing) melintasi sistem otonom, sedangkan IGP digunakan untuk menghubungkan router dalam satu AS. Protokol perutean ini dikenal sebagai exterior gateway protocol karena digunakan untuk perutean di luar AS. Contoh dari EGP adalah BGP (Border Gateway Protocol).

Berikut ini adalah masing-masing routing protocol yang telah dibahas sebelumnya:

a. ***RIP (Routing Information Protocol)***

Protokol perutean vektor jarak disebut RIP. berdasarkan jalur terpendek antara router dan tujuan saat memilih jalur perutean. Jarak antar router disebut sebagai hop, tetapi jarak dari router ke tujuan disebut sebagai hop count. Ada dua variasi RIP. RIPv1 telah diperbaiki dengan RIPv2. Jika VLSM tidak didukung oleh RIP versi 1, RIP versi 2 dapat mendukung VLSM. Meskipun RIP versi satu dapat memperoleh pembaruan perutean dari RIPv1 dan RIPv2, RIPv2 hanya dapat menerima pembaruan dari RIPv2 lainnya.

RIP biasa digunakan pada jaringan yang berskala kecil hingga sedang karena protokol RIP memiliki keterbatasan hop maksimal 15. RIP versi satu mapun RIPv2 merupakan open standart protocol, artinya dapat digunakan pada perangkat yang berbeda vendor. Jadi apabila jarak antar router ke tujuan melebihi 15 hop maka paket akan dibuang sehingga tidak sampai ke tujuan. Oleh karena itu RIP akan sulit jika digunakan pada jaringan berskala besar.

Kelebihan :
- Mendukung VLSM dan CIDR (RIPv2)
- Mudah dalam konfigurasi
- Tidak kompleks
- Mampu menonaktifkan auto-summary route (RIPv2)
- Mendukung mekanisme autentikasi

Kekurangan :
- Tidak mendukung VLSM dan CIDR (RIPv1)
- Memiliki batas maksimal 15 hop
- Tidak bisa menerima update informasi dari RIP versi satu (RIPv2)
- Proses convergence yang lambat
- Melakukan update informasi secara berkala sehingga membuat trafik menjadi padat

b. ***EIGRP (Enhanced Interior Gateway Routing Protocol)***

EIGRP termasuk dalam distance vector routing protocol, namun EIGRP tidak menggunakan hop count untuk melakukan pemilihan jalur routing. Selain itu EIGRP merupakan Cisco Proprietary, maksudnya adalah, IGRP merupakan routing protocol yang hanya terdapat pada router Cisco. EIGRP menggunakan beberapa parameter yang kemudian dikalkulasi sehingga menghasilkan hasil yang akan digunakan untuk menentukan jalur routing. Adapun parameter-parameter yang digunakan oleh EIGRP antara lain : bandwidth, load, delay, reliability. EIGRP juga menggunakan algoritma DUAL (Diffused Update Algorithm) untuk mengkalkulasi jalur routing yang akan digunakan.

Selain itu, EIGRP juga melakukan kalkulasi untuk menentukan jalur cadangan (backup), jadi apabila jalur utama yang digunakan tiba-tiba down, EIGRP akan otomatis menggunakan jalur backup tadi. Jalur backup pada EIGRP ini disebut Feasible Successor. Untuk keperluan routing, EIGRP mengelola tiga buah tabel, yaitu : tabel routing (routing), tabel neighbor *(neighbor table)*, dan tabel topologi *(topology table)*. Routing table berisi kumpulan entry routing yang digunakan oleh router. Neighbor table berisi informasi router-router yang terkoneksi secara langsung (directly connected) Topology table berisi keseluruhan jalur routing yang terdapat dalam topologi jaringan. EIGRP ini cocok digunakan untuk jaringan berskala kecil hingga menengah.

Kelebihan :
- Mendukung VLSM dan CIDR
- cepat dalam melakukan proses convergence
- jumlah hop count maksimal 224
- Dapat menonaktifkan auto-summary route
- Menjangkau network yang lebih luas dari RIP

Kekurangan :
- hanya dapat digunakan pada Router Cisco
- Melakukan update informasi terus menerus
- Menggunakan lebih banyak resource router

c. OSPF (Open Shortest Path First)

OSPF merupakan *link state routing protocol* dimana pemilihan jalur routingnya melihat kondisi link. OSPF akan memberikan harga (cost) untuk setiap link yang ada. Cost yang memiliki nilai terkecil dijadikan sebagai acuan sebagai jalur routing. OSPF menggunakan algoritma Djikstra untuk menentukan jalur terpendek.

Pada OSPF juga menggunakan konsep area untuk mengurangi penyebaran paket LSA (Link State Advertisment) yang akan digunakan untuk bertukar informasi routing update. Pada OSPF memiliki sebuah area yang harus ada dalam setiap konfigurasi OSPF, yakni area 0 atau disebut area backbone. Selain area backbone, administrator dapat menentukan area sendiri, misalnya area 1, area 15, area 30, namun area-area tersebut harus terhubung ke area 0. Untuk menghubungkan area-area yang kita buat sendiri dengan area backbone perlu terdapat sebuah router yang berperan sebagai ABR (Area Border Router). Router ini menjadi penghubung antara area backbone dengan area lain.

Pada OSPF memiliki Internal Router yang keseluruhan interface/linknya terletak dalam satu area. Backbone Router, adalah router yang salah satu link atau seluruhnya terletak di area

backbone Autonomous System Boundary Router, adalah router yang salah satu interface/linknya mengarah ke jaringan yang menggunakan routing protocol selain OSPF.

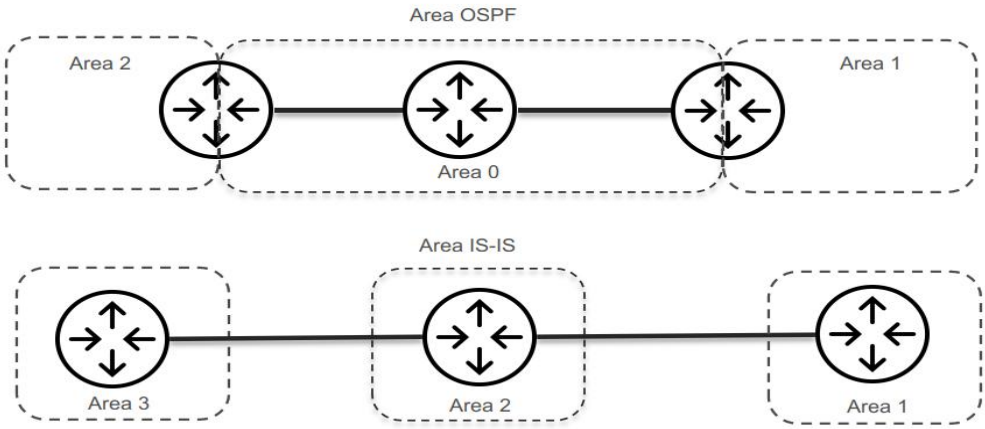
Kelebihan :
- OSPF sering diimplementasikan untuk jaringan skala besar.
- Mendukung penggunaaan VLSM dan CIDR pada pengalamatan
- hop count (unlimited hop count) yang tak terbatas
- OSPF adalah open standard protocol, dapat digunakan pada vendor yang berbeda
- Proses convergence yang cepat
- Mendukung mekanisme autentikasi
- update hanya dilakukan jika terjadi perubahan jaringan

Kekurangan :
- Mengkonsumsi banyak resource
- Membutuhkan perencanaan dan desain yang matang untuk mengimplementasikan OSPF

Konsep jaringan telah dapat menghubungkan beberapa segmen tersebut, tetapi ada beberapa kekurangan yaitu setiap segmen dapat mengakses langsung sehingga dalam segmen tidak memiliki batasan dan dalam prosesnya sangat lambat. Tugas anda sebagai administrator jaringan adalah memperbaiki jaringan tersebut dengan membaginya menjadi beberapa segmen. Sebelum anda beraksi untuk memperbaiki jaringan tersebut. Ada beberapa pet untuk yang akan membantu kita dalam proses perubahan sistem jaringan. Petunjuk tersebut adalah gambar skema jaringan yang lama. Seperti dibawah ini.

d. IS-IS (Intermediate System - Intermediate System)

IS-IS merupakan link state routing protocol yang termasuk dalam kategori IGP (Interior Gateway Protocol). IS-IS menggunakan algoritma Dijkstra seperti OSPF untuk menentukan jalur routing. Pada IS-IS juga terdapat konsep area seperti OSPF. Jika pada OSPF, antar area dipisahkan oleh interface yang berbeda area, maka pada IS-IS, antar area dipisahkan oleh link yang menghubungkan router pada area satu dengan router pada area lain. Dengan kata lain, satu router hanya akan memiliki satu area, namun satu area bisa terdapat beberapa router.



Gambar 5.1. Perbedaan Area OSPF dan IS-IS

Pada IS-IS terdapat istilah level, dimana terdapat level 1, level 2, dan level 12 (level satu dan dua). Level 1 adalah intra-area router yang hanya mengetahui jalur routing dalam satu area. Level 2 merupakan backbone router, mengetahui seluruh jalur routing baik intra-area maupun inter area. Level 12, yakni router yang menerapkan kebijakan baik level 1 maupun level 2. Router dengan level 1-2 akan memiliki dua database, satu untuk level 1, satu lagi untuk yang level 2.

Kelebihan :

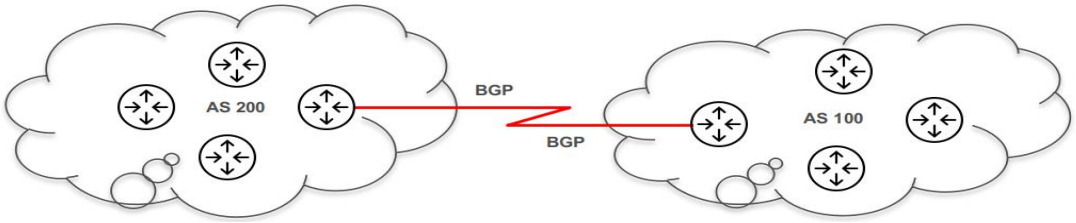
- Memiliki keamanan yang lebih terhadap informasi routing update
- Mendukung VLSM dan CIDR
- Proses convergence yang cepat
- Scalable
- Hanya melakukan update ketika terjadi perubahan jaringan

Kekurangan :

- Konfigurasi lebih rumit

e. ***BGP (Border gateway Protocol***

Fungsi routing protocol BGP adalah sebagai exterior gateway protocol. BGP dapat menghubungkan router-router yang berbeda AS. BGP terletak di bagian terluar dari suatu AS. Protocol BGP termasuk dalam kategori advanced distance vector, tetapi dalam pemilihan jalur, BGP tidak hanya menggunakan acuan jarak, namun juga menggunakan parameter dan atribut lain yang lebih kompleks. BGP juga disebut sebagai path vector routing protocol karena BGP tidak hanya menentukan jalur terbaik (best path) tapi juga membentuk mekanisme routing yang bebas dari routing loop. Pada implementasinya, BGP banyak digunakan untuk koneksi antar ISP.



Gambar 5.2. BGP (Border Gateway Protocol)

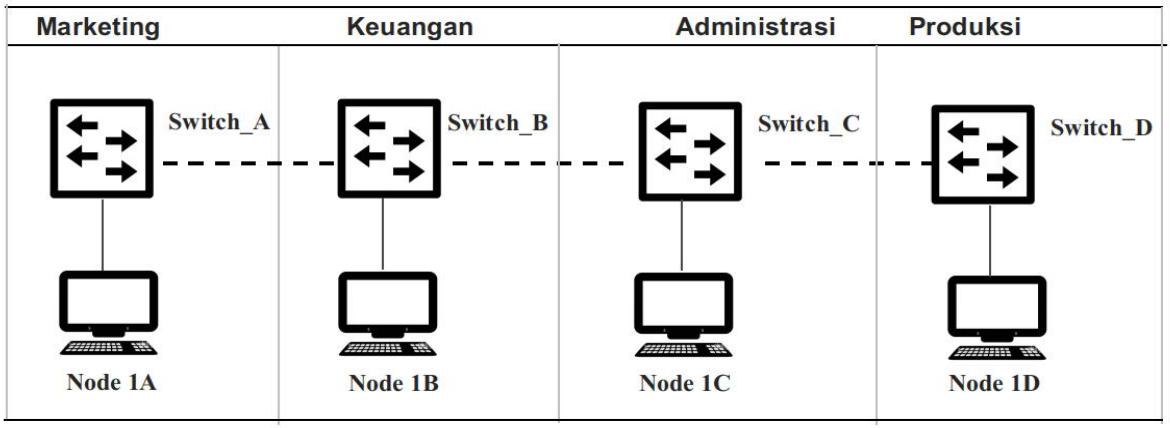
Kelebihan :
- Lebih powerfull dari routing protocol yang lain
- Mendukung VLSM dan CIDR

Kekurangan :
- Konfigurasi yang lebih kompleks

5.3.Implementasi Routing

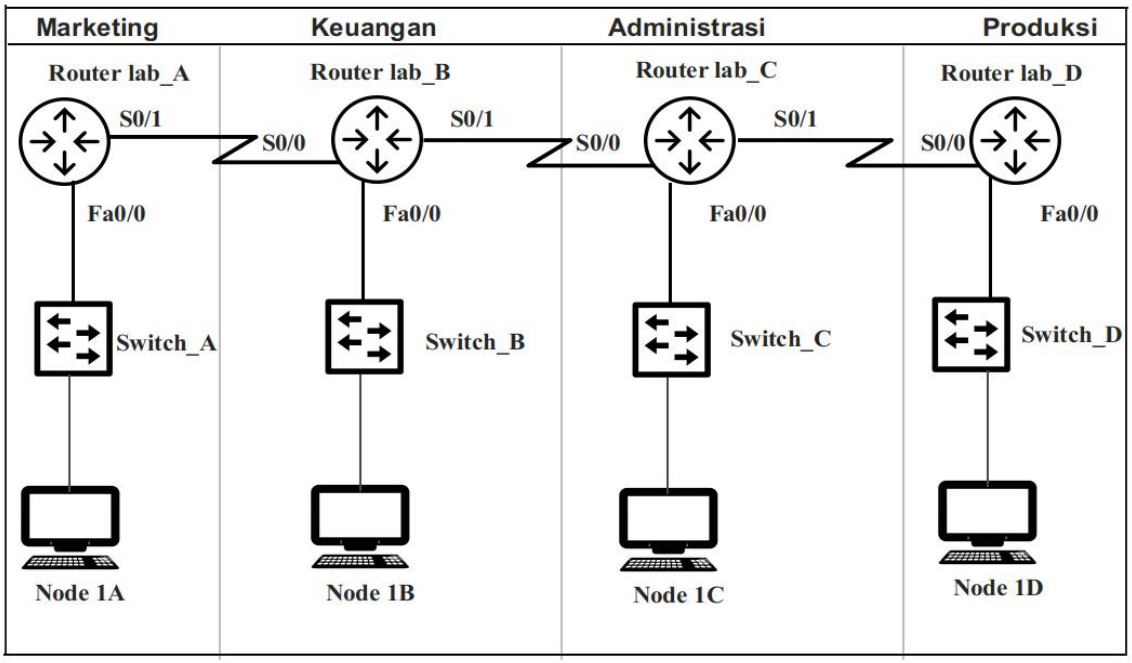
Untuk memahami cara kerja routing protocol kita akan mencoba melakukan konfigurasi router dengan menggunakan routing static, static routing adalah konfigurasi router dengan melakukan konfigurasi tanpa menggunakan protokol routing dinamis, static routing memiliki kelebihan lebih cepat, dikarenakan konfigurasi yang dilakukan telah ditetapkan secara permanen dan tidak akan ada perubahan, tentunya memiliki kelemahan tersendiri, static routing memiliki kelemahan tidak dapat secara otomatis melakukan update tabel routing apabila terjadi perubahan kondisi jaringan, untuk jaringan dalam skala besar yang sering mengalami perubahan jumlah router dan bentuk topologi, maka sangat tidak efisien jika harus dilakukan secara manual.
Contoh implementasi : Salah satu perusahaan di lampung ingin membagi jaringan dalam beberapa segmen, dalam perusahaan tersebut terdapat beberapa bagian :

- ✓ Divisi Marketing
- ✓ Divisi Keuangan
- ✓ Divisi Administrasi
- ✓ Divisi Produksi



Gambar 5.3. Skema Jaringan Lama

Jika kita lihat pada gambar diatas. Peralatan yang digunakan masih menggunakan switch (layer2). Berarti dalam proses pengalamatan jaringan diatas masih menggunakan satu alamat network dari seluruh segmen. Berarti jika kita ingin memisahkan segmen jaringan, kita dapat menggunakan alamat network yang berbeda dari tiap-tiap segmen. Hanya kita membutuhkan peralatan yang dapat menghubungkan alamat yang berbeda. Peralatan yang dibutuhkan adalah router. Dengan router segmen yang berbeda alamat dapat berkomunikasi dengan adanya proses routing pada tiap segmen. Jadi anda tinggal menambahkan router pada setiap segmen. Tugas anda yang pertama adalah menyediakan alamat untuk tiap-tiap segmen dengan alamat yang berbeda , dan menambahkan satu buah router pada setiap segmen.



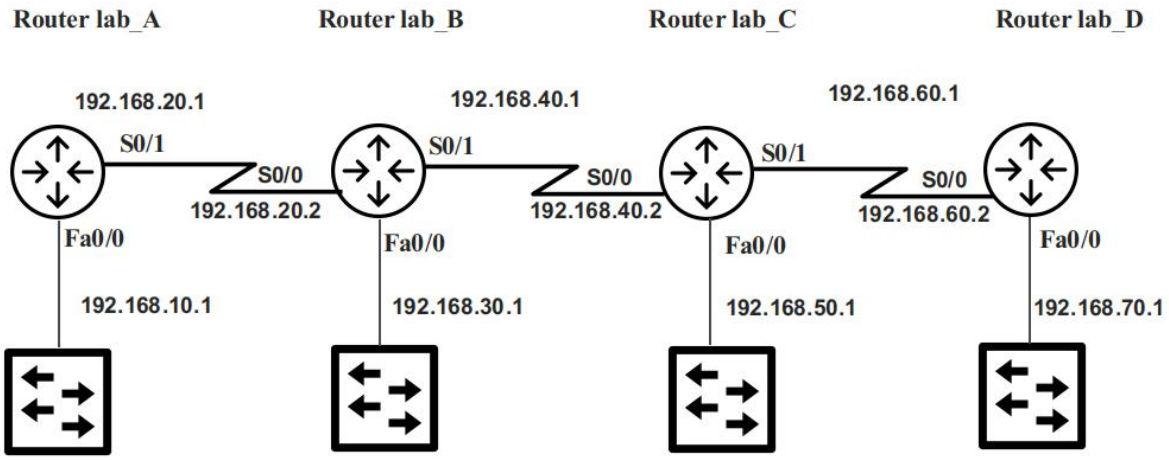
Gambar 5.4. Skema Jaringan Baru

Secara otomatis network network dapat terhubung dengan interface-interface yang terhubung secara langsung, jadi untuk interface yang terhubung secara langsung tidak perlu dilakukan proses routing. Hanya yang perlu kita lakukan adalah mengkonfigurasi interface yang tidak terhubung secara langsung.

Tabel 5.1. Tabel pengalamatan IP

Router	Alamat Network	Interface	IP Address
Lab_A	192.168.10.0	Fa0/0	192.168.10.1
Lab_A	192.168.20.0	S0/1	192.168.20.1
Lab_B	192.168.30.0	Fa0/0	192.168.30.1
Lab_B	192.168.40.0	S0/1	192.168.40.1
Lab_C	192.168.50.0	Fa0/1	192.168.50.1
Lab_C	192.168.60.0	S0/1	192.168.60.1
Lab_D	192.168.70.0	Fa0/1	192.168.70.1

Secara otomatis network network dapat terhubung dengan interface-interface yang terhubung secara langsung, jadi untuk interface yang terhubung secara langsung tidak perlu dilakukan proses routing. Hanya yang perlu kita lakukan adalah mengkonfigurasi interface yang tidak terhubung secara langsung.



Gambar 5.5. Alokasi IP pada Skema Jaringan Baru

a. Routing router lab_A (Divisi Marketing)

Tabel 5.2. Tabel pengalamatan IP bagian marketing

Router	Alamat	Interface	IP Address
Lab_A	192.168.10.	Fa0/0	192.168.10.1
Lab_A	192.168.20.	S0/1	192.168.20.1

Router Alamat Network Interface IP Address
Lab_A 192.168.10.0 Fa0/0 192.168.10.1
Lab_A 192.168.20.0 S0/1 192.168.20.1

untuk router lab_A memiliki 2 interface yang digunakan yaitu

1. Fa0/0 yang terhubung LAN dengan alamat network 192.168.10.0
2. Interface S0/1 yang terhubung langsung dengan interface S0/0 pada router lab_B dengan alamat network 192.168.20.0.

berarti kita harus melakukan routing yang tidak terhubung secara langsung yaitu :

Tabel 5.3. Tabel routing bagian marketing

NO	DESTINATION	SUBNET MASK	HOP ADDRESS
1	192.168.30.0	255.255.255.0	192.168.20.2
2	192.168.40.0	255.255.255.0	192.168.20.2
3	192.168.50.0	255.255.255.0	192.168.20.2
4	192.168.60.0	255.255.255.0	192.168.20.2
5	192.168.70.0	255.255.255.0	192.168.20.2

b. Routing router lab_B (Divisi Keuangan)

Tabel 5.4. Tabel pengalamatan IP bagian keuangan

Router	Alamat	Interface	IP Address
Lab_B	192.168.30.	Fa0/0	192.168.30.1
Lab_B	192.168.30.	S0/0	192.168.20.2
Lab_B	192.168.40.	S0/1	192.168.40.1

untuk router lab_B memiliki 3 interface yang digunakan yaitu

1. fa0/0 yang terhubung LAN dengan alamat network 192.168.30.0 dan
2. interface S0/0 yang terhubung langsung dengan interface S0/1 pada router lab_A dengan alamat network 192.168.20.0.
3. interface S0/1 yang terhubung langsung dengan interface S0/0 pada router lab_C dengan alamat network 192.168.40.0

berarti kita harus melakukan routing yang tidak terhubung secara langsung yaitu :

Tabel 5.5. Tabel routing bagian keuangan

NO	DESTINATION	SUBNET MASK	HOP ADDRESS
1	192.168.10.0	255.255.255.0	192.168.20.1
2	192.168.50.0	255.255.255.0	192.168.40.2
3	192.168.60.0	255.255.255.0	192.168.40.2
4	192.168.70.0	255.255.255.0	192.168.40.2

c. Routing router lab_C (Divisi Administrasi)

Tabel 5.6. Tabel pengalamatan IP bagian administrasi

Router	Alamat	Interface	IP Address
Lab_C	192.168.40.0	S0/0	192.168.40.2
Lab_C	192.168.50.0	Fa0/0	192.168.50.1
Lab_C	192.168.60.0	S0/1	192.168.60.1

untuk router lab_C memiliki 3 interface yang digunakan yaitu

1. interface S0/0 yang terhubung langsung dengan interface S0/1 pada router lab_B dengan alamat network 192.168.40.0 dan
2. interface F0/0 terhubung langsung dengan LAN dengan alamat network 192.168.50.0.
3. interface S0/1 yang terhubung langsung dengan interface S0/0 pada router lab_D dengan alamat network 192.168.60.0

berarti kita harus melakukan routing yang tidak terhubung secara langsung yaitu :

Tabel 5.7. Tabel routing bagian administrasi

NO	DESTINATION	SUBNET MASK	HOP ADDRESS
1	192.168.70.0	255.255.255.0	192.168.60.2
2	192.168.10.0	255.255.255.0	192.168.40.1
3	192.168.20.0	255.255.255.0	192.168.40.1
4	192.168.30.0	255.255.255.0	192.168.40.1

d. Routing router lab_D (Divisi Produksi)

Tabel 5.8. Tabel pengalamatan IP bagian produksi

Router	Alamat	Interface	IP Address
Lab_C	192.168.60.	S0/0	192.168.60.2
Lab_C	192.168.70.	Fa0/0	192.168.70.1

untuk router lab_D memiliki 2 interface yang digunakan yaitu

1. interface S0/0 yang terhubung langsung dengan interface S0/1 pada router lab_B dengan alamat network 192.168.40.0 dan
2. interface F0/0 terhubung langsung dengan LAN dengan alamat network 192.168.50.0.

3. interface S0/1 yang terhubung langsung dengan interface S0/0 pada router lab_D dengan alamat network 192.168.60.0

berarti kita harus melakukan routing yang tidak terhubung secara langsung yaitu :

Tabel 5.9. Tabel routing bagian produksi

NO	DESTINATIO	SUBNET MASK	HOP ADDRESS
2	192.168.10.	255.255.255.0	192.168.20.1
3	192.168.20.	255.255.255.0	192.168.20.1
4	192.168.30.	255.255.255.0	192.168.20.1
5	192.168.40.	255.255.255.0	192.168.20.1
5	192.168.50.	255.255.255.0	192.168.20.1

e. Static Routing

- Konfigurasi pada Linux

Contoh konfigurasi untuk router lab_A pada mesin linux

```
Ip route add [gateway] via [hop address]
Ip route add 192.168.30.1/24 via 192.168.20.2
Ip route add 192.168.40.1/24 via 192.168.20.2
Ip route add 192.168.50.1/24 via 192.168.20.2
Ip route add 192.168.60.1/24 via 192.168.20.2
Ip route add 192.168.70.1/24 via 192.168.20.2
```

- Konfigurasi pada Cisco Router

Contoh konfigurasi untuk router lab_A pada Router Cisco Iproute [destintion network] [subnet mask] [next-hop address]

```
Ip route 192.168.30.0 255.255.255.0 192.168.20.2
Ip route 192.168.40.0 255.255.255.0 192.168.20.2
Ip route 192.168.50.0 255.255.255.0 192.168.20.2
Ip route 192.168.60.0 255.255.255.0 192.168.20.2
```

5.4. Rangkuman

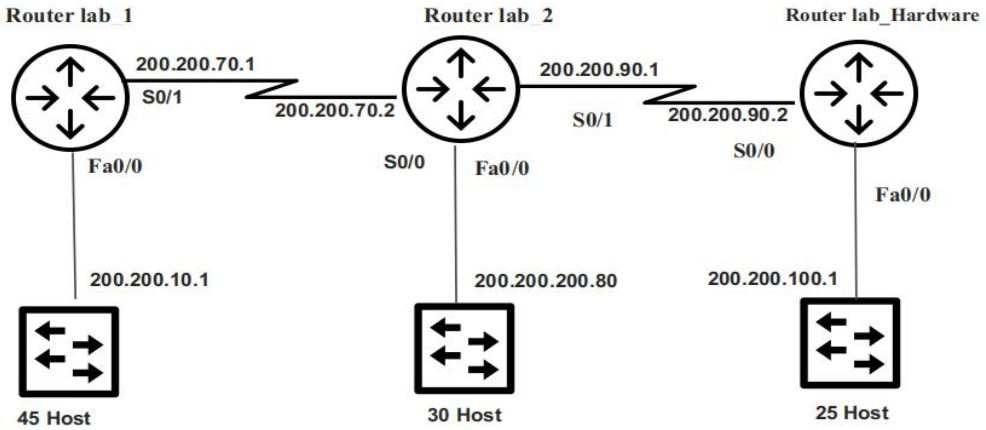
1. Routing adalah proses pengiriman paket data dari sumber ke tujuan melalui satu atau lebih jaringan. Proses ini melibatkan pemilihan jalur terbaik untuk mencapai tujuan berdasarkan informasi yang tersedia.
2. Routing Protocol: Protokol yang digunakan untuk menentukan jalur yang akan diambil paket data dalam jaringan. Terdapat dua kategori utama: Static Routing: Jalur yang ditentukan secara manual oleh administrator jaringan. Cocok untuk jaringan kecil dan stabil. Dynamic Routing: Jalur yang ditentukan secara otomatis oleh router menggunakan

algoritma dan informasi dari protokol routing. Memungkinkan penyesuaian otomatis terhadap perubahan dalam jaringan.

