Edi Surya Negara
Aan Restu Mukti
Chairul Mukmin

JARINGAN KOMPUTER

Roating dan Switching Essentials

Penerbit
PPP-UBD Press

Edi Surya Negara
Aan Restu Mukti
Chairul Mukmin

Jaringan Komputer

Routing dan Switching Essentials

Penerbit :
PPP-UBD Press

Jaringan Komputer
Routing dan Switter Essensial

Penyusun : Edi Surya Negara
Aan Restu Mukti
Chairul Mukmin

Penerbit : Pusat Penerbitan dan Percetakan Universitas Bina Darma Press (PPP- UBD Press)

ISBN : 978-979-3877-34-1

Kata Pengantar

Buku ini ditulis sebagai pedoman ajar untuk matakuliah Jaringan Komputer pada fakultas ilmu komputer. Materi yang ada dalam buku ini adalah Pengenalan Switched Networks, Konsep Dasar Switching dan Konfigurasi, VLANs, Konsep Routing, Inter VLAN Routing, Routing Statis, Routing Dinamis, Single Area OSPF, Access Control List (ACL), DHCP, dan Network Address Translation untuk IPv4.

Teknologi jaringan komputer terus mengalami perkembangan yang sangat signifikan. Untuk memenuhi kebutuhan referensi, materi-materi yang ada didalam buku ini terus diperbaharui. Buku ini mampu memberikan konsep teori dan praktis yang dilengkapi dengan contoh kasus.

Penulis menyadari buku ini akan semakin bermanfaat apabila terus dilakukan evaluasi dan pembaharuan materi, sehingga mampu dijadikan pedoman di era teknologi informasi yang terus berkembang. Oleh karena ini penulis meminta saran, kritik, dan koreksi yang membangun untuk penyempurnaan buku ini.

Tidak lupa penulis mengucapkan puji dan syukur kepada ALlah SWT dan terimakasih yang sebesar-besarnya kepada Pusat Penerbitan dan Percetakan Universitas Bina Darma Press (PP P- UBD Press) dan semua pihak yang telah banyak membantu dalam penyelesaian buku ini. Semoga bermanfaat dan dapat menjadi pedoman untuk matakuliah jaringan komputer.

Palembang, April 2017

Edi Surya Negara

Daftar Isi

Chapter 1
Pengenalan Switched Networks

1.1 Pendahuluan

Jaringan modern terus berkembang untuk mengimbangi cara organisasi mengubah dan melaksanakan bisnis mereka sehari-hari. Pengguna sekarang mengharapkan akses cepat ke sumber daya perusahaan dari mana saja dan kapan saja. Sumber daya ini tidak hanya mencakup data tradisional tetapi juga video dan suara. Ada juga kebutuhan yang meningkat untuk teknologi kolaborasi yang memungkinkan berbagi real-time dari sumber antara beberapa individu jauh seolah-olah mereka berada di lokasi fisik yang sama.

Perangkat yang berbeda harus dapat bekerja sama untuk menyediakan koneksi yang cepat, aman, dan handal antara host. LAN beralih menyediakan titik koneksi untuk pengguna akhir ke jaringan perusahaan dan juga terutama bertanggung jawab untuk mengontrol informasi dalam lingkungan LAN. Router memfasilitasi pergerakan informasi antara LAN dan umumnya tidak menyadari host individu. Semua layanan bergantung pada ketersediaan routing yang kuat dan beralih terhadap infrastruktur di mana mereka dapat membangun komunikasi. Infrastruktur ini harus dirancang dengan cermat, handal, dan mampu menyediakan platform yang stabil.

1.2 LAN Design

1.2.1 Converged Networks

Dunia digital kita berubah. Kemampuan untuk mengakses internet dan jaringan perusahaan tidak lagi terbatas pada kantor fisik, lokasi geografis, atau zona waktu. Di tempat kerja global saat ini, karyawan dapat mengakses sumber daya dari mana saja di dunia dan informasi harus tersedia setiap saat, dan pada perangkat apapun, seperti yang ditunjukkan pada Gambar 1. Persyaratan ini mendorong kebutuhan

untuk membangun jaringan generasi mendatang yang aman, handal dan dengan ketersediaan tinggi.

Fig. 1.1 Kompleksitas Networks

Jaringan generasi berikutnya tidak hanya harus mendukung harapan saat ini, tetapi juga harus mampu mengintegrasikan platform sebelumnya. Gambar 1.2 menunjukkan beberapa perangkat sebelumnya umum yang harus sering dimasukkan ke dalam desain jaringan.

Gambar 1.3 menggambarkan beberapa platform yang lebih baru (konvergensi jaringan) yang membantu untuk menyediakan akses ke jaringan kapan saja, di mana saja, dan pada perangkat apapun.

Untuk mendukung kolaborasi, jaringan bisnis mempekerjakan solusi konvergensi menggunakan sistem suara, IP Phone, gateway suara, dukungan video, dan konferensi video . Termasuk layanan data, jaringan terkonvergensi dengan dukungan kolaborasi dapat mencakup fitur seperti berikut:

- Call Control : Telepon pemrosesan panggilan, caller ID, call transfer, Meneruskan Panggilan, dan konferensi
- Voice Messaging : Voicemail
- Mobility : Menerima panggilan penting di manapun Anda berada
- Automated Attendant : Melayani pelanggan lebih cepat oleh routing panggilan langsung ke departemen yang tepat atau individu

Salah satu manfaat utama dari transisi ke jaringan konvergensi adalah bahwa hanya ada satu jaringan fisik untuk menginstal dan mengelola. Hal ini menghasilkan

Fig. 1.2 Perangkat Jaringan

penghematan besar atas instalasi dan pengelolaan jaringan suara, video, dan data yang terpisah. solusi jaringan konvergensi seperti mengintegrasikan manajemen TI sehingga setiap gerakan, penambahan, dan perubahan selesai dengan antar-muka manajemen intuitif. Sebuah solusi jaringan terkonvergensi juga menyediakan dukungan aplikasi PC softphone, serta video point-to-point, sehingga pengguna dapat menikmati komunikasi pribadi dengan kemudahan yang sama administrasi dan digunakan sebagai panggilan suara.

1.2.2 Cisco Borderless Networks

Dengan tuntutan peningkatan jaringan terkonvergensi, jaringan harus dikembangkan dengan pendekatan arsitektur yang menyematkan intelijen, menyederhanakan operasi, dan scalable untuk memenuhi kebutuhan masa depan. Salah satu perkembangan terbaru dalam desain jaringan adalah Cisco Borderless Network.

Cisco Borderless Network adalah arsitektur jaringan menggabungkan inovasi dan desain yang memungkinkan organisasi untuk mendukung jaringan tanpa batas yang dapat menghubungkan siapapun, dimanapun, kapanpun, pada perangkat apapun dengan aman, andal, dan mulus. Arsitektur ini dirancang untuk mengatasi IT dan

Fig. 1.3 Platform Konvergensi Jaringan

tantangan bisnis, seperti mendukung jaringan terkonvergensi dan mengubah pola kerja.

Cisco Borderless Network menyediakan kerangka kerja untuk menyatukan akses kabel dan nirkabel, termasuk kebijakan, kontrol akses, dan manajemen kinerja di berbagai jenis perangkat yang berbeda. Menggunakan arsitektur ini, jaringan tanpa batas dibangun di atas infrastruktur hirarki hardware yang scalable dan tangguh, seperti yang ditunjukkan pada Gambar 1.5. Dengan menggabungkan infrastruktur perangkat ini dengan solusi perangkat lunak berbasis kebijakan, Cisco Borderless Network menyediakan dua set utama layanan: layanan jaringan dan pengguna dan titik akhir layanan, semua dikelola oleh solusi manajemen terpadu. Hal ini memungkinkan elemen jaringan yang berbeda untuk bekerja bersama-sama dan memungkinkan pengguna untuk mengakses sumber dari mana saja kapan saja, sambil memberikan optimasi, skalabilitas, dan keamanan

1.2.3 Hierarchy in the Borderless Switched Network

Ini bukan prinsip independen. Memahami bagaimana setiap prinsip yang cocok dalam konteks lain sangat penting. Merancang jaringan diaktifkan tanpa batas se-

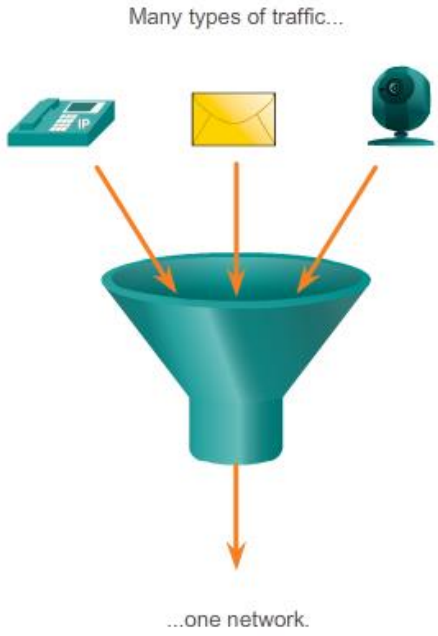


Fig. 1.4 Platform Konvergensi Data

cara hirarkis menciptakan landasan yang memungkinkan desainer jaringan untuk overlay keamanan, mobilitas, dan fitur komunikasi terpadu. Dua kerangka desain hirarkis waktu diuji dan terbukti untuk jaringan kampus adalah lapisan tiga layer dan dua layer model lapisan, seperti yang diilustrasikan pada gambar 1.6.

Tiga lapisan kritis dalam desain ini berjenjang adalah lapisan akses (access), distribusi (distribution), dan inti (core). Setiap lapisan dapat dilihat sebagai didefinisikan dengan baik, modul terstruktur dengan peran tertentu dan fungsi dalam jaringan kampus. Memperkenalkan modularitas ke kampus desain hirarkis lebih lanjut memastikan bahwa jaringan kampus tetap tangguh dan fleksibel cukup untuk menyediakan layanan jaringan kritis. Modularitas juga membantu untuk memungkinkan pertumbuhan dan perubahan yang terjadi dari waktu ke waktu.

1.2.4 Access, Ditribution Dan Core Layer

1.2.4.1 Access Layer

Lapisan akses merupakan ujung jaringan, di mana lalu lintas masuk atau keluar jaringan kampus. Secara tradisional, fungsi utama dari sebuah switch lapisan ak-

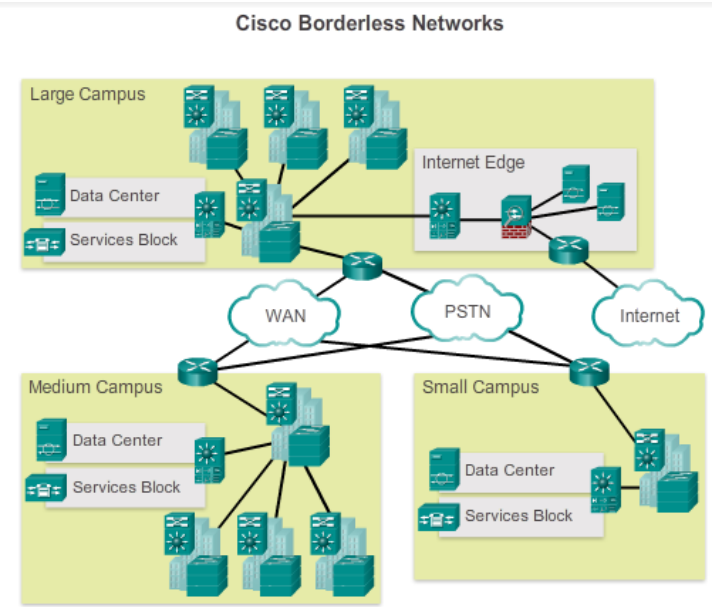


Fig. 1.5 Cisco Borderless Networks

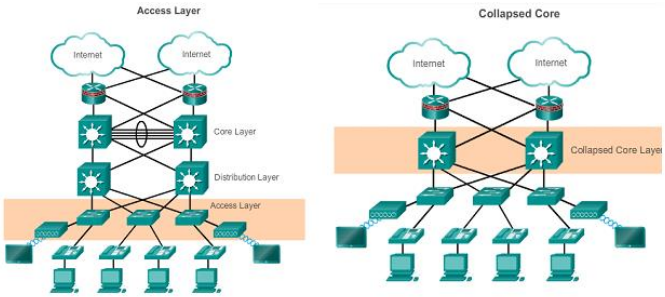


Fig. 1.6 Hierarchy Networks

ses adalah untuk menyediakan akses jaringan ke pengguna. lapisan akses switch terhubung ke distribusi lapisan switch, yang menerapkan teknologi dasar jaringan seperti routing, kualitas pelayanan, dan keamanan.

Untuk memenuhi aplikasi jaringan dan permintaan pengguna akhir, platform beralih generasi sekarang menyediakan lebih terkonvergensi, terintegrasi, dan jasa cerdas untuk berbagai jenis end point di tepi jaringan. Bangunan intelijen ke dalam lapisan akses switch memungkinkan aplikasi untuk beroperasi pada jaringan lebih efisien dan aman.

1.2.4.2 Distibution Layer

Distribution layer disebut juga layer workgroup yang menerapkan titik kumunikasi antara access layer dan core layer. Fungsi utama distribution layer adalah menyediakan routing, filtering dan untuk menentukan cara terbaik unutk menangani permintaan layanan dalam jaringan. Setelah distribution layer mentukan lintasan terbaik maka kemudian permintaan diteruskan ke core layer. Core layer dengan cepat meneruskan permintaan itu ke layanan yang benar.

- Menggabungkan skala besar jaringan
- Menggabungkan Layer 2 domain broadcast dan Layer 3 batas routing
- Menyediakan switching, routing, dan fungsi kebijakan akses jaringan cerdas untuk mengakses seluruh jaringan
- Menyediakan ketersediaan tinggi melalui layer distribusi berlebihan beralih ke pengguna akhir
- Memberikan layanan dibedakan berbagai kelas dari layanan aplikasi

1.2.4.3 Core Layer

Lapisan inti merupakan tulang punggung jaringan. Ini menghubungkan beberapa lapisan jaringan kampus. Lapisan inti berfungsi sebagai agregator untuk semua blok kampus lain dan mengikat kampus bersama-sama dengan seluruh jaringan. Tujuan utama dari lapisan inti adalah untuk memberikan isolasi kesalahan dan konektivitas backbone kecepatan tinggi.

Dalam lapisan ini tidak diperbolehkan melakukan penyaringan atau filter paket data karena dapat memperlambat transmisi data dan tidak mendukung wordgroup. Untuk toleransi kesalahan digunakan peralatan jalur ganda. Oleh sebab itu swicth dikonfigurasikan dengan menggunakan Spanning Tree Topology dimana dapat diciptakan jalur ganda tanpa harus memiliki resiko terjadi lingkaran/looping jaringan.

Spesifikasi Desain yang tidak boleh dilakukan : Tidak diperkenankan menggunakan access list, packet filtering, atau routing VLAN. Tidak diperkenankan mendukung akses workgroup dan masih banyak lagi.

1.3 The Switched Environment

Konsep switching dan forwarding frame bersifat universal dalam jaringan dan telekomunikasi. Berbagai jenis switch yang digunakan dalam LAN, WAN, dan masyarakat beralih jaringan telepon (PSTN). Konsep dasar switching mengacu pada perangkat membuat keputusan berdasarkan dua kriteria:

- Ingrees Port
- Destination Address

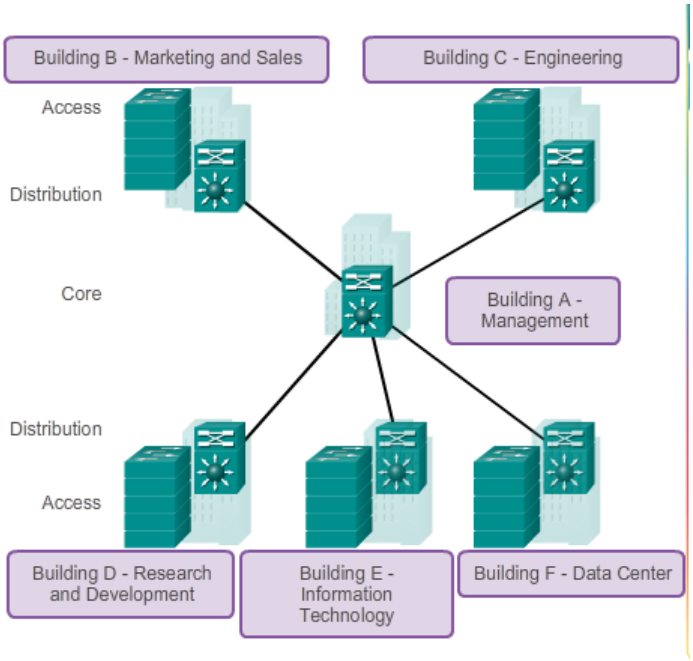


Fig. 1.7 Desain Jaringan Antar Gedung

Keputusan tentang cara switch ke depan lalu lintas dibuat dalam kaitannya dengan arus lalu lintas itu. Masuknya istilah digunakan untuk menggambarkan di mana frame memasuki perangkat pada port. The egress istilah digunakan untuk menggambarkan frame meninggalkan perangkat dari port tertentu.

Ketika switch membuat keputusan, itu didasarkan pada port ingress dan alamat tujuan pesan. Sebuah switch LAN memelihara sebuah tabel yang menggunakan untuk menentukan bagaimana untuk meneruskan lalu lintas melalui switch.

Switch menggunakan alamat MAC untuk jaringan komunikasi langsung melalui switch ke port yang sesuai menuju tujuan. Sebuah switch terdiri dari sirkuit terintegrasi dan software yang menyertainya yang mengontrol jalur data melalui saklar. Untuk switch untuk mengetahui port yang digunakan untuk mengirimkan sebuah frame, pertama kali harus belajar yang perangkat ada pada masing-masing port. Sebagai saklar belajar hubungan port ke perangkat, itu membangun meja disebut alamat MAC, atau isi memori beralamat (CAM) tabel. CAM adalah tipe khusus dari memori yang digunakan dalam aplikasi pencarian kecepatan tinggi.

LAN switch menentukan bagaimana menangani frame data yang masuk dengan mempertahankan tabel alamat MAC. Sebuah switch membangun tabel alamat MAC dengan merekam alamat MAC dari setiap perangkat yang terhubung ke masing-masing port. beralih menggunakan informasi dalam tabel alamat MAC untuk men-

girim frame ditakdirkan untuk perangkat tertentu keluar pelabuhan yang telah ditetapkan untuk perangkat tersebut.

Sebuah switch akan mengisi tabel alamat MAC berdasarkan sumber alamat MAC. Ketika switch menerima sebuah frame masuk dengan tujuan alamat MAC yang tidak ditemukan di tabel alamat MAC, switch meneruskan frame keluar dari semua port (banjir) kecuali untuk pelabuhan masuknya frame. Ketika perangkat tujuan merespon, switch menambahkan sumber alamat MAC dari frame dan port mana frame diterima untuk tabel alamat MAC. Dalam jaringan dengan beberapa switch yang saling berhubungan, tabel alamat MAC berisi beberapa alamat MAC untuk port yang terhubung ke switch lain.

1.3.1 Switching Domains

1.3.1.1 Collision Domains dan Broadcast Domain

Collision Domain adalah segmen jaringan fisik (physical) di mana paket data dapat bertabrakan dengan satu sama lain ketika dikirim pada medium bersama, khususnya bila menggunakan protokol jaringan Ethernet. Sebuah tabrakan jaringan terjadi ketika lebih dari satu untuk mengirim paket pada segmen jaringan pada waktu yang sama. Tabrakan diselesaikan menggunakan carrier sense multiple access atau variannya di mana paket yang bersaing akan dibuang dan kembali mengirim satu per satu. Hal ini menjadi sumber inefisiensi dalam jaringan.

Situasi ini biasanya ditemukan dalam lingkungan hub dimana setiap segmen host terhubung ke sebuah hub yang merepresentasikan hanya satu collision domain dan hanya satu broadcast domain. Collision domain juga ditemukan dalam jaringan nirkabel seperti Wi-Fi. Hanya satu perangkat di collision domain dapat mengirimkan pada satu waktu, dan perangkat lain dalam domain yang mendengarkan jaringan untuk menghindari tabrakan data. Karena hanya satu perangkat dapat transmisi pada satu waktu, bandwidth jaringan total dibagi di antara semua perangkat. Collision juga menurunkan efisiensi jaringan pada collision domain, jika dua perangkat transmisi secara bersamaan, tabrakan terjadi, dan kedua perangkat harus mengirim ulang di lain waktu. Untuk meringankan jaringan collision domain, disarankan untuk menggunakan switch yang meningkatkan jumlah collision domain, tapi menurun ukuran setiap domain collisions. Hal ini karena setiap port pada switch adalah collision domain sendiri.

Broadcast Domain adalah sebuah divisi logika dalam jaringan komputer dimana semua Host dan Nodes dapat menjangkaunya atau terhubung dengan host dan node yang lainnya melalui Broadcast pada layer Data Link. Broadcast Domain ini dapat berada pada segmen jaringan yang sama maupun berbeda.

LAN Switch memiliki karakteristik khusus yang membuat mereka efektif mengurangi kemacetan jaringan. Pertama, mereka memungkinkan segmentasi LAN menjadi collision domain yang terpisah. Setiap port switch merupakan collision domain yang terpisah dan memberikan bandwidth penuh ke perangkat atau perangkat

yang terhubung ke port. Kedua, mereka menyediakan komunikasi full-duplex antara perangkat.

Switch interkoneksi segmen LAN (collision domain), menggunakan tabel alamat MAC untuk menentukan segmen mana frame yang akan dikirim, dan dapat mengurangi atau menghilangkan tabrakan seluruhnya. Berikut ini adalah beberapa karakteristik penting dari switch yang berkontribusi untuk mengurangi kemacetan jaringan:

Fig. 1.8 Switches Alleviate Congestion

- High port density : Switches memiliki kepadatan tinggi-port: 24- dan switch 48-port yang sering hanya 1 unit rak (1,75 inci) tinggi dan beroperasi pada kecepatan 100 Mb / s, 1 Gb / s, dan 10 Gb / s . perusahaan switch besar dapat mendukung ratusan port.
- Large frame buffers : Kemampuan untuk menyimpan frame lebih besar
- Port Speed : Tergantung pada biaya switch, dimungkinkan untuk mendukung campuran kecepatan. Port dari 100 Mb / s, dan 1 atau 10 Gb / s yang umum (100 Gb / s juga mungkin).
- Fast internal switching - Memiliki cepat kemampuan forwarding internal yang memungkinkan kinerja tinggi. Metode yang digunakan mungkin bus internal cepat atau memori bersama, yang mempengaruhi kinerja keseluruhan saklar.
- Low per-port cost : Switches memberikan kepadatan tinggi-port dengan biaya lebih rendah. Untuk alasan ini, switch LAN dapat mengakomodasi desain

jaringan menampilkan lebih sedikit pengguna per segmen, oleh karena itu, peningkatan rata-rata bandwidth yang tersedia per pengguna.

1.4 Basic Switch Configuration

Berikut merupakan perintah-perintah dasar pada switch layer 3. Pada dasarnya perintah-perintah ini ini sama halnya yang dapat kita lakukan pada router hanya saja beberapa perintah ada yang tidak bisa dilakukan di router dan sebaliknya ada juga perintah-perintah yang hanya bisa dilakukan dilakukan di router saja.

Chapter 2
Konsep Dasar Switching dan Konfigurasi

2.1 Pendahuluan

Sama dengan PC, router atau switch tidak akan berfungsi tanpa operating system. Tanpa operating system, hardware tidak akan berguna. Cisco IOS mempunyai kemampuan:

- Dasar routing dan fungsi switching
- Akses ke jaringan dijamin keamannya
- Beroperasi di skala jaringan

CLI dapat diakses dengan beberapa cara. Secara umum, CLI diakses melalui terminal console. Console menggunakan koneksi serial kecepatan rendah yang dihubungkan langsung dari router ke PC. CLI juga bisa diakses melalui remote koneksi dialup modem ke router lewat AUX port. Cara ketiga adalah melalui telnet ke router. Untuk akses melalui telnet ini, paling tidak satu interface router sudah dikonfigurasi alamat jaringannya (IP address), dan virtual terminal harus dikonfigurasi untuk login dan password. CLI pada cisco mempunyai struktur hirarki. Struktur ini berguna untuk melakukan jenis-jenis perintah ke router. Contoh, untuk mengkonfigurasi interface router, user harus masuk ke configuration mode. Semua konfigurasi yang dimasukkan ke interface tadi hanya berlaku untukinetrface yang dikonfigurasi saja. IOS menyediakan interpreter service yang dikenal dengan command executive (EXEC). Setelah masing-masing perintah dimasukkan, EXEC akan memvalidasi dan menjalankan perintah.

Cisco IOS dibagi menjadi dua level akses, yaitu user EXEC mode dan privileged EXEC mode. Privileged EXEC mode juga dikenal sebagai enable mode. Di bawah ini adalah fitur-fitur dari user EXEC mode dan privileged.

- USER mode :
  User EXEC mode hanya memiliki perintah-perintah terbatas. Biasanya hanya meliputi perintah-perintah yang bersifat monitoring atau view. User EXEC tidak mengijinkan user untuk melakukan perubahan konfigurasi pada router. User EXEC mode ini ditandai dengan prompt >.

- PRIVILEGED mode :
  Privileged EXEC mode berisi perintah - perintah untuk akses ke router. Mode ini dapat digunakan untuk mengkonfigurasi password. Dan biasanya mode ini sering digunakan oleh administrator untuk perintahperintah yang bersifat konfigurasi dan manajemen. Global configuration mode dan mode konfigurasi lainnya hanya dapat dilakukan melalui mode ini. Privileged EXEC mode ditandai dengan prompt # .

Untuk akses ke level privileged EXEC mode, user yang berada pada level user EXEC harus mengetikkan perintah enablepada prompt >, jika password yang dimasukkan benar maka prompt akan berubah menjadi # . Ini menunjukkan bahwa user sekarang berada pada level privileged EXEC. Pada saat dimasukkan perintah ?, maka akan tampil perintah-perintah apa saja yang boleh dilakukan pada saat itu.

EXEC Mode	Prompt	Typical Use
User	GAD>	check the router status
Privileged	GAD#	accessing the router

Fig. 2.1 Level User Mode pada Cisco IOS

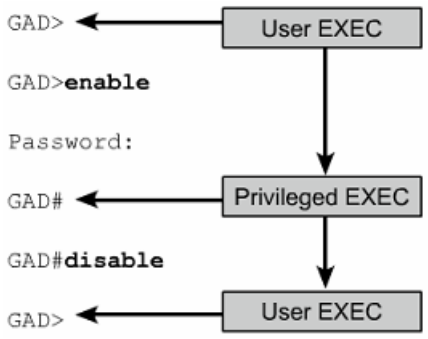


Fig. 2.2 Perubahan User EXEC Privileged EXEC

Cisco selalu mengembangkan software image IOS untuk update fitur-fitur dan teknologi yang terbaru. Tiap-tiap image menunjukkan fitur-fitur dan layanan. Meskipun terdapat banyak IOS image, namun struktur perintah dasar tetap sama. Penamaan dari berbagai macam release Cisco IOS terdiri dari 3 bagian:

- Platform dimana image itu dijalankan
- Fitur-fitur tertentu yang didukung oleh image
- Diamanapun image dijalankan selalu dalam bentuk file terkompresi

Pada perangkat Cisco Switch menggunakan LED sebagai indikator status. LED untuk indikator interface menunjukkan indikator dari masing-masing status interface. Nyala LED menunjukkan interface sedang aktif dan terhubung ke jaringan, sebaliknya LED tidak nyala menunjukkan interface tidak aktif. Jika interface terlalu sibuk, nyala LED ditandai warna hijau. Warna hijau berarti OK.

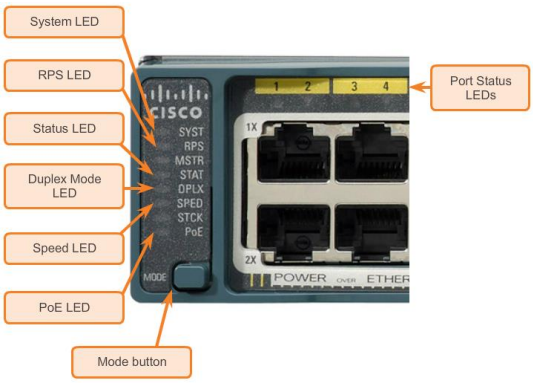


Fig. 2.3 Cisco Catalyst 2960

2.2 Konfigurasi Switch

Untuk masuk CLI dan dapat mengkonfigurasi switch, user harus login ke switch. Untuk tujuan keamanan, cisco mempunyai dua level akses keamanan (security) yang secara standar biasa digunakan:

- User EXEC mode berisi perintah-perintah untuk kebutuhan pengecekan status router.
- Privileged EXEC mode berisi perintah-perintah untuk merubah konfigurasi router.

Untuk memasuki privileged mode, ketik enable pada prompt >. Jika password sudah diatur, masukkan password pada prompt password : . Dua perintah yang digunakan untuk setting password pada privileged EXEC mode adalah enable password dan enable secret. Setelah login dilakukan, prompt akan berubah menjadi # . Yang menunjukkan bahwa sekarang user masuk ke privileged EXEC mode. Global configuration mode hanya dapat diakses melalui privileged EXEC mode.

Untuk kembali ke user EXEC mode dari privileged EXEC mode, perintah disable digunakan. Ketik exit atau endatau tekan tombol Ctrl-Z untuk kembali ke privileged EXEC mode dari global configuration mode. Ctrl-Z juga digunakan untuk kembali ke privileged EXEC mode dari sub-mode global configuration.

```
User Access Verification

Password:

Switch>
Switch>enable
Password:
Switch#
Switch#disable
Switch>
Switch>exit
```

User Mode

Previleged Mode

Fig. 2.4 Level mode konfigurasi

Untuk tingkat security lebih lanjut Cisco telah support terhadap Secure Shell (SSH) protocol kemanan pada remote access perangkat dimana menggunakan default port 22. Pada komunikasi remote access yang telah mengaktifkan SSH, maka berarti menyediakan encrypted (enkripsi) bagi remote akses yang biasa menggunakan port 23 pada TCP Telnet. Berikut ini contoh sederhana.