3. Router: Perangkat yang bertanggung jawab untuk melakukan routing. Router menggunakan tabel routing untuk menentukan jalur terbaik untuk mengirimkan paket data.
4. Tabel Routing: Struktur data yang menyimpan informasi tentang jalur yang tersedia dan metrik yang terkait, seperti biaya atau jarak. Tabel ini diperbarui secara dinamis dalam routing dinamis
5. RIP (Routing Information Protocol): Protokol routing berbasis jarak yang menggunakan hop count sebagai metrik.
6. OSPF (Open Shortest Path First): Protokol routing berbasis link-state yang menggunakan algoritma Dijkstra untuk menentukan jalur terpendek.
7. EIGRP (Enhanced Interior Gateway Routing Protocol): Protokol routing hybrid yang menggabungkan fitur dari RIP dan OSPF.
8. Pentingnya Routing adalah Efisiensi Jaringan: Routing yang efektif memastikan pengiriman data yang cepat dan efisien, mengurangi kemacetan dan meningkatkan kinerja jaringan. Keandalan: Protokol routing yang baik dapat menyesuaikan jalur secara otomatis jika terjadi kegagalan pada jalur utama, meningkatkan keandalan komunikasi data. Skalabilitas: Routing dinamis memungkinkan jaringan untuk tumbuh dan beradaptasi dengan perubahan tanpa memerlukan konfigurasi manual yang ekstensif.

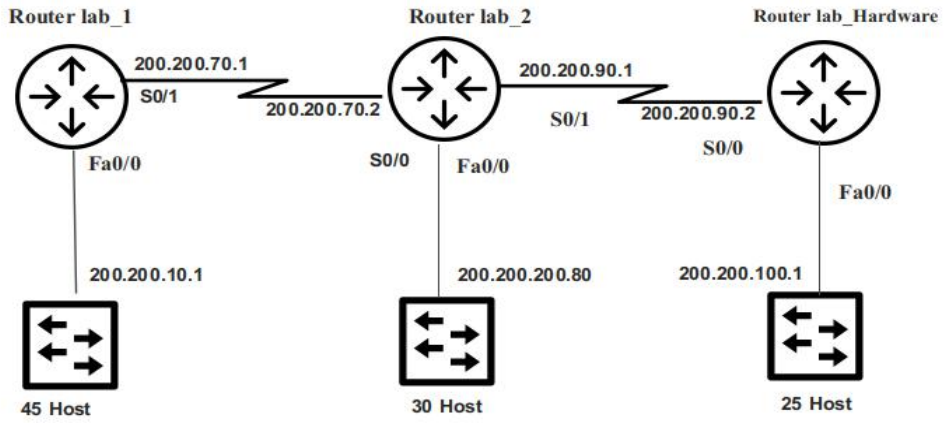
5.5.Latihan Soal

Anda seorang administrator ditugaskan untuk mengkonfigurasi router yang ada pada perusahaan seperti pada gambar 7. Tugas anda adalah menentukan routing dari tiap-tiap router. Tuliskan proses routing dengan menggunakan linux atau cisco router.



Gambar 5.6. Skema Latihan Jaringan 1

Latihan 2



Gambar 5.7. Skema Latihan Jaringan 2

Sebagai administrator jaringan konfigurasikan router yang terdapat pada TEKNOKRAT 1 dapat mengakses koneksi internet yang terhubung ke ISP, dan konfigurasikan Router yang terdapat pada TEKNOKRAT 2 agar dapat mengakses koneksi internet dan terhubung pada gedung ICT CENTER. Dan lakukan proses routing pada masing-masing router.

5.6. Daftar Pustaka

Veza, Okta, , dan . (2024). *Jaringan Komputer Lanjutan*. Batam: Cendikia Mulia Mandiri.

Wahyudi, Mochamad, Rachmat Adi Purnama, dan Firmansyah. (2019). *Cisco routing and switching Cisco routing and switching*. Yogyakarta: Graha Ilmu.

Wibowo, Sastya Hendri. (2022). *Jaringan Komputer dan Komunikasi Data.* Jakarta: Deepublish.

Wahyudi, Mochamad, Firmansyah. (2021). *15 Best Practice Skill Cisco Routing and Switching*. Jakarta: Bintang Pustaka Madani.

BAB 6

STATIK ROUTING

6.1.Pendahuluan Statik Routing

Statik routing merupakan routing yang umumnya digunakan dalam sistem jaringan komputer dalam semua skala. Seorang admin jaringan dapat melakukan konfigurasi secara manual untuk menentukan jalur yang harus dilalui untuk menuju ke sebuah node didalam jaringan. Tidak seperti dinamik routing protokol, statik routing tidak otomatis melakukan update dan menemukan jalur terbaik menuju sebuah node didalam jaringan, namun harus dicoonfigurasi secara manual setiap saat ketika ada perubahan topologi jaringan. Statik routing tidak akan berubah hingga admin jaringan melakukan konfigurasi ulang. Mengapa harus menggunakan statik routing? Statik routing memiliki beberapa kelebihan dibandingkan dengan dinamik routing yaitu:

1. Statik routing tidak melakukan update melalui jaringan, hal ini memiliki keamanan yang lebih baik.
2. Statik routing menggunakan bandwidt yang lebih kecil dibandingkan dengan dinamik routing karena tidak ada proses pertukaran informasi routing.
3. Tidak membutuhkan sumberdaya CPU untuk menghitung dan komunikasi route.
4. Jalur dari sebuah statik routing digunakan untuk mengirimkan data yang sudah diketahui.

Selain memiliki kelebihan, statik routing juga memiliki kekurangan yaitu:

1. Konfigurasi awal dan maintenance membutuhkan waktu yang cukup lama seiring dengan bertambah besarnya topologi jaringan.
2. Memungkinkan terjadi kesalahan saat konfigurasi terutama pada jaringan yang memiliki skala yang besar.
3. Sulit untuk beradaptasi terhadap pertumbuhan jaringan yang semakin besar sehingga proses maintenance menjadi lebih sulit.
4. Untuk menggunakan statik routing membutuhkan pengetahuan yang lengkap dari seluruh jaringan dan topologi yang ada untuk dapat diimplementasikan dengan baik.

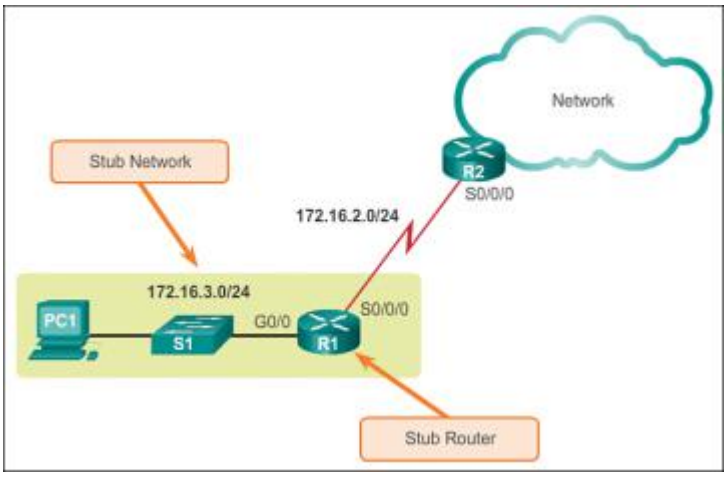
Statik routing sangat baik digunakan dan diimplementasikan dalam jaringan skala kecil yang memiliki hanya satu jalur untuk keluar jaringan. Statik routing juga menyediakan keamanan yang lebih baih dalam sebuah jaringan skala besar untuk trafik tertentu atau link ke jaringan lain yang membutuhkan kontrol yang lebih ketat. Umumnya jaringan skala menengah mengkombinasikan statik routing dan protokol dinamik routing. Statik routing memiliki nilai administrative distance (AD) 1 (satu) sehingga statik route menjadi jalur utama yang akan

dipilih dibandingkan dengan dinamik routing apabila untuk menuju sebuah node memiliki jalur lebih dari satu.

Statik routing baik digunakan pada:

1. Sebuah jaringan skala kecil yang diperkirakan tidak tumbuh secara signifikan.
2. Jaringan stub yaitu jaringan yang hanya dapat diakses melalui sebuah router dan router tersebut hanya memiliki 1 (satu) tetangga.
3. Default routeyaitu sebuah route yang mewakili jalur ke jaringan manapun yang tidak memiliki kecocokan yang lebih spesifik dengan route yang ada dalam tabel routing. Default route digunakan untuk mengirimkan trafik ke tujuan manapun diluar router.

Berikut ini adalah contoh jaringan stub (stub network).



Gambar 6.1. Contoh stub network

Statik route dapat dikonfigurasi untuk IPv4 dan IPv6 dan keduanya support untuk tipe statik route berikut ini:

1. Standard static route yaitu sebuah route yang otomatis terisi dalam routing tabel berdasarkan jaringan yang terhubung langsung dengan router.
2. Default static route yaitu sebuah route yang menentukan kemana paket akan dikirim apabila tidak ditemukan route spesifik untuk jaringan tujuan yang tercantum dalam tabel routing. Jika tidak ada default route, maka router akan membuang semua paket dengan alam tujuan yang tidak ditemukan didalam tabel routing.
3. Floating static route yaitu statik routing yang memiliki nilai administrative distance (AD) lebih besar dari nilai AD statik atau dinamik routing yang lain. Floating static route biasanya digunakan sebagai route backup.
4. Summary static route yaitu statik routing yang ditujukan untuk meminimalisir jumlah baris pada routing table. Beberapa baris routing dapat digabung menjadi 1 baris routing dengan menggunakan mekanisme tertentu sehingga dapat menghemat memori router.

6.2. Implementasi statik dan default routing

Statik routing dan default routing dapat diimplementasikan pada semua perangkat router. Implementasi statik dan default routing kali ini akan dilakukan menggunakan perangkat cisco. Untuk implementasi statik route pada cisco router dapat menggunakan perintah **ip route** dan **ipv6 route.** Berikut ini adalah bentuk umum perintah ipv4 statik routing:

```
Router(config)# ip route network-address subnet-mask { ip-
address | exit-intf [ip-address]} [distance]
```

Keterangan :

Parameter	Keterangan
network-address	merupakan alamat network IP tujuan yang akan ditambahkan pada tabel routing
subnet-mask	merupakan subnet mask dari network tujuan dan dapat dimodifikasi sehingga beberapa network dapat digabung menjadi satu untuk membuat sebuah summary static route
ip-address	merupakan alamat IP router nex-hop kemana paket akan dilewatkan
exit-intf	Merupakan interface yang digunakan untuk meneruskan paket, biasanya digunakan untuk konfigurasi koneksi poin to poin
exit-intf ip-address	Membuat statik route yang ditentukan sepenuhnya lewat interface dan alamat IPv4 hop berikutnya
distance	perintah opsional yang dapat digunakan untuk merubah nilai AD antara 1 .. 255. Biasanya digunakan untuk melakukan konfigurasi *floating static route* dengan nilai AD yang lebih besar dan digunakan sebagai jalur backup.

Sedangkan untuk konfigurasi statik routing menggunakan IPv6 adalah sebagai berikut:

```
Router(config)# ipv6 route ipv6-prefix/prefix-length {ipv6-
address | exit-intf [ipv6-address]} [distance]
```

Keterangan :

Parameter	Keterangan
ipv6-prefix	merupakan alamat network IPv6 tujuan yang akan ditambahkan pada tabel routing
/prefix-length	merupakan panjang prefix yang digunakan pada remote network tujuan
ipv6-address	merupakan alamat IPv6 router nex-hop kemana paket akan

	dilewatkan
exit-intf	Merupakan interface yang digunakan untuk meneruskan paket, biasanya digunakan untuk konfigurasi koneksi poin to poin
exit-intf ipv6-address	Membuat statik route yang ditentukan sepenuhnya lewat interface dan alamat IPv6 hop berikutnya
distance	perintah opsional yang dapat digunakan untuk merubah nilai AD antara 1 .. 255. Biasanya digunakan untuk melakukan konfigurasi *floating static route* dengan nilai AD yang lebih besar dan digunakan sebagai jalur backup.

Untuk melakukan konfigurasi statik routing dapat mengikuti langkah-langkah seperti dalam tabel berikut ini:

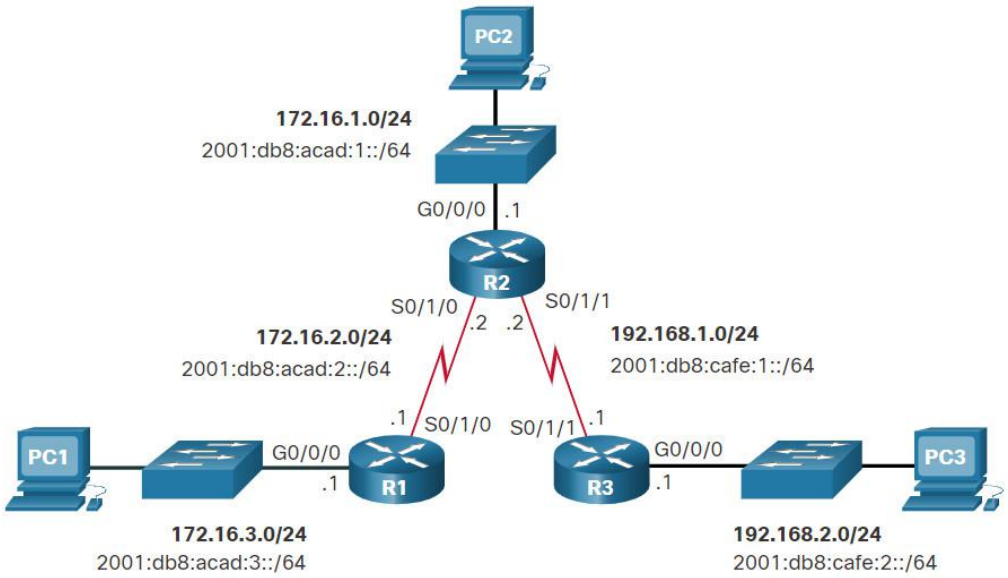
	Perintah	Fungsi

Langkah 1	configure terminal
	contoh:
	`switch# configure terminal`
	`switch(config)#`
		Masuk ke dalam mode configurasi

Langkah 2	`ip route {ip-prefix | ip-addr ip-mask} {[next-hop | nh-prefix] | [interface next-hop | nh-prefix]} [tag tag-value [pref]`
	contoh:
	`switch(config)# ip route 192.0.2.0/8 ethernet 1/2 192.0.2.4`
		Konifigurasi sebuah static routing. Nilai AD defaultnya adalah 1 dan dapat diubah 1..255.

Langkah 3	`show ip static-route`
	Example:
	`switch(config)# show ip static-route`
		Menampilkan informasi tentang static routing

Langkah 4	`copy running-config startup-config`
	Example:
	`switch(config)# copy running-config startup-config`
		Menyimpan perubahan konfigurasi



Gambar 6.2. Contoh topologi implementasi statik routing

Berikut ini adalah contoh konfigurasi statik routing berdasarkan topologi sederhana diatas dan dapat disesuaikan dengan kebutuhan. Perintah untuk konfigurasi statik route IPv4 dan IPv6 sedikit berbeda. Berikut ini adalah langkah-langkah untuk melakukan konfigurasi statik routing pada R1 dan R2 agar paket dari R1 dapat diteruskan ke jaringan yang berbeda sehingga PC1 dapat mengirimkan paket ke PC2.

```
R1# configure terminal
R1(config)# ip route 172.16.1.0/24 172.16.2.2
R1(config)# copy running-config startup-config

R2# configure terminal
R2(config)# ip route 172.16.3.0/24 172.16.2.1
R2(config)# copy running-config startup-config
```

Untuk menghapus static routing dari tabel routing dapat menggunakan perintah:

```
R1(config)#no ip static-route
```

Konfigurasi yang telah dilakukan perlu diverifikasi untuk memastikan tidak terjadi kesalahan. Untuk melakukan verifikasi dari konfigurasi dapat menggunakan perintah sebagai berikut:

```
R3#show ip static-route
```

atau

```
R3#show ip route static
```

Berikut ini adalah contoh output yang dihasilkan (simbol S mengindikasikan statik routing):

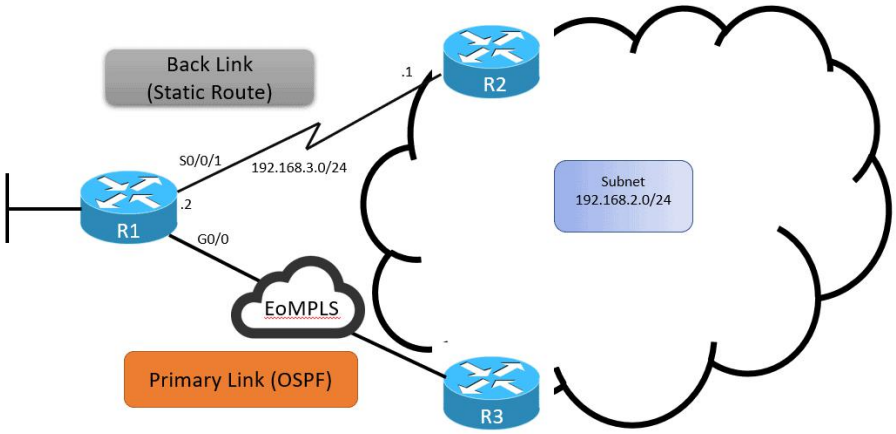
```
 172.16.0.0/24 is subnetted, 3 subnets
S        172.16.1.0 is directly connected, Serial0/0/1
S        172.16.2.0 is directly connected, Serial0/0/1
S        172.16.3.0 is directly connected, Serial0/0/1
R3#
```

6.3. Konfigurasi floating statik routes

Statik routing memiliki nilai AD sangat rendah yaitu 1 (satu) artinya router akan memilih route statik dari pada rute dinamik. Jika ingin menggunakan statik routing sebagai rute cadangan, maka kita dapat merubah nilai AD nya yang dikenal dengan istilah *floating static route.* Floating static route merupakan rute statik yang digunakan oleh router untuk membuat cadangan rute secara dimanis. Kita harus mengkonfigurasi floating static route dengan nilai administrative distance (AD) yang lebih tinggi dari rute yang akan dicadangkan. Dalam hal ini, router akan lebih memilih route yang dicadangkan dan apabila rute yang dicadangkan tidak dapat digunakan, maka dapat digunakan sebagai backup sehingga komunikasi akan tetap dapat berjalan. *Floating static route* memiliki karakteristik sebagai berikut:

1. Digunakan sebagai opsi cadangan atau file over dalam sebuah sistem jaringan. Floating static route dikonfigurasi sebagai jalur cadangan untuk digunakan apabila jalur utama tidak tersedia.
2. Konfigurasi floating statik route diberi nilai administrative distance (AD) yang lebih tinggi dibandingkan dengan nilai AD routing dinamik yang biasa digunakan dalam jaringan. Hal ini akan menyebabkan sebuah router akan tetap menggunakan jalur yang dihasilkan oleh dinamik route namun akan kembali ke jalur statik route apabila route dinamik tidak tersedia.
3. Floating static route biasanya dikonfigurasi berdasarkan next hop dan nilai AD, tetapi tidak memiliki metrik seperti dinamik routing.
4. Digunakan untuk merutekan lalu lintas jaringan sekunder jika link utama tidak berfungsi atau tidak tersedia.
5. Floating static route dikonfigurasi secara manual, tidak belajar otomatis seperti dinamik route.
6. Biasanya digunakan dalam jaringan perusahaan yang memiliki jalur cadangan untuk akses ke sumberdaya penting perusahaan.
7. Floating static route dapat di buat secara permanen, artinya, jalur tersebut tetap akan disediakan dan tidak akan dihapus saat perangkat di-restart.

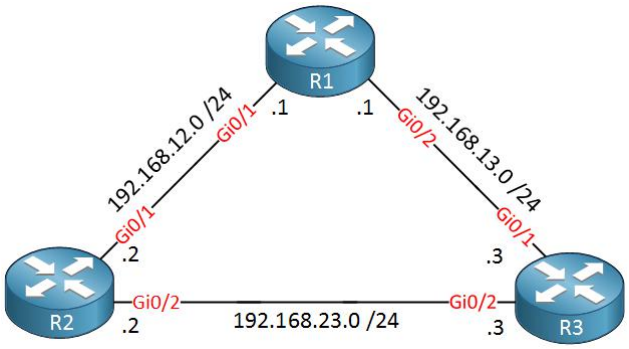
Untuk memahami floating static route, mari kita gunakan topologi seperti gambar dibawah ini.



Gambar 6.3. Contoh topologi untuk *floating static route*

Berdasarkan topologi pada gambar diatas, dapat dilihat bahwa R1 terhubung dengan 2 (dua) link WAN. Satu link melalui gigabit ethernet (G0/0) menggunakan OSPF dan satu link lagi melalui link serial (S0/0/1) dengan statik routing. Berdasarkan topologi diatas, link utama yang digunakan adalah jalur yang melalui gigabit ehternet. Namun apabila link gigabit tidak dapat digunakan maka paket akan dilewatkan melalui link serial. Hal tersebut dapat dilakukan apabila kita mengkonfigurasi floating static route yaitu dengan merubah nilai AD saat mengkonfigurasi statik routing. Apabila nilai AD saat konfigurasi statik routing tidak dirubah, maka jalur yang secara default akan digunakan router adalah jalur serial karena nilai AD secara default adalah 1 dan nilai AD OSPF adalah 110.

Sebagai contoh kita akan melakukan konfigurasi floating static route berdasarkan topologi pada gambar berikut.



Gambar 6.4. Konfigurasi topologi untuk floating static route

Berdasarkan pada topologi diatas, router 1 (R1) dapat menggunakan R2 dan R3 untuk menuju ke jaringan 192.168.23.0/24.Jalur R1 ke R2 dibangun menggunakan routing protokol RIP. Berikut ini adalah konfigurasi R1 dan R2.

```
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#no auto-summary
R1(config-router)#network 192.168.12.0

R2(config-router)#version 2
R2(config-router)#no auto-summary
R2(config-router)#network 192.168.12.0
R2(config-router)#network 192.168.23.0
```

Setelah dikonfigurasi seperti perintah diatas, maka R1 dapat mengirimkan paket ke jaringan 192.168.23.0/24 melalui R2. Untuk memastikan jalur yang dilalui dapat dicek pada tabel routing yang ada di R1 menggunakan perintah berikut:

```
R1#show ip route | begin 192.168.23.0
R     192.168.23.0/24 [120/1] via 192.168.12.2, 00:00:22,
GigabitEthernet0/1
```

Router 1 (R1) telah memiliki route untuk menuju ke jaringan 192.168.23.0/24 melalui router 2 (R2). Sekarang kita akan membuat router 3 (R3) sebagai backup dengan menggunakan statik routing. Berikut ini adalah perintahkonfigurasi pada R1.

```
R1(config)#ip route 192.168.23.0 255.255.255.0 192.168.13.3 ?
  <1-255>    Distance metric for this route
  multicast  multicast route
  name       Specify name of the next hop
  permanent  permanent route
  tag        Set tag for this route
  track      Install route depending on tracked item
  <cr>
```

Nilai AD dari routing protokol RIP adalah 120, maka kita harus memilih angka yang lebih besar dari 120 agar statik route dapat digunakan sebagai backup. Misalnya kita memilih angka 121, berikut ini adalah perintahnya.

```
R1(config)#ip route 192.168.23.0 255.255.255.0 192.168.13.3 121
```

Saat kita cek tabel routing saat ini adalah sebagai berikut:

```
R1#show ip route | begin 192.168.23.0
```

```
R     192.168.23.0/24 [120/1] via 192.168.12.2, 00:00:26,
GigabitEthernet0/1
```

Dapat dilihat bahwa routing RIP yang masih digunakan oleh router. Untuk memastikan link backup berjalan, maka interface R2 yang terhubung langsung ke R1 kita shutdown menggunakan perintah berikut.

```
R2(config)#interface GigabitEthernet 0/1
R2(config-if)#shutdown
```

RIP merupakan protokol routing yang cukup lambat dalam menemukan jalur baru, tunggu beberapa saat, kemudian cek kembali tabel routing pada R1 menggunakan perintah berikut ini.

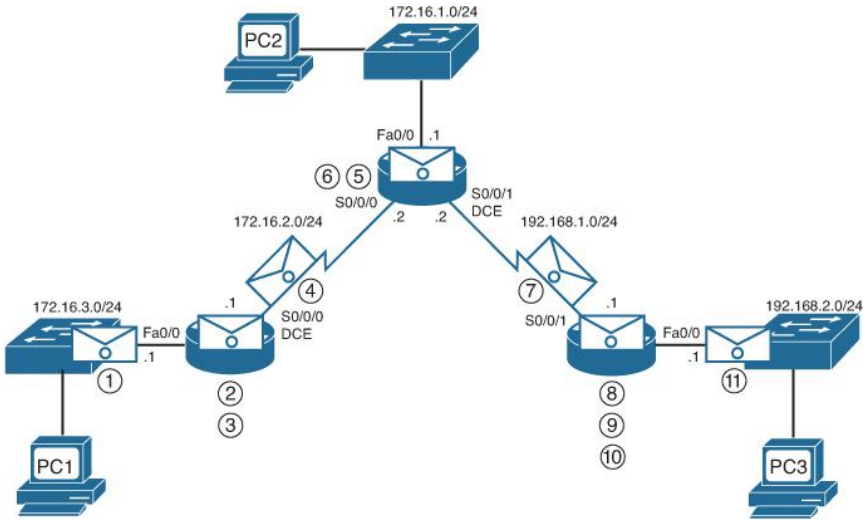
```
R1#show ip route | begin 192.168.23.0
S     192.168.23.0/24 [121/0] via 192.168.13.3
```

Floating static route sudah terinstall di R1 dan telah masuk dalam routing table. Dapat dilihat bahwa nilai AD saat ini adalah 121 sesuai dengan yang kita konfig sebelumnya. Jika interface R2 di aktifkan kembali, maka RIP akan mencari jalur kembali dan jalur dinamik routing RIP yang akan digunakan oleh R1.