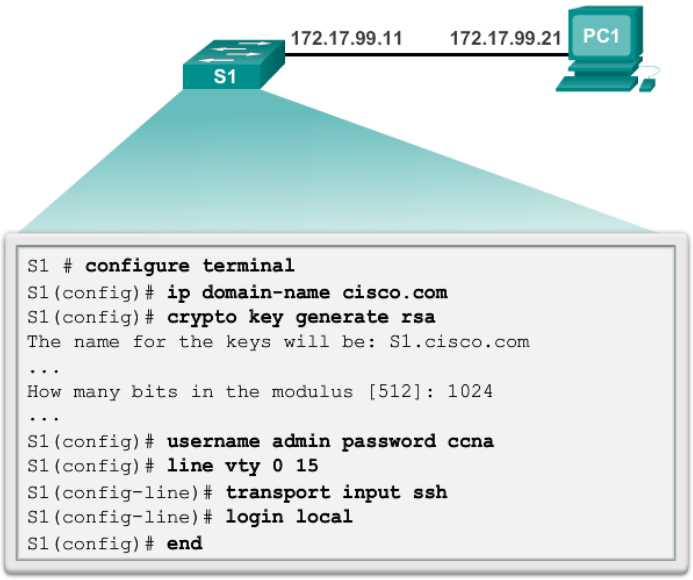


Fig. 2.5 Contoh Konfigurasi SSH

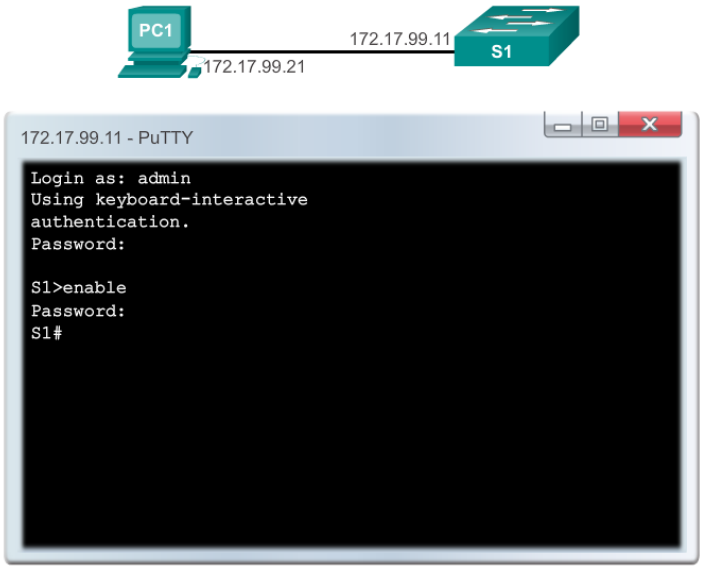


Fig. 2.6 Telnet setelah SSH diaktifkan

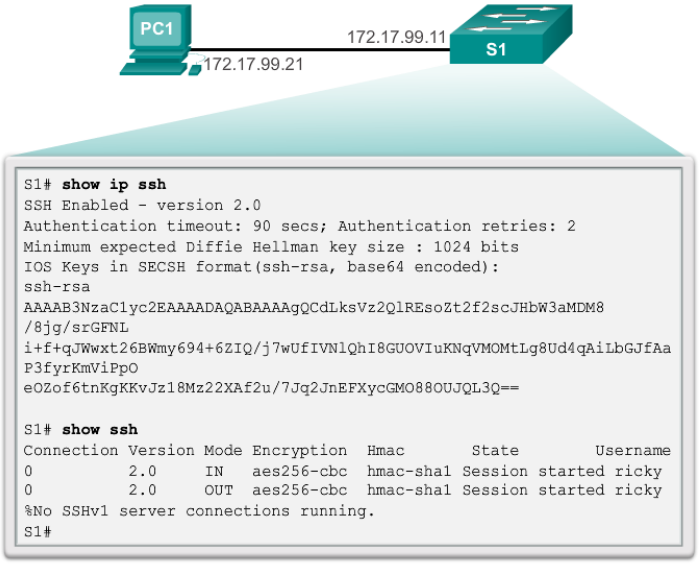


Fig. 2.7 Enkripsi SSH

Silahkan bandingkan Telnet sebelum dan sesudah SSH diaktifkan agar mengetahui letak perbedaannya secara jelas dan silahkan berdiskusi dengan teman atau dosen agar lebih paham.

Keamanan lainnya yang bisa kita gunakan yaitu Switch Port Security, keamanan ini biasa digunakan untuk mengamankan port yang tidak terpakai pada switch. Mengapa port yang tidak terpakai pada switch perlu diamankan? Karena port yang tidak terpakai dapat dimanfaatkan sebagai media DHCP Spoofing dan Mac Address Flooding yang bisa menyebabkan Ddos Attack oleh pihak yang tidak bertanggung jawab.

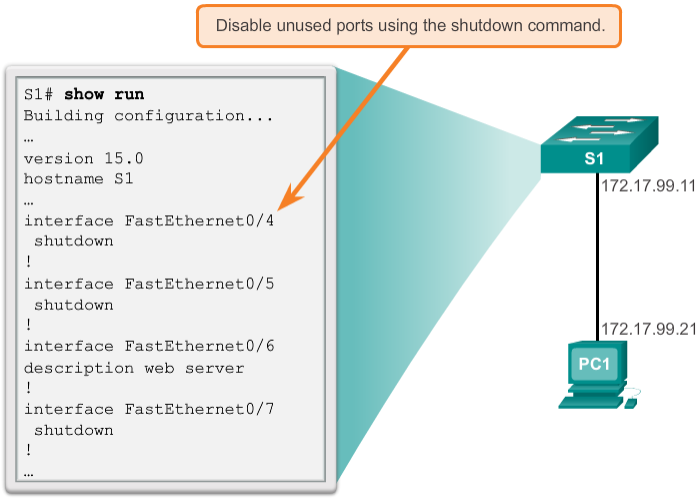


Fig. 2.8 Port yang Tidak Terpakai Pada Switch

Switch Port Security menggunakan mac address sebagai kunci utama dalam keamananya. Hanya mac address yang terdaftar yang dizinkan untuk bisa mengakses switch, secara umum dapat dikonfigurasi menjadi 3.

- Static Secure Mac Address
- Dynamics Secure Mac Address
- Sticky Secure Mac Address

Setelah kita melakukan input mac address yang diperbolehkan untuk mengakses, maka komputer atau laptop yang mac address tidak terdaftar akan diblokir aksesnya walaupun secara fisik telah menggunakan kabel yang benar. Blokir akses pada switch port security memiliki 3 tipe yaitu :

- Protect
- Restrict
- Shutdown

Untuk keperluan bantuan digunakan perintah ?. Misalkan user ingin meng-set clock dan tidak tahu perintah apa yang harus digunakan, untuk melakukannya dapat diikuti perintah-perintah berikut ini:

Feature	Default Setting
Port security	Disabled on a port.
Maximum number of secure MAC addresses	1
Violation mode	Shutdown. The port shuts down when the maximum number of secure MAC addresses is exceeded, and an SNMP trap notification is sent.
Sticky address learning	Disabled.

Fig. 2.9 Default Dynamics Port Security

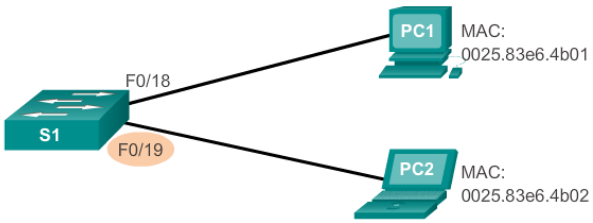
Cisco IOS CLI Commands	
`S1(config)#interface fastethernet 0/18`	Specify the interface to be configured for port security.
`S1(config-if)#switchport mode access`	Set the interface mode to access.
`S1(config-if)#switchport port-security`	Enable port security on the interface.

Fig. 2.10 Konfigurasi Dynamics Port Security

- Gunakan perintah ? untuk setting clock. Maka akan tampil perintah clock.
- Cek perintah untuk merubah waktu.
- Tekan tombol Ctrl-P atau Up Arrow untuk mengulang perintah perintah sebelumnya. Kemudian tambahkan ? untuk perintah tambahan sebagai argumen.
- Simbol caret (^) menunjukkan terjadi error perintah.
- Masukkan tahun, menggunakan format yang benar dan tekan Return atau Enter untuk menjalankan perintah.

Masih banyak perintah konfigurasi lain yang perlu dicoba dirumah (belajar mandiri). Menurut pendapat beberapa orang (yang sudah pernah lulus ujian tes CCNA), ada baiknya mengupayakan aplikasi berikut ini untuk membantu proses belajar. Berikut ini beberapa aplikasi yang disarankan.

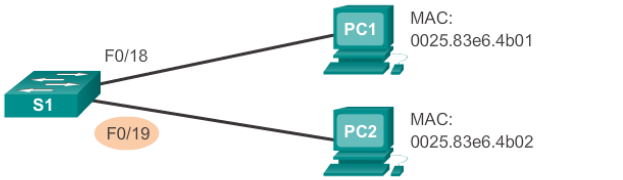
1. Packet Tracer, merupakan aplikasi simulator yang dibuat secara resmi oleh cisco dan menjadi aplikasi standar dan digunakan oleh siswa Networking Academy.
2. Dynamips (GNS3), dibuat oleh komunitas open source dan merupakan aplikasi emulator router serta hardware NM-16ESW. Sayangnya Dynamips mem-



Cisco IOS CLI Commands

`S1(config)#interface fastethernet 0/18`	Specify the interface to be configured for port security.
`S1(config-if)#switchport mode access`	Set the interface mode to access.
`S1(config-if)#switchport port-security`	Enable port security on the interface.
`S1(config-if)#switchport port-security maximum 50`	Set the maximum number of secure addresses allowed on the port.
`S1(config-if)#switchport port-security mac-address sticky`	Enable sticky learning.

Fig. 2.11 Konfigurasi Sticky Port Security



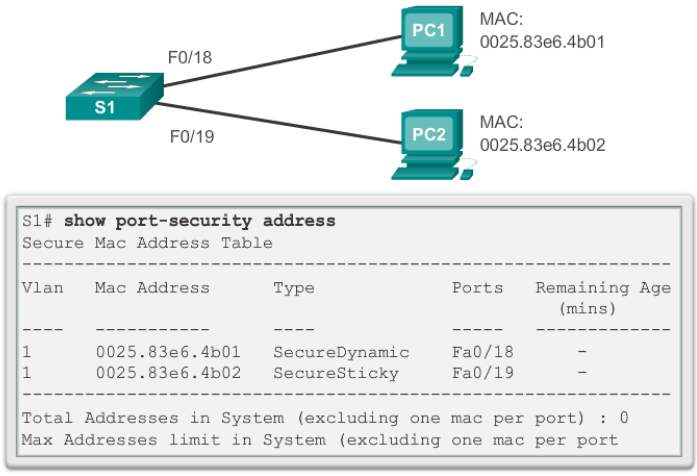

```
S1# show run | begin FastEthernet 0/19
interface FastEthernet0/19
 switchport mode access
 switchport port-security maximum 50
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0025.83e6.4b02
```

Fig. 2.12 Melihat Port Security Sticky Running Config

butuhkan IOS Image yang harus diambil dari router sungguhan (atau bisa dicari dan diunduh menggunakan google).

3. Network Visualizer, dibuat oleh RouterSim dan bersifat komersial. Informasinya ada di http://www.routersim.com/ . Secara umum mirip dengan Packet Tracer.

Tentu saja masih ada banyak aplikasi lain yang tidak kalah bagus, seperti Boson dan sebagainya. Silahkan mencari informasi lebih lengkap menggunakan Internet.




```
S1# show port-security address
Secure Mac Address Table
------------------------------------------------------------------
Vlan   Mac Address       Type             Ports   Remaining Age
                                                    (mins)
----   -----------       ----             -----   -------------
1      0025.83e6.4b01    SecureDynamic    Fa0/18      -
1      0025.83e6.4b02    SecureSticky     Fa0/19      -
------------------------------------------------------------------
Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port
```

Fig. 2.13 Melihat Port Security Secure Mac Address

```
Switch>
Switch>?
Exec commands:
  connect     Open a terminal connection
  disable     Turn off privileged commands
  disconnect  Disconnect an existing network connection
  enable      Turn on privileged commands
  exit        Exit from the EXEC
  logout      Exit from the EXEC
  ping        Send echo messages
  resume      Resume an active network connection
  show        Show running system information
  telnet      Open a telnet connection
  terminal    Set terminal line parameters
  traceroute  Trace route to destination
```

Fig. 2.14 Contoh Perintah di User Mode

2.3 Tugas Lab

Dari perintah konfigurasi dibawah ini, Informasi apa saja yang kalian dapatkan ?. Silahkan catat dan berikan kepada dosen lembar jawabannya.

```
Switch#
Switch#?
Exec commands:
  clear        Reset functions
  clock        Manage the system clock
  configure    Enter configuration mode
  connect      Open a terminal connection
  copy         Copy from one file to another
  debug        Debugging functions (see also 'undebug')
  delete       Delete a file
  dir          List files on a filesystem
  disable      Turn off privileged commands
  disconnect   Disconnect an existing network connection
  enable       Turn on privileged commands
  erase        Erase a filesystem
  exit         Exit from the EXEC
  logout       Exit from the EXEC
  more         Display the contents of a file
  no           Disable debugging informations
  ping         Send echo messages
  reload       Halt and perform a cold restart
  resume       Resume an active network connection
  setup        Run the SETUP command facility
  show         Show running system information
```

Fig. 2.15 Contoh Perintah di Previliged Mode

S1# **show interfaces [interface-id]**
S1# **show startup-config**
S1# **show running-config**
S1# **show flash**
S1# **show version**
S1# **show history**
S1# **show ip [interface-id]**
S1# **show mac-address-table**

Fig. 2.16 Tugas Lab

Chapter 3
VLANs

3.1 Pendahuluan

Kinerja jaringan merupakan faktor kunci dalam produktivitas organisasi. Salah satu teknologi yang digunakan untuk meningkatkan kinerja jaringan adalah pemisahan domain broadcast besar menjadi lebih kecil. Broadcast domain yang lebih kecil akan membatasi device yang terlibat dalam aktivitas broadcast dan membagi device ke dalam beberapa grup berdasar fungsinya, seperti layanan databasse untuk unit akuntansi, dan data transfer yang cepat untuk unit teknik. Router akan memblokir lalu lintas broadcast pada sebuah antarmuka. Namun, router biasanya memiliki sejumlah interface LAN. Peran utama router adalah untuk memindahkan informasi antara jaringan, tidak memberikan akses jaringan untuk perangkat akhir. Peran menyediakan akses ke LAN biasanya disediakan untuk switch lapisan akses. Sebuah jaringan virtual lan (VLAN) dapat dibuat pada Layer 2 saklar untuk mengurangi ukuran broadcast domain, mirip dengan perangkat Layer 3. VLAN biasanya dimasukkan ke dalam desain jaringan sehingga memudahkan jaringan untuk mendukung tujuan organisasi.

Dalam internetwork diaktifkan VLAN memberikan segmentasi dan fleksibilitas organisasi. VLAN adalah kelompok device dalam sebuah LAN yang dikonfigurasi (menggunakan software manajemen) sehingga mereka dapat saling berkomunikasi asalkan dihubungkan dengan jaringan yang sama walaupun secara fisikal mereka berada pada segmen LAN yang berbeda. Jadi VLAN dibuat bukan berdasarkan koneksi fisikal namun lebih pada koneksi logikal, yang tentunya lebih fleksibel. Secara logika, VLAN membagi jaringan ke dalam beberapa subnetwork. VLAN mengijinkan banyak subnet dalam jaringan yang menggunakan switch yang sama. Konfigurasi VLAN itu sendiri dilakukan melalui perangkat lunak (software), sehingga walaupun computer tersebut berpindah tempat, tetapi ia tetap berada pada jaringan Dengan menggunakan VLAN, kita dapat melakukan segmentasi jaringan switch berbasis pada fungsi, departemen atau pun tim proyek. Kita dapat juga mengelola jaringan kita sejalan dengan kebutuhan pertumbuhan perusahaan sehingga

para pekerja dapat mengakses segmen jaringan yang sama walaupun berada dalam lokasi yang berbeda.

VLAN memungkinkan administrator untuk mengatur jaringan segmen berdasarkan faktor-faktor seperti fungsi, tim proyek, atau aplikasi, tanpa memperhatikan lokasi fisik dari pengguna atau perangkat. Perangkat dalam tindakan VLAN seolah-olah mereka berada di jaringan independen mereka sendiri, bahkan jika mereka berbagi infrastruktur umum dengan VLAN lainnya. Setiap port switch dapat milik VLAN, dan unicast, broadcast, dan paket-paket multicast akan diteruskan dan membanjiri hanya untuk stasiun akhir dalam VLAN mana paket yang bersumber. Setiap VLAN dianggap sebagai jaringan logis yang terpisah, dan paket ditakdirkan untuk stasiun yang tidak termasuk dalam VLAN harus diteruskan melalui perangkat yang mendukung routing.