6.4. Troubleshooting statik dan default routes

Setelah anda mempelajari cara konfigurasi statik route, default route, dan floating statik route, langkah berikutnya kita akan mempelajari langkah-langkah dalam memecahkan masalah umum yang mungkin muncul. Latihan memecahkan masalah merupakan metode terbaik untuk membantu memahami konsep statik routing dalam jaringan. Ketika statik route tidak lagi diperlukan, maka route tersebut harus dihapus dari konfigurasi yang berjalan.

Untuk melakukan troubleshooting dalam memecahkan masalah yang mungkin terjadi dalam statik routing, maka kita perlu mengetahui proses bagaimana sebuah paket diteruskan oleh router didalam jaringan. Berikut ini adalah penjelasan penerusan paket oleh router dengan statik routing.



Gambar 6.5. Penerusan paket pada statik routing

Berdasarkan gambar diatas, dimana PC 1 mengirimkan paket ke PC3:

1. Paket tiba pada interface FastEthernet 0/0 pada R1.
2. R1 tidak memiliki route spesifik untuk menuju network 192.168.2.0/24, maka R1 menggunakan default route.
3. R1 akan meng-enkapsulasi paket yang datang dalam bentuk frame baru.
4. Frame yang telah dienkapsulasi oleh R1 dan diteruskan keluar melalui interface Serial 0/0/0. Paket akan tiba di R2 di melalui interface serial 0/0/0 pada R2.
5. R2 melakukan de-enkapsulasi dan melihat tujuan dari paket tersebut. R2 memiliki statik route menuju 192.168.2.0/24 melalui interface serial 0/0/1.
6. Kemudian R2 melakukan enkapsulasi paket kedalam frame baru.
7. R2 kemudian meneruskan paket yang telah dienkapsulasi keluar melalui interface S0/0/1. Paket akan tiba di R3 melalui interface serial 0/0/1.
8. R3 melakukan de-enkapsulasi dari frame untuk melihat alamat tujuan dari paket tersebut. Untuk menuju jaringan 192.168.2.0/24 pada R3 berdasarkan routing tabel yaitu melalui interface FastEthernet 0/0.
9. R3 akan melihat tabel ARP untuk mendapatkan alamat MAC dari PC3. Jika ketemu, maka R3 akan mengirimkan permintaan address resolution protocol (ARP) keluar melalui interface fastEthernet 0/0 dan PC3 akan merespon dengan ARP reply berikut dengan alamat MAC dari PC3.
10. R3 akan mengenkapsulasi paket kedalam frame baru dengan alamat MAC FastEthernet 0/0 sebagai alama sumber dan alamat MAC PC3 sebagai alamat MAC tujuan.
11. Frame akan diteruskan melalui interface FastEthernet 0/0. Paket tiba di PC3 melalui network interface card (NIC) yang terhubung dengan router.

Contoh troubleshooting konfigurasi IPv4 statik dan default route.

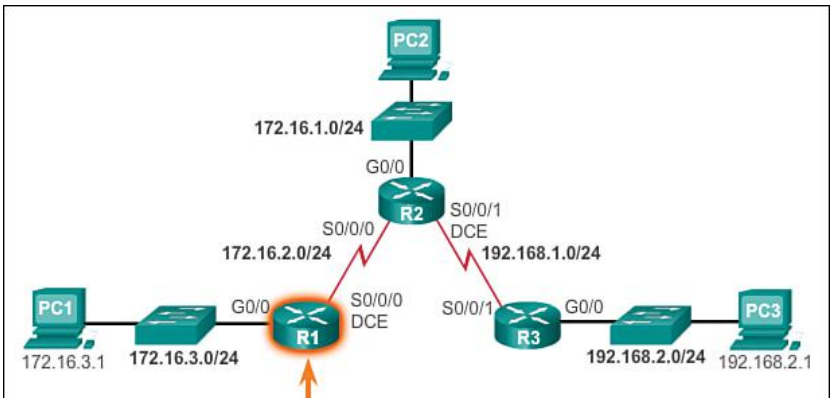
Troubleshooting merupakan keterampilan yang akan berkembang seiring dengan bertambahnya pengalaman. Hal terbaik yang harus dilakukan adalah mencari permasalahan yang jelas dan paling sederhana terlebih dahulu, seperti interface aktif atau tidak, atau dengan mengecek alamat IP pada interface salah atau tidak. Setelah permasalah sederhana tersebut terverifikasi, baru memulai mencari kemungkinan lain yang lebih rumit seperti mencari kesalah dalam konfigurasi statik routing.

Ketika koneksi end to end menjadi masalah, mulailah dengan memastikan bahwa kita dapat melakukan ping ke interface sendiri dan perangkat lain dalam jaringan yang terhubung langsung dengan router. Jika hal ini sudah dipastikan tidak ada masalah, maka melanjutkan dengan menguji konektivitas ke jaringan yang lebih jauh misalnya menguji koneksi ke perangkat lain yang melalui router1 router atau beberapa router.

Ketika ada perubahan dalam jaringan, konektivitas mungkin akan terganggu atau bahkan akan terputus. Admin jaringan harus bertanggung jawab untuk menentukan dan memecahkan masalah yang terjadi. Untuk menemukan masalah yang terjadi, admin jaringan harus memahami tool yang dapat digunakan untuk mengatasi masalah tersebut dengan cepat. Berikut ini adalah beberapa perintah yang dapat digunakan untuk melakukan troubleshooting pada perangkat Cisco.

```
1. ping
2. traceroute
3. show ip route
4. show ip interface brief
5. show cdp eighbors detail
```

Gambar berikut ini menggambarkan hasil ping dari interface R1 menuju LAN interface pada R3.



Gambar 6.6. Pengujian menggunakan perintah ping

Berikut ini adalah hasil menjalankan traceroute dari R1 menuju LAN pada R3.

```
R1# traceroute 192.168.2.1
Type escape sequence to abort.
Tracing the route to 192.168.2.1
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.2.2 4 msec 4 msec 8 msec
  2 192.168.1.1 12 msec 12 msec *
R1#
```

Isi dari tabel routing pada R1 adalah:

```
R1# show ip route | begin Gateway
Gateway of last resort is not set
      172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
S        172.16.1.0/24 [1/0] via 172.16.2.2
C        172.16.2.0/24 is directly connected, Serial0/0/0
L        172.16.2.1/32 is directly connected, Serial0/0/0
C        172.16.3.0/24 is directly connected,
GigabitEthernet0/0
L        172.16.3.1/32 is directly connected,
GigabitEthernet0/0
S     192.168.1.0/24 [1/0] via 172.16.2.2
S     192.168.2.0/24 [1/0] via 172.16.2.2
R1#
```

Berikut ini adalah perintah untuk mengecek status dari semua interface pada router

```
R1# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down down
GigabitEthernet0/0         172.16.3.1      YES manual up                    up
GigabitEthernet0/1         unassigned      YES unset  administratively down down
Serial0/0/0                172.16.2.1      YES manual up                    up
Serial0/0/1                unassigned      YES unset  administratively down down
R1#
```

Perintah show cdp neighbors dapat digunakan untuk melihat daftar perangkat cisco yang terhubung langsung dengan router. Hal ini dilakukan untuk memvalidasi konektivitas pada layer 2 dan juga layer 1. Misalnya jika ada perangkat tetangga terdaftar dalam out perintah show cdp, namun tidak dapat diping, maka perlu dicek pengalamatan IP pada layer 3.

```
R1# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
netlab-cs5       Gig 0/0             156              S I   WS-C2960- Fas 0/1
R2               Ser 0/0/0           153            R S I  CISCO1941 Ser
0/0/0
R1#
```

Contoh kasus berikut ini adalah bahwa pengguna PC1 melaporkan bahwa tidak dapat mengakses sumberdaya yang terhubung dengan PC3 berdasarkan gambar topologi sebelumnya. Untuk memperbaiki langkah awal yang harus dilakukan adalah memastikan PC 1 sudah terhubung ke gateway dalam hal ini adalah R1. Di asumsikan PC1 sudah dikonfigurasi dengan benar dan dapat melakukan ping ke R1. Berikutnya yang harus dilakukan adalah mengecek koneksi ke LAN pada R3 dari R1 menggunakan perintah traceroute berikut ini.

```
R1# traceroute 192.168.2.1
Type escape sequence to abort.
Tracing the route to 192.168.2.1
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.2.2 4 msec 4 msec 8 msec
  2 172.16.2.1 12 msec 12 msec 12 msec
  3 172.16.2.2 12 msec 8 msec 8 msec
  4 172.16.2.1 20 msec 16 msec 20 msec
  5 172.16.2.2 16 msec 16 msec 16 msec
  6 172.16.2.1 20 msec 20 msec 24 msec
  7 172.16.2.2 20 msec
R1#
```

Langkah berikutnya adalah mengecek tabel routing di R2 menggunakan perintah seperti berikut ini.

```
R2# show ip route | begin Gateway
Gateway of last resort is not set
      172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
C        172.16.1.0/24 is directly connected, GigabitEthernet0/0
L        172.16.1.1/32 is directly connected, GigabitEthernet0/0
C        172.16.2.0/24 is directly connected, Serial0/0/0
L        172.16.2.2/32 is directly connected, Serial0/0/0
S        172.16.3.0/24 1/0] via 172.16.2.1
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Serial0/0/1
L        192.168.1.2/32 is directly connected, Serial0/0/1
S     192.168.2.0/24 [1/0] via 172.16.2.1
R2#
```

Berdasarkan output yang ada dapat dilihat bahwa terdapat masalah pada tabel routing yaitu tujuan ke alamat network 192.168.2.0/24 adalah directly connected yang artinya salah konfigurasi alamat IP. Kemudian juga belum ada dalam tabel routing yang mengarahkan jalur menuju network 192.168.2.0/24. Maka untuk memperbaiki hal tersebut dapat dikonfigurasi sebagai berikut.

```
R2# show running-config | section ip route
ip route 172.16.3.0 255.255.255.0 172.16.2.1
```

```
ip route 192.168.2.0 255.255.255.0 172.16.2.1
R2#
R2# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)# no ip route 192.168.2.0 255.255.255.0 172.16.2.1
R2(config)# ip route 192.168.2.0 255.255.255.0 192.168.1.1
R2(config)#
```

Langkah terakhir adalah menguji ulang koneksi dari PC1 ke PC3. Hal tersebut juga dapat dilakukan pengujian ping ke alamat IP 192.168.2.1 melalui router 1 seperti berikut ini.

```
R1# ping 192.168.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2
seconds:
Packet sent with a source address of 172.16.3.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
28/28/28 ms
R1#
```

6.5. Rangkuman

1. Statik routing adalah metode pengaturan jalur dalam jaringan di mana administrator secara manual menentukan rute yang akan digunakan untuk mengirimkan paket data. Metode ini cocok untuk jaringan kecil atau yang tidak sering berubah.
2. Default routing adalah rute yang digunakan ketika tidak ada rute spesifik yang ditemukan dalam tabel routing. Ini biasanya digunakan untuk mengarahkan lalu lintas ke gateway atau router lain ketika tujuan tidak dikenal.
3. Floating Static Route adalah rute statik yang memiliki metrik lebih tinggi dibandingkan rute dinamis, sehingga hanya digunakan jika rute dinamis gagal. Floating static routes memberikan cadangan untuk meningkatkan keandalan jaringan.
4. Untuk mengkonfigurasi floating static routes, administrator harus menetapkan metrik yang lebih tinggi pada rute statik dibandingkan dengan rute dinamis yang ada.
5. Beberapa masalah yang mungkin terjadi dalam statik dan default routing termasuk kesalahan konfigurasi, alamat tujuan yang salah, dan masalah konektivitas.
6. Statik routing lebih sederhana dan mudah dipahami, terutama untuk jaringan kecil dengan sedikit perubahan. Memberikan kontrol penuh kepada administrator atas jalur yang digunakan, memungkinkan pengaturan yang lebih tepat sesuai kebutuhan jaringan. Dengan tidak bergantung pada protokol routing dinamis, statik routing dapat mengurangi risiko serangan yang memanfaatkan kerentanan dalam protokol dinamis.
7. Statik routing tidak memerlukan penggunaan bandwidth tambahan untuk pembaruan routing, karena tidak ada proses komunikasi antara router untuk berbagi informasi routing.

6.6. Latihan Soal

1. Apa yang dimaksud dengan statik routing?
a) Routing yang dilakukan secara otomatis oleh protokol
b) Routing yang dikonfigurasi secara manual oleh administrator
c) Routing yang tidak memerlukan alamat IP
d) Routing yang hanya digunakan dalam jaringan kecil
e) Routing yang menggunakan algoritma dinamis

2. Apa keuntungan utama dari menggunakan statik routing?
a) Mudah diimplementasikan dan dikelola
b) Secara otomatis memperbarui jalur
c) Mengurangi penggunaan bandwidth
d) Menyediakan jalur alternatif secara otomatis
e) Memungkinkan pengaturan jalur berdasarkan beban jaringan

3. Dalam situasi apa statik routing paling cocok digunakan?
a) Jaringan besar dengan banyak perubahan
b) Jaringan kecil yang tidak sering berubah
c) Jaringan dengan banyak router
d) Jaringan yang memerlukan kecepatan tinggi
e) Jaringan yang tidak memerlukan keamanan

4. Apa yang harus dilakukan ketika sebuah statik route tidak lagi diperlukan?
a) Mengabaikannya
b) Menghapusnya dari konfigurasi
c) Mengubah metriknya
d) Menyimpannya untuk referensi di masa depan
e) Mengkonfigurasi ulang router

5. Apa yang dimaksud dengan default route dalam konteks statik routing?
a) Jalur yang digunakan untuk mengirimkan trafik ke jaringan tertentu
b) Jalur yang mewakili jalur ke jaringan manapun yang tidak memiliki kecocokan lebih spesifik
c) Jalur yang hanya digunakan dalam jaringan kecil
d) Jalur yang tidak memerlukan konfigurasi
e) Jalur yang digunakan untuk menghubungkan dua router

6. Apa yang dimaksud dengan floating static route?
a) Rute yang tidak aktif

b) Rute yang memiliki prioritas lebih rendah
c) Rute yang digunakan untuk pengujian
d) Rute yang selalu aktif
e) Rute yang tidak dapat diubah

7. Dalam troubleshooting statik routing, apa yang harus diperiksa terlebih dahulu?
a) Koneksi fisik
b) Konfigurasi perangkat lunak
c) Alamat IP
d) Subnet mask
e) Semua jawaban benar

8. Apa yang terjadi jika rute statik tidak dikonfigurasi dengan benar?
a) Data akan dikirim dengan lebih cepat
b) Jaringan akan menjadi lebih aman
c) Data tidak akan dapat mencapai tujuan
d) Jaringan akan berfungsi dengan baik
e) Tidak ada dampak yang signifikan

9. Dalam statik routing, rute dapat ditentukan berdasarkan:
a) Alamat IP tujuan
b) Protokol yang digunakan
c) Kecepatan transfer data
d) Jenis perangkat keras
e) Semua jawaban benar

10. Apa yang dimaksud dengan troubleshooting dalam konteks statik routing?
a) Proses mengatur rute secara otomatis
b) Proses memperbaiki masalah yang terjadi dalam routing
c) Proses menambahkan rute baru
d) Proses menghapus rute yang tidak digunakan
e) Proses mengamankan jaringan

Soal Esai

11. Jelaskan perbedaan antara statik routing dan dinamik routing.
12. Apa saja langkah-langkah yang diperlukan untuk mengkonfigurasi statik routing pada router?
13. Jelaskan bagaimana troubleshooting dilakukan pada statik routing.
14. Apa yang dimaksud dengan floating static route dan bagaimana cara kerjanya?
15. Jelaskan situasi di mana penggunaan default route sangat penting dalam statik routing.

6.7.Daftar Pustaka

Putra, M. (2021). *Pengantar Jaringan Komputer: Fokus pada Routing dan Switching*. Yogyakarta: Graha Ilmu.

Rudiantoro, A. (2021). *Routing dan Switching dalam Jaringan Komputer: Panduan Lengkap*. Bandung: Informatika.

Syamsul, I. (2020). *Teknik Routing dan Switching untuk Jaringan Skala Kecil dan Menengah*. Yogyakarta: Andi.

BAB 7

DINAMIK ROUTING

7.1.Definisi

Kalau pada bab sebelumnya membahas tentang routing statis, maka pada bab kali ini membahas tentang routing dinamis. Routing dinamis adalah mekanisme pertukaran informasi perutean (routing) antar router untuk menentukan jalur optimal antar perangkat jaringan. Protokol perutean digunakan untuk mengidentifikasi dan mengumumkan jalur jaringan. Namanya menyiratkan protokol routing dinamis memungkinkan router untuk mengkomunikasikan informasi routing dengan cepat. Dengan menerapkannya, topologi jaringan dapat dibuat untuk beradaptasi secara dinamis terhadap perubahan kondisi jaringan dan mempertahankan perutean yang berlebihan dan efektif terlepas dari perubahan tersebut. Selain itu, karena overhead administratif yang diperlukan untuk membangun situasi perutean yang sangat rumit relatif sedikit, hal ini penting untuk manajemen, administrasi, dan penyiapan jaringan. Skalabilitas jaringan meningkat pesat dengan menerapkan protokol perutean dinamis dibandingkan dengan menentukan perutean secara statis dalam topologi.

Teknologi Exterior Gateway (EGP), dibuat pada tahun 1982 oleh Eric C. Rosen, adalah teknologi routing dinamis pertama. Sejak itu, banyak protokol canggih telah dikembangkan dan disempurnakan seiring berjalannya waktu; kami akan membahas secara rinci tentang protokol-protokol ini dalam rangkaian artikel ini.

Kelemahan dari perutean statis—seperti perlunya campur tangan manusia untuk merutekan lalu lintas di sekitar malfungsi, kesalahan manusia dalam memasukkan rute, dan terbatasnya jumlah rute yang dapat dilacak oleh satu orang dalam file teks—dapat diatasi dengan pengembangan protokol perutean dinamis. Keuntungan ini datang dengan mengorbankan router yang memerlukan banyak kekuatan pemrosesan dan persyaratan untuk mempekerjakan administrator jaringan dengan pengalaman dalam menjinakkan algoritma routing.

Kelebihan Routing Dinamis adalah sebagai berikut:

- ✓ Cocok untuk area besar/luas
- ✓ Hanya mengenalkan alamat yang terhubung langsung dengan routernya
- ✓ Bila terjadi penambahan suatu network baru tidak perlu semua router dikonfigurasi, hanya router yang berkaitan saja
- ✓ Router secara otomatis berbagi informasi
- ✓ Routing table dibuat secara dinamik
- ✓ Tidak perlu mengetahui semua alamat network yang ada

✓ Administrator tidak ikut campur tangan

Kelemahan Routing Dinamis adalah sebagai berikut:

✓ Beban kerja router menjadi lebih berat karena selalu memperbarui IP Table pada setiap waktu tertentu

✓ Kecepatan pengenalan dan kelengkapan IP Table terbilang lama karena router membroadcast ke semua router lainnya sampai ada yang cocok sehingga setelah konfigurasi harus menunggu beberapa saat agar setiap router mendapat semua alamat IP yang ada.

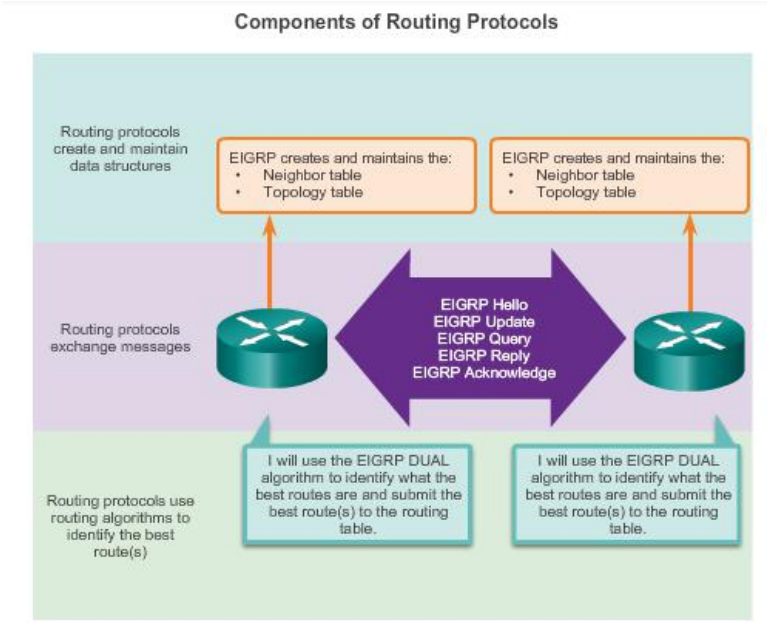
Komponen utama dari protokol routing dinamis meliputi:

✓ Struktur data - Protokol perutean biasanya menggunakan tabel atau database untuk operasinya. Informasi ini disimpan dalam RAM.

✓ Pesan protokol routing - Protokol perutean menggunakan berbagai jenis pesan untuk menemukan router tetangga, bertukar informasi perutean, dan tugas lain untuk mempelajari dan memelihara informasi akurat tentang jaringan.

✓ Algoritma - Protokol perutean menggunakan algoritma untuk memfasilitasi informasi perutean untuk penentuan jalur terbaik.

Pada gambar 2.1 berikut adalah Komponen utama dari protokol routing.



Gambar 7.1. Komponen utama dari protokol routing

Secara umum, pengoperasian protokol routing dinamis dapat digambarkan sebagai berikut:

1. Router mengirim dan menerima pesan routing pada antarmukanya.

2. Router berbagi pesan routing dan informasi routing dengan router lain yang menggunakan protokol routing yang sama.
3. Router bertukar informasi perutean untuk mempelajari tentang jaringan jarak jauh.
4. Ketika router mendeteksi perubahan topologi, protokol routing dapat mengumumkan perubahan ini ke router lain.

7.2.Dasar-dasar Protokol Routing

Routing dinamis melibatkan penggunaan protokol perutean yang menukar informasi perutean antar perangkat perutean. Protokol perutean menjalankan fungsi berikut:

1. Penemuan jaringan jarak jauh
2. Perhitungan jalur terbaik ke jaringan jarak jauh
3. Memperbarui tabel perutean
4. Menghitung ulang jalur terbaik baru jika terjadi kegagalan pada jalur terbaik saat ini
5. Ada lebih sedikit overhead administratif saat menggunakan protokol perutean dibandingkan perutean statis. Namun, menjalankan protokol perutean memerlukan sumber daya CPU dan memori ekstra.

Protokol perutean dapat dibandingkan menggunakan karakteristik berikut:

1. Skalabilitas: Seberapa besar suatu jaringan jika protokol perutean tertentu digunakan
2. Kecepatan Konvergensi: Seberapa cepat router bertukar informasi routing dan mencapai keadaan informasi yang konsisten
3. Kompleksitas: Menjelaskan tingkat pengetahuan yang dibutuhkan untuk mengimplementasikan dan mengoperasikan protokol routing tertentu
4. Penggunaan Sumber Daya: Sumber daya CPU dan memori yang diperlukan untuk menjalankan protokol.

7.3.Jenis Protokol Routing

Protokol perutean dinamis terbagi dalam salah satu dari dua kategori: protokol gateway interior (IGP) dan protokol gateway eksterior (EGP). Secara umum, protokol gateway interior beroperasi dalam Sistem Otonomi (AS) tertentu, sedangkan protokol gateway eksterior beroperasi antar AS. Sistem otonom adalah sekumpulan router di bawah administrasi umum dengan kebijakan perutean yang sama.

Perlu diperhatikan bahwa istilah “protokol gateway eksterior” tidak sama dengan protokol spesifik bernama sama, Exterior Gateway Protocol (EGP). Agak membingungkan, Exterior Gateway Protocol hanyalah salah satu contoh protokol gateway eksterior, seperti halnya BGP, penerusnya. Protokol gateway interior dapat dikategorikan lebih lanjut ke dalam protokol vektor jarak dan protokol link-state berdasarkan operasinya:

- ✓ Router yang menggunakan protokol perutean vektor jarak tidak mengetahui topologi jaringan. Ia hanya mengetahui jaringan yang terhubung langsung dan jaringan jarak

jauh yang dapat dijangkau melalui tetangganya.

- ✓ Protokol link-state lebih kompleks: router yang menggunakannya mengetahui topologi jaringan.

Satu-satunya protokol gerbang luar yang digunakan saat ini adalah Border Gateway Protocol (BGP), yang merupakan protokol perutean antar-domain standar de-facto yang digunakan di Internet. BGP dikenal sebagai protokol jalur-vektor. Pendahulunya, EGP sudah tidak digunakan lagi dan dianggap ketinggalan jaman. RIPv2 dan EIGRP memiliki pendahulunya yang tidak lagi didukung dalam rilis perangkat lunak saat ini. Protokol perutean yang paling umum digunakan ditunjukkan pada tabel 2.1 berikut.

Tabel 7.1. Jenis Dinamis Routing Protocol

Protocol Name	Interior or Exterior Gateway Protocol?	Distance Vector or Link-State Protocol?
Routing Information Protocol (RIPv2)	Interior	Distance Vector
Enhanced Interior Gateway Routing Protocol (EIGRP)	Interior	Distance Vector
Open Shortest Path First (OSPF)	Interior	Link-State
Intermediate System to Intermediate System (IS-IS)	Interior	Link-State
Border Gateway Protocol (BGP)	Exterior	Path-Vector

Seperti disebutkan sebelumnya, tujuan utama dari protokol routing adalah untuk menemukan jalur terbaik ke suatu tujuan. Bukan hal yang aneh jika sebuah router memiliki banyak jalur ke suatu tujuan yang dipelajari melalui satu protokol perutean, sehingga jalur tersebut perlu dibandingkan untuk menemukan jalur terbaik. Ketika sumber informasi untuk beberapa jalur adalah sama — semua jalur diketahui router melalui protokol perutean yang sama — router menggunakan metrik yang dihitung oleh protokol perutean untuk menemukan jalur terbaik.