Sebuah VLAN menciptakan broadcast domain logis yang dapat span beberapa segmen LAN fisik. VLAN meningkatkan kinerja jaringan dengan memisahkan broadcast domain besar menjadi lebih kecil. Jika perangkat dalam satu VLAN mengirimkan broadcast Ethernet Frame, semua perangkat dalam VLAN menerima frame, tetapi perangkat di VLAN lain tidak.

3.2 Manfaat VLANs

Produktivitas pengguna dan kemampuan beradaptasi jaringan yang penting bagi pertumbuhan bisnis. VLAN membuat lebih mudah untuk merancang jaringan untuk mendukung tujuan organisasi. Manfaat utama dari menggunakan VLAN adalah sebagai berikut :

1. Security (Keamanan) : Kelompok yang memiliki data sensitif dipisahkan dari jaringan yang lain, mengurangi kemungkinan pelanggaran informasi rahasia. Seperti yang ditunjukkan pada gambar, komputer fakultas yang berada di VLAN 10 dan benar-benar terpisah dari lalu lintas mahasiswa dan tamu.
2. Cost Reduction (pengurangan biaya) : penghematan dari penggunaan bandwidth yang ada dan dari upgrade perluasan network yang bisa jadi mahal.
3. Better Perfomance (kinerja yang lebih baik) : Pembagian jaringan layer 2 ke dalam beberapa kelompok broadcast domain yang lebih kecil, yang tentunya akan mengurangi lalu lintas packet yang tidak dibutuhkan dalam jaringan.
4. Shrink broadcast domains (Mengecilkan domain broadcast) : Pembagian jaringan ke dalam VLAN-VLAN akan mengurangi banyaknya device yang berpartisipasi dalam pembuatan broadcast storm. Hal ini terjadinya karena adanya pembatasan broadcast domain. Seperti yang ditunjukkan pada gambar diatas, ada enam komputer di jaringan ini, tetapi ada tiga domain broadcast: Fakultas, Mahasiswa, dan Guest.
5. Improved IT staff efficiency (Peningkatan efisiensi staf TI) : VLAN memudahkan manajemen jaringan karena pengguna yang membutuhkan sumber daya yang dibutuhkan berbagi dalam segmen yang sama. Ketika switch baru ditetapkan,

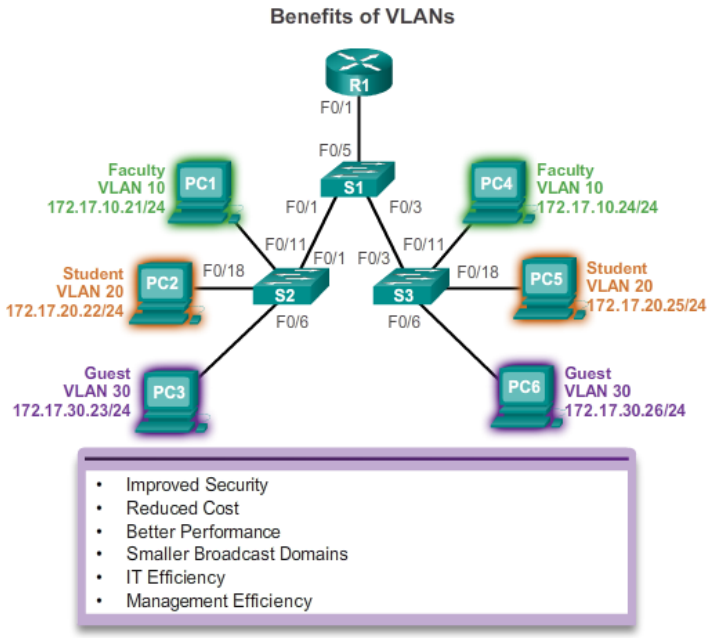


Fig. 3.1 Manfaat VLANs

semua kebijakan dan prosedur sudah dikonfigurasi untuk VLAN tertentu dilaksanakan ketika port ditugaskan. Hal ini juga mudah untuk staf TI untuk mengidentifikasi fungsi dari VLAN dengan memberi nama yang sesuai. Dalam gambar, untuk memudahkan identifikasi VLAN 10 telah bernama ”Fakultas”, VLAN 20 bernama ”Student”, dan VLAN 30 ”Guest.”

6. Simpler project and application management (Sederhana proyek dan aplikasi manajemen) : VLAN menggabungkan para pengguna jaringan dan peralatan jaringan untuk mendukung perusahaan dan menangani permasalahan kondisi geografis; contoh aplikasi tersebut adalah sebuah platform pengembangan e-learning untuk fakultas.

Setiap VLAN dalam jaringan diaktifkan sesuai dengan jaringan IP. Oleh karena itu, desain VLAN harus mempertimbangkan pelaksanaan skema jaringan pengalamatan hirarkis. jaringan hirarkis menangani berarti nomor jaringan IP diterapkan untuk segmen jaringan atau VLAN secara teratur yang mengambil jaringan secara keseluruhan menjadi pertimbangan.

3.3 Jenis - jenis VLANs

Ada beberapa jenis yang berbeda dari VLAN digunakan dalam jaringan modern. Beberapa jenis VLAN didefinisikan oleh kelas lalu lintas. Jenis lain dari VLAN didefinisikan oleh fungsi tertentu yang mereka layani.

- Data VLAN (VLAN Data)
  VLAN Data adalah VLAN yang dikonfigurasi hanya untuk membawa data-data yang digunakan oleh user. Dipisahkan dengan lalu lintas data suara atau pun manajemen switch. Seringkali disebut dengan VLAN pengguna, User VLAN.
- Default VLAN
  Semua port switch pada awalnya menjadi anggota VLAN Default. VLAN Default untuk Switch Cisco adalah VLAN 1. VLAN 1 tidak dapat diberi nama dan tidak dapat dihapus.. Switch port yang berpartisipasi dalam VLAN default adalah bagian dari domain broadcast yang sama. Hal ini memungkinkan perangkat apapun yang terhubung ke port switch untuk berkomunikasi dengan perangkat lain pada port switch lainnya. Dalam gambar, perintah ”show vlan brief” perintah singkat dikeluarkan pada switch menjalankan konfigurasi default. Perhatikan bahwa semua port ditugaskan untuk VLAN 1 secara default. VLAN 1 memiliki semua fitur dari setiap VLAN, kecuali ia tidak dapat diubah atau dihapus. Secara default, semua Layer 2 lalu lintas kontrol dikaitkan dengan VLAN 1.

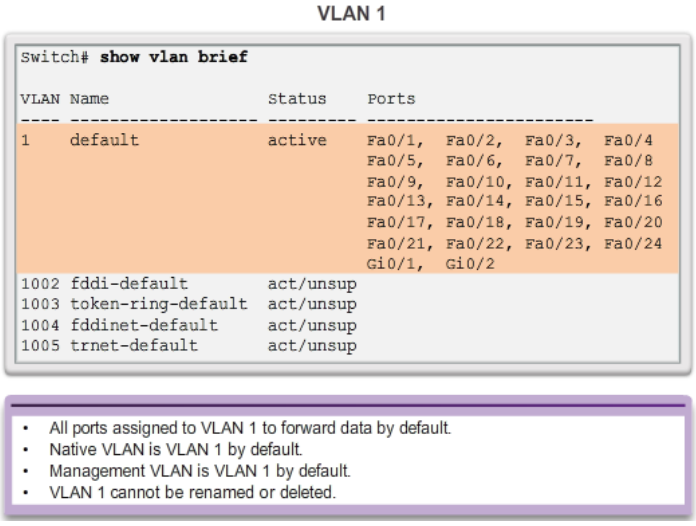


Fig. 3.2 Verifikasi VLANs

- Native VLAN
- Native VLAN dikeluarkan untuk port trunking 802.1Q. port trunking 802.1Q mendukung lalu lintas jaringan yang datang dari banyak VLAN (tagged traffic)

sama baiknya dengan yang datang dari sebuah VLAN (untagged traffic). Port trunking 802.1Q menempatkan untagged traffic pada Native VLAN.

- Management VLAN (VLAN Management)
  VLAN Manajemen adalah VLAN yang dikonfigurasi untuk memanajemen switch. VLAN 1 akan bekerja sebagai Management VLAN jika kita tidak mendefinisikan VLAN khusus sebagai VLAN Manajemen. Kita dapat memberi IP address dan subnet mask pada VLAN Manajemen, sehingga switch dapat dikelola melalui HTTP, Telnet, SSH, atau SNMP.
- Voice VLAN (VLAN Voice)
  VLAN yang dapat mendukung Voice over IP (VoIP). VLAN yang dikhusukan untuk komunikasi data suara.

3.4 VLAN Trunks

Sebuah trunk adalah link point-to-point antara dua perangkat jaringan yang membawa lebih dari satu VLAN. Cisco mendukung IEEE 802.1Q untuk mengkoordinasikan trunk di Fast Ethernet, Gigabit Ethernet, dan 10-Gigabit Ethernet interface.

VLAN tidak akan sangat berguna tanpa trunk VLAN. Trunk VLAN memungkinkan semua lalu lintas VLAN untuk menyebarkan antara switch, sehingga perangkat yang berada di VLAN yang sama, tetapi terhubung ke switch yang berbeda dapat berkomunikasi tanpa intervensi dari router.

Sebuah trunk VLAN bukan milik suatu VLAN tertentu. Trunk adalah saluran untuk beberapa VLAN antara switch dan router. Sebuah trunk juga bisa digunakan antara perangkat jaringan dan server atau perangkat lain yang dilengkapi dengan NIC 802.1Q. Secara default, pada switch Cisco Catalyst, semua VLAN didukung pada port trunk.

Pada Gambar diatas, link antara switch S1 dan S2, dan S1 dan S3 dikonfigurasi untuk mengirimkan lalu lintas yang datang dari VLAN 10, 20, 30, dan 99 di seluruh jaringan. Jaringan ini tidak bisa berfungsi tanpa trunk VLAN.

3.5 IEEE 802.1Q

IEEE melakukan standardisasi beberapa protokol yang berhubungan dengan LAN, termasuk protokol VLAN trunking. 802.1Q menggunakan header yang berbeda dari ISL untuk menyematkan angka VLAN pada frame. Sebenarnya 802.1Q tidak melakukan enkapsulasi penuh seperti halnya ISL. Sebagai gantinya, 802.1Q menyisipkan 4-byte VLAN header pada header original dari ethernet frame. Hasilnya, tidak seperti ISL, frame yang dikirimkan masih memiliki source dan destination MAC address yang original. Dan juga, karena headernya berubah, maka enkapsulasi 802.1Q terpaksa menghitung ulang frame check sequence (FCS) yang asli yang berada pada ethernet trailer.

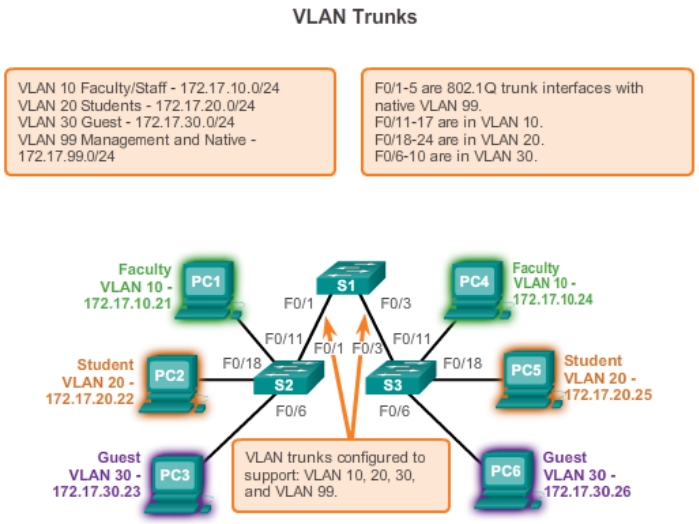


Fig. 3.3 VLAN Trunk

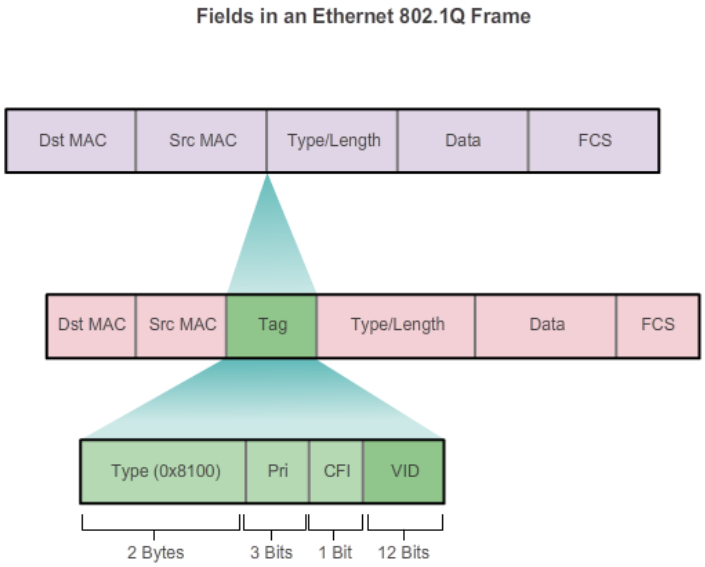


Fig. 3.4 Field Ethernet 802.1Q Frame

3.6 VLAN Ranges Pada Catalyst Switches

Berbeda switch Cisco Catalyst mendukung berbagai jumlah VLAN. Jumlah VLAN didukung cukup besar untuk mengakomodasi kebutuhan sebagian besar organ-

isasi. Sebagai contoh, Switch Catalyst 2960 dan 3560 Series dukungan lebih dari 4.000 VLAN. VLAN kisaran normal pada switch ini diberi nomor 1 sampai 1005 dan diperpanjang VLAN kisaran diberi nomor 1006 sampai 4094. Angka tersebut menggambarkan VLAN tersedia pada Catalyst 2960 saklar menjalankan Cisco IOS Rilis 15.x.

Normal Range VLANs

```
Switch# show vlan brief

VLAN Name                Status    Ports
---- ----------------------------- --------- -----------------------
1    default             active    Fa0/1,  Fa0/2,  Fa0/3,  Fa0/4
                                   Fa0/5,  Fa0/6,  Fa0/7,  Fa0/8
                                   Fa0/9,  Fa0/10, Fa0/11, Fa0/12
                                   Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                   Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                   Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                   Gi0/1, Gi0/2
1002 fddi-default        act/unsup
1003 token-ring-default  act/unsup
1004 fddinet-default     act/unsup
1005 trnet-default       act/unsup
```

Fig. 3.5 Normal Range VLANs

3.7 Membuat VLAN

Gambar 3.6 dibawah ini menampilkan sintaks perintah Cisco IOS digunakan untuk menambah VLAN ke switch dan memberikan nama.

Create a VLAN

Cisco Switch IOS Commands	
Enter global configuration mode.	`S1# configure terminal`
Create a VLAN with a valid id number.	`S1(config)# vlan vlan-id`
Specify a unique name to identify the VLAN.	`S1(config-vlan)# name vlan-name`
Return to the privileged EXEC mode.	`S1(config-vlan)# end`

Fig. 3.6 Create VLANs

Gambar 3.7 menunjukkan bagaimana VLAN siswa (VLAN 20) dikonfigurasi pada switch S1. Dalam contoh topologi, komputer mahasiswa (PC2) belum dikaitkan dengan VLAN, tetapi memiliki alamat IP dari 172.17.20.22.

Selain memasukkan ID VLAN tunggal, serangkaian VLAN ID dapat di masukkan dipisahkan dengan koma, atau berbagai VLAN ID dipisahkan dengan tanda hubung menggunakan vlan perintah vlan-id. Misalnya, gunakan perintah berikut untuk membuat VLAN 100, 102, 105, 106, dan 107.

```
S1 (config) # vlan 100,102,105-107
```

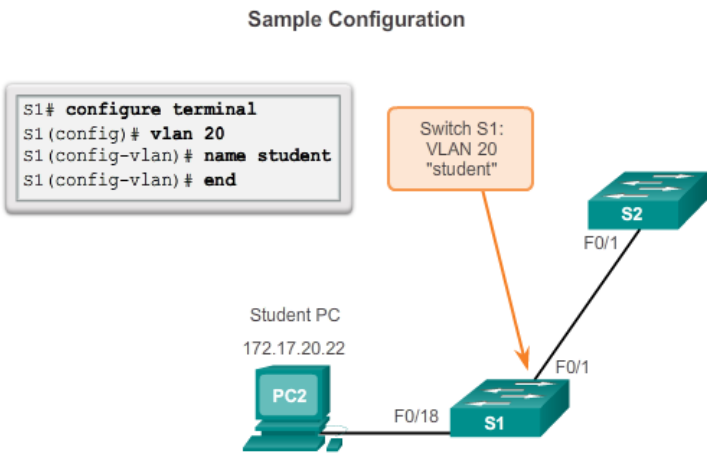


Fig. 3.7 Contoh Konfigurasi VLANs

3.8 Mengkonfigurasi Ports pada VLANs

Setelah membuat VLAN, langkah berikutnya adalah untuk menetapkan port ke VLAN. Gambar dibawah ini menampilkan sintaks untuk mendefinisikan port menjadi port akses dan menugaskan ke VLAN. Switchport port akses perintah opsional, tetapi sangat dianjurkan sebagai keamanan praktek terbaik. Dengan perintah ini, perubahan interface ke mode akses permanen.

Note : Gunakan perintah ”range interface” untuk secara bersamaan mengkonfigurasi beberapa interface.

Pada contoh diatas, VLAN 20 ditugaskan ke port F0 / 18 pada switch S1. Oleh karena itu, komputer siswa (PC2) adalah di VLAN 20. Ketika VLAN 20 dikonfigurasi pada switch lain, administrator jaringan tahu untuk mengkonfigurasi komputer siswa lain untuk berada di subnet yang sama dengan PC2 (172.17.20.0/2.

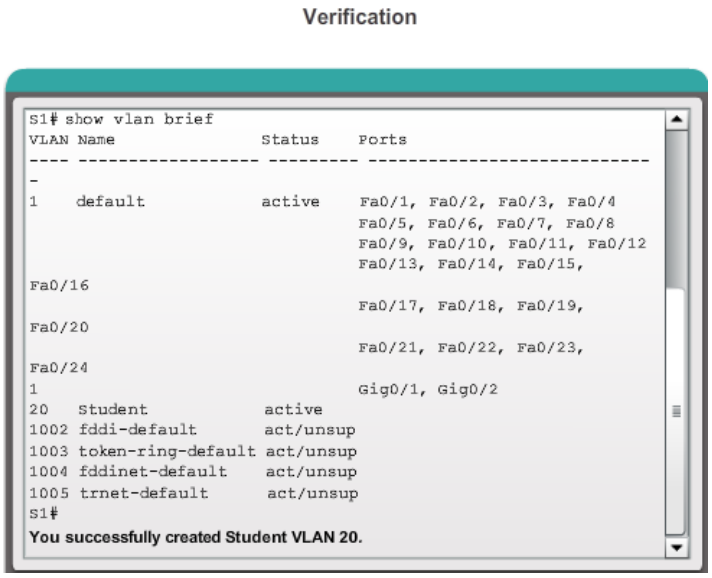


Fig. 3.8 Verifikasi

3.9 Konfigurasi IEEE 802.1Q Trunk Links

Sebuah VLAN trunk adalah OSI Layer 2 hubungan antara dua switch yang membawa lalu lintas untuk semua VLAN (kecuali daftar VLAN diperbolehkan dibatasi secara manual atau secara dinamis). Untuk mengaktifkan link trunk, mengkonfigurasi port pada kedua ujung link fisik dengan set perintah paralel.

Untuk mengkonfigurasi port switch pada salah satu ujung link trunk, menggunakan perintah switchport mode trunk. Dengan perintah ini, perubahan interface ke mode trunking permanen. Port masuk ke dalam Dinamis Trunking Protocol (DTP) negosiasi untuk mengkonversi link menjadi link switch bahkan jika interface menghubungkan ke sana tidak menyetujui perubahan tersebut. Dalam kursus ini, perintah switchport mode trunk adalah satu-satunya metode yang diterapkan untuk konfigurasi trunk. Gunakan Cisco IOS switchport trunk diperbolehkan vlan vlan-daftar perintah untuk menentukan daftar VLAN diizinkan pada link trunk.

Assign Ports to VLANs

Cisco Switch IOS Commands	
Enter global configuration mode.	`S1# configure terminal`
Enter interface configuration mode.	`S1(config)# interface interface_id`
Set the port to access mode.	`S1(config-if)# switchport mode access`
Assign the port to a VLAN.	`S1(config-if)# switchport access vlan vlan_id`
Return to the privileged EXEC mode.	`S1(config-if)# end`

Fig. 3.9 Assingn Port VLANs

Example Configuration

```
s1# configure terminal
s1(config)# interface F0/18
s1(config-if)# switchport mode access
s1(config-if)# switchport access vlan 20
s1(config-if)# end
```

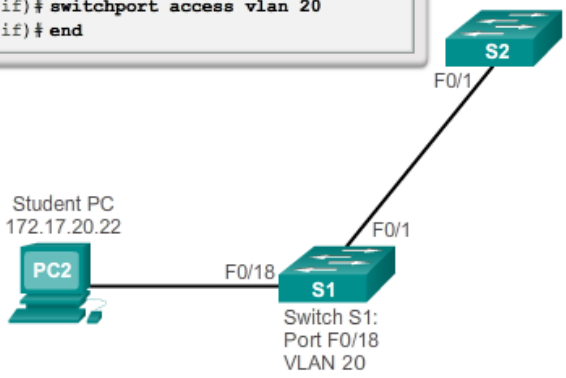


Fig. 3.10 Contoh Konfigurasi Port VLANs

3.10 Dynamic Trunking Protocol

Sebuah Port pada Switch Cisco Catalyst mempunyai beberapa mode trunk. Mode trunking tersebut didefinisikan untuk negosiasi antar port yang saling berhubungan

Trunk Configuration

Cisco Switch IOS Commands	
Enter global configuration mode.	`S1# configure terminal`
Enter interface configuration mode.	`S1(config)# interface interface_id`
Force the link to be a trunk link.	`S1(config-if)# switchport mode trunk`
Specify a native VLAN for untagged 802.1Q trunks.	`S1(config-if)# switchport trunk native vlan vlan_id`
Specify the list of VLANs to be allowed on the trunk link.	`S1(config-if)# switchport trunk allowed vlan vlan-list`
Return to the privileged EXEC mode.	`S1(config-if)# end`

Fig. 3.11 Konfigurasi Trunk

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Limited Connectivity
Access	Access	Access	Limited Connectivity	Access

Fig. 3.12 DTP - Negotiated Interface Modes

dengan menggunakan Dynamic Trunking Protocol (DTP) adalah protokol proprietary Cisco yang secara otomatis diaktifkan pada Catalyst 2960 dan Catalyst 3560 switch Seri. Switch dari vendor lain tidak mendukung DTP. DTP mengatur negosiasi mode trunk hanya jika port switch dikonfigurasi dalam mode trunk yang mendukung DTP. DTP mendukung baik ISL maupun 802.1Q. Ada tiga mode trunk pada DTP, yaitu: Trunk, Access, Dynamic Auto dan Dynamic Desirable.

3.11 Latihan

Buatlah topologi seperti Gambar 3.12 dibawah ini

1. Verifikasi Konektivitas
   - PC1 bisa PING PC4
   - PC2 bisa PING PC5
   - PC3 bisa PING PC6

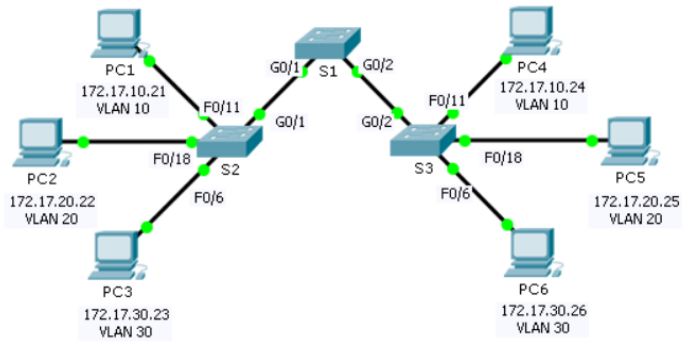


Fig. 3.13 Latihan Topologi

Device	Interface	IP Address	Subnet Mask	VLAN
PC1	NIC	172.17.10.21	255.255.255.0	10
PC2	NIC	172.17.20.22	255.255.255.0	20
PC3	NIC	172.17.30.23	255.255.255.0	30
PC4	NIC	172.17.10.24	255.255.255.0	10
PC5	NIC	172.17.20.25	255.255.255.0	20
PC6	NIC	172.17.30.26	255.255.255.0	30

Fig. 3.14 Tabel IP Address

2. Buatlah Vlan di S1, S2 dan S3
   - VLAN 10 : Faculty/Staff
   - VLAN 20 : Students
   - VLAN 30 : Guest
3. Menetapkan VLAN ke port
   - VLAN 10 : Fast Ethernet 0/11
   - VLAN 20 : Fast Ethernet 0/18
   - VLAN 30 : Fast Ethernet 0/6

Chapter 4
Konsep Routing

4.1 Pendahuluan

Jaringan memungkinkan orang untuk berkomunikasi, berkolaborasi, dan berinteraksi dengan berbagai cara. Jaringan yang digunakan untuk mengakses halaman web, berbicara menggunakan telepon IP, berpartisipasi dalam konferensi video, bersaing dalam permainan interaktif, toko menggunakan Internet, lengkap kursus online, dan masih banyak lagi.

Fungsi Ethernet switch pada lapisan data link, Layer 2, dan digunakan untuk meneruskan frame Ethernet antara perangkat dalam jaringan yang sama. Namun, ketika alamat IP sumber dan tujuan IP berada pada jaringan yang berbeda, frame Ethernet harus dikirim ke router.

Sebuah router menghubungkan satu jaringan ke jaringan lain. router bertanggung jawab untuk pengiriman paket di jaringan yang berbeda. Tujuan paket IP mungkin server web di negara lain atau server email pada jaringan area lokal. Router menggunakan tabel routing untuk menentukan jalur terbaik untuk digunakan untuk meneruskan paket. Ini adalah tanggung jawab router untuk memberikan paket-paket pada waktu yang tepat. Efektivitas komunikasi internetwork tergantung, untuk tingkat besar, pada kemampuan router untuk meneruskan paket dengan cara yang paling efisien mungkin.

Ketika sebuah host mengirimkan sebuah paket ke perangkat pada jaringan IP yang berbeda, paket diteruskan ke default gateway karena perangkat host tidak dapat berkomunikasi langsung dengan perangkat luar jaringan lokal. Default gateway adalah tujuan yang rute lalu lintas dari jaringan lokal ke perangkat pada jaringan jarak jauh. Hal ini sering digunakan untuk menghubungkan jaringan lokal ke Internet.

Bab ini juga akan menjawab pertanyaan, ”Apa yang router lakukan dengan paket yang diterima dari satu jaringan dan ditujukan untuk jaringan lain?” Rincian dari tabel routing yang terhubung akan diperiksa, statis, dan rute yang dinamis. Karena router dapat rute paket antara jaringan, perangkat pada jaringan yang berbeda dapat berkomunikasi.

4.2 Karakteristik Networks

Jaringan memiliki dampak yang signifikan terhadap kehidupan kita. Mereka telah mengubah cara kita hidup, bekerja, dan bermain. Jaringan memungkinkan kita untuk berkomunikasi, berkolaborasi, dan berinteraksi dengan cara kami tidak pernah melakukan sebelumnya. Kami menggunakan jaringan dalam berbagai cara, termasuk aplikasi web, IP telephony, video conferencing, game interaktif, perdagangan elektronik, pendidikan, dan banyak lagi. Seperti yang ditunjukkan pada gambar, ada banyak struktur kunci dan karakteristik yang berhubungan dengan kinerja disebut ketika membahas jaringan:

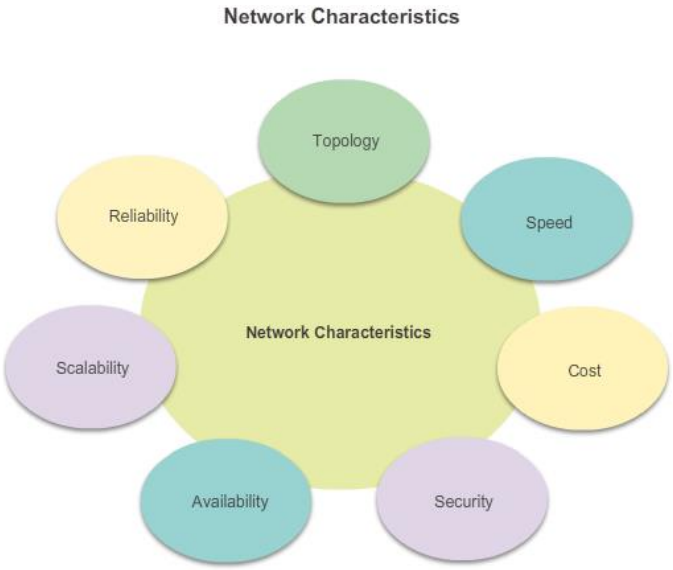


Fig. 4.1 Karakteristik Networks

- Topologi : Ada topologi fisik dan logis. Topologi fisik adalah pengaturan kabel, perangkat jaringan, dan sistem akhir. Ini menggambarkan bagaimana perangkat-perangkat jaringan sebenarnya saling berhubungan dengan kawat dan kabel. Topologi logis adalah jalur di mana data ditransfer dalam suatu jaringan. Ini menggambarkan bagaimana perangkat jaringan muncul terhubung ke pengguna jaringan.
- Kecepatan : adalah ukuran data rate dalam bit per detik (bps) dari link yang diberikan dalam jaringan.
- Biaya : menunjukkan beban umum untuk pembelian komponen jaringan, dan instalasi dan pemeliharaan jaringan.

- Keamanan : menunjukkan bagaimana jaringan dilindungi adalah, termasuk informasi yang ditransmisikan melalui jaringan. Masalah keamanan adalah soal penting, seriring teknik dan praktek yang terus berkembang. Pertimbangkan keamanan setiap kali tindakan yang diambil yang mempengaruhi jaringan.
- Ketersediaan : adalah ukuran probabilitas bahwa jaringan tersedia untuk digunakan bila diperlukan.
- Skalabilitas : menunjukkan betapa mudahnya jaringan dapat menampung lebih banyak pengguna dan persyaratan transmisi data. Jika desain jaringan dioptimalkan untuk hanya memenuhi kebutuhan saat ini, itu bisa sangat sulit dan mahal untuk memenuhi kebutuhan baru ketika jaringan berkembang.
- Keandalan : menunjukkan ketergantungan dari komponen yang membentuk jaringan, seperti router, switch, PC, dan server.

4.3 Why Routing ?

Bagaimana meng-klik link di web browser kembali informasi yang diinginkan hanya dalam hitungan detik? Meskipun ada banyak perangkat dan teknologi kolaboratif bekerja sama untuk mengaktifkan ini, perangkat utama adalah router. Lain sederhana, router menghubungkan satu jaringan ke jaringan lain.