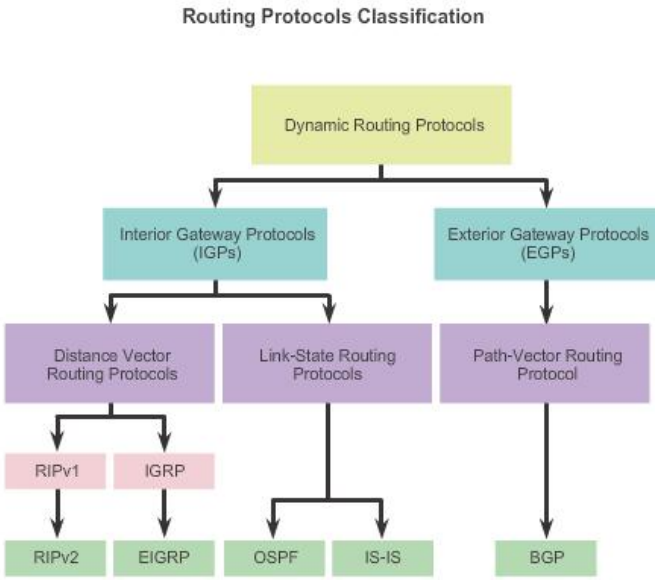
Protokol perutean yang berbeda menggunakan cara berbeda untuk menghitung metrik. Metrik yang dihitung oleh satu protokol perutean tidak dapat dibandingkan dengan metrik yang dihitung oleh protokol perutean lainnya. Protokol perutean yang berbeda mungkin tidak memilih jalur terbaik yang sama karena cara mereka menghitung metriknya.

Beberapa protokol hanya menggunakan satu variabel untuk menghitung metrik, sementara protokol lain mungkin menggunakan kombinasi beberapa variabel. Misalnya, RIPv2, yang merupakan protokol perutean vektor jarak, menggunakan metrik jumlah hop, yaitu berapa banyak router yang ada antara router dan jaringan jarak jauh. Sebaliknya, OSPF, yang merupakan protokol routing link-state, menggunakan biaya sebagai metrik, yang secara default terikat pada bandwidth antarmuka yang dapat digunakan untuk mencapai tujuan jarak jauh.

Selain itu, tidak seperti IGP, BGP menukar informasi perutean dan keterjangkauan antar AS. Jalur terbaik ditentukan berdasarkan serangkaian atribut yang diperiksa, dan jalur terbaik dinotasikan sebagai daftar ASes yang harus dilalui untuk mencapai jaringan tujuan yang dituju.

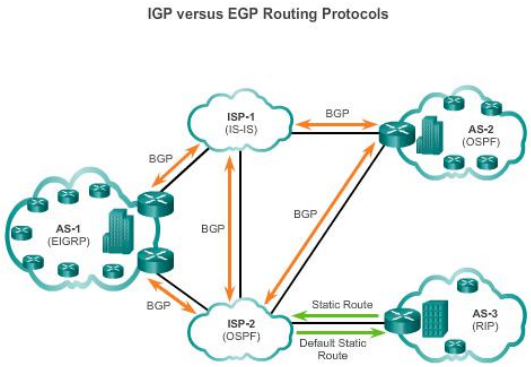
7.4.Klasifikasi Protokol Routing

Routing protocol adalah protokol yang terdapat pada routing dinamik (dynamic routing). Routing protocol bertugas untuk menentukan jalur terbaik yang akan dilewati oleh data serta memperbarui informasi tabel routing apabila terjadi perubahan jaringan. erdapat macam-macam routing protocol yang dapat kita gunakan untuk melakukan routing dinamik. Setiap protokol memiliki kelebihan dan kekurangan masing-masing. Beberapa routing protocol juga menggunakan sebuah algoritma yang bertugas untuk melakukan kalkulasi untuk mendapatkan jalur terbaik (best path). Pada gambar 2.2 berikut adalah klasifikasi dari protokol routing.



Gambar 7.2. Klasifikasi dari protokol routing

Interior Gateway Protocol (IGP) - Digunakan untuk routing dalam AS Termasuk RIP, EIGRP, OSPF, dan IS-IS. Sedangkan Exterior Gateway Protocol (EGP) - Digunakan untuk perutean antar AS Protokol perutean resmi yang digunakan oleh Internet. Pada gambar 2.3 berikut adalah perbedaan antara Interior Gateway Protocol (IGP) dan Exterior Gateway Protocol (EGP).



Gambar 7.3. Interior Gateway Protocol (IGP) vs Exterior Gateway Protocol (EGP)

a. Protokol Perutean Vektor Jarak (Distance Vector Routing Protocols).

Protokol vektor jarak menggunakan router sebagai tiang penanda di sepanjang jalur menuju tujuan akhir. Perutean vektor jarak dinamakan demikian karena melibatkan dua faktor: jarak, atau metrik, dari suatu tujuan, dan vektor, atau arah yang harus diambil untuk sampai ke sana. Informasi perutean hanya dipertukarkan antara tetangga yang terhubung langsung. Ini berarti router mengetahui dari tetangga mana suatu rute dipelajari, namun tidak mengetahui dari mana tetangga tersebut mempelajari rute tersebut; sebuah router tidak dapat melihat melampaui tetangganya sendiri. Aspek perutean vektor jarak ini kadang-kadang disebut sebagai “perutean berdasarkan rumor”. Tindakan seperti split horizon dan poison reverse digunakan untuk menghindari loop routing.

b. Link-state routing protocol

Protokol perutean link-state seperti memiliki peta topologi jaringan yang lengkap. Posting tanda sepanjang perjalanan dari sumber ke tujuan tidak diperlukan, karena semua router link-state menggunakan peta jaringan yang identik. Router link-state menggunakan informasi link-state untuk membuat peta topologi dan memilih jalur terbaik ke semua jaringan tujuan dalam topologi tersebut. Tidak seperti Distance Vector Routing Protocol, Sebaliknya, routing link-state mengharuskan semua router mengetahui jalur yang dapat dijangkau oleh semua router lain dalam jaringan. Informasi link-state dibanjiri ke seluruh domain link-state (area di OSPF atau IS-IS) untuk memastikan semua router memiliki salinan database link-state area tersebut yang tersinkronisasi. Dari database umum ini, setiap router membangun pohon jalur terpendek relatifnya sendiri, dengan dirinya sendiri sebagai root, untuk semua rute yang diketahui.

c. Path Vector Routing Protocol

Path Vector Routing Protocol adalah jenis protokol perutean jaringan komputer yang melacak informasi jalur yang terus diperbarui. Sangat mudah untuk mengidentifikasi dan menghapus pembaruan yang berputar kembali ke node yang sama setelah melakukan perjalanan melalui jaringan. Untuk mencegah masalah "Hitung hingga Tak Terhingga",

teknik ini kadang-kadang digunakan dalam algoritma perutean Bellman-Ford. Dibandingkan dengan perutean link state dan perutean vektor jarak, ini berbeda. Jaringan tujuan, router berikutnya, dan rute menuju ke sana semuanya disertakan dalam setiap entri tabel routing.

Pesan Vektor Jalur di BGP: Keterjangkauan jaringan diumumkan oleh router batas sistem otonom (ASBR), yang mengambil bagian dalam perutean vektor jalur. Setelah menerima pesan vektor jalur, setiap router perlu mengonfirmasi bahwa jalur yang diiklankan mematuhi kebijakannya. ASBR memperbarui pesan dan tabel peruteannya sebelum meneruskannya ke tetangga berikutnya jika pesan tersebut mematuhi kebijakan. Ia mengirimkan nomor AS sendiri dalam pesan yang diperbarui dan menggantikan identitasnya sendiri untuk entri router berikut. Salah satu contoh protokol vektor jalur adalah BGP. Sistem otonom yang harus dilalui untuk mencapai sistem tujuan dikelola oleh tabel routing di BGP. Vektor jalur tidak digunakan oleh Exterior Gateway Protocol (EGP).

7.5.Rangkuman

1. Dinamik routing adalah metode pengaturan jalur dalam jaringan di mana router secara otomatis berbagi informasi routing dan memperbarui tabel routing mereka berdasarkan perubahan dalam topologi jaringan. Ini memungkinkan penyesuaian otomatis terhadap kondisi jaringan yang berubah.
2. Beberapa protokol routing dinamik yang umum digunakan meliputi: RIP (Routing Information Protocol): Protokol berbasis jarak yang menggunakan hop count sebagai metrik untuk menentukan jalur terbaik. OSPF (Open Shortest Path First): Protokol berbasis link-state yang menggunakan algoritma Dijkstra untuk menghitung jalur terpendek berdasarkan informasi topologi jaringan. EIGRP (Enhanced Interior Gateway Routing Protocol): Protokol hybrid yang menggabungkan fitur dari RIP dan OSPF, menawarkan kecepatan dan efisiensi dalam pembaruan routing.
3. Keuntungan Dinamik Routing : Adaptabilitas: Dinamik routing dapat menyesuaikan jalur secara otomatis jika terjadi perubahan dalam jaringan, seperti kegagalan link atau penambahan perangkat baru. Pengelolaan yang Lebih Mudah: Mengurangi beban kerja administrator jaringan, karena tidak perlu melakukan konfigurasi manual setiap kali ada perubahan dalam topologi jaringan.
4. Kelemahan Dinamik Routing: Overhead Jaringan: Proses berbagi informasi routing dapat menghasilkan overhead tambahan, yang dapat mempengaruhi kinerja jaringan, terutama pada jaringan yang lebih besar. Keamanan: Protokol dinamik dapat rentan terhadap serangan, seperti spoofing, jika tidak dilindungi dengan baik, karena informasi routing dapat diakses oleh pihak yang tidak berwenang.
5. Untuk mengimplementasikan protokol dinamik, administrator harus mengkonfigurasi router untuk menggunakan protokol tertentu dan memastikan bahwa semua router dalam

jaringan menggunakan protokol yang sama untuk berbagi informasi routing. Penting untuk memantau kinerja protokol dinamik dan melakukan pemeliharaan rutin untuk memastikan bahwa jaringan berfungsi dengan baik dan aman.

6. Router secara berkala mengirimkan informasi tentang rute yang mereka ketahui kepada router lain, memungkinkan mereka untuk memperbarui tabel routing mereka dengan informasi terbaru.
7. Router menggunakan algoritma tertentu untuk menentukan jalur terbaik berdasarkan metrik yang ditetapkan, seperti biaya, kecepatan, dan keandalan jalur.

7.6.Latihan Soal

1. Apa yang dimaksud dengan dinamik routing?

a) Pengaturan jalur secara manual
b) Pengaturan jalur secara otomatis berdasarkan informasi yang diterima
c) Proses pengiriman data tanpa routing
d) Penggunaan tabel statis untuk routing
e) Protokol untuk keamanan jaringan

2. Protokol mana yang menggunakan algoritma Bellman-Ford untuk menentukan jalur terbaik?

a) OSPF
b) EIGRP
c) RIP
d) BGP
e) IS-IS

3. Apa batas maksimum hop count yang diperbolehkan oleh RIP?

a) 10
b) 15
c) 20
d) 30
e) 50

4. Apa yang menjadi keunggulan OSPF dibandingkan dengan RIP?

a) OSPF lebih sederhana dalam konfigurasi
b) OSPF menggunakan metrik hop count
c) OSPF dapat mendukung jaringan yang lebih besar dan kompleks
d) OSPF tidak memerlukan pembaruan berkala
e) OSPF lebih cepat dalam konvergensi

5. Apa yang dilakukan router ketika mendeteksi perubahan topologi dalam dinamik

routing?

a) Mengabaikan perubahan
b) Mengumumkan perubahan kepada router lain
c) Menghapus semua jalur
d) Menghentikan semua komunikasi
e) Mengalihkan ke jalur statis

6. Protokol mana yang menggunakan algoritma link-state untuk dinamik routing?

a) RIP
b) EIGRP
c) OSPF
d) BGP
e) IGRP

7. Apa yang dimaksud dengan routing loop dalam dinamik routing?

a) Proses pengiriman data yang tidak teratur
b) Situasi di mana paket data berputar tanpa henti di jaringan
c) Proses pengaturan rute secara manual
d) Proses penghapusan rute yang tidak digunakan
e) Proses mengamankan jaringan

8. Dalam dinamik routing, apa yang dilakukan oleh router untuk berbagi informasi routing?

a) Mengirimkan paket data
b) Menggunakan protokol routing untuk bertukar informasi
c) Mengatur koneksi fisik
d) Menghapus rute yang tidak digunakan
e) Mengamankan jaringan

9. Apa yang menjadi tantangan utama dalam implementasi dinamik routing?

a) Memerlukan lebih banyak bandwidth
b) Memerlukan lebih banyak perangkat keras
c) Potensi untuk terjadinya routing loop dan masalah konvergensi
d) Sulit untuk dikonfigurasi
e) Tidak aman

10. Apa yang dimaksud dengan administrative distance dalam konteks dinamik routing?

a) Ukuran kecepatan transfer data
b) Ukuran keandalan rute yang ditentukan oleh protokol routing
c) Ukuran bandwidth yang digunakan
d) Ukuran keamanan jaringan

e) Ukuran jumlah perangkat dalam jaringan

Soal Esai

11. Jelaskan perbedaan antara dinamik routing dan statik routing.
12. Apa saja kelebihan dan kekurangan dari menggunakan protokol OSPF dalam dinamik routing?
13. Bagaimana cara kerja EIGRP dalam menentukan jalur terbaik?
14. Jelaskan proses pertukaran informasi routing antar router dalam dinamik routing.
15. Apa yang dimaksud dengan route summarization dan mengapa penting dalam dinamik routing?

7.7.Daftar Pustaka

Januari, R. (2022). *Cisco Networking: Panduan Lengkap Routing dan Switching*. Yogyakarta: Graha Ilmu.

Lestari, N. (2022). *Pengenalan dan Implementasi Routing serta Switching pada Jaringan Cisco.* Jakarta: Elex Media Komputindo.

Tukino. (2020). *Network Design and Management CISCO CCNA Routing and Switching (Network Simulation with Packet Tracer)*. Batam: Batam Publisher.

BAB 8

ROUTING INFORMATION PROTOCOL (RIP)

8.1. Pendahuluan *Rouitng Information Protocol* (RIP)

Routing Information Protocol (RIP) adalah salah satu protokol routing yang digunakan untuk pertukaran informasi routing di dalam jaringan komputer. RIP termasuk dalam kategori protokol routing berbasis vektor jarak (*distance vector*), yang artinya algoritma routingnya berdasarkan informasi jarak dan arah terhadap tujuan. RIP menggunakan metrik jumlah lompatan (*hop count*) sebagai ukuran jarak. *Hop count* adalah jumlah router yang harus dilalui untuk mencapai tujuan. Secara default, maksimum jumlah lompatan yang dapat dilalui adalah 15, dan apabila suatu rute melebihi nilai ini, maka tujuan dianggap tidak dapat dijangkau. RIP menggunakan algoritma belman-ford untuk menemukan route terbaiknya. Setiap router akan mengirimkan tabel routingnya ke router tetangga pada interval tertentu yang artinya tabel akan diupdate secara periodik jika terjadi perubahan. Router menerima update routing dari router tetangga dan menggabungkannya didalam tabel routing lokal.

Pembaruan RIP dikirim secara periodik kesemua router tetangga meskipun tidak selalu mengirimkan seluruh tabel routing. Pembaruan dilakukan setiap 30 detik secara default, namun kita dapat mengatur sesuai dengan kebutuhan jaringan. RIP mencapai konvergensi ketika tidak ada lagi perubahan pada tabel routing atau perubahan sudah terdistribusi dan diterima oleh semua router. Konvergensi merupakan proses dimana semua router dalam jaringan memiliki informasi routing yang konsisten. RIP sudah mendukung subnetting dan otentikasi dan saat ini sudah mendukung untuk IPv6.

RIP umumnya digunakan dalam jaringan skala kecil hingga menengah yang tidak kompleks. Untuk jaringan yang lebih besar dan kompleks, protokol routing yang digunakan lebih baik menggunakan OSPF atau EIGRP. RIP tidak menyediakan keamanan bawaan, namun untuk meningkatkan keamanan, RIP v2 dan RIPng sudah mendukung otentikasi menggunakan kata sandi. RIP memiliki keterbatasan yaitu memungkinkan terjadi perhitungan tak terhingga jika ada perubahan topologi yang signifikan dan keterbatasan jumlah lompatan yang hanya 15 sehingga jaringan yang lebih besar dan kompleks tidak dapat dihandel menggunakan routing protokol ini. Berikut ini adalah perbandingan antara RIP v1, RIP v2, dan RIPng.

Tabel 8.1. Perbandingan RIP v1, v2 dan RIPng

RIP v1	RIP v2	RIPng
Update informasi routing dikirimkan secara broadcast	Update informasi routing dilakukan secara multicast	Update informasi routing dilakukan secara multicast
Broadcast pada alamat 255.255.255.255	Multicast dengan alamat 224.0.0.9	Multicast at FF02::9 (RIPng hanya berjalan pada IPv6 networks)
Tidak support autentikasi	Support autentikasi	-
Protokol routing classfull	Suppot classfull dan classless	Classless

8.2. Cara Kerja RIP

RIP dirancang untuk digunakan dalam jaringan berbasis protokol *internet protocol* (IP). RIP bekerja berdasarkan algoritma Belman-Ford dan menggunakan metrik *hop count* (jumlah hop atau lompatan) untuk menentukan jalur terbaik menuju jaringan tujuan. Berikut ini adalah cara kerja protokol RIP.

1. Inisialisasi
   Setiap router RIP didalam jaringan akan memulai dengan menginisialisasi tabel routingnya. Tabel ini berisi informasi tentang jaringan terdekat dan jumlah hop menuju masing-masing jaringan.
2. Broadcast pesan RIP
   Router RIP secara periodik akan mengirimkan pesan broadcast keseluruh router didalam jaringan. Pesan ini berisi tentang tabel routing lokal masing-masing router.
3. Update tabel routing
   Setelah menerima pesan RIP dari router tetangga, router akan melakukan update pada tabel routingnya. Router akan mengevaluasi informasi dalam pesan RIP dan memutuskan apakah jalur baru yang diumumkan lebih baik daripada jalur yang telah diketeahui sebelumnya. Evaluasi ini dilakukan berdasarkan metrik *hop count.*
4. *Split horizon*
   RIP menggunakan metode *split horizon* untuk menghindari broadcast routing melalui interface yang digunakan untuk menerima informasi routing. Hal ini dapat membantu mencegah perjadinya loop routing didalam jaringan tersebut.
5. Hold down timer
   RIP menggunakan *hold-down timer* untuk menghindari flapping atau fluktuasi yang cepat dalam pengumuman routing. Jika sebuah jalur dianggap rusak, router akan menunggu sejumlah waktu sebelum menerima informasi baru tentang jalur tersebut. Hal ini akan sangat membantu mencegah pengumuman yang tidak stabil.
6. Triggered update
   Jika terjadi perubahan dalam topologi jaringan, seperti pemutusan atau perbaikan jalur, router akan mengirimkan pesan triggered update ke router tetangga untuk memberi tahu

perubahan tersebut. Hal ini membantu mengurangi waktu konvergensi dalam mengatasi perubahan topologi.

7. Penanganan metrik infinity
   RIP menggunakan nilai infinity (hops tak terbatas) untuk menunjukkan bahwa suatu jalur tidak dapat dijangkau. Secara default, nilai infinity dalam RIP adalah 16 hops.
8. Route poisoning
   Untuk menghindari pembentukan loop, RIP menggunakan teknik yang disebut "*Route Poisoning*". Ketika suatu jalur menjadi tidak dapat dijangkau, router mengumumkan informasi tentang jalur tersebut dengan metrik infinity kepada router tetangga.
9. Auto summarization
   RIP mendukung autosummarization, yang berarti bahwa router akan secara otomatis mengumumkan ringkasan jaringan jika memiliki beberapa subnet. Hal ini membantu mengurangi jumlah entri dalam tabel routing dan mengoptimalkan penggunaan bandwidth.

8.3. Kelebihan dan Kekurangan RIP

Protokol routing RIP banyak diigunakan dalam jaringan komputer dengan mempertimbangkan kelebihan dan kekurangannya. Kelebihan RIP adalah:

1. Simplicity
   Protokol routing RIP relatif simple untuk dikonfig dan dimanage sehingga membuat RIP menjadi pilihan yang tepat untuk jaringan dalam skala kecil dan menengah dengan keterbatasan sumber daya jaringan.
2. Mudah diimplementasikan
   RIP sangat mudah untuk diimplementasikan, tidak membutuhkan keahlian dalam bidang teknik yang tinggi untuk membangun dan memelihara jaringan berbasis protokol RIP.
3. Waktu konvergensi
   RIP membutuhkan waktu yang cukup singkat untuk konvergen dan dapat beradaptasi terhadap perubahan topologi dan jaringan serta dapat merutekan paket secara efisien.
4. Otomatis update
   RIP mampu melakukan update secara otomatis dalam interval waktu tertentu untuk menjamin informasi routing dapat diperbarui sesuai dengan kondisi jaringan.
5. Pemakain bandwidth rendah
   Protokol routing RIP membutuhkan bandwidth yang cukup rendah dalam melakukan pertukaran informasi routing sehingga dapat dijadikan pilihan untuk jaringan dengan keterbatasan link bandwidth.
6. Kompatibility
   RIP memiliki kompatibilitas yang tinggi dengan berbagai tipe dan perangkat router sehingga mudah untuk diintegrasikan dalam jaringan yang ada.

Sedangkan kekurangan dari protokol routing RIP adalah:

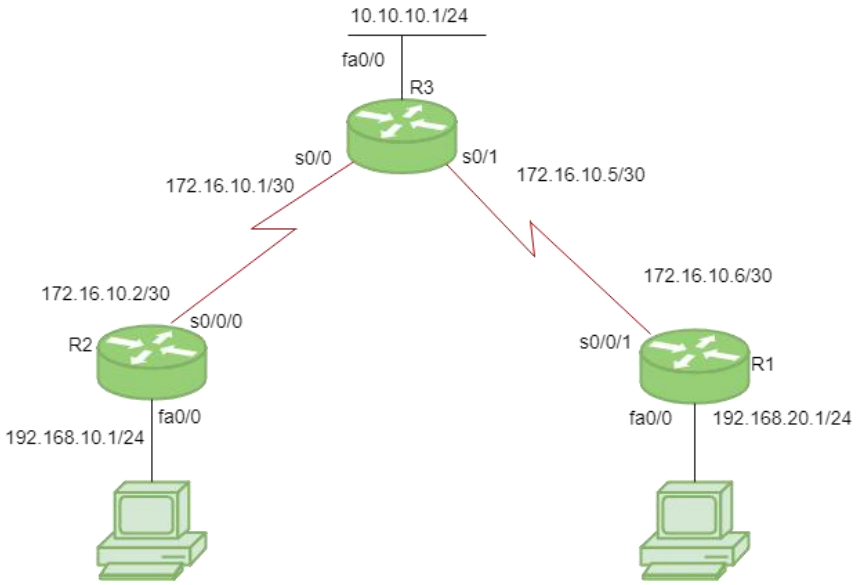
1. Skalability yang terbatas
   Protokol routing RIP memiliki keterbatasan dalam skalabilitas sehingga tidak cocok digunakan untuk jaringan berskala besar dan memiliki kompleksitas yang tinggi. RIP hanya support 15 hop, sehingga tidak dapat menghandel jaringan dalam skala besar.
2. Waktu konvergen yang lambat
   Meskipun waktu konvergensi RIP cepat, namun jika dibandingkan dengan protokol routing yang lain RIP memiliki kecepatan konvergensi yang paling lambat. Hal ini dapat menyebabkan terjadinya delay dan penurunan efisiensi dan kinerja jaringan.
3. Mungkin terjadi routing loop
   Penggunaan protokol RIP masih memungkinkan terjadi routing loop didalam jaringan yang dapat menyebabkan kemacetan sehingga menurunkan kinerja jaringan.
4. Tidak support load balancing
   RIP tidak support load balancing, dimana distribusi penerusan paket didalam jaringan tidak optimal.
5. Memiliki keamanan yang cukup rendah
   RIP tidak menyediakan fitur keamanan sehingga memungkinkan terjadi serangan seperti *spoofing* dan *tampering.*
6. Pemakaian bandwidth yang tidak efisien.
   RIP cukup memakan bandwidth dalam proses update berkaala sehingga menyebabkan kinerja jaringan tidak efisien terutama pada jaringan yang memiliki bandwidthterbatas.

8.4.Implementasi RIP

Implementasi protokol routing didalam jaringan sangat mudah untuk dilakukan. Berikut ini adalah langkah-langkah yang umum dilakukan untuk konfigurasi RIP.

1. Masuk ke mode konfigurasi dengan perintah **configure terminal**
2. Jalankan perintah **router rip**
3. Jalankan perintah **neighbor <ip-address>**
4. Jalankan perintah **receive version { 1 | 2 | 1 2 }**
5. Jalankan perintah **send version { 1 | 2 | 1 2 }**
6. Jalankan perintah **commit** atau **end.**

Sebagai contoh, kita akan melakukan konfigurasi RIP pada router sesuai dengan topologi berikut ini,



Gambar 8.1. Contoh topologi routing RIP

Berdasarkan gambar topologi diatas, terdapatt 3 router yaitu R1, R2 dan R3 dengan masih-masing router memiliki alamat IP lokal.