Komunikasi antara jaringan tidak akan mungkin tanpa router menentukan jalur terbaik ke tujuan dan forwarding lalu lintas ke router berikutnya di sepanjang jalan itu. Router bertanggung jawab untuk routing lalu lintas antara jaringan.Pada gambar, diagram topologi jaringan terdiri dari dua host, dua switch dan Cisco 1841 Integrated Series Router (ISR).

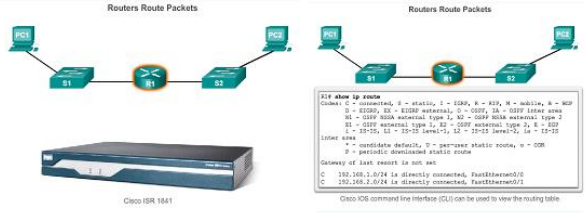


Fig. 4.2 Proses routing

Ketika sebuah paket tiba pada antarmuka router, router menggunakan tabel routing untuk menentukan bagaimana untuk mencapai jaringan tujuan. Tujuan paket IP mungkin server web di negara lain atau server email pada jaringan area lokal. Ini adalah tanggung jawab router untuk menyampaikan paket tersebut secara efisien. Efektivitas komunikasi internetwork tergantung, untuk tingkat besar, pada kemampuan router untuk meneruskan paket dengan cara yang paling efisien mungkin.

Fungsi utama dari router adalah untuk:

1. Menentukan jalur terbaik untuk mengirimkan paket
2. meneruskan paket ke tujuan

Router menggunakan tabel routing dalam menentukan jalur terbaik untuk digunakan meneruskan paket. Ketika router menerima paket, router memeriksa alamat tujuan paket dan menggunakan tabel routing untuk mencari jalur terbaik ke jaringan tersebut. Tabel routing juga termasuk interface yang akan digunakan dalam meneruskan paket untuk setiap jaringan yang dikenal. Ketika kecocokan ditemukan, router merangkum paket ke dalam frame data link dari interface keluar atau exit, dan paket diteruskan menuju tujuan.

Hal ini dimungkinkan untuk router untuk menerima paket yang dikemas dalam satu jenis frame data link, dan untuk meneruskan paket dari sebuah interfcae yang menggunakan berbagai jenis frame data link. Misalnya, router dapat menerima paket pada sebuah interface Ethernet, tetapi harus meneruskan paket dari interface dikonfigurasi dengan Point-to-Point Protocol (PPP). Enkapsulasi data link tergantung pada jenis interface pada router dan jenis media yang menghubungkan. Berbeda teknologi data link yang router dapat terhubung ke termasuk Ethernet, PPP, Frame Relay, DSL, kabel, dan wireless (802.11, Bluetooth).

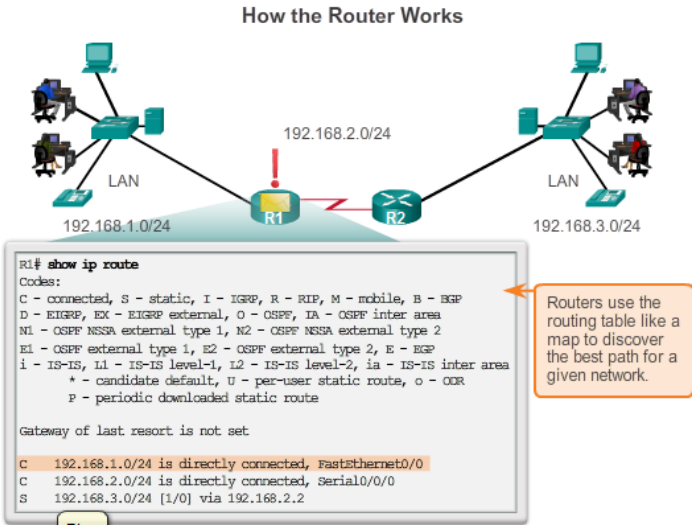


Fig. 4.3 Cara kerja routing

Pada gambar 4.3 diatas paket dari PC sumber ke PC tujuan. Perhatikan bahwa itu adalah tanggung jawab dari router untuk menemukan jaringan tujuan dalam tabel routing dan meneruskan paket pada arah tujuannya. Dalam contoh ini, router R1 menerima paket dikemas dalam sebuah frame Ethernet. Setelah de-encapsulating paket, R1 menggunakan IP Address tujuan paket untuk mencari tabel routing untuk alamat jaringan yang cocok. Setelah alamat jaringan tujuan ditemukan pada tabel

routing, R1 merangkum paket dalam frame PPP dan meneruskan paket ke R2. Sebuah proses serupa yang dilakukan oleh R2.

4.4 Akses Konsul

Dalam lingkungan produksi, perangkat infrastruktur umumnya diakses dari jarak jauh menggunakan Secure Shell (SSH) atau HyperText Transfer Protocol Secure (HTTPS). Akses konsol benar-benar hanya diperlukan bila awalnya mengkonfigurasi perangkat, atau jika akses remote gagal.

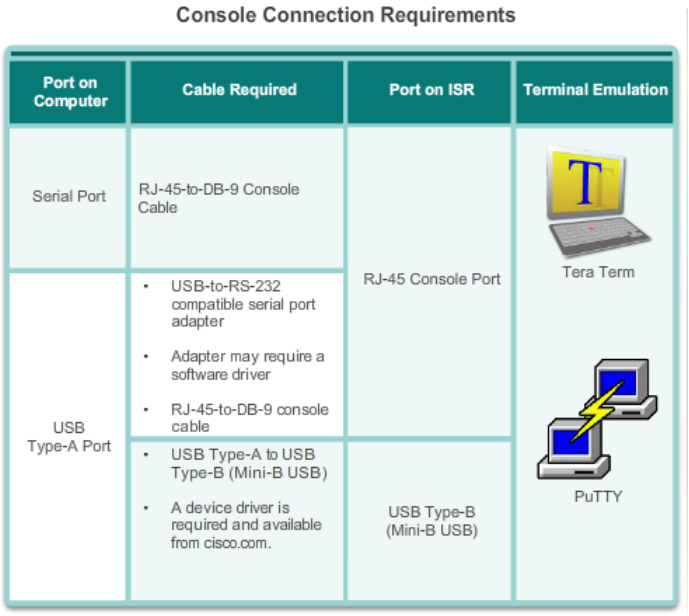


Fig. 4.4 Akses konsul

4.5 Konfigurasi Dasar Router

Router Cisco dan switch Cisco memiliki banyak kesamaan. Mereka mendukung sistem operasi serupa, struktur perintah yang sama, dan banyak dari perintah yang sama. Selain itu, kedua perangkat memiliki langkah-langkah konfigurasi awal yang sama.

Ketika mengkonfigurasi switch Cisco atau router, tugas pokok berikut harus dilakukan pertama:

- Nama perangkat : Membedakan dari router lainnya.
- Akses manajemen aman : Mengamankan EXEC istimewa, EXEC pengguna, dan akses Telnet, dan mengenkripsi password ke tingkat tertinggi.

Mengkonfigurasi banner - Menyediakan pemberitahuan hukum dari akses yang tidak sah. Pada gambar 4.5 sampai 4.8 contoh konfigurasi pengaturan dasar pada router R1:

Dalam Gambar 4.5, penamaan perangkat. Pada Gambar 4.6, akses manajemen. Pada Gambar 4.7, banner dikonfigurasi. Pada Gambar 4.8, konfigurasi tersebut disimpan.

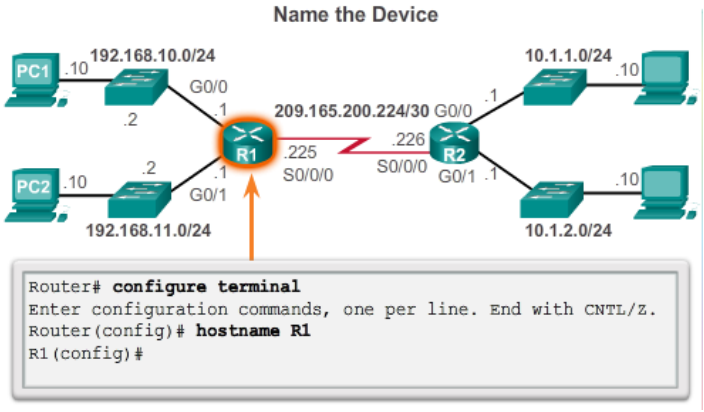


Fig. 4.5 Konfigurasi nama perangkat

4.6 Konfigurasi IPv4 Router Interface

Salah satu fitur yang membedakan antara switch dan router adalah jenis interface yang didukung oleh masing-masing perangkat. Misalnya, Layer 2 dukungan LAN switch karena itu memiliki beberapa FastEthernet atau port Gigabit Ethernet.

Router dukungan LAN dan WAN dan dapat interkoneksi berbagai jenis jaringan. Oleh karena itu, mereka mendukung banyak jenis interfaces. Misalnya, ISRS G2 memiliki satu atau dua terintegrasi Gigabit Ethernet interface dan High-Speed WAN Interface Card (HWIC) slot untuk mengakomodasi jenis interface jaringan, termasuk serial, DSL, dan cable interfaces.

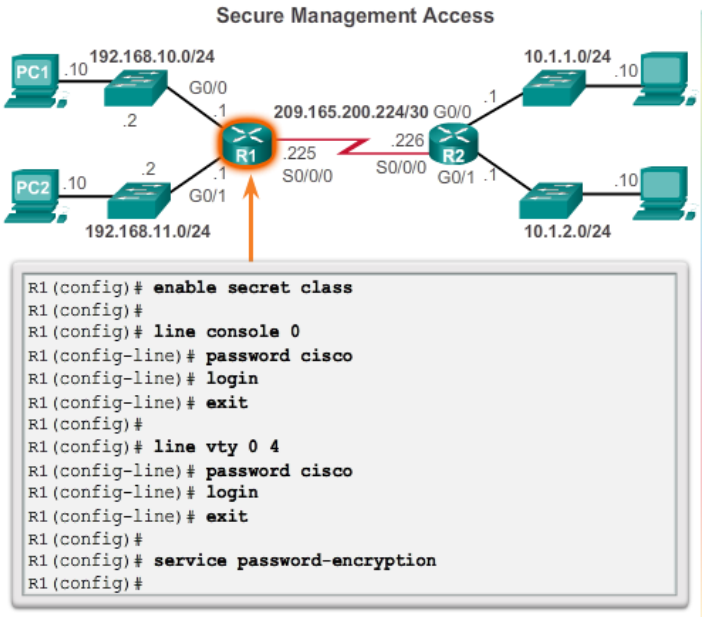


Fig. 4.6 Konfigurasi akses manajemen

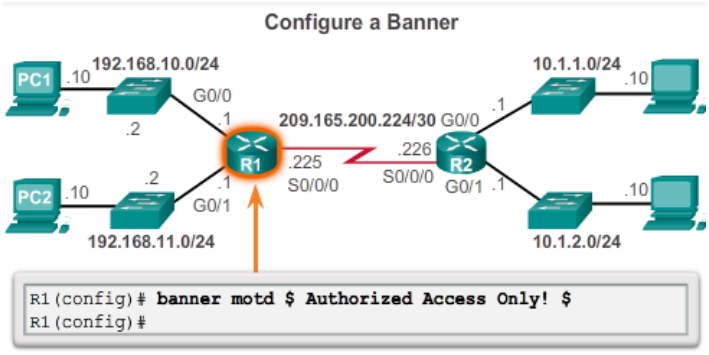


Fig. 4.7 Konfigurasi banner

4.7 Konfigurasi IPv6 Router Intaface

Konfigurasi pada interface IPv6 mirip dengan mengkonfigurasi sebuah interfcae IPv4. Kebanyakan IPv6 konfigurasi dan verifikasi perintah dalam IOS Cisco sangat mirip dengan IPv4. Dalam banyak kasus, satu-satunya perbedaan menggunakan ipv6 di perintah.

Sebuah interface IPv6 harus:

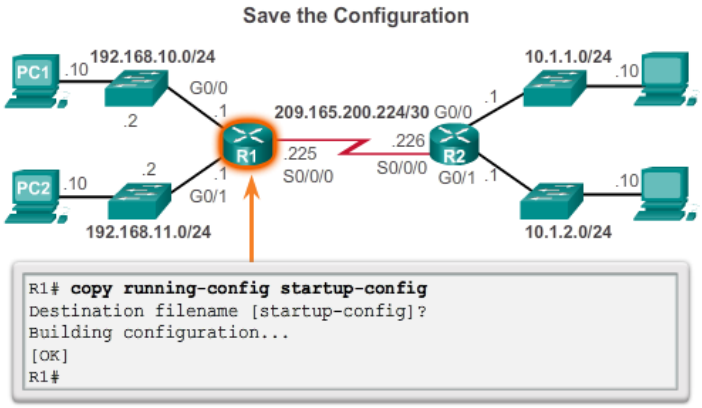


Fig. 4.8 Menyimpan konfigurasi

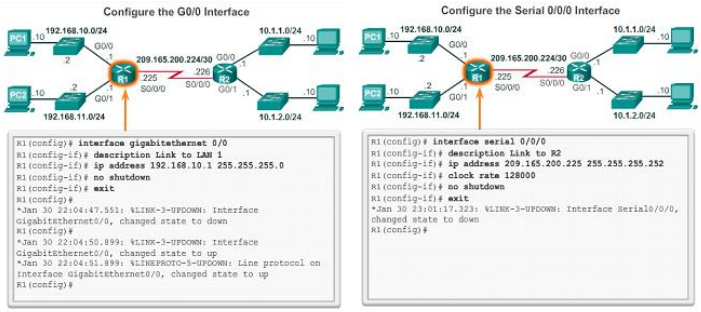


Fig. 4.9 Konfigurasi IPv4 router interface

- Konfigurasi IPv6 dengan alamat dan subnet mask : ”ipv6-address / prefix-length [link-lokal — eui-64]”.
- Aktifkan - Interface harus diaktifkan menggunakan perintah ”no shutdown”.

4.8 Lab Configurasi Basic Router Settings with IOS CLI

Verifikasi konektivitas jaringan

1. PING PC-B dari comand prompt pada PC-A
2. Akses jarak jauh R1 dari PC-A Menggunakan perintah Telnet pada comand prompt

   Pertanyaan :

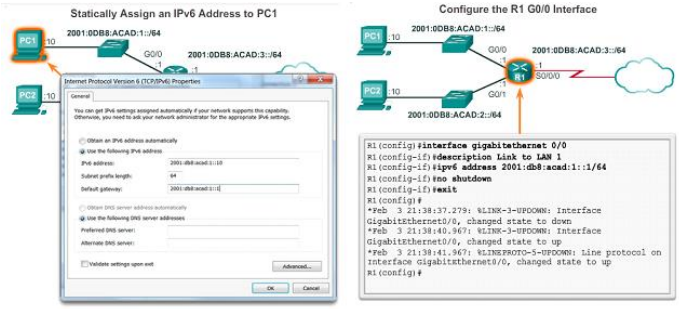
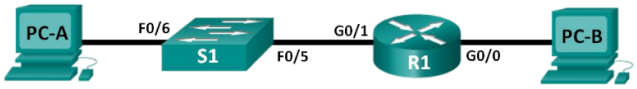


Fig. 4.10 Konfigurasi IPv6 router interface

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.0.1	255.255.255.0	N/A
	G0/1	192.168.1.1	255.255.255.0	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.0.3	255.255.255.0	192.168.0.1

Fig. 4.11 Lab Topology

1. Apakah akses remote sukses?
2. Mengapa protokol Telnet dianggap sebagai risiko keamanan?

4.9 Fungsi Router Switching

Fungsi utama dari router adalah untuk meneruskan paket ke tujuan mereka. Hal ini dicapai dengan menggunakan fungsi switching, yang merupakan proses yang digunakan oleh router untuk menerima paket dari satu interface dan meneruskannya dari antarmuka lain. Tanggung jawab utama dari fungsi switching untuk merangkum paket dalam data link tipe frame yang sesuai untuk data link keluar.

Catatan: Dalam konteks ini, istilah ”switching” secara benar berarti bergerak paket dari sumber ke tujuan dan tidak harus bingung dengan fungsi dari Layer 2 switch.

Apa yang router lakukan dengan paket yang diterima dari satu jaringan dan ditujukan untuk jaringan lain? Router melakukan berikut tiga langkah utama :

Konfigurasi R1

```
Router>enable
Router#
Router#config terminal
Router(config)#
Router(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#security passwords min-length 10
R1(config)#enable secret cisco12345

R1(config)#line con 0
R1(config-line)#password ciscoconpass
R1(config-line)#exec-timeout 5 0
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#
R1(config)#line vty 0 4
R1(config-line)#password ciscovtypass
R1(config-line)#exec-timeout 5 0
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#
R1(config)#service password-encryption
R1(config)#banner motd #Cisco Networking Academy Program"#

R1(config)# int g0/0
R1(config-if)# decription Connection to PC-B
R1(config-if)# ip address 192.168.0.1 255.255.255.0
R1(config-if)# no shutdown
R1(config)# int g0/1
R1(config-if)# decription Connection to S1
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# exit
R1# clock set 17:00:00 18 Sep 2016
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Fig. 4.12 Konfigurasi R1

1. De-encapsulates Layer 2 frame header dan trailer yang mengekspos Layer 3 paket.

2. Memeriksa alamat IP tujuan dari paket IP untuk menemukan jalan terbaik dalam tabel routing.
3. Jika router menemukan jalan ke tujuan, itu encapsulates Layer 3 paket menjadi baru Layer 2 frame dan meneruskan frame keluar interface exit

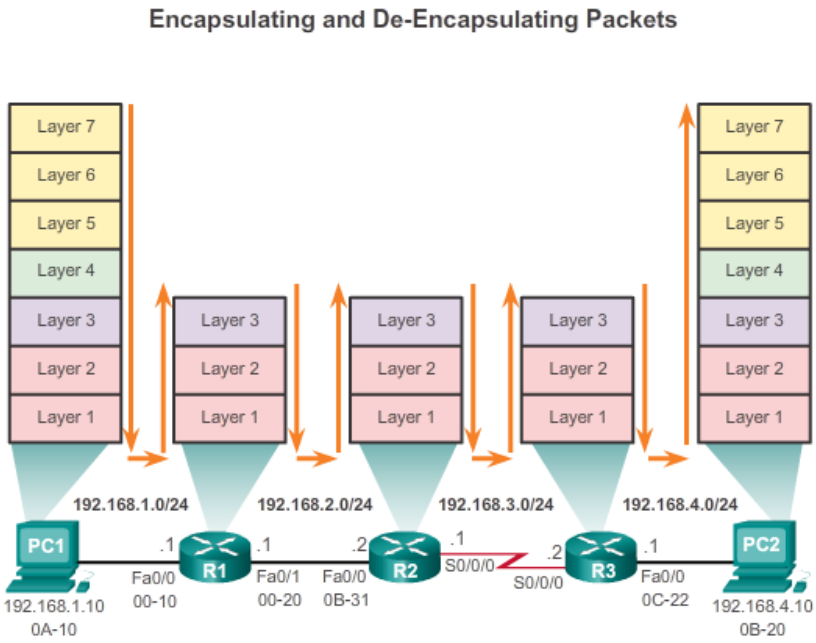


Fig. 4.13 Enkapsulasi dan De-enkapsulasi packet

Seperti yang ditunjukkan pada gambar, perangkat Layer 3 memiliki alamat IPv4 dan interface Ethernet memiliki alamat Layer 2 data link. Misalnya, PC1 dikonfigurasi dengan alamat IPv4 192.168.1.10 dan contoh alamat MAC 0A-10. Sebagai sebuah paket perjalanan dari perangkat sumber ke perangkat tujuan akhir, Layer 3 IP address tidak berubah. Namun, Layer 2 address data link berubah pada setiap hop sebagai paket adalah de-encapsulated dan kembali dikemas dalam frame baru oleh masing-masing router. Hal ini sangat mungkin bahwa paket yang dikemas dalam berbagai jenis frame Layer 2 dari yang di mana ia diterima. Sebagai contoh, sebuah frame Ethernet mungkin diterima oleh router pada interface FastEthernet, kemudian diproses untuk diteruskan keluar dari interface serial sebagai Point-to-Point Protocol (PPP) encapsulated frame.

Pada gambar 4.14, PC1 mengirimkan sebuah paket ke PC2. PC1 harus menentukan apakah tujuan alamat IPv4 adalah jaringan yang sama. Jika alamat jaringan tujuan adalah jaringan yang sama dengan PC1, maka PC1 tidak menggunakan de-

fault gateway. Sebaliknya, PC1 mengacu ke cache ARP untuk alamat MAC dari perangkat dengan alamat IPv4 tujuan.

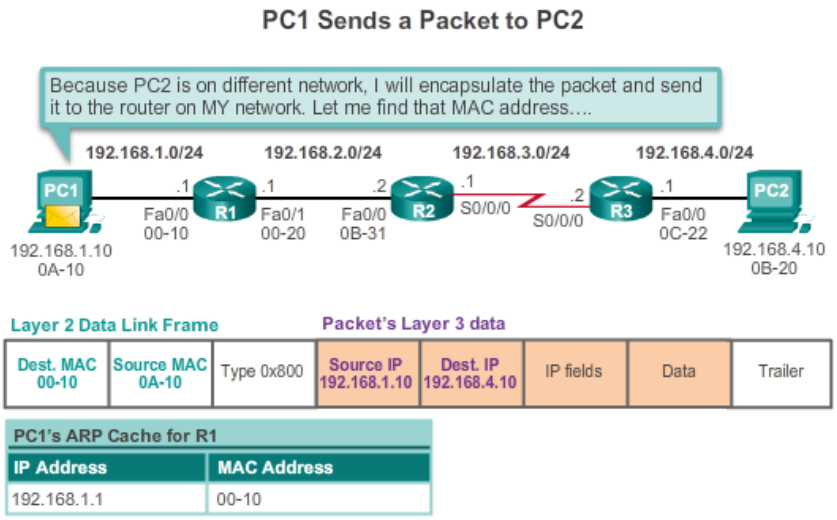


Fig. 4.14 Pengiriman paket

Jika alamat MAC tidak dalam cache, maka PC1 menghasilkan permintaan ARP untuk memperoleh alamat untuk menyelesaikan paket dan mengirimkannya ke tujuan. Jika alamat jaringan tujuan adalah pada jaringan yang berbeda, maka PC1 meneruskan paket ke gateway default. Untuk menentukan alamat MAC dari default gateway, PC1 memeriksa tabel ARP untuk alamat IPv4 dari default gateway dan alamat MAC yang terkait. Jika entri ARP tidak ada dalam tabel ARP untuk gateway default, PC1 mengirimkan sebuah permintaan ARP. Router R1 mengirimkan kembali balasan ARP. PC1 kemudian dapat meneruskan paket ke alamat MAC dari default gateway, Fa0 / 0 interface router R1.

Proses berikut terjadi ketika R1 menerima Ethernet Frame dari PC1:

1. R1 memeriksa alamat tujuan MAC, yang sesuai dengan alamat MAC dari interface penerima, FastEthernet 0/0. R1, oleh karena itu, salinan frame ke buffer.
2. R1 mengidentifikasi Ethernet Type lapangan sebagai 0x800, yang berarti bahwa Ethernet Frame mengandung sebuah paket IPv4 di bagian data dari frame.
3. R1 de-encapsulates Ethernet Frame.
4. Karena alamat IPv4 tujuan dari paket tidak cocok dengan jaringan yang terhubung langsung dari R1, R1 berkonsultasi dengan tabel routing untuk rute paket ini. R1 mencari tabel routing untuk alamat jaringan yang akan mencakup alamat IPv4 tujuan dari paket sebagai alamat host dalam jaringan tersebut. Dalam contoh ini, tabel routing memiliki rute untuk 192.168.4.0/24 jaringan. Alamat IPv4 tujuan paket adalah 192.168.4.10, yang merupakan alamat host IPv4 pada jaringan.

Rute yang R1 menemukan ke 192.168.4.0/24 jaringan memiliki alamat IPv4 next-hop dari 192.168.2.2 dan antarmuka keluar dari FastEthernet 0/1. Ini berarti bahwa paket IPv4 di encapsulated dalam Frame Ethernet baru dengan tujuan alamat MAC dari alamat IPv4 dari router next-hop. Karena interface keluar adalah jaringan Ethernet, R1 harus menyelesaikan alamat IPv4 next-hop dengan tujuan alamat MAC menggunakan ARP:

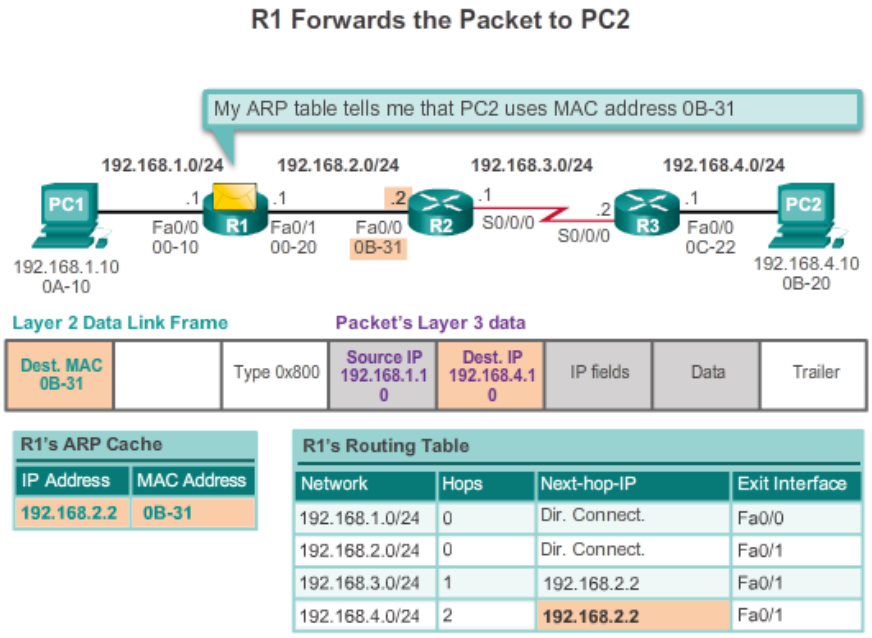


Fig. 4.15 Forward paket

1. R1 melihat next-hop alamat IPv4 dari 192.168.2.2 dalam cache ARP nya. Jika entri tidak dalam cache ARP, R1 akan mengirim permintaan ARP keluar dari antarmuka FastEthernet 0/1 dan R2 akan mengirim kembali balasan ARP. R1 maka akan memperbarui cache ARP dengan entri untuk 192.168.2.2 dan alamat terkait MAC.
2. IPv4 packet sekarang di encapsulated menjadi frame Ethernet baru dan diteruskan keluar interface FastEthernet 0/1 dari R1.

4.10 Summary

Ada banyak kunci struktur dan karakteristik yang berhubungan dengan kinerja ketika membahas jaringan : topologi, kecepatan, biaya, keamanan, ketersediaan, skalabilitas, dan kehandalan.

Router Cisco dan Switch Cisco memiliki banyak kesamaan. Mereka mendukung sistem serupa sistem operasi, struktur comand yang sama, dan banyak dari perintah yang sama. Salah satu fitur yang membedakan antara switch dan router adalah jenis interface yang didukung oleh masing-masing.

Tujuan utama dari router adalah untuk menghubungkan beberapa jaringan dan meneruskan paket dari satu jaringan ke jaringan berikutnya. Ini berarti bahwa router biasanya memiliki beberapa interface. Setiap interface adalah anggota atau host pada jaringan IP yang berbeda.

Cisco IOS menggunakan apa yang dikenal sebagai jarak administratif (AD) untuk menentukan rute untuk menginstal ke dalam IP tabel routing. Tabel routing adalah daftar jaringan yang dikenal oleh router. Tabel routing termasuk alamat jaringan untuk interface itu sendiri, yang merupakan jaringan yang terhubung langsung, serta alamat jaringan untuk jaringan jarak jauh. Sebuah jaringan remote adalah jaringan yang hanya dapat dicapai dengan meneruskan paket ke router lain. Jaringan jarak jauh ditambahkan ke tabel routing dalam dua cara: baik oleh administrator jaringan secara manual mengkonfigurasi rute statis atau dengan menerapkan protokol routing dinamis. rute statis tidak memiliki banyak overhead protokol routing dinamis; Namun, rute statis dapat memerlukan perawatan lebih jika topologi terus berubah atau tidak stabil.

Protokol routing dinamis secara otomatis menyesuaikan diri dengan perubahan tanpa intervensi dari administrator jaringan. protokol routing dinamis memerlukan lebih banyak pemrosesan CPU dan juga menggunakan sejumlah kapasitas link untuk routing update dan pesan. Dalam banyak kasus, tabel routing akan berisi rute kedua statis dan dinamis.

Router membuat keputusan forwarding utama mereka di Layer 3, lapisan Network. Namun, Interface router berpartisipasi dalam Layers 1, 2, dan 3. paket Layer 3 IP diringkas menjadi Layer 2 data link frame dan dikodekan menjadi bit pada Layer 1. interface Router berpartisipasi dalam Layer 2 proses yang terkait dengan enkapsulasi mereka. Sebagai contoh, sebuah interface Ethernet pada router berpartisipasi dalam proses ARP seperti host lain pada LAN.

Cisco IP tabel routing bukan database datar. Tabel routing sebenarnya adalah sebuah struktur hirarkis yang digunakan untuk mempercepat proses pencarian ketika mencari rute dan meneruskan paket.

Chapter 5
Inter-VLAN Routing

5.1 Pendahuluan

VLAN dibuat dengan encapsulation dot 1Q berdasarkan IEEE 802.1Q, yaitu terjadi peristiwa tagging oleh switch pada header frame ethernet, berupa VLAN ID, dan dengan tag yang terdapat pada header frame inilah maka switch akan melihat port mana saja yang mempunyai VLAN ID yang sama dengan frame tersebut, frame hanya akan diteruskan menuju port yang di set dengan VLAN ID yang sama dan tidak akan diteruskan menuju port dengan VLAN ID yang berbeda, dengan metode inilah maka terjadilah segmentasi LAN berdasarkan port pada switch, sehingga broadcast yang dihasilkan oleh salah satu host tidak akan diteruskan menuju port dengan VLAN ID yang berbeda atau hanya akan diteruskan ke port dengan VLAN ID yang sama, sehingga terjadi efisiensi pemakaian bandwidth. Kondisi inilah yang membuat VLAN seolah-olah mempunyai banyak LAN dalam pengertian logical tetapi sebenarnya berada dalam satu LAN dalam pengertian physical.

LAN-LAN yang berbeda pada VLAN ini harus mempunyai alamat network yang berbeda, sesuai dengan prinsip dasar di network, maka jika ada dua atau lebih alamat network yang berbeda ingin berkomunikasi maka harus melakukan peristiwa routing. Pada peralatan Cisco, routing antar VLAN bisa dilakukan oeh switch itu sendiri asalkan switch tersebut mempunyai fasilitas routing yaitu Layer 3 Switch, jadi ada switch yang hanya mendukung layer 2 dan ada switch yang mendukung layer 3, tentu dari sisi praktis layer 3 switch lebih praktis, dalam artian kita bisa membuat VLAN sekaligus melakukan routing sehingga antar VLAN yang berbeda tadi bisa berkomunikasi, tetapi darisisi cost, peralatan switch layer 3 mempunyai harga yang lebih mahal dari switch layer 2. Jadi inter-VLAN dibedakan menjadi 3 yaitu:

- Multilayer Switch *Untuk Switch layer 3.
- Inter-VLAN Router
- Router On a Stick

5.2 Konfigurasi Inter-VLAN

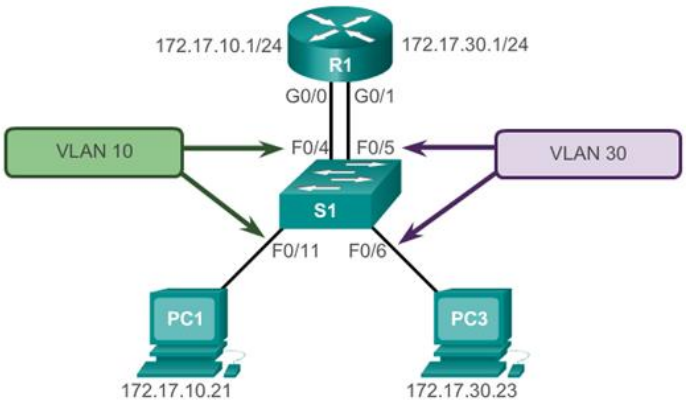


Fig. 5.1 Topologi Inter-VLAN

Dari gambar 5.1 diatas kita dapat melihat bahwa kabel yang terkoneksi dari Switch dengan Router sebanyak vlan sejumlah 2 buah (vlan 10 dan vlan 30), maka perhatikan port yang akan kita gunakan. Gambar 5.2 merupakan konfigurasi sesuai dengan letak vlan berada di port switch.