Konfigurasi RIP pada R1 adalah:

```
R1(config)# router rip
R1(config-router)# network 192.168.20.0
R1(config-router)# network 172.16.10.4
R1(config-router)# version 2
R1(config-router)# no auto-summary
```

Konfigurasi RIP pada R2 adalah:

```
R2(config)# router rip
R2(config-router)# network 192.168.10.0
R2(config-router)# network 172.16.10.0
R2(config-router)# version 2
R2(config-router)# no auto-summary
```

Terakhir konfigurasi RIP untuk R3 adalah:

```
R3(config)# router rip
R3(config-router)# network 10.10.10.0
R3(config-router)# network 172.16.10.4
R3(config-router)# network 172.16.10.0
R3(config-router)# version 2
R3(config-router)# no auto-summary
```

8.5. Troubleshooting RIP

Troubleshooting (penyelidikan masalah) pada protokol RIP melibatkan serangkaian langkah untuk mengidentifikasi dan memperbaiki masalah dalam distribusi informasi routing. Berikut

adalah beberapa langkah umum yang dapat Anda ambil ketika menghadapi masalah dengan RIP:

1. Verifikasi Konfigurasi RIP:
    a) Pastikan konfigurasi RIP di semua router terkait sudah benar.
    b) Periksa apakah jaringan yang seharusnya diumumkan sudah ditetapkan dengan benar.
    c) Perhatikan apakah protokol RIP diaktifkan pada antarmuka yang tepat.
2. Periksa Tabel Routing:
    a) Gunakan perintah **show ip route** pada router untuk memeriksa tabel routing.
    b) Perhatikan apakah rute yang diharapkan sudah masuk ke dalam tabel routing.
3. Periksa Status RIP:
    a) Gunakan perintah **`show ip protocols`** pada router untuk melihat status protokol RIP.
    b) Perhatikan apakah RIP telah mengumumkan atau menerima pembaruan.
4. Verifikasi Koneksi Fisik:
    a) Pastikan bahwa koneksi fisik antara router-ke-router atau router-ke-jaringan berfungsi dengan baik.
    b) Periksa lampu indikator antarmuka untuk memastikan bahwa koneksi fisik aktif.
5. Monitoring RIP Pembaruan:
    a) Gunakan perintah **`debug ip rip`** untuk memantau pembaruan RIP secara real-time.
    b) Pemantauan dapat membantu Anda melihat apakah router mengirim atau menerima pembaruan dengan benar.
6. Periksa Timer dan Konfigurasi Usang:
    a) Pastikan bahwa timer RIP dikonfigurasi dengan benar, dan pembaruan dikirim sesuai dengan interval yang diharapkan.
    b) Periksa apakah ada entri dalam tabel routing yang sudah usang dan dihapus.
7. Periksa Filter dan Akses Kontrol:
    a) Pastikan bahwa tidak ada filter atau akses kontrol yang menghalangi pembaruan RIP.
    b) Periksa konfigurasi firewall atau ACL untuk memastikan bahwa protokol RIP dan port yang diperlukan tidak diblokir.
8. Cek Jarak dan Metrik:
    a) Periksa hop count ke destinasi untuk memastikan bahwa tidak melebihi batas maksimum (15 hop) yang diizinkan oleh RIP.
    b) Perhatikan metrik RIP untuk memastikan bahwa rute dengan metrik terendah dipilih.
9. Baca Log Perangkat:
    a) Periksa log perangkat untuk melihat apakah ada pesan kesalahan atau informasi penting yang dapat membantu Anda mengidentifikasi masalah.

Pastikan, untuk melakukan perubahan konfigurasi dengan hati-hati dan diuji terlebih dahulu pada lingkungan yang tidak mengganggu sistem keseluruhan. Pemahaman yang baik tentang

konfigurasi RIP dan kemampuan troubleshooting akan membantu kita dalam mengatasi masalah dengan efisien.

8.6. Rangkuman

1. RIP merupakan Protokol routing berbasis jarak yang digunakan untuk mengatur jalur dalam jaringan. RIP memungkinkan router untuk berbagi informasi tentang rute yang tersedia dan memilih jalur terbaik berdasarkan hop count.
2. RIP menggunakan jumlah hop (lompatan) sebagai metrik untuk menentukan jalur terbaik, dengan batas maksimum 15 hop.
3. Router RIP secara berkala mengirimkan informasi tentang rute yang mereka ketahui kepada router lain dalam jaringan.
4. Administrator harus mengkonfigurasi router untuk mengaktifkan RIP dan menentukan jaringan yang akan diikutsertakan dalam proses routing.
5. Terdapat dua versi utama, yaitu RIP v1 (hanya mendukung kelasful) dan RIP v2 (mendukung kelasless dan multicast).
6. Kelebihan dan Kekurangan RIP. Kelebihan: Sederhana dan mudah diimplementasikan, Cocok untuk jaringan kecil hingga menengah. Kekurangan: Terbatas pada 15 hop, tidak cocok untuk jaringan besar, Rentan terhadap masalah konvergensi yang lambat.
7. Konvergensi merupakan waktu yang dibutuhkan untuk semua router dalam jaringan untuk mencapai kesepakatan tentang rute terbaik setelah terjadi perubahan.

8.7. Latihan Soal

1. Apa yang dimaksud dengan RIP?

a) Protokol untuk pengiriman email
b) Protokol routing yang menggunakan hop count
c) Protokol untuk manajemen jaringan
d) Protokol untuk keamanan jaringan
e) Protokol untuk pengaturan bandwidth

2. Berapa batas maksimum hop count yang diperbolehkan oleh RIP?

a) 10
b) 15
c) 20
d) 30
e) 50

3. Apa yang dilakukan RIP ketika suatu jalur menjadi tidak dapat dijangkau?

a) Mengabaikan jalur tersebut
b) Mengumumkan metrik infinity

c) Menghapus jalur dari tabel routing
d) Mengirimkan pesan kesalahan
e) Mengalihkan ke jalur alternatifJawaban: B

4. Versi berapa dari RIP yang mendukung autosummarization?
a) Versi 1
b) Versi 2
c) Keduanya
d) Tidak ada
e) Versi 3

5. Apa perintah yang digunakan untuk memverifikasi status protokol RIP pada router?
a) show ip route
b) show ip protocols
c) debug ip rip
d) ping
e) traceroute

6. Dalam RIP, pembaruan routing dikirimkan setiap:
a) 10 detik
b) 30 detik
c) 60 detik
d) 90 detik
e) 120 detik

7. Apa yang menjadi kelemahan utama dari RIP?
a) Tidak dapat digunakan dalam jaringan besar
b) Memerlukan lebih banyak bandwidth
c) Sulit untuk dikonfigurasi
d) Tidak aman
e) Memerlukan lebih banyak perangkat keras

8. Apa yang dimaksud dengan "split horizon" dalam konteks RIP?
a) Teknik untuk menghindari pengulangan informasi routing
b) Proses pengiriman data yang cepat
c) Proses pengaturan rute secara manual
d) Teknik untuk mengamankan data yang dikirim
e) Proses penghapusan rute yang tidak digunakan

9. Dalam konfigurasi RIP, perintah untuk mengaktifkan RIP pada router Cisco adalah:

a) router rip
b) enable rip
c) start rip
d) activate rip
e) ip rip

10. Apa yang harus dilakukan jika terjadi masalah dalam distribusi informasi routing dengan RIP?

a) Menghapus semua rute
b) Memeriksa koneksi fisik dan konfigurasi
c) Mengganti protokol routing
d) Menambah bandwidth
e) Mengubah alamat IP

Soal Esai

11. Jelaskan cara kerja Routing Information Protocol (RIP) dalam jaringan.
12. Apa kelebihan dan kekurangan dari menggunakan RIP dalam jaringan?
13. Bagaimana cara melakukan troubleshooting pada protokol RIP?
14. Apa yang dimaksud dengan route poisoning dalam konteks RIP?
15. Jelaskan langkah-langkah implementasi RIP pada router.

8.8. Daftar Pustaka

Tukino. (2020). *Network Design and Management CISCO CCNA Routing and Switching (Network Simulation with Packet Tracer)*. Batam: Batam Publisher.

Veza, Okta, , dan . (2024). *Jaringan Komputer Lanjutan*. Batam: Cendikia Mulia Mandiri.

BAB 9

OPEN SHORTEST PATH FIRST (OSPF)

9.1. Definisi

Routing yang umum digunakan adalah RIP, OSPF dan BGP. RIP dan OSPF dikategorikan sebagai interior gateway routing protocol (IGP) sedangkan BGP atau bordeway routing protocol termasuk kategori external routing protocol. OSPF *(Open Shortest Path First)* adalah protokol yang digunakan dalam jaringan router sistem otonomi yang lebih besar dalam preferensi untuk Routing Information Protocol (RIP), protokol routing yang lebih tua yang dipasang di banyak jaringan perusahaan saat ini. Seperti RIP, OSPF ditunjuk oleh Internet Engineering Task Force (IETF) sebagai salah satu dari beberapa Protokol Interior Gateway.

Protocol ini termasuk dalam link-state protocol, kelebihan utama dari protokol ini adalah dapat dengan cepat mendeteksi perubahan dan menjadikan routing kembali konvergen dalam waktu singkat dengan sedikit pertukaran data. Routing ini membentuk peta jaringan dalam tiga tahap, tahap pertama setiap router mengenali seluruh tetangganya, lalu router saling bertukar informasi dan router akan menghitung jarak terpendek ke setiap tujuan. Peta jaringan nya akan disimpan dalam basis data sebagai hasil dari pertukaran informasi antar router. OSPF dapat menangani routing jaringan TCP/IP yang besar dan membuat hirarki routing dengan membagi jaringan menjadi beberapa area. Setiap paket yang dikirim dapat dibungkus dengan autentikasi, namun protocol ini membutuhkan kemampuan CPU dan memori yang besar.

9.2. Fitur OSPF

OSPF bekerja dengan menggunakan algoritma Dijkstra, meskipun mungkin tidak secepat EIGRP, OSPF juga dapat melakukan konvergensi dengan cepat dan mendukung banyak rute dengan biaya yang sama ke tujuan yang sama. OSPF juga mendukung protokol rute IP dan IPv6. fitur-fitur yang disediakan oleh protokol OSPF antara lain :

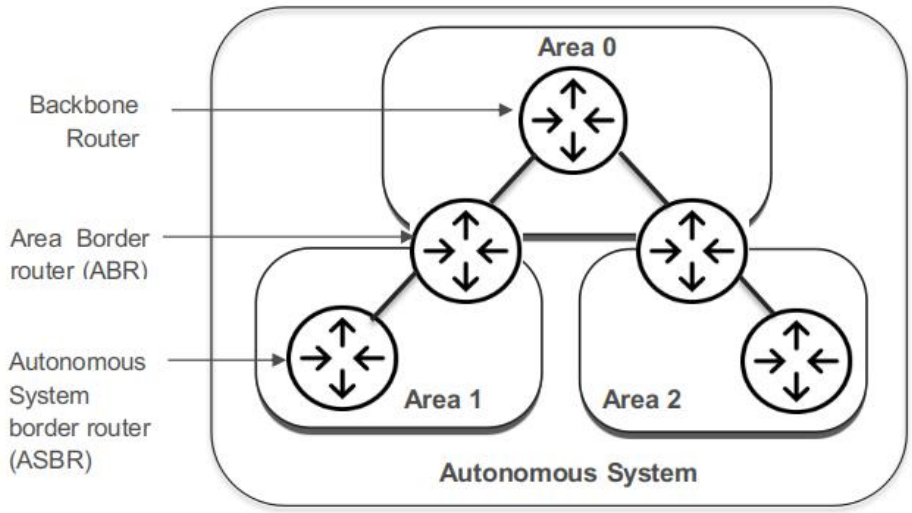
1. Terdiri dari wilayah dan sistem otonom.
2. OSPF Meminimalkan lalu lintas dengan melakukan pembaruan perutean.
3. Memungkinkan skalabilitas.
4. Mendukung VLSM/CIDR.
5. Memiliki jumlah hop yang tidak terbatas.
6. Mengizinkan penerapan multi-vendor (standar terbuka).

OSPF adalah protokol routing link-state pertama yang dikenalkan kebanyakan orang, jadi berguna untuk melihat perbandingannya dengan protokol distance-vector yang lebih tradisional seperti RIPv2 dan RIPv1. Tabel 7.3 memberi Anda perbandingan dari ketiga protokol ini.

Tabel 9.1. Perbandingan OSPF dan RIP

Karakteristik	OSPF	RIPv2	RIPv1
Tipe Protokol	Link state	Distance Vector	Destance Vector
Dukungan Classless	Ya	Ya	Tidak
Dukungan VLSM	Ya	Ya	Tidak
Auto-summarization	No	Ya	Ya
Manual summarization	Ya	Tidak	Tidak
Discontiguous support	Ya	Ya	Tidak
Route propagation	Multicast on change	Periodic multicast	Periodic broadcast
Path metric	Bandwidth	Hops	Hops
Hop count limit	None	15	15
Convergence	Cepat	Lambat	Lambat
Peer authentication	Ya	Ya	Tidak
Hierarchical network	Ya (using areas)	Tidak (flat only)	Tidak (flat only)
Updates	Event triggered	Route table updates	Route table updates
Route computation	Dijkstra	Bellman-Ford	Bellman-Ford

OSPF dirancang secara hierarkis, yang artinya OSPF dapat dapat memisahkan internetwork yang lebih besar menjadi internetwork yang lebih kecil yang disebut area. Ini yang menjadi keunggulan routing untuk OSPF. Beberapa alasan mengapa OSPF dapat mendukung desain hirarki adalah, untuk mengurangi overhead pada proses perutean, mempercepat konvergensi, membatasi ketidakstabilan jaringan ke area tunggal jaringan.



Gambar 9.1. Desain OSPF

OSPF berjalan di dalam sistem otonom, tetapi juga dapat menghubungkan beberapa sistem otonom secara bersamaan. Router yang menghubungkan AS ini bersama disebut Autonomous System Boundary Router (ASBR).

9.3. Terminologi OSPF

Untuk dapat mengerti tentang routing OSPF maka setiap administrator perlu mengetahui terminologi yang dapat membantu bagaimana memahami OSPF. Berikut ini adalah istilah-istilah OSPF yang penting untuk dipahami :

Tabel 9.2. Daftar istilah pada OSPF

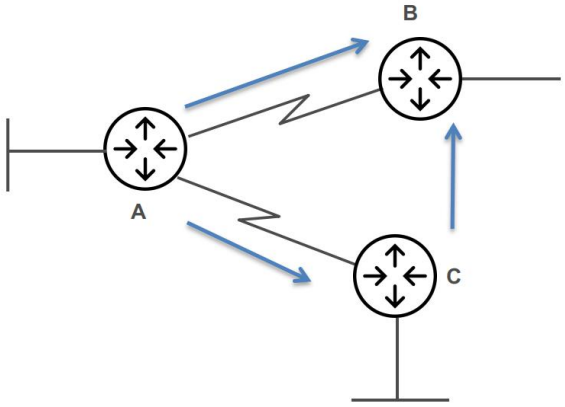
Istilah	**Deskripsi**
Link	Tautan antarmuka jaringan atau router yang ditugaskan ke jaringan tertentu. Saat antarmuka ditambahkan ke proses OSPF, itu dianggap oleh OSPF sebagai tautan. Setiap tautan akan memiliki informasi status yang terkait dengannya naik atau turunnya (up or down) status, serta satu atau lebih alamat IP.
Router ID	Router ID (RID) adalah alamat IP yang digunakan untuk mengidentifikasi router. Cisco memilih ID Router dengan menggunakan alamat IP tertinggi dari semua antarmuka loopback yang dikonfigurasi. Jika tidak ada antarmuka loopback yang dikonfigurasi dengan alamat, OSPF akan memilih alamat IP tertinggi dari semua antarmuka fisik yang aktif.
Neighbors	adalah dua atau lebih router yang memiliki antarmuka pada jaringan yang

	sama, seperti dua router yang terhubung pada tautan serial point-to-point.
Adjacency	Adcacency adalah hubungan antara dua router OSPF yang memungkinkan pertukaran langsung pembaruan rute. OSPF secara langsung berbagi rute hanya dengan tetangga yang juga menjalin kedekatan. Dan tidak semua tetangga akan berdekatan—ini bergantung pada jenis jaringan dan konfigurasi router.
Hello protocol	Protokol OSPF Hello menyediakan penemuan tetangga yang dinamis dan memelihara hubungan tetangga. Halo paket dan Link State Advertisements (LSA) membangun dan memelihara basis data topologi. Paket Hello dialamatkan ke 224.0.0.5.
Neighborship database	adalah daftar semua router OSPF yang telah melihat paket Hello. Berbagai detail, termasuk ID Router dan status, disimpan di setiap router di database tetangga.
Topology database	Database topologi berisi informasi dari semua Link State Paket Advertisement yang telah diterima untuk suatu daerah. Router menggunakan informasi dari database topologi sebagai masukan ke dalam algoritma Dijkstra yang menghitung jalur terpendek ke setiap jaringan.
Link State Advertisement	Link State Advertisement (LSA) adalah paket data OSPF yang berisi-informasi link-state dan routing yang dibagikan di antara router OSPF. Ada berbagai jenis paket LSA, dan saya akan membahasnya sebentar lagi. Router OSPF akan bertukar paket LSA hanya dengan router yang telah menjalin kedekatan
Designated router	Router yang ditunjuk (DR) dipilih setiap kali router OSPF terhubung ke jaringan multi-akses yang sama.
Backup designated router	Router yang ditunjuk cadangan (BDR) adalah hot standby untuk DR pada tautan multi-akses (ingat bahwa Cisco terkadang suka menyebut jaringan "siaran" ini). BDR menerima semua pembaruan perutean dari router yang berdekatan OSPF, tetapi tidak membanjiri pembaruan LSA.
OSPF areas	Area OSPF adalah pengelompokan jaringan dan router yang berdekatan. Semua router di area yang sama berbagi ID Area yang sama. Karena router dapat menjadi anggota lebih dari satu area pada satu waktu, ID Area diasosiasikan dengan interface tertentu pada router. Ini akan memungkinkan beberapa antarmuka menjadi milik area 1 sedangkan antarmuka yang tersisa dapat menjadi milik area 0. Semua router dalam

	area yang sama memiliki tabel topologi yang sama.
Broadcast (multi-access)	Jaringan siaran (multi-akses) seperti Ethernet memungkinkan banyak perangkat untuk terhubung ke (atau mengakses) jaringan yang sama, serta menyediakan kemampuan siaran di mana satu paket dikirim ke semua node di jaringan. Di OSPF, DR dan BDR harus dipilih untuk setiap jaringan multi-akses siaran.
Non-broadcast multi-access	Jaringan Non-Broadcast Multi-Access (NBMA) adalah jenis seperti Frame Relay, X.25, dan Asynchronous Transfer Mode (ATM). Jaringan ini memungkinkan multi-akses, tetapi tidak memiliki kemampuan siaran seperti Ethernet. Jadi, jaringan NBMA memerlukan konfigurasi OSPF khusus agar berfungsi dengan baik dan hubungan tetangga harus ditentukan.
Point-to-point	Point-to-point mengacu pada jenis topologi jaringan yang terdiri dari koneksi langsung antara dua router yang menyediakan jalur komunikasi tunggal. Koneksi point-to-point dapat bersifat fisik, seperti pada kabel serial yang langsung menghubungkan dua router, atau dapat juga secara logis, seperti pada dua router yang terpisah ribuan mil namun terhubung oleh sirkuit dalam jaringan Frame Relay.
Point-to-multipoint	Point-to-multipoint mengacu pada jenis topologi jaringan yang terdiri dari serangkaian koneksi antara antarmuka tunggal pada satu router dan beberapa router tujuan. Semua interface pada semua router yang berbagi koneksi point-to-multipoint milik jaringan yang sama. Seperti point-to-point, tidak diperlukan DR atau BDR.

9.4. Proses Routing OSPF

Proses dasar routing OSPF adalah menghidupkan adjacency, proses flooding, dan perhitungan table routing. Router-router mengirimkan paket halo ke seluruh jaringan yang terhubung secara periodic, jika paket tidak terdengar maka jaringan dianggap down, default mengirimkan 4 kali paket hello. Router-router selalu berusaha adjacent dengan router tetangganya berdasarkan paket halo yang diterima. Dalam jaringan multi access, router memilih Designated Router (DR) dan Backup Designated Router (BDR) dan mencoba adjacent dengan kedua router tersebut.



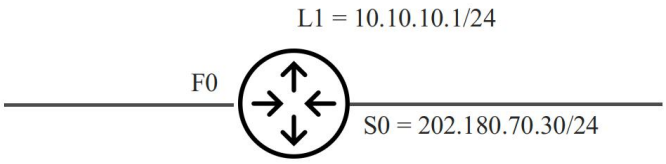
Gambar 9.2. Proses Adjecency

Sebagai contoh pada gambar 1. ketika jaringan baru terkoneksi, dan semua router telah aktif, maka proses yang terjadi adalah :

1. Pada router A akan membroadcast paket halo ke setiap interface yang terkoneksi pada router tetangga *(neighboard router)* dengan memberikan informasi tentang dirinya (router A), Begitu juga sebaliknya router A akan mengetahui informasi tentang tetangganya berdasarkan informasi yang diterima dan mengetahui berapa biaya (cost) untuk mencapai router lain. Data-data ini disimpan dalam basis data.
2. Selanjutnya, setelah semua router yang saling terhubung mengirimkan basis data tersebut dalam satu paket LSA *(link state advertisement)*, maka router yang menerima LSA harus mengirimkan ke semua router yang terhubung dengannya.
3. Karena router B telah menerima paket LSA dari router A maka jika LSA yang dikirimkan C sama dengan yang ada pada basis data B atau bukan yang baru, maka paket LSA dari C akan di drop.
4. Antara router satu dengan yang lain akan mengirimkan paket hello dengan interval tertentu misalnya 120 detik , jika tidak terdapat hello packet dari jaringan yang terkoneksi dengannya atau tidak mendapat balasan maka jaringan tersebut dianggap down. Maka jika terjadi NT down maka paket LSA akan disebarkan ke semua jaringan dengan menggunakan flooding dan akan menyebabkan basis data LSA berubah untuk mencari jalan yang terbaik dalam paket data.

a. Router ID

Router ID pada routing OSPF didapatkan dari IP address yang memiliki nilai tertinggi yang dimiliki semua interface router, apabila router mempunyai interfaces loopback maka yang digunakan adalah IP address tertinggi dari interface loopback tersebut.



Gambar 9.3. Router ID

Seperti pada gambar diatas, bagian router id adalah, ip address pada (L1) 10.10.10.1/24, apabila tidak memiliki interface loopback maka yang menjadi router Id adalah 202.180.70.30 (S0), router id akan diambil dari interface yang di UP sebelum proses OSPF dimulai. Router ID digunakan dalam proses penentuan DR/BDR yang dalam pembentukan hubungan bi-directional

b. Tahap Pembentukan Adjacency

Ketika pertama kali menghidupkan perangkat router, dengan menekan tombol ON, router OSPF sama sekali tidak mengetahui tentang router tetangganya (neighbor router), untuk mengetahui router tetangga, maka router akan mulai mengirimkan paket Hello ke seluruh interface jaringan, tujuanya adalah untuk memperkenalkan dirinya. Jika router yang baru ON ini menerima paket hello yang menyimpan informasi tentang dirinya maka router ini dapat saling berhubungan dua arah dengan router pengirim hello, Default nilai hello pada broadcast multi-access adalah 10 detik dan 40 detik jika tidak ada respon akan mati, dan pada NBMA hello 30 detik dan akan mati pada 120 detik jika tidak terdapat respon. Berikut ini adalah beberapa kondisi router pada saat melakukan adjacency.

- ✓ down : router tidak dapat hello packet dari router manapun
- ✓ attempt : router mengirimkan hello packet tetapi belum mendapat respon, hanya ada pada tipe NT non broadcast multi-access (NBMA) dan tidak ada respon dari router lain.
- ✓ Init : router mendapatkan hello packet dari router lain, tetapi belum terbentuk hubungan yang bidirectional (2 way).
- ✓ 2 way : pada tahap ini hubungan antar router sudah bi-directional, untuk NT broadcast DR & BDR nya akan melanjutkan ke tahap full, router non DR & BDR akan melanjutkan Full hanya dengan DR & BDR saja.
- ✓ Exstart : terjadi pemilihan Master dan Slave, master adalah router yang memiliki router id tertinggi.
- ✓ exchange : terjadi pertukaran Database Descriptor (DBD) paket DBD ini digambarkan dari topologi DB router, proses dimulai oleh master
- ✓ loading : router akan memeriksa DBD dari router lain dan apabila ada entry yang tidak diketahui maka router akan mengira link state request (LSR) , LSR akan dibalas dengan link state state ACK dan link state reply, diakhir tahap ini semua router yang di adjacent memiliki topologi DB yang sama.
- ✓ Full : masing-masing router sudah membentuk hubungan yang Adjacency.

c. **Pemilihan DR & BDR pada Routing OSPF**

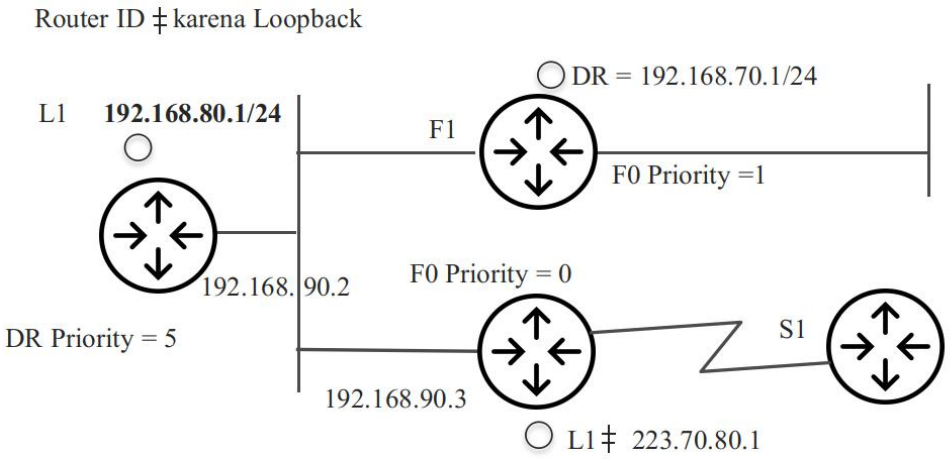
Dalam jaringan multi akses router-router akan memilih DR (designated router) dan BDR Backup designated router) dan berusaha adjacent dengan kedua router tersebut. Beberapa kondisi router pada saat melakukan pemilihan DR dan BDR adalah sebagai berikut:

1. Router melakukan pemilihan terhadap tipe network multi access, dengan melihat metode pengiriman (broadcast & non broadcast) Pemilihan dilakukan berdasarkan nilai (Router Priority dan Router ID)
2. Nilai Router priority diatur pada interface menggunakan range nilai 0-255, pada console router dengan cara mengetikan perintah : IP OSPF Priority [0-255]

```
Router#config t
Router(config)# int fa0/0
Router(config-if)# ip ospf priority
<0-255>  priority
Router(config-if)# ip ospf priority 2
```

3. Router yang diatur dengan nilai priority 0, maka router tidak akan menjadi DR/BDR, atau statusnya menjadi DROTHER, administrator dapat mengatur nilai priority yang tinggi apabila status router memungkinkan menjadi BR, semakin besar nilai priority maka akan semakin besar kemungkinan dipilih menjadi BR (Priority paling tinggi) dan BDR (kedua paling tinggi / slave). administrator dapat mengatur sesuai dengan prioritas manakah router yang lebih dulu UP.
4. Secara default penentuan router priority untuk semua router adalah : Apabila priority router sama maka yang digunakan untuk menentukan DR/BDR adalah Router ID, Pada tiap NT non broadcast (ex : Frame Relay) router yang menjadi DR adalah router yang memiliki link ke semua router yang lain (multipoint).

Apabila router yang memiliki status DR & BDR mati, maka router-router lain akan melakukan pemilihan agar dapat menggantikan router yang mati tersebut. Proses flooding adalah router dengan packet LSA harus meneruskan paket ke semua jaringan, dan memasukkan informasi LSA dalam databasenya , apabila paket yang diterima mengalami pengulangan dengan kesamaan paket sebelumnya, maka paket tersebut akan di drop, karna paket yang datang berulang ulang, akan dianggap sebagai flooding attack, karena seolah-olah membanjiri jaringan dengan LSA (link state advertisement). Setiap kali BD link state router berubah, maka router kembali akan menghitung rute terbaik dan membentuk tabel routing terbaru, dengan biaya terendah dan shortest path terpendek.



Gambar 9.4. Link state advertisement)

```
Router(config)#router ospf 1
Router(config-router)#default-information originate
```

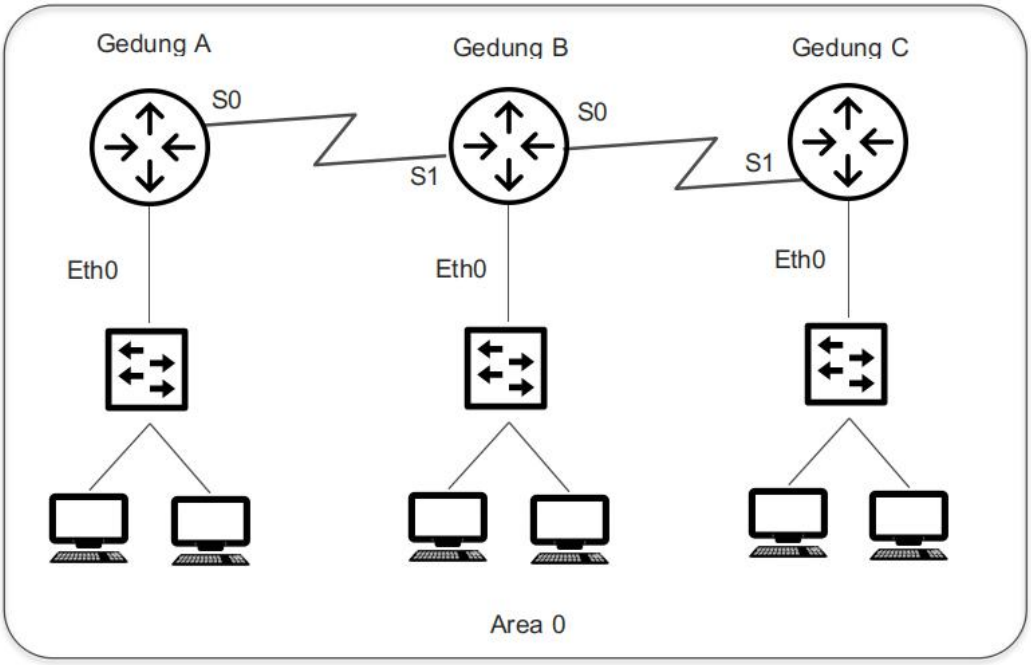
Perintah di atas hanya untuk default router Perintah redistribute static metric 100 – semua static routing akan didistribusikan

d. Konfigurasi Area OSPF

Setelah mengidentifikasi proses OSPF, kita perlu mengidentifikasi antarmuka yang ingin diaktifkan komunikasi OSPF serta area tempat masing-masing berada. Ini juga akan mengkonfigurasi jaringan yang akan di iklankan (advertise) kepada jaringan lain. Berikut adalah contoh konfigurasi dasar OSPF.

```
Router#config t
Router(config)# router ospf 1
Router(config-if)# network 10.0.0.0 0.255.255.255
    area ?
<0-4294967295> OSPF area ID as a decimal value
A.B.C.D OSPF area ID in IP address format
Router(config-router)# network 10.0.0.0 0.255.255.255
area 0
```

Berikut adalah contoh konfigurasi OSPF dengan menggunakan 3 router dalam 1 area OSPF



Gambar 9.5. Topologi OSPF 3 Router

Gedung A	Gedung B	Gedung C
eth0:192.168.10.65/29	eth0: 192.168.10.49/29	eth0: 192.168.10.17/29
s0:10.255.255.81/30	s1: 10.255.255.82/30	s0: 10.255.255.10/30
-	s0: 10.255.255.9/30	-

Alamat IP untuk setiap antarmuka ditunjukkan pada gambar. Gedung A memiliki dua subnet yang terhubung langsung: 192.168.10.64/29 dan 10.255.255.80/30. Berikut konfigurasi OSPF menggunakan wildcard:

```
Gedung_A#config t
Gedung_A(config)#router ospf 1
Gedung_A(config-if)#network 192.168.10.64 0.0.0.7 area 0
Gedung_A(config-if)#network 10.255.255.80 0.0.0.3 area 0
```

Router Gedung_A menggunakan mask /29 atau 255.255.255.248 pada antarmuka ethernet0. Ini adalah ukuran blok 8, yang merupakan wildcard 7. Antarmuka s0 adalah mask dari 255.255.255.252— ukuran blok 4, dengan wildcard 3. kita tidak dapat mengkonfigurasi OSPF dengan cara ini jika kita tidak dapat melihat alamat IP dan notasi garis miring, dengan cara ini kita dapat mengetahui subnet, mask, dan wildcard.

```
Gedung_B#config t
Gedung_B(config)#router ospf 1
Gedung_B(config-if)#network 192.168.10.48 0.0.0.7 area 0
Gedung_B(config-if)#network 10.255.255.80 0.0.0.3 area 0
Gedung_B(config-if)#network 10.255.255.8 0.0.0.3 area 0

Gedung_C#config t
Gedung_C(config)#router ospf 1
Gedung_C(config-if)#network 192.168.10.16 0.0.0.7 area 0
Gedung_C(config-if)#network 10.255.255.8 0.0.0.3 area 0
```

Seperti konfigurasi Gedung A, kita harus dapat menentukan subnet, mask, dan wildcard hanya dengan melihat alamat IP antarmuka. Jika kita tidak dapat melakukannya, maka kita tidak akan dapat mengkonfigurasi OSPF menggunakan wildcard .

e. Perintah Dasar OSPF

Untuk dapat memahami OSPF, administrator jaringan juga harus mengetahui perintah perintah dasar OSPF, adapun perintah dasar dapat dilihat dibawah ini.

- ✓ **Perintah show ip ospf**

Perintah show ip ospf digunakan untuk menampilkan informasi OSPF untuk satu atau semua proses OSPF yang berjalan di router. Informasi yang terkandung di dalamnya meliputi Router ID, informasi area, statistik SPF, dan informasi timer LSA.

```
Router#sh ip ospf
Routing Process "ospf 132" with ID 10.1.5.1
Start time: 04:32:04.116, Time elapsed: 01:27:10.156
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Router is not originating router-LSAs with maximum metric
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPFs 10000 msecs
Maximum wait time between two consecutive SPFs 10000 msecs
Incremental-SPF disabled
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msecs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
```

```
Retransmission pacing timer 66 msecs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Number of areas transit capable is 0
External flood list length 0
Area BACKBONE(0)
Number of interfaces in this area is 5
Area has no authentication
SPF algorithm last executed 00:14:52.220 ago
SPF algorithm executed 14 times
Area ranges are
Number of LSA 6. Checksum Sum 0x03C06F
Number of opaque link LSA 0. Checksum Sum 0x000000
Number of DCbitless LSA 0
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0
```

Perhatikan Router ID (RID) 10.1.5.1, yang merupakan alamat IP tertinggi yang dikonfigurasi pada router.

- ✓ **Perintah show ip ospf database**

Dengan menggunakan perintah show ip ospf database maka akan memberikan informasi database topologi yang saya sebutkan sebelumnya). Berbeda dengan perintah topologi show ip eigrp, perintah ini menunjukkan "router OSPF", bukan setiap tautan di AS seperti yang dilakukan EIGRP.

```
Router#sh ip database

       OSPF Router with ID (10.1.5.1) (Process ID 132)

                Router Link States (Area 0)

Link ID    ADV Router      Age  Seq#       Checksum   Link count
10.1.5.1   10.1.5.1        72   0x80000002 0x00F2CA   9
10.1.7.1   10.1.7.1        83   0x80000004 0x009197   6
10.1.9.1   10.1.9.1        73   0x80000001 0x00DA1C   4
10.1.11.1  10.1.11.1       67   0x80000005 0x00666A   4
```

```
10.1.12.1  10.1.12.1   67   0x80000004   0x007631   2

                Net Link States (Area 0)

Link ID    ADV          Age  Seq#         Checksum
           Router

10.1.11.2  10.1.12.1   68   0x80000001   0x00A337
```

Kita dapat melihat kelima router dan RID dari setiap router (alamat IP tertinggi di setiap router). Keluaran router menunjukkan ID tautan—ingat bahwa antarmuka juga merupakan tautan—dan RID router pada tautan tersebut di bawah router ADV, atau router advertise.

✓ **Perintah show ip ospf interface**

Perintah show ip ospf interface menampilkan semua informasi OSPF yang berhubungan dengan interface. Data ditampilkan tentang informasi OSPF untuk semua antarmuka atau untuk antarmuka tertentu.

```
Router#sh ip ospf interface f0/1
FastEthernet0/1 is up, line protocol is up
Internet Address 10.1.1.1/24, Area 0
Process ID 132, Router ID 10.1.5.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 10.1.5.1, Interface address 10.1.1.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
oob-resync timeout 40
Hello due in 00:00:01
Supports Link-local Signaling (LLS)
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
```

Informasi berikut adalah bagian dari seluruh informasi yang ditampilkan dari perintah sh ip ospf interface

- Interface IP address
- Area assignment
- Process ID
- Router ID
- Network type
- Cost
- Priority

- DR/BDR election information (if applicable)
- Hello and Dead timer intervals
- Adjacent neighbor information

✓ **Perintah show ip ospf neighbor**

Perintah show ip ospf neighbour sangat berguna karena meringkas informasi OSPF terkait dengan neighbour dan status adjacency. Jika ada DR atau BDR, informasi itu juga akan ditampilkan. Ini contohnya:

```
Router#sh ip ospf neighbor

Neighbor ID  Pri  state  Dead Time   Address   Interface
10.1.11.1    0    FULL/  - 00:00:37 10.1.5.2  Serial0/2/0
10.1.9.1     0    FULL/  - 00:00:34 10.1.4.2  Serial0/1/0
10.1.7.1     0    FULL/  - 00:00:38 10.1.3.2  Serial0/0/1
10.1.7.1     0    FULL/  - 00:00:34 10.1.2.2  Serial0/0/0
```

✓ **Perintah show ip protocols**

Perintah show ip protocols juga berguna, apakah Anda menjalankan OSPF, EIGRP, IGRP, RIP, BGP, IS-IS, atau protokol perutean lainnya yang dapat dikonfigurasi di router Anda. Ini memberikan gambaran yang sangat baik dari operasi sebenarnya dari semua protokol yang sedang berjalan.

```
Router#sh ip protocol
Routing Protocol is "ospf 132"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 10.1.5.1
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
10.1.1.1 0.0.0.0 area 0
10.1.2.1 0.0.0.0 area 0
10.1.3.1 0.0.0.0 area 0
10.1.4.1 0.0.0.0 area 0
10.1.5.1 0.0.0.0 area 0
Reference bandwidth unit is 100 mbps
Routing Information Sources:
```

```
Gateway    Distance  Last Update
10.1.11.1  110       00:28:53
10.1.11.2  110       00:28:53
10.1.9.1   110       00:28:53
10.1.7.1   110       00:28:53
Distance: (default is 110)
```

Dari melihat keluaran ini, Anda dapat menentukan ID Proses OSPF, ID Router OSPF, jenis area OSPF, jaringan dan area yang dikonfigurasi untuk OSPF, dan ID Router OSPF

9.5. Rangkuman

1. OSPF (Open Shortest Path First) adalah protokol routing dinamis yang digunakan untuk mengatur jalur dalam jaringan IP. OSPF dirancang untuk mengoptimalkan pengiriman data dengan menghitung jalur terpendek menggunakan algoritma Dijkstra.
2. Fitur OSPF yaitu Hierarchical Design: OSPF mendukung desain jaringan hierarkis dengan membagi jaringan menjadi area untuk efisiensi. Link-State Protocol: OSPF menggunakan informasi status tautan untuk membangun dan memperbarui tabel routing. Scalability: OSPF dapat menangani jaringan besar dengan banyak router dan subnet. Support for VLSM/CIDR: OSPF mendukung Variable Length Subnet Masking (VLSM) dan Classless Inter-Domain Routing (CIDR).
3. Terminologi dalam OSPF antara lain: Router ID: Identifikasi unik untuk setiap router dalam OSPF. Area: Subset dari jaringan OSPF yang membantu dalam pengelompokan dan pengelolaan routing. Link State Advertisement (LSA): Pesan yang digunakan oleh router untuk berbagi informasi tentang status tautan dengan router lain.
4. Proses Routing OSPF dimulai dari Pengumpulan Informasi: Router mengumpulkan informasi tentang tautan dan status dari router tetangga. Perhitungan SPF: Menggunakan algoritma Dijkstra untuk menghitung jalur terpendek berdasarkan informasi yang diterima. Pembaruan Tabel Routing: Router memperbarui tabel routing mereka berdasarkan hasil perhitungan SPF.
5. Konfigurasi OSPF: Perintah Dasar: Menggunakan perintah seperti untuk mengaktifkan OSPF pada router. Pengaturan Area: Mengidentifikasi dan mengkonfigurasi area OSPF untuk setiap antarmuka yang terhubung. Redistribusi Rute: Mengizinkan redistribusi rute dari protokol lain ke OSPF menggunakan perintah.
6. Kelebihan OSPF: Kecepatan Konvergensi: OSPF memiliki waktu konvergensi yang cepat dibandingkan dengan protokol routing lainnya. Multi-Vendor Support: OSPF adalah protokol standar terbuka yang dapat digunakan di berbagai perangkat dari vendor yang

berbeda. Autentikasi: OSPF mendukung mekanisme autentikasi untuk meningkatkan keamanan.

7. Kekurangan OSPF: Konsumsi Sumber Daya: OSPF dapat mengkonsumsi lebih banyak CPU dan memori dibandingkan dengan protokol routing lainnya. Kompleksitas Konfigurasi: Memerlukan perencanaan dan desain yang matang untuk implementasi yang efektif.

9.6. Latihan Soal

1. Apa kepanjangan dari OSPF?
a) Open Shortest Path First
b) Open Standard Path Forwarding
c) Optimal Shortest Path First
d) Open Source Path Finding
e) Open System Path Forwarding

2. Apa yang menjadi keunggulan utama OSPF dibandingkan dengan protokol routing lainnya?
a) Menggunakan metrik hop count
b) Mendukung VLSM dan CIDR
c) Hanya dapat digunakan dalam jaringan kecil
d) Tidak memerlukan konfigurasi
e) Menggunakan metode distance-vector

3. Apa yang dimaksud dengan "area" dalam konteks OSPF?
a) Sebuah subnet yang terpisah
b) Bagian dari jaringan yang memiliki topologi yang sama
c) Jaringan yang tidak terhubung
d) Sebuah protokol routing
e) Alamat IP yang digunakan

4. Algoritma apa yang digunakan oleh OSPF untuk menentukan rute terbaik?
a) Bellman-Ford
b) Dijkstra
c) A*
d) Floyd-Warshall
e) Prim

5. Apa yang dilakukan OSPF untuk meminimalkan lalu lintas pembaruan routing?
a) Menggunakan broadcast
b) Menggunakan multicast pada perubahan

c) Menggunakan unicast
d) Menggunakan static routing
e) Menggunakan periodic updates

6. OSPF adalah protokol routing jenis:
a) Distance Vector
b) Link State
c) Hybrid
d) Static
e) Dynamic

7. OSPF mendukung pengalamatan:
a) Hanya IPv4
b) Hanya IPv6
c) IPv4 dan IPv6
d) Hanya alamat IP statis
e) Hanya alamat IP dinamis

8. Apa yang dimaksud dengan router OSPF yang berfungsi sebagai Designated Router (DR)?
a) Router yang mengelola semua lalu lintas data
b) Router yang bertanggung jawab untuk mengumpulkan dan mendistribusikan informasi routing
c) Router yang tidak aktif dalam jaringan
d) Router yang hanya digunakan untuk pengujianE. Router yang menghubungkan beberapa jaringan

9. Dalam OSPF, berapa banyak bit yang digunakan untuk mengidentifikasi area?
a) 8 bit
b) 16 bit
c) 24 bit
d) 32 bit
e) 64 bit

10. Apa yang dimaksud dengan Link State Advertisement (LSA) dalam OSPF?
a) Proses pengiriman data
b) Informasi yang dibagikan oleh router OSPF untuk menginformasikan status link
c) Protokol untuk mengamankan data
d) Alamat IP yang digunakan untuk routing
e) Proses penghapusan rute yang tidak digunakan

Soal Esai

11. Jelaskan bagaimana OSPF membagi jaringan menjadi area dan mengapa hal ini penting untuk skalabilitas.
12. Diskusikan proses konvergensi OSPF dan bagaimana algoritma Dijkstra berperan dalam proses tersebut.
13. Analisis keuntungan dan kerugian menggunakan OSPF dalam jaringan besar dibandingkan dengan protokol routing lainnya seperti RIP.
14. Deskripsikan langkah-langkah yang diperlukan untuk mengkonfigurasi OSPF pada router Cisco.
15. Berikan contoh situasi di mana OSPF lebih menguntungkan dibandingkan dengan protokol routing lainnya, dan jelaskan alasannya.

9.7. Daftar Pustaka

Januari, R. (2022). *Cisco Networking: Panduan Lengkap Routing dan Switching*. Yogyakarta: Graha Ilmu.

Lestari, N. (2022). *Pengenalan dan Implementasi Routing serta Switching pada Jaringan Cisco.* Jakarta: Elex Media Komputindo.

BAB 10

ENHANCED INTERIOR GATEWAY ROUTING PROTOCOL (EIGRP)

10.1. Pendahuluan EIGRP

EIGRP merupakan protokol routing dengan menyempurnakan protokol distance-vector dengan menggunakan algoritma Diffused Update Algorithm (DUAL) untuk mencari jalur terpendek dalam jaringan. EIGRP adalah protokol routing propietary dari Cisco yang artinya protokol ini hanya tersedia pada vendor cisco.

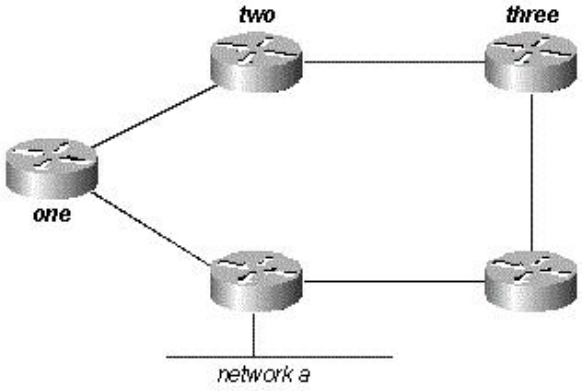
EIGRP merupakan salah satu protokol routing yang memiliki keunggulan sebagai berikut:

1. Mendukung jaringan dengan IPv4 dan IPv6.
2. Mampu menangani jaringan dalam skala besar.
3. Memiliki waktu konvergensi yang sangat cepat saat terjadi perubahan topologi jaringan.
4. Efisiensi dalam penggunaan bandwidth dimana hanya informasi tentang perubahan topologi yang akan dikirimkan, bukan seluruh tabel routing.
5. Mendukung VLSM (Variable Length Subnet Masking) guna mengalokasikan alamat IP secara lebih efisien.
6. Mendukung summarisasi routing.
7. EIGRP menggunakan teknik split horizon untuk mencegah terjadinya loop dalam topologi jaringan sehingga aka mengurangi terjadinya loop dan membantu menjaga kestabilan jaringan.

Meskipun protokol EIGRP memiliki keunggulan, namun EIGRP memiliki beberapa kekurangan yaitu:

1. Propietary cisco juga menjadi kekurangan dari EIGRP dimana protokol ini hanya dapat diimplementasikan antar perangkat cisco dan memiliki keterbatasan terhadap vendor lain.
2. EIGRP membutuhkan sumbet daya perangkat keras yang signifikan pada beberapa perangkat.
3. Meskipun EIGRP memiliki kecepatan dalam konvergensi, dalam beberapa kondisi topologi yang kompleks, konvergensi mungkin tidak secepat yang diinginkan.
4. EIGRP tidak memiliki dukungan natif yang kuat untuk protokol non cisco atau protokol dinamik lainnya.

Umumnya protokol routing berbasis distance vector menyimpan informasi saat menghitung jalur terbaik ke tujuan seperti jarak (total metrik atau jarak seperti jumlah hop atau lompatan) dan vector (lompatan berikutnya). Misalnya untuk routing information protocol (RIP) seperti gambar berikut ini, semua router menjalankan RIP. Router 2 akan memilih jalur menuju jaringan A dengan menghitung jumlah hop atau lompatan setiap jalur yang tersedia.



Gambar 10.1. Contoh topologi

Berdasarkan gambar diatas, karena jalur melalui router 3 adalah tiga lompatan, dan jalur melalui router satu adalah dua lompatan, router dua akan memilih jalur melalui router satu. dan membuang informasi yang dipelajari melalui router tiga. Jika jalur antara router satu dan jaringan A terputus, maka router dua akan kehilangan semua informasi konektivitas dengan tujuan hingga tiga kali update dimana update terjadi setiap 30 detik. Router tiga akan mengiklankan ulang rute ke network A setelah 30 detik sehingga total waktu yang dibutuhkan untuk mengalihkan jalur dari router satu ke router tiga adalah antara 90 sampai 120 detik.

EIGRP tidak bergantung pada pembaruan periodik penuh untuk melakukan konvergensi ulang, melainkan membangun tabel topologi dari masing-masing iklan router tetangganya (data tidak dibuang) dan melakukan konvergensi dengan mencari kemungkinan rute bebas loop dalam tabel topologi, jika tidak menemukan rute lain, EIGRP akan menanyakan kepada router tetangganya. Dalam hal ini, router dua akan menerima informasi dari router satu dan tiga. EIGRP akan menggunakan jalur satu sebagai jalur utamanya dan jalur melalui router tiga sebagai jalur backup. Ketika jalur melalui router satu tidak tersedia, maka EIGRP akan dapat mengguanakan jalur melalui router tiga tanpa harus menghitung ulang metrik untuk menemukan jalur terdekat seperti RIP.

Berikut ini adalah karakteristik dari routing protokol EIGRP:

1. EIGRP hanya akan mengirimkan pembaruan yang diperlukan saja dan pada waktu tertentu. Hal ini dapat dilakukan melalui penemuan dan pemeliharaan router tetangga.
2. EIGRP memiliki cara untuk menentukan jalur mana yang telah dipelajari dan jalur tersebut bebas loop.

3. EIGRP mampu menghapus route yang buruk dari tabel topologi semua router yang ada didalam jaringan.
4. EIGRP mampu mencari tetangga untuk menemukan jalur menuju tujuan yang hilang.

Sebuah router yang mengaktifkan EIGRP harus menjadi tetangga terlebih dahulu sebelum bertukar infomasi routing. Untuk menemukan tetangga secara dinamis, router EIGRP menggunakan alamat multicast 224.0.0.10. Setiap router EIGRP menyimpan informasi routing dan topologi dalam 3 (tiga) tabel yaitu:

1. Neighbor table yang digunakan untuk menyimpan informasi tentang router tetangga EIGRP.
2. Topology table yang digunakan untuk menyimpan informasi routing yang telang dipelajari dari router tetangga.
3. Routing table yang digunakan untuk menyimpan informasi jalur terbaik untuk mencapai tujuan.

EIGRP memiliki nilai AD 90 dimana nilainya lebih kecil dari nilai AD protokol routing RIP dan OSPF sehingga jalur yang ditemukan akan dipilih dan digunakan untuk meneruskan paket yang masuk ke router. EIGRP menggunakan Reliable Transport Protocol (RTP) untuk mengirimkan pesan. EIGRP menghitung metrik menggunakan bandwidth, delay, reliability dan load jaringan. Secara default, hanya bandwidth dan delay yang digunakan saat menghitung metrik ketika nilai reliability dan load bernilai 0. EIGRP menggunakan konsep autonomous system (AS). Sebuah AS merupakan sekumpulan router yang mengaktifkan EIGRP dan harus menjadi tetangga EIGRP. Setiap router didalam AS harus memiliki nomor AS yang sama, jika tidak, maka router tidak akan menjadi tetangga.

10.1.1. Tetangga router EIGRP

EIGRP herus membangun koneksi dengan tetangga EIGRP yang lain sebelum melakukan pertukaran informasi routing. Untuk membangun konektivitas dengan sebuah tetangga, router mengirimkan pesan *hello packet* setiap beberapa detik. *Hello packet* dikirim menggunakan alamat multicast 224.0.0.10. Pada interface LAN, *hello packet* dikirim setiap 5 detik, sedangkan pada *interface* WAN *hello packet* dikirim setiap 60 detik. Berikut ini adalah isi dari pesan *hello packet* dan harus identik untuk menjadi tetangga router EIGRP yaitu:

1. ASN (*autonomous system number*)
2. Subnet number
3. K value (merupakan komponen dari metrik EIGRP)

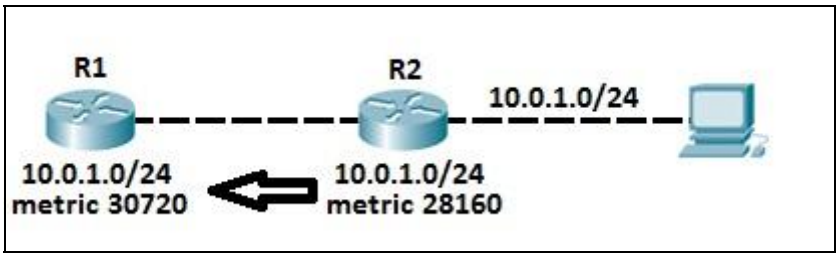
Router EIGRP mengirimkan pesan *hello packet* setiap beberapa detik untuk menjamin bahwa router tetangga yang terhubung tetap aktif. Secara default router EIGRP akan menganggap router tetangga sudah tidak aktif apabila timer *hold down* sudah habis. Timer *hold down*

secara default adalah 3 kali interval dari paket hello. Pada jaringan LAN, *hold timer* adalah 15 detik.

Istilah lain yang digunakan dalam protokol routing EIGRP adalah feasible dan reported distance.

- ✓ Feasible distance (FD) merupakan metrik atau jalur terbaik untuk mencapai jaringan tujuan. Route ini akan masuk kedalam tabel routing.
- ✓ Reported distance (RD) merupakan iklan metrik dari router tetangga untuk jalur tertentu. Dengan kata lain, metrik ini digunakan oleh router tetangga untuk menuju ke jaringan tujuan.

Untuk memahami konsep diatas, perhatikan gambar berikut ini.



Gambar 10.2. Metrik untuk memahami FD dan RD

EIGRP sudah dikonfigurasi pada R1 dan R2. R2 terhubung langsung dengan subnet 10.0.1.0/24 dan mengiklankan subnet tersebut ke EIGRP. Misalkan metrik R2 untuk mencapai subnet tersebut adalah 28160. Ketika R2 mengiklankan subnet ke R1, R2 menginformasikan kepada R1 bahwa untuk mencapai jaringan 10.0.1.0/24 adalah 28160. Dari perspektif R1, metrik tersebut adalah sebagai *reported distance.* R1 menerima update dan memasukkan metrik dari tetangga ke dalam reported distance. Metrik tersebut sebagai *feasible distance* dan akan disimpan pada tabel routing R1 (dalam hal ini metrik nya 30720). *Feasible* dan *reported distance* dalam tabel topologi EIGRP router 1 ditampilkan sebagai berikut:

```
R1#show ip eigrp topology
IP-EIGRP Topology Table for AS 1/ID(192.168.0.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 10.0.1.0/24, 1 successors, FD is 30720
         via 192.168.0.2 (30720/28160), FastEthernet0/0
P 192.168.0.0/24, 1 successors, FD is 28160
         via Connected, FastEthernet0/0
```

Istilah lain yang digunakan dalam protokol routing EIGRP adalah *successor dan feasible successor. Succesor* merupakan rute dengan metrik terbaik untuk menuju tujuan yang

disimpan dalam tabel routing. Sedangkan *feasible successor* merupakan jalur backup untuk menuju tujuan yang sama dan digunakan saat rute *successor* tidak tersedia. Rute backup ini disimpan dalam tabel topologi.

Untuk menampilkan tetang dari router yang menaktifkan EIGRP dapat menggunakan perintah berikut ini.

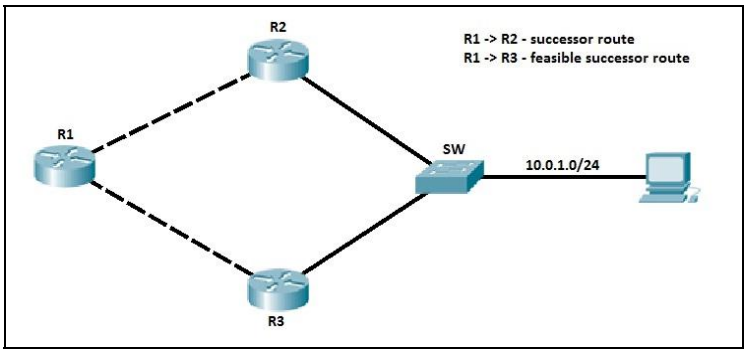
```
router#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address         Interface   Hold Uptime   SRTT   RTO  Q  Seq  Type
                                           (sec)         (ms)       Cnt Num
1   10.1.1.2        Et1           13 12:00:53   12   300  0  620
0   10.1.2.2        S0           174 12:00:56   17   200  0  645

rp-2514aa#show ip eigrp neighbor
IP-EIGRP neighbors for process 1
H   Address         Interface   Hold Uptime   SRTT   RTO  Q  Seq  Type
                                           (sec)         (ms)       Cnt Num
1   10.1.1.2        Et1           12 12:00:55   12   300  0  620
0   10.1.2.2        S0           173 12:00:57   17   200  0  645

rp-2514aa#show ip eigrp neighbor
IP-EIGRP neighbors for process 1
H   Address         Interface   Hold Uptime   SRTT   RTO  Q  Seq  Type
                                           (sec)         (ms)       Cnt Num
1   10.1.1.2        Et1           11 12:00:56   12   300  0  620
0   10.1.2.2        S0           172 12:00:58   17   200  0  645
```

10.1.2. Tabel topologi EIGRP

Tabel topologi EIGRP berisi semua route ke sebuah tujuan yang telah dipelajari. Tabel ini berisi informasi semua route yang diterima dari router tetangga, *successor* dan *feasible successor* dari setiap rute, dan interface tempat pembaruan diterima. Tabel ini juga menampung semua subnet yang terhubung langsung dan disertakan dalam proses EIGRP. Rute terbaik (*successor*) dari tabel topologi disimpan dalam tabel *routing. Feasible successor* hanya disimpan dalam tabel topologi dan dapat digunakan langsung jika jalur utama tidak tersedia. Untuk lebih memahami, perhatikan gambar berikut ini.

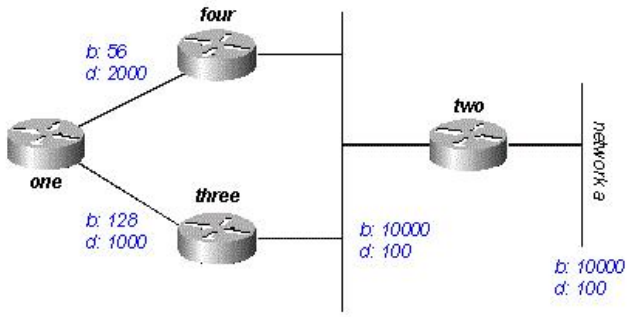


Gambar 10.3. Topologi untuk memahami feasible successor

EIGRP aktif pada 3 (tiga) router R1, R2 dan R3. Router R2 dan R3 keduanya terhubung ke subnet 10.0.1.0/24 dan mengiklankan subnet tersebut ke R1. R1 akan menerima kedua informasi tersebut dan akan menghitung metrik untuk mendapatkan jalur terbaik. Misalkan jalur terbaik adalah jalur melalui R2, maka R1 akan menyimpan route melalui R2 kedalam tabel *routing*. Router R1 juga menghitung metrik jalur melalui R3, anggaplah jalur R3 memiliki nilai yang kurang baik dari *feasible distance* jalur terbaik. Maka R1 akan menyimpannya kedalam tabel topologi sebagai *feasible successor route* yang dapat digunakan secara langsung jika jalur utama tidak tersedia.

10.1.3. Metrik EIGRP

EIGRP menggunakan minimum bandwidth pada sebuah jalur dan total delay untuk menghitung metrik routing. Tidak direkomendasikan untuk melakukan konfigurasi metrik lain karena dapat menyebabkan terjadi *routing loop* pada jaringan. Metrik bandwidth dan delay ditentukan dari nilai yang dikonfigurasi pada interface router menuju jaringan tujuan. Sebagai contoh, pada gambar berikut ini, Router 1 (satu) menghitung metrik jalur menuju jaringan A.



Gambar 10.4. Topologi dengan metrik EIGRP

Berdasarkan gambar diatas, dari touter satu, jalur menuju jaringan A dapat dilakukan melalui router tiga dan router empat. Jalur melalui router empat memiliki bandwidth 56 dan total delay 2200, sedangkan jalur melalui router tiga memiliki bandwidth minimum 128 dan delay 1200. Maka router satu akan memilih jalur dengan metrik terendah. Untuk menghitung metrik EIGRP menggunakan formula sebagai berikut:

```
Metrik = ([K1 * bandwidth + (K2 * bandwidth) / (256 - load) +
K3 * delay] * [K5 / (reliability + K4)]) * 256

bandwidth = (10.000.000/bandwidth(i)) * 256
```

dimana bandwidth (i) merupakan bandwidth paling kecil semua interface pada router dalam satuan kilobits.

```
delay = delay(i) * 256
```

dimana delay(i) merupakan total delay pada interface dari sebuah router menuju jaringan tujuan dalam satuan mikro detik. Untuk melihat delay dapat dilakukan dengan menjalankan perintah **show ip eigrp topology** atau **show interface.**

Penentuan nilai K harus hati-hati karena apabila salah akan menyebabkan konektivitas antar tetanggga tidak dapat dibangun. Jika nilai K5 = 0, maka formula metrik berubah menjadi:

```
Metrik = ([K1 * bandwidth + (k2 * bandwidth) / (256 - load) +
K3 * delay]) * 256
```

Nilai default dari K adalah : K1 = 1, K2 = 0, K3 = 1, K4 = 0, dan K5 = 0.

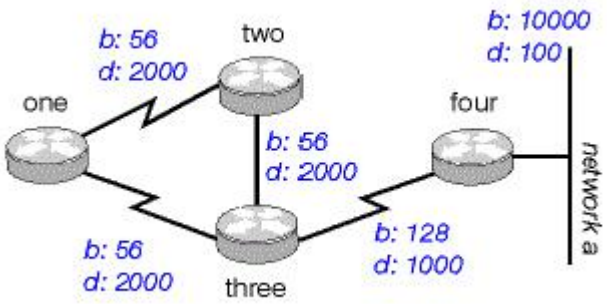
Jadi berdasarkan topologi sebelumnya, metrik melalui router empat adalah:

Minimum bandwidt = 56k
Total delay = 100 + 100 + 2000 = 2200
Metrik = [(10.000.000/56) + 2200] * 256 = (178571 + 2200) * 256 = 180771 * 256 = **46277376**

Sedangkan metrik melalui router tiga adalah:
Minimum bandwidth = 128k
Total delay = 100 + 100 + 1000 + 1200
Metrik = [(10.000.000/128) + 1200] * 256 = (78125 + 1200) * 256 = 79325 * 256 = **20307200**

Berdasarkan perhitungan metrik diatas jalur router satu menuju ke jaringan A digunakan jalur melalui router tiga karena memiliki metrik yang lebih kecil, namun apabila jalur melalui router tiga tidak tersedia maka paket akan diteruskan melalui router empat sebagai jalur backup.

EIGRP juga mampu menemukan route yang bebas loop. Routing loop adalah suatu kondisi dimana paket yang masuk ke dalam router akan bolak balik antara dua router karena kesalahan konfigurasi atau informasi routing. Sebagai contoh, perhatikan topologi pada gambar berikut ini.



Gambar 10.5. Topologi dengan kemungkinan routing loop

Berdasarkan gambar pada topologi, untuk mencapai network A dapat melalui semua router yang ada. Router tiga mendapatkan informasi menuju network A melalui router empat, router dua (rutenya dua, satu, tiga, empat) dan router satu (routenya satu, dua, tiga, empat). Jika router tiga menerima semua informasi dan menggunakannya maka akan terjadi routing loop. Router tiga akan mengira bahwa untuk mencapai network A melalui router dua, namun router dua mendapatkan informasi rute menuju network A melalui router tiga. Untuk mengatasi permasalahan tersebut, protokol routing EIGRP menerapkan teknologi *split horizondan poison reverse.*

EIGRP mendukung summarisasi manual dan auto. Summarisasi merupakan teknik yang digunakan dalam routing untuk menggabungkan beberapa route menjadi satu sehingga dapat menghemat tabel routing.

10.2. Implementasi EIGRP menggunakan cisco packet tracer

Untuk mengkonfigurasi routing protokol EIGRP dapat dilakukan dengan mudah. Langkah pertama adalah mengaktifkan protokol EIGRP. Langkah berikutnya adalah konfigurai detail EIGRP. Berikut ini adalah langkah-langkah lengkap konfigurasi protokol routing EIGRP.

1. Mengaktifkan routing EIGRP

Untuk mengaktifkan EIGRP, jalankan perintah berikut ini pada mode global configuration

```
Router(config)# router eigrp AS_number
```

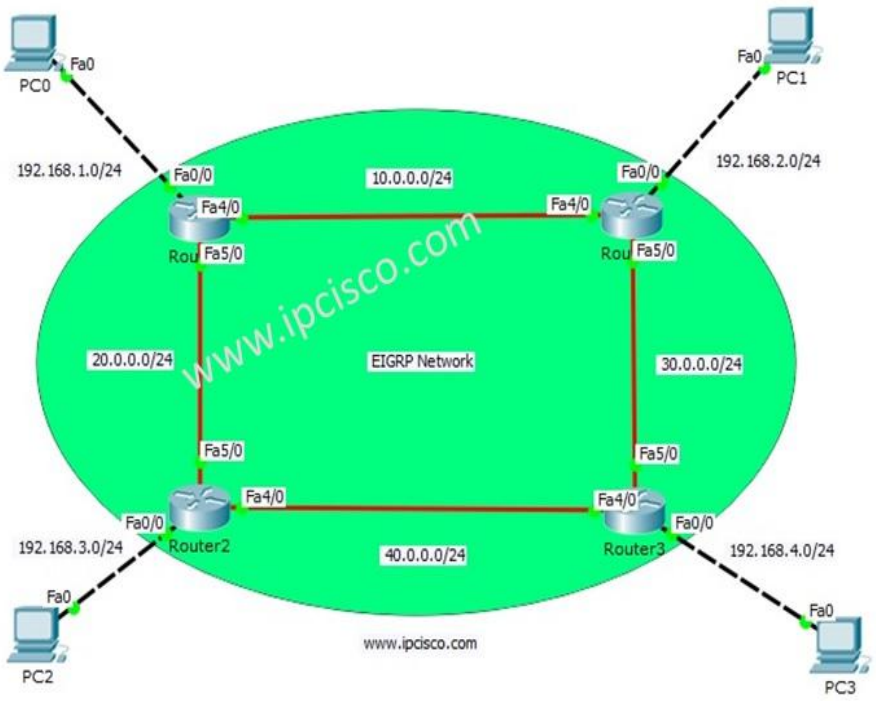
Perintah diatas digunakan untuk mengaktifkan protokol routing EIGRP. Untuk mengaktifkan EIGRP membutuhkan nomor AS yang digunakan untuk membuat grup router yang dapat bertukar informasi routing. Nomor AS yang dapat digunakan adalah range 1 sampai 65535. Setelah menentukan nomor AS, berikutnya nomor AS ini akan digunakan pada semua router. Jika dua router memiliki nomor AS yang berbeda, maka router tidak akan berbagi informasi routing.

2. Konfigurasi EIGRP

Gunakan perintah **network** untuk mendaftarkan jaringan yang terhubung langsung dengan router. Jaringan atau subnet yang boleh diakses perlu didaftarkan kedalam EIGRP agar dapat diakses oleh jaringan lain. Misal kita akan mendaftarkan subnet 172.16.0.0/24 kedalam routing EIGRP, maka dapat menggunakan perintah sebagai berikut:

```
Router(config-router)# network 172.16.0.0
```

Sebagai contoh, perhatikan gambar topologi berikut ini. Kita akan lakukan konfigurasi routing EIGRP pada semua router.



Gambar 10.6. Topologi contoh implementasi EIGRP

Berdasarkan topologi diatas, diasumsikan semua perangkat PC sudah terkonfigurasi sesuai dengan topologi. Kita akan mulai dengan konfigurasi EIGRP pada semua router mulai dari router 0, dilanjutkan dengan router1, router2 dan router3.

Konfigurasi IP address pada interface router0:

```
Router0(config)# interface FastEthernet0/0
Router0(config-if)# ip address 192.168.1.2 255.255.255.0
Router0(config-if)# no shutdown
Router0(config-if)# exit
```

```
Router0(config)# interface FastEthernet4/0
Router0(config-if)# ip address 10.0.0.1 255.255.255.0
Router0(config-if)# no shutdown
Router0(config-if)# exit
Router0(config)# interface FastEthernet5/0
Router0(config-if)# ip address 20.0.0.1 255.255.255.0
Router0(config-if)# no shutdown
Router0(config-if)# end
Router0# copy running-config startup-config
```

Konfigurasi IP address pada interface router1:

```
Router1(config)# interface FastEthernet0/0
Router1(config-if)# ip address 192.168.2.2 255.255.255.0
Router1(config-if)# no shutdown
Router1(config-if)# exit
Router1(config)# interface FastEthernet4/0
Router1(config-if)# ip address 10.0.0.2 255.255.255.0
Router1(config-if)# no shutdown
Router1(config-if)# exit
Router1(config)# interface FastEthernet5/0
Router1(config-if)# ip address 30.0.0.1 255.255.255.0
Router1(config-if)# no shutdown
Router1(config-if)# end
Router1# copy running-config startup-config
```

Konfigurasi IP address pada interface router2:

```
Router2(config)# interface FastEthernet0/0
Router2(config-if)# ip address 192.168.3.2 255.255.255.0
Router2(config-if)# no shutdown
Router2(config-if)# exit
Router2(config)# interface FastEthernet4/0
Router2(config-if)# ip address 40.0.0.1 255.255.255.0
Router2(config-if)# no shutdown
Router2(config-if)# exit
Router2(config)# interface FastEthernet5/0
Router2(config-if)# ip address 20.0.0.2 255.255.255.0
Router2(config-if)# no shutdown
Router2(config-if)# end
Router2# copy running-config startup-config
```

Konfigurasi IP address pada interface router3:

```
Router3(config)# interface FastEthernet0/0
Router3(config-if)# ip address 192.168.4.2 255.255.255.0
Router3(config-if)# no shutdown
Router3(config-if)# exit
Router3(config)# interface FastEthernet4/0
Router3(config-if)# ip address 40.0.0.2 255.255.255.0
Router3(config-if)# no shutdown
Router3(config-if)# exit
Router3(config)# interface FastEthernet5/0
Router3(config-if)# ip address 30.0.0.2 255.255.255.0
Router3(config-if)# no shutdown
Router3(config-if)# end
Router3# copy running-config startup-config
```

Selanjutnya kita mulai melakukan konfigurasi router untuk menjalankan routing protokol EIGRP. Untuk konfigurasi EIGRP, kita akan menggunakan nomor AS dengan perintah **router eigrp.** Setelah perintah **router eigrp** maka akan masuk ke dalam mode cinfiguration. Selanjutnya kita tambahkan alamat network dari masing-masing interface satu persatu. Dan terakhir kita tambahkan perintah **no auto-summary** untuk mencegak summarization otomatis pada tabel routing. Pada contoh kali ini kita gunakan nomor AS 100 untuk semua router.

Konfigurasi EIGRP pada router0:

```
Router0(config)# router eigrp 100
Router0(config-router)# network 192.168.1.0
Router0(config-router)# network 10.0.0.0
Router0(config-router)# network 20.0.0.0
Router0(config-router)# no auto-summary
Router0(config-router)# end
Router0# copy running-config startup-config
```

Konfigurasi EIGRP pada router1:

```
Router1(config)# router eigrp 100
Router1(config-router)# network 192.168.2.0
Router1(config-router)# network 10.0.0.0
Router1(config-router)# network 30.0.0.0
Router1(config-router)# no auto-summary
Router1(config-router)# end
Router1# copy running-config startup-config
```

Konfigurasi EIGRP pada router2:

```
Router2(config)# router eigrp 100
Router2(config-router)# network 192.168.3.0
Router2(config-router)# network 20.0.0.0
Router2(config-router)# network 40.0.0.0
Router2(config-router)# no auto-summary
Router2(config-router)# end
Router2# copy running-config startup-config
```

Konfigurasi EIGRP pada router3:

```
Router3(config)# router eigrp 100
Router3(config-router)# network 192.168.4.0
Router3(config-router)# network 30.0.0.0
Router3(config-router)# network 40.0.0.0
Router3(config-router)# no auto-summary
Router3(config-router)# end
Router3# copy running-config startup-config
```

Untuk melakukan verifikasi konfigurasi yang telah dilakukan, kita dapat menggunakan perintah show berikut ini:

- ✓ show ip eigrp
- ✓ show ip eigrp neigbors
- ✓ show ip eigrp interface
- ✓ show ip route eigrp
- ✓ show ip protocols

Sebagai contoh kita gunakan perintah **show ip eigrp neighbors** pada router1 dan router2 untuk melihat router tetangga dari masing-masing.

```
Router0# show ip eigrp neighbors
IP-EIGRP neighbors for process 100
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 10.0.0.2 Fa4/0 14 00:14:53 40 1000 0 12
1 20.0.0.2 Fa5/0 12 00:14:53 40 1000 0 11

Router1# show ip eigrp neighbors
IP-EIGRP neighbors for process 100
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 30.0.0.2 Fa5/0 14 00:16:57 40 1000 0 11
```

```
1 10.0.0.1 Fa4/0 13 00:16:57 40 1000 0 13
```

Berikutnya kita coba melihat status interface EIGRP dengan menggunakan perintah **show ip eigrp interfaces** pada router0 dan router1.

```
Router0# show ip eigrp interfaces
IP-EIGRP interfaces for process 100

Xmit Queue Mean Pacing Time Multicast Pending
Interface Peers Un/Reliable SRTT Un/Reliable Flow Timer Routes
Fa4/0 1 0/0 1236 0/10 0 0
Fa5/0 1 0/0 1236 0/10 0 0
Fa0/0 0 0/0 1236 0/10 0 0

Router1# show ip eigrp interfaces
IP-EIGRP interfaces for process 100

Xmit Queue Mean Pacing Time Multicast Pending
Interface Peers Un/Reliable SRTT Un/Reliable Flow Timer Routes
Fa4/0 1 0/0 1236 0/10 0 0
Fa5/0 1 0/0 1236 0/10 0 0
Fa0/0 0 0/0 1236 0/10 0 0
```

Berikutnya kita dapat melihat tabel topologi pada router0 dan router1 dengan menggunakan perintah **show ip eigrp topology.**

```
Router0# show ip eigrp topology
IP-EIGRP Topology Table for AS 100/ID(192.168.1.2)

Codes: P - Passive, A - Active, U - Update, Q - Query, R -
Reply,
r - Reply status

P 10.0.0.0/24, 1 successors, FD is 28160
via Connected, FastEthernet4/0
P 20.0.0.0/24, 1 successors, FD is 28160
via Connected, FastEthernet5/0
P 30.0.0.0/24, 1 successors, FD is 30720
via 10.0.0.2 (30720/28160), FastEthernet4/0
P 40.0.0.0/8, 1 successors, FD is 30720
via 20.0.0.2 (30720/28160), FastEthernet5/0
P 192.168.1.0/24, 1 successors, FD is 28160
```

```
via Connected, FastEthernet0/0
P 192.168.2.0/24, 1 successors, FD is 30720
via 10.0.0.2 (30720/28160), FastEthernet4/0
P 192.168.3.0/24, 1 successors, FD is 30720
via 20.0.0.2 (30720/28160), FastEthernet5/0
P 192.168.4.0/24, 1 successors, FD is 33280
via 10.0.0.2 (33280/30720), FastEthernet4/0

Router1# show ip eigrp topology
IP-EIGRP Topology Table for AS 100/ID(192.168.2.2)

Codes: P - Passive, A - Active, U - Update, Q - Query, R -
Reply,
r - Reply status

P 10.0.0.0/24, 1 successors, FD is 28160
via Connected, FastEthernet4/0
P 20.0.0.0/24, 1 successors, FD is 30720
via 10.0.0.1 (30720/28160), FastEthernet4/0
P 30.0.0.0/24, 1 successors, FD is 28160
via Connected, FastEthernet5/0
P 40.0.0.0/8, 1 successors, FD is 30720
via 30.0.0.2 (30720/28160), FastEthernet5/0
P 192.168.1.0/24, 1 successors, FD is 30720
via 10.0.0.1 (30720/28160), FastEthernet4/0
P 192.168.2.0/24, 1 successors, FD is 28160
via Connected, FastEthernet0/0
P 192.168.3.0/24, 1 successors, FD is 33280
via 10.0.0.1 (33280/30720), FastEthernet4/0
P 192.168.4.0/24, 1 successors, FD is 30720
via 30.0.0.2 (30720/28160), FastEthernet5/0
```

10.3. Troubleshooting konfigurasi EIGRP

Dalam melakukan troubleshooting protokol jaringan apapun, hal penting yang harus diperhatikan adalah langkah-langkah atau metodologi dalam melakukan troubleshooting. Aspek utama dalam melakukan torubleshooting protokol routing adalah memastikan memastikan komunikasi antar router. Komponen utama dalam melakukan troubleshooting EIGRP ada tiga yaitu:

1. Hubungan antar tetangga router EIGRP

2. Jalur yang ada di tabel routing EIGRP
3. Autentikasi EIGRP

Berikut ini adalah penjelasan dari tiga komponen utama dalam melakukan troubleshooting EIGRP.

1. Troubleshooting Konektivitas antar tetangga router EIGRP
Gunakan perintah **show ip eigrp** untuk memastikan koneksi antar tetangga antara 2 router aktif seperti berikut ini.

```
RouterX# show ip eigrp neighbors
IP-EIGRP neighbors for process 100
H   Address         Interface       Hold Uptime   SRTT  RTO  Q   Seq
                                    (sec)         (ms)       Cnt Num
1   10.23.23.2      Se0/0/1         13 00:02:26   29    2280 0   15
0   10.140.1.1      Se0/0/0         10 00:28:26   24    2280 0   25
```

Pastikan antar 2 router tetangga EIGRP share subnet IP yang terhubung langsung. Apabila subnet tetangga tidak tampil maka perlu dipastikan apakah konfigurasi alamat IP sudah benar dilakukan untuk kedua router. Gunakan perintah **shop interface <interface>** untuk verifikasi alamat IP seperti berikut ini.

```
RouterX# show ip interface fa0/0
FastEthernet0/0 is up, line protocol is up
  Internet address is 10.2.2.3/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound access list is not set
```

Perintah **network** pada saat konfigurasi EIGRP mengindikasikan router mana yang akan digunakan untuk routing protokol EIGRP. Gunakan perintah **show ip protocol** untuk memastikan network atau subnet mana saja yang sudah dikonfigurasi yang digunakan untuk routing EIGRP. Sebagai contoh, berikut ini interface dengan alamat 10.0.0.0 dan 192.168.1.0 digunakan pada routing EIGRP.

```
RouterX# show ip protocols
Routing Protocol is "eigrp 100"
```

```
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 100
--output omitted --
  Maximum path: 4
  Routing for Networks:
    10.0.0.0
    192.168.1.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    (this router)          90      00:01:08
    10.140.1.1             90      00:01:08
  Distance: internal 90 external 170
```

Perintah **show ip eigrp interface** dapat digunakan secara cepat untuk melihat interface mana yang aktif untuk routing EIGRP dan berapa banyak tetangga yang ditemukan pada setiap interface seperti contoh berikut ini.

```
RouterX# show ip eigrp interfaces
IP-EIGRP interfaces for process 100

              Xmit Queue   Mean   Pacing Time   Multicast    Pending
Int     Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Fa0/0     0        0/0         0       0/1            0           0
Se0/0/0   1        0/0        38      10/380        552           0
```

Router EIGRP membuat hubungan dengan router tetangga dengan bertukar paket **hello.** Field dalam paket **hello** harus sama sebelum hubungan router tetangga EIGRP dibangun yaitu nomor AS EIGRP dan nilai K. Kita dapat menggunakan perintah **debug eigrp packets** untuk memastikan informasi paket **hello** sesuai.

```
RouterX# debug eigrp packets

Mismatched adjacency values
01:39:13: EIGRP: Received HELLO on Serial0/0 nbr 10.1.2.2
01:39:13:AS 100, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0 peerQ
un/rely 0/0
```

```
01:39:13:        K-value mismatch
```

2. Troubleshooting tabel routing EIGRP

Jika hubungan router antar tetangga sudah terbangun, router akan dapat bertukar informasi. Jika tidak, maka langkah berikutnya yang harus dilakukan adalah melakukan troubleshooting tabel routing. Routing EIGRP ditandai dengan huruf "D" pada tabel routing yang mengindikasikan routing intra-AS, dan "D EX" untuk eksternal AS. Jika tidak ada tabel routing EIGRP artinya terdapat masalah pada layer 1 atau 2 pada router yang bertetangga. Sebagai contoh untuk melihat tabel routing EIGRP dapat menggunakan perintah **show ip route** yang dalam contoh ini merupakan routing intra-AS dan 10.3.3.0/24 adalah didistribusikan ulang oleh EIGRP (eksternal AS).

```
RouterX# show ip route
Codes: C - connected, S - static, 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

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
D       172.16.31.0/24 [90/40640000] via 10.140.1.1, 00:01:09, Serial0/0/0
O       172.16.31.100/32 [110/1563] via 10.140.1.1, 00:26:55, Serial0/0/0
     10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
C       10.23.23.0/24 is directly connected, Serial0/0/1
D EX      10.3.3.0/24 [170/40514560] via 10.23.23.2, 00:01:09, Serial0/0/1
C       10.2.2.0/24 is directly connected, FastEthernet0/0
```

Perintah **show ip eigrp topology** akan menampilkan ID router. ID router diperoleh dari alamat IP tertinggi yang di setting pada interface *loopback.* Jika tidak ada interface *loopback,* maka alamat IP tertinggi yang digunakan dalam interface yang aktif yang akan dipilih sebagai ID router. ID router tidak boleh sama dalam routing EIGRP karena akan menimbulkan masalah pada saat pertukaran informasi dan routing. Berikut ini adalah contoh output dari perintah **show ip eigrp topology.**

```
RouterX# show ip eigrp topology
IP-EIGRP Topology Table for AS(100)/ID(192.168.1.65)

Codes: P - Passive, A - Active, U - Update, Q - Query, R -
Reply,
       r - reply Status, s - sia Status

P 10.1.1.0/24, 1 successors, FD is 40514560
```

```
        via 10.140.1.1 (40514560/28160), Serial0/0/0
P 10.2.2.0/24, 1 successors, FD is 28160
        via Connected, FastEthernet0/0
P 10.3.3.0/24, 1 successors, FD is 40514560
        via 10.23.23.2 (40514560/28160), Serial0/0/1
P 10.23.23.0/24, 1 successors, FD is 40512000
        via Connected, Serial0/0/1
P 192.168.1.64/28, 1 successors, FD is 128256
        via Connected, Loopback0
P 192.168.1.0/24, 1 successors, FD is 40640000
        via 10.23.23.2 (40640000/128256), Serial0/0/1
P 10.140.2.0/24, 2 successors, FD is 41024000
        via 10.23.23.2 (41024000/40512000), Serial0/0/1
        via 10.140.1.1 (41024000/40512000), Serial0/0/0
P 10.140.1.0/24, 1 successors, FD is 40512000
        via Connected, Serial0/0/0
P 172.16.31.0/24, 1 successors, FD is 40640000
```

Secara default EIGRP merupakan protokol classfull dan mengaktifkan *network summarization.* Kita dapat menggunakan perintah **show ip protokol** untuk mengecek apakah automatic *network summarization* bekerja. Sebagai contoh berikut menampilkan hasil dari automatic network summarization.

```
RouterX# show ip protocols
Routing Protocol is "eigrp 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 100
  EIGRP NSF-aware route hold timer is 240s
  Automatic network summarization is in effect
  Automatic address summarization:
    192.168.1.0/24 for FastEthernet0/0, Serial0/0/0, Serial0/0/1
      Summarizing with metric 128256
    10.0.0.0/8 for Loopback0
      Summarizing with metric 28160
  Maximum path: 4
```

3. Troubleshooting atuentikasi EOGRP

Langkah terakhir troubleshooting EIGRP adalah terkait dengan autentikasi untuk memastikan autentikasi EIGRP sukses. Sebagai contoh, kita dapat menggunakan perintah **debug eigrp packets** untuk memastikan bahwa router X menerima paket EIGRP dengan autentikasi MD5 dan kunci ID 1 dari router Y.

```
RouterX# debug eigrp packets
EIGRP Packets debugging is on
    (UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK, STUB,
SIAQUERY, SIAREPLY)
*Jan 21 16:38:51.745: EIGRP: received packet with MD5 authentication,
key id = 1
*Jan 21 16:38:51.745: EIGRP: Received HELLO on Serial0/0/1 nbr
192.168.1.102
*Jan 21 16:38:51.745:    AS 100, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ
un/rely 0/0 peerQ
  un/rely 0/0
```

Hal yang sama untuk router Y dimana router Y menerima paket EIGRP dengan autentikasi MD5 dan kunci ID 2 dari router X.

```
RouterY# debug eigrp packets
EIGRP Packets debugging is on
    (UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK, STUB,
SIAQUERY,
SIAREPLY)
RouterY#
*Jan 21 16:38:38.321: EIGRP: received packet with MD5 authentication,
key id = 2
*Jan 21 16:38:38.321: EIGRP: Received HELLO on Serial0/0/1 nbr
192.168.1.101
*Jan 21 16:38:38.321:    AS 100, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ
un/rely 0/0 peerQ
  un/rely 0/0
```

Apabila atuentikasi tidak berhasil, maka output dari perintah debug eigrp packets adalah sebagai berikut:

```
RouterY# debug eigrp packets
EIGRP Packets debugging is on
    (UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK, STUB,
SIAQUERY, SIAREPLY)
RouterY#
```

```
*Jan 21 16:50:18.749: EIGRP: pkt key id = 2, authentication mismatch
*Jan 21 16:50:18.749: EIGRP: Serial0/0/1: ignored packet from
192.168.1.101, opc
ode = 5 (invalid authentication)
*Jan 21 16:50:18.749: EIGRP: Dropping peer, invalid authentication
*Jan 21 16:50:18.749: EIGRP: Sending HELLO on Serial0/0/1
*Jan 21 16:50:18.749:    AS 100, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ
un/rely 0/0
*Jan 21 16:50:18.753: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor
192.168.1.101
 (Serial0/0/1) is down: Auth failure
```

10.4. Rangkuman

1. EIGRP (Enhanced Interior Gateway Routing Protocol) adalah protokol routing yang dikembangkan oleh Cisco, menggabungkan fitur dari protokol distance-vector dan link-state. EIGRP digunakan untuk menemukan jalur terpendek dalam jaringan dengan menggunakan algoritma Diffused Update Algorithm (DUAL).
2. Fitur EIGRP: Dukungan untuk IPv4 dan IPv6: EIGRP dapat digunakan untuk jaringan yang menggunakan kedua versi protokol IP. Waktu Konvergensi Cepat: EIGRP memiliki waktu konvergensi yang sangat cepat saat terjadi perubahan topologi jaringan. Penggunaan Metrik Berbasis Beberapa Parameter: EIGRP menggunakan bandwidth, delay, reliability, dan load untuk menghitung metrik jalur.
3. Tabel Routing pada EIGRP: Tabel Topologi: Menyimpan semua rute yang dipelajari, termasuk successor dan feasible successor. Routing Table: Menyimpan rute terbaik (successor) yang digunakan untuk pengiriman data. Neighbor Table: Menyimpan informasi tentang router tetangga yang terhubung.
4. Proses EIGRP: Discovery: Router EIGRP mengirimkan paket hello untuk menemukan tetangga dan membangun hubungan. Update: Router mengirimkan pembaruan rute hanya ketika ada perubahan, bukan secara berkala. Query: Jika jalur utama tidak tersedia, router akan mengirimkan query untuk menemukan jalur cadangan.
5. Kelebihan EIGRP: Kecepatan Konvergensi: EIGRP dapat merespons perubahan topologi dengan cepat, mengurangi downtime. Efisiensi Bandwidth: Mengirimkan pembaruan rute hanya saat diperlukan, mengurangi penggunaan bandwidth. Dukungan untuk Rute Cadangan: EIGRP dapat menyimpan feasible successor sebagai jalur cadangan jika jalur utama tidak tersedia.
6. Kekurangan EIGRP: Proprietary: EIGRP adalah protokol proprietary dari Cisco, sehingga tidak dapat digunakan di perangkat dari vendor lain. Kompleksitas: Meskipun lebih mudah dibandingkan dengan OSPF, EIGRP masih memerlukan pemahaman yang baik tentang konsep routing.

7. EIGRP cocok untuk jaringan besar karena kemampuannya untuk menangani banyak rute dan cepat dalam konvergensi. EIGRP dapat mengelola rute dengan lebih efisien, termasuk penggunaan rute cadangan dan penghapusan rute yang buruk.
8. EIGRP lebih sederhana dalam konfigurasi dan memiliki waktu konvergensi yang lebih cepat. EIGRP lebih efisien dan dapat menangani jaringan yang lebih besar dengan lebih baik dibandingkan dengan RIP.

10.5. Latihan Soal

1. Apa yang menjadi keunggulan utama EIGRP dibandingkan dengan protokol routing lainnya?

a) Sederhana dan mudah dikonfigurasi
b) Menggunakan metrik hop count
c) Kecepatan konvergensi yang tinggi
d) Hanya mendukung IPv4
e) Tidak memerlukan bandwidth

2. Metrik apa saja yang digunakan oleh EIGRP untuk menentukan jalur terbaik?

a) Bandwidth dan hop count
b) Delay, load, dan reliability
c) Hanya bandwidth
d) Hanya delay
e) Hanya hop count

3. Apa yang dimaksud dengan "*feasible successors*" dalam EIGRP?

a) Rute utama yang sedang digunakan
b) Rute cadangan yang dapat digunakan jika rute utama gagal
c) Rute yang tidak valid
d) Rute yang memiliki metrik tertinggi
e) Rute yang tidak terhubung

4. Fitur apa yang memungkinkan EIGRP untuk mengurangi penggunaan bandwidth saat memperbarui informasi routing?

a) Route summarization
b) Split horizon
c) Route poisoning
d) Static routing
e) Dynamic routing

5. Apa yang harus dilakukan jika terjadi masalah dalam konvergensi EIGRP?

a) Menghapus semua rute
b) Memeriksa tabel routing dan tabel topologi

c) Mengganti protokol routing
d) Menonaktifkan EIGRP
e) Menggunakan protokol RIP

6. Algoritma yang digunakan oleh EIGRP untuk menentukan rute terbaik adalah:
a) Distance Vector
b) Link State
c) Diffused Update Algorithm (DUAL)
d) Path Vector
e) Bellman-Ford

7. Apa yang dimaksud dengan "load balancing" dalam konteks EIGRP?
a) Proses menghapus rute yang tidak digunakan
b) Proses mendistribusikan lalu lintas secara merata di beberapa rute
c) Proses meningkatkan kecepatan transfer data
d) Proses mengamankan jaringan
e) Proses mengatur koneksi fisik

8. Dalam EIGRP, K value digunakan untuk:
a) Menentukan kecepatan transfer data
b) Menghitung metrik rute
c) Mengatur koneksi fisik
d) Mengamankan data yang dikirim
e) Menghapus rute yang tidak digunakan

9. Apa yang terjadi jika dua router EIGRP memiliki nomor AS (Autonomous System) yang berbeda?
a) Router akan berbagi informasi routing
b) Router tidak akan berbagi informasi routing
c) Router akan terhubung secara otomatis
d) Router akan menghapus rute yang tidak digunakan
e) Router akan mengalami routing loop

10. EIGRP menggunakan alamat multicast untuk mengirimkan hello packets, yaitu:
a) 224.0.0.1
b) 224.0.0.5
c) 224.0.0.10
d) 239.255.255.255
e) 255.255.255.255

Soal Esai

11. Jelaskan bagaimana EIGRP menggabungkan fitur dari protokol distance-vector dan link-state dalam operasinya.
12. Diskusikan proses konvergensi EIGRP dan mengapa kecepatan konvergensi menjadi faktor penting dalam jaringan.
13. Deskripsikan langkah-langkah yang diperlukan untuk mengkonfigurasi EIGRP pada router Cisco.
14. Analisis kelebihan dan kekurangan EIGRP dibandingkan dengan protokol routing lainnya seperti RIP dan OSPF.
15. Berikan contoh situasi di mana penggunaan EIGRP lebih menguntungkan dibandingkan dengan protokol routing lainnya, dan jelaskan alasannya.

10.6. Daftar Pustaka

Academy, Cisco Networking Cisco Networking. (2020). *Switching, Routing, and Wireless Essentials Companion Guide (CCNAv7)*. London: Pearson Education.

Damanik, Hillman Akhyar, Merry Anggraeni, dan Farida Ayu Avisena Nusantar. (2023). *Konsep dan Penerapan Switching dan Routing Implementasi Jaringan Komputer Berbasis Cisco*. Jawa Barat: Mega Press Nusantara.

Wahyudi, Mochamad, Rachmat Adi Purnama, dan Firmansyah. (2019). *Cisco routing and switching Cisco routing and switching*. Yogyakarta: Graha Ilmu.

GLOSARIUM

A

Address Resolution Protocol (ARP)	:	Protokol yang digunakan untuk mengonversi alamat IP menjadi alamat MAC.
Administrative Distance	:	Ukuran keandalan rute yang ditentukan oleh protokol routing.
Alamat IP	:	Identifikasi unik untuk perangkat dalam jaringan, terdiri dari 32 bit untuk IPv4.
Application Layer:	:	Lapisan OSI yang berinteraksi langsung dengan aplikasi pengguna.
Area	:	Subset dari jaringan OSPF yang digunakan untuk mengurangi ukuran tabel routing.

B

Bandwidth	:	Kapasitas maksimum dari jalur komunikasi untuk mentransfer data dalam satuan waktu.

C

CIDR (Classless Inter-Domain Routing)	:	Metode pengalamatan yang memungkinkan penggunaan subnet mask yang lebih fleksibel.
Client-Server	:	Model arsitektur jaringan di mana satu perangkat (server) menyediakan layanan kepada perangkat lain (client)
Convergence	:	Proses di mana semua router dalam jaringan memiliki informasi routing yang sama

D

Data Link Layer:	:	Lapisan OSI yang bertanggung jawab untuk pengiriman data antar perangkat dalam satu jaringan.
Decapsulation	:	Proses menghapus header dan trailer saat data diterima.
Default Route	:	Rute yang digunakan ketika tidak ada rute spesifik yang ditemukan
Distance Vector Protocol	:	Protokol routing yang mengirimkan informasi tentang jarak ke tujuan
DR (Designated Router)	:	Router yang dipilih untuk mengurangi jumlah LSA yang dikirim dalam jaringan OSPF
DUAL (Diffusing Update Algorithm)	:	Algoritma yang digunakan oleh EIGRP untuk menentukan rute terbaik dan cadangan

Dynamic IP Address	:	Alamat IP yang diberikan secara otomatis oleh DHCP dan dapat berubah.
Dynamic Routing	:	Pengaturan rute secara otomatis oleh protokol routing

E

EIGRP	:	Protokol routing yang menggunakan algoritma DUAL untuk menentukan rute terbaik
EIGRP Authentication	:	Proses untuk memastikan bahwa informasi routing yang diterima adalah valid
EIGRP Hello Packets	:	Pesan yang digunakan untuk mendeteksi tetangga dalam EIGRP
EIGRP Load Balancing	:	Proses mendistribusikan lalu lintas secara merata di beberapa rute yang tersedia
EIGRP Metric Calculation		Proses menghitung metrik rute berdasarkan bandwidth, delay, load, dan reliability
Encapsulation	:	Proses membungkus data dengan header dan trailer pada setiap lapisan model OSI.

F

Feasible Successor	:	Rute cadangan yang dapat digunakan jika rute utama tidak tersedia
Floating Static Route	:	Rute statik yang memiliki prioritas lebih rendah dan hanya digunakan jika rute utama tidak tersedia

G

Gateway	:	Perangkat yang menghubungkan dua jaringan yang berbeda.

H

Hop Count	:	Metrik yang digunakan oleh RIP untuk menentukan jarak ke tujuan

I

Internet Layer	:	Lapisan dalam model TCP/IP yang bertanggung jawab untuk pengalamatan dan routing.
IP Addressing:	:	Proses memberikan alamat IP kepada perangkat dalam jaringan.

J

Jaringan Komputer	:	Kumpulan perangkat yang saling terhubung untuk berbagi data dan sumber daya.

K

K Value	:	Parameter yang digunakan oleh EIGRP untuk menghitung metrik rute

L

Latency	:	Waktu yang dibutuhkan untuk mengirimkan data dari sumber ke tujuan
Layer TCP/IP:	:	Tiga lapisan dalam model TCP/IP, yaitu Application, Transport, dan Internet.
Link Failure	:	Kejadian di mana jalur komunikasi antara dua perangkat tidak berfungsi.
Link State Protocol	:	Protokol routing yang mengumpulkan informasi tentang status link dari semua router
Loopback Address	:	Alamat IP khusus (127.0.0.1) yang digunakan untuk menguji koneksi jaringan pada perangkat itu sendiri.
LSA (Link State Advertisement)	:	Pesan yang digunakan oleh OSPF untuk berbagi informasi tentang status link

M

Model OSI	:	Kerangka kerja yang membagi proses komunikasi jaringan menjadi tujuh lapisan.

N

Network Devices	:	Perangkat yang digunakan untuk menghubungkan dan mengelola jaringan, seperti router, switch, dan hub
Network Architecture:	:	Desain keseluruhan dari jaringan, termasuk perangkat keras, perangkat lunak, dan protokol yang digunakan.
Network Layer:	:	Lapisan OSI yang mengatur pengalamatan dan routing paket data.
Next Hop	:	Alamat IP dari router berikutnya yang harus dilalui paket data untuk mencapai tujuan.

O

OSPF	:	Protokol routing link-state yang digunakan untuk jaringan besar.
OSPF Convergence	:	Proses di mana semua router OSPF memiliki informasi routing yang konsisten
OSPF Metric	:	Ukuran yang digunakan oleh OSPF untuk menentukan rute terbaik, biasanya berdasarkan bandwidth
OSPF Database	:	Struktur data yang menyimpan informasi tentang topologi jaringan
OSPF Hello Packets	:	Pesan yang digunakan untuk membangun dan memelihara hubungan tetangga

P

Peer-to-Peer (P2P)	:	Model jaringan di mana setiap perangkat dapat berfungsi sebagai client dan server
Physical Layer:	:	Lapisan OSI yang berfokus pada pengiriman bit melalui media fisik.

R

Policy-Based Routing	:	Metode routing yang menggunakan kebijakan tertentu untuk menentukan jalur pengiriman paket.
Private IP Address	:	Alamat IP yang digunakan dalam jaringan lokal dan tidak dapat diakses dari internet.
Protocol	:	Aturan dan konvensi yang digunakan untuk komunikasi antar perangkat dalam jaringan.
Public IP Address	:	Alamat IP yang dapat diakses dari internet.
Route Redistribution	:	Proses berbagi informasi routing antara protokol routing yang berbeda
RIP	:	Protokol routing yang menggunakan algoritma distance-vector untuk menentukan rute terbaik
RIP Authentication	:	Proses untuk memastikan bahwa informasi routing yang diterima adalah valid
Route Advertisement	:	Proses di mana router menginformasikan rute yang tersedia kepada tetangga
RIP Metric Calculation	:	Proses menghitung jarak ke tujuan berdasarkan hop count
Route Metric	:	Ukuran yang digunakan untuk menentukan rute terbaik dalam routing.
Route Summarization	:	Proses menggabungkan beberapa rute menjadi satu rute untuk mengurangi ukuran tabel routing
Routing	:	Proses pengiriman paket data dari sumber ke tujuan melalui jaringan.
Routing Information Update	:	Proses di mana router berbagi informasi routing terbaru dengan tetangga
Route Poisoning	:	Metode untuk menandai rute yang tidak valid dengan metrik yang sangat tinggi
Router ID	:	Identifikasi unik untuk setiap router dalam jaringan OSPF.
Routing Protocol	:	Protokol yang digunakan untuk berbagi informasi routing antar router.
Routing Loop	:	Situasi di mana paket data berputar tanpa henti di jaringan.
Routing Loop Prevention	:	Teknik yang digunakan untuk mencegah terjadinya loop dalam routing
Routing Table	:	Tabel yang menyimpan informasi tentang rute yang tersedia dalam jaringan

S

Split Horizon	:	Teknik yang digunakan untuk mencegah routing loop dengan tidak mengirimkan informasi rute kembali ke arah asalnya
Static IP Address	:	Alamat IP yang ditetapkan secara manual dan tidak berubah.
Static Routing	:	Pengaturan rute secara manual oleh administrator.

Subnet Mask	:	Angka yang digunakan untuk membedakan bagian network dan host dari alamat IP.
Subnetting	:	Proses membagi jaringan menjadi sub-jaringan yang lebih kecil untuk efisiensi penggunaan alamat IP.

T

TCP/IP:	:	Protokol komunikasi yang digunakan untuk menghubungkan perangkat di internet.
TCP (Transmission Control Protocol)	:	Protokol transport yang menjamin pengiriman data yang andal.
Topology Table	:	Tabel yang menyimpan informasi tentang semua rute yang diketahui oleh EIGRP
Transport Layer:	:	Lapisan OSI yang memastikan pengiriman data yang andal dan urutan yang benar.
Topologi Jaringan	:	Cara pengaturan fisik atau logis dari perangkat dalam jaringan.

U

UDP (User Datagram Protocol)	:	Protokol transport yang tidak menjamin pengiriman data.

INDEX

DAFTAR PUSTAKA

Academy, Cisco Networking Cisco Networking. (2020). *Switching, Routing, and Wireless Essentials Companion Guide (CCNAv7)*. London: Pearson Education.

Damanik, Hillman Akhyar, Merry Anggraeni, dan Farida Ayu Avisena Nusantar. (2023). *Konsep dan Penerapan Switching dan Routing Implementasi Jaringan Komputer Berbasis Cisco*. Jawa Barat: Mega Press Nusantara.

Januari, R. (2022). *Cisco Networking: Panduan Lengkap Routing dan Switching*. Yogyakarta: Graha Ilmu.

Lestari, N. (2022). *Pengenalan dan Implementasi Routing serta Switching pada Jaringan Cisco.* Jakarta: Elex Media Komputindo.

Haryanto, B. (2023). *Jaringan Komputer untuk Pemula: Routing dan Switching.* Jakarta: Salemba Empat.

Putra, M. (2021). *Pengantar Jaringan Komputer: Fokus pada Routing dan Switching.* Yogyakarta: Graha Ilmu.

Rudiantoro, A. (2021). *Routing dan Switching dalam Jaringan Komputer: Panduan Lengkap*. Bandung: Informatika.

Syamsul, I. (2020). *Teknik Routing dan Switching untuk Jaringan Skala Kecil dan Menengah*. Yogyakarta: Andi.

Santoso, H. (2022). *Jaringan Komputer: Teori dan Praktik Routing serta Switching*. Jakarta: Erlangga.

Tukino. (2020). *Network Design and Management CISCO CCNA Routing and Switching (Network Simulation with Packet Tracer)*. Batam: Batam Publisher.

Veza, Okta, , dan . (2024). *Jaringan Komputer Lanjutan*. Batam: Cendikia Mulia Mandiri.

Wahyudi, Mochamad, Rachmat Adi Purnama, dan Firmansyah. (2019). *Cisco routing and switching Cisco routing and switching*. Yogyakarta: Graha Ilmu.

Wibowo, Sastya Hendri. (2022). *Jaringan Komputer dan Komunikasi Data.* Jakarta: Deepublish.

Wahyudi, Mochamad, Firmansyah. (2021). *15 Best Practice Skill Cisco Routing and Switching*. Jakarta: Bintang Pustaka Madani.

ROUTING & SWITCHING

"Routing & Switching" adalah buku panduan lengkap yang dirancang untuk membantu para profesional IT, mahasiswa, dan siapa saja yang tertarik dalam bidang jaringan komputer untuk memahami dan menguasai konsep routing dan switching. Buku ini dimulai dengan pengenalan dasar tentang arsitektur jaringan, protokol, dan teknologi yang digunakan dalam routing dan switching. Pembaca akan dipandu melalui berbagai topik mulai dari konsep dasar routing & switching, konfigurasi perangkat jaringan, implementasi statik routing, protokol routing seperti RIP, OSPF, dan EIGRP. Setiap bab buku ini dilengkapi dengan contoh-contoh praktis, studi kasus, dan panduan konfigurasi yang mudah diikuti. Buku ini juga mencakup strategi troubleshooting untuk membantu pembaca dalam menyelesaikan masalah jaringan yang kompleks. Baik Anda seorang pemula yang baru memulai karir di bidang jaringan atau seorang profesional yang ingin memperdalam pengetahuan, buku "Routing & Switching" menawarkan sumber daya yang komprehensif dan dapat diandalkan untuk mencapai keunggulan dalam dunia jaringan komputer khususnya menggunakan perangkat cisco.

Jupriyadi, S.Kom., M.T. Merupakan Dosen tetap pada program studi Teknologi Informasi Fakultas Teknik dan Ilmu Komputer Universitas Teknokrat Indonesia. Menyelesaikan Program Magister di STEI ITB tahun 2014 pada Program Studi Informatika. Fokus penelitian dibidang jaringan khususnya keamanan Named Data Networking (NDN)

Syaiful Ahdan, S.Kom., M.T. Merupakan Dosen tetap pada program studi Teknologi Informasi Fakultas Teknik dan Ilmu Komputer Universitas Teknokrat Indonesia. Menyelesaikan Program Magister di STEI ITB tahun 2017 pada Program Studi Elektro. Fokus penelitian dibidang Named Data Networking (NDN) yang diimplementasikan pada sistem transportasi cerdas.

Adi Sucipto, S.Kom., M.T. Merupakan Dosen tetap pada program studi Teknologi Informasi Fakultas Teknik dan Ilmu Komputer Universitas Teknokrat Indonesia. Menyelesaikan Program Magister di STEI ITB tahun 2016 pada Program Studi Informatika. Fokus penelitian dibidang Named Data Networking (NDN) dan tata kelola teknologi informasi.

ISBN:

Penerbit:
Universitas Teknokrat Indonesia Press