```
S1(config)# vlan 10
S1(config-vlan)# vlan 30
S1(config-vlan)# interface f0/11
S1(config-if)# switchport access vlan 10
S1(config-if)# interface f0/4
S1(config-if)# switchport access vlan 10
S1(config-if)# interface f0/6
S1(config-if)# switchport access vlan 30
S1(config-if)# interface f0/5
S1(config-if)# switchport access vlan 30
S1(config-if)# end
*Mar 20 01:22:56.751: %SYS-5-CONFIG_I: Configured from console by
console
S1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Fig. 5.2 Konfigurasi Inter-VLAN

Dari gambar 5.3 terdapat 1 kabel yang terkoneksi antara switch dengan router, maka pada sisi port router kita perlu membuat enkapsulasi dot1qdan subinterface. Subinterface berfungsi sebagai representasi interface secara logika pada satu inter-

face pisik pada port, sehingga satu interface pisik mampu diisi lebih dari 2 subinterface (interface secara logika) dan tiap tiap subinterface bisa diberikan alamat IP.

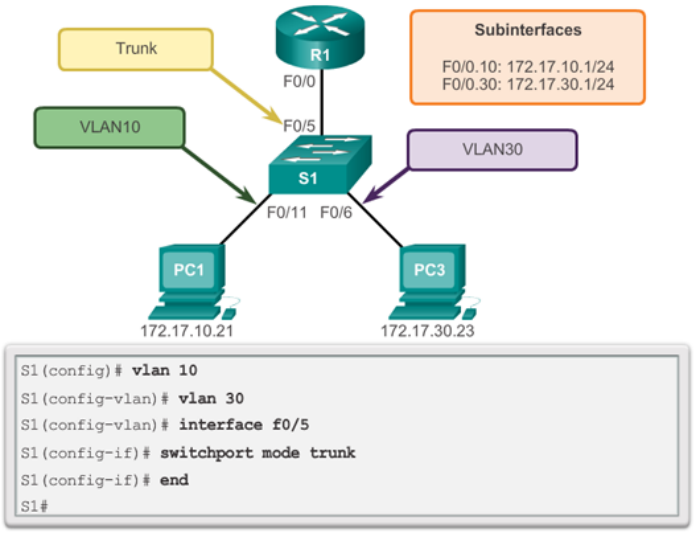


Fig. 5.3 Topologi Router On A Stick

Setelah melakukan enkapsulasi, inputkan konfigurasi subinterface sesuai dengan ID vlan yang sudah dibuat.

5.3 Tugas Lab

Buatlah topologi dan lakukan konfigurasi sesuai dengan gambar dibawah ini. *untuk alamat IP dibebaskan. Lakukan konfigurasi dengan benar dan kumpulkan file PKA pada dosen.

```
R1(config)# interface g0/0.10
R1(config-subif)# encapsulation dot1q 10
R1(config-subif)# ip address 172.17.10.1 255.255.255.0
R1(config-subif)# interface g0/0.30
R1(config-subif)# encapsulation dot1q 30
R1(config-subif)# ip address 172.17.30.1 255.255.255.0
R1(config)# interface g0/0
R1(config-if)# no shutdown
*Mar 20 00:20:59.299: %LINK-3-UPDOWN: Interface GigabitEthernet0/0,
 changed state to down
*Mar 20 00:21:02.919: %LINK-3-UPDOWN: Interface GigabitEthernet0/0,
 changed state to up
*Mar 20 00:21:03.919: %LINEPROTO-5-UPDOWN: Line protocol on
 changed state to down
*Mar 20 00:21:02.919: %LINK-3-UPDOWN: Interface GigabitEthernet0/0,
 changed state to up
*Mar 20 00:21:03.919: %LINEPROTO-5-UPDOWN: Line protocol on
 Interface GigabitEthernet0/0, changed state to up
```

Fig. 5.4 Konfigurasi Router On A Stick

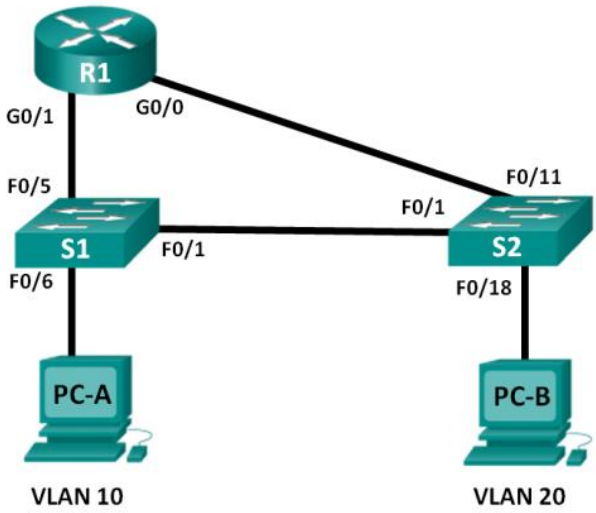


Fig. 5.5 Tugas Lab

Chapter 6
Routing Statis

6.1 Pendahuluan

Routing adalah inti dari setiap proses pengiriman paket data dari jaringan sumber (source) ke jaringan tujuan (destination). Seperti yang telah dijelaskan dalam bab I, router akan belajar tentang network tujuan baik secara statis menggunakan static routing maupun secara dinamis menggunakan prokotol routing untuk dapat meneruskan sebuah paket dari sumber (source) ke tujuan (destination). Pada bab II ini akan dibahas secara mendalam tentang konsep, konfigurasi dan implementasi salah protokol routing yang dapat menjadi salah satu pilihan dalam membangun sebuah jaringan komputer, routing tersebut adalah static routing.

Static Routing dikonfigurasi secara manual dengan menambahkan route route pada tabel routing di setiap router. Proses routing yang dilakukan dengan manambahkan secara manual information routing ke dalam tabel routing disebut dengan Static Routing. Suatu static route akan berfungsi sempurna jika routing table berisi suatu route untuk setiap jaringan di dalam internetwork yang mana di konfigurasi dilakukan secara manual oleh administrator jaringan. Setiap host pada jaringan harus dikonfigurasi untuk mengarahkan paket data kepada default route atau default gateway agar sesuai dengan IP address dari interface local router, di mana router memeriksa routing table dan menentukan route yang mana digunakan untuk meneruskan paket tersebut.

Static route terdiri dari perintah-perintah yang konfigurasi secara tersendiri untuk setiap route yang dituju disetiap router. Sebuah router hanya akan meneruskan paket kepada subnet-subnet yang ada pada routing table. Sebuah router selalu mengetahui route dari interface yang bersentuhan langsung kepadanya keluar dari interface router yang mempunyai status up and up pada line interface dan protokolnya. Dengan menambahkan static route, sebuah router dapat diberitahukan kemana harus meneruskan paket-paket kepada subnet-subnet yang tidak bersentuhan langsung kepadanya.

Ada beberapa keuntungan dan kekurangan pada saat menggunakan static routing dibandingankan dengan menggunakan dinamic routing.

- Keuntungan keuntungan yang didapat pada saat menggunakan static routing antara lain : Tidak ada overhead (waktu pemrosesan) pada CPU router.
- Tidak ada bandwith yang digunakan pada saat melakukan proses routing diantara beberapa router.
- Static Routing lebih aman daripada Dinamic Routing, karena network administrator dapat memilih untuk mengizinkan akses routing ke network tertentu saja.

Sedangakan kekurangan Static Routing antara lain :

- Network administrator harus benar banar memahami internetwork dan bagaimana mengkonfigurasi router dengan benar agar dapat terhubungan dengan baik.
- Jika sebuah network ditambahkan ke internetwork, administrator harus menambahkan sebuah route ke sumua router secara manual. Dengan kata lain, pekerjaan network adminstrator sangat tidak fleksibel.
- Static Routing tidak cocok digunakan untuk network network yang besar.

Static Routing biasanya digunakan untuk menghubungkan sebuah jaringan dengan spesifik jaringan tertentu dengan menyediakan gateway sehingga dapat terhubung ke stub-network. Static Routing biasanya digunakan juga untuk mengurangi jumlah rute yang tersedia dalam tabel routing melalui proses summarizing dan membuat rute cadangan untuk dapat sampai ke jaringan tujuan apabila rute utama mengalami ganguan. Static Routing umumnya digunakan ketika melakukan proses routing dari stub-network ke stub-network. Sebuah stub-network merupakan network yang memiliki rute tunggal. Sebagai contoh , pada Gambar 2.1 kita melihat bahwa setiap network yang terhubung ke R1 hanya akan memiliki satu cara untuk mencapai tujuan lain, baik ke network R2 atau tujuan lain diluar R2. Oleh karena itu network 172.16.3.0 adalah stub-network dan R1.

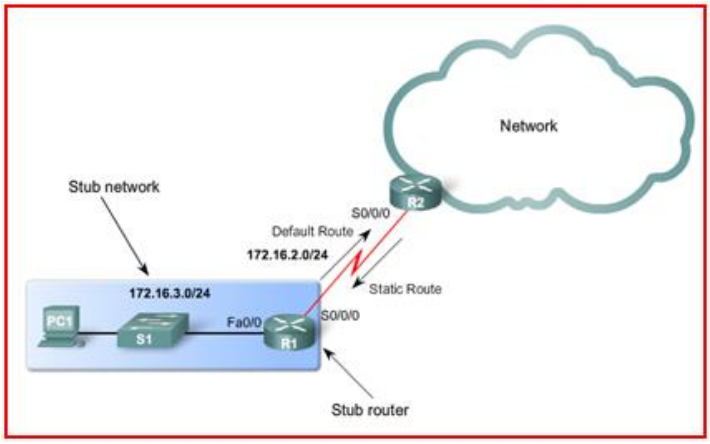


Fig. 6.1 Stub-network

Dalam static routing ada yang disebut dengan default route. Defalut route adalah jalur default untuk paket yang mempunyai alamat network tujuan tertentu tapi tidak terdapat di routing table router yang disinggahi. Jika terdapat default route yang di-set pada router tersebut, maka paket tersebut akan mengikuti rute default yang telah ditetapkan, jika tidak ada default route maka paket akan dibuang/discard. Default route didefiniskan dengan alamat : 0.0.0.0/0 . Default route pada routing table ditandai dengan flag ”S*”.

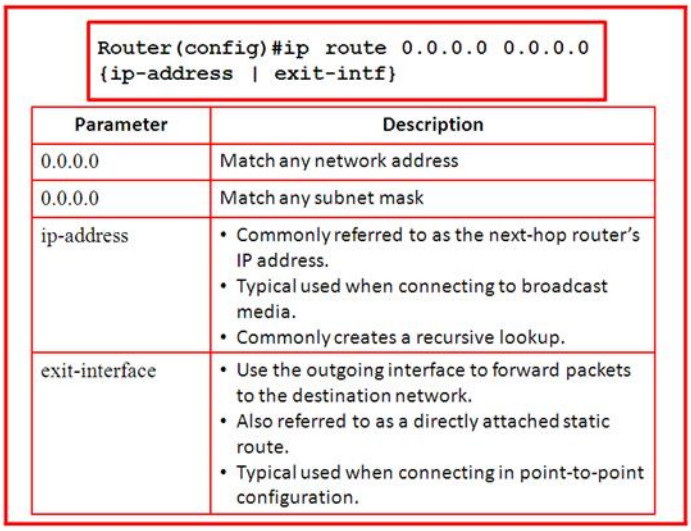


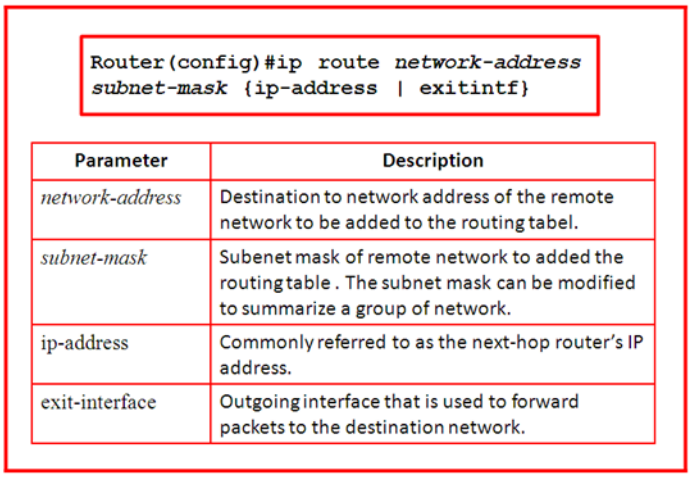
Fig. 6.2 Perintah Default Static Route

6.2 Konfigurasi IPv4 Static Routing

Perintah yang digunakan untuk mengkonfigurasi IPv4 static routing adalah dengan menuliskan perintah ip route pada mode config dalam CLI. Sintaks lengkap yang untuk mengkonfigurasi static routing adalah sebagai berikut :

Keterangan :

- Ip route : perintah ini digunakan untuk menciptakan route statis.
- Network address : perintah yang digunakan untuk menentukan network tujuan didalam jaringan.
- Subnet mask : subnet mask dari network tujuan.



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

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

Fig. 6.3 Konfigurasi IPv4 static routing

- IP address / exit interface : IP address adalah alamat dari router di hop berikutnya (next hop) yang akan menerima paket dan meneruskannya ke network tujuan. Alamat netx hop address adalah sebuah interface router yang berada disebuah network yang terhubung secara langsung. Sedangkan exit interface adalah penulisan nama interface router untuk meneruskan paket ke next hop.

Setelah konfigursi IPv4 static routing dilakukan pada router, untuk memastikan apakah routing telah dikonfigurasi dengan baik, dapat menggunakan perintah show ip route, show ip route static dan show ip route network untuk melakukan verifikasi. Adapun fungsi-fungsi perintah tersebut adalah :

- Show ip route : perintah ini digunakan untuk menampilkan isi tabel routing.
- Show ip route static : perintah ini digunakan untuk mempilkan informasi static routing yang ada di dalam tabel routing.

6.3 Konfigurasi IPv6 Static Routing

Perintah yang digunakan untuk mengkonfigurasi IPv6 static routing adalah dengan menuliskan perintah ipv6 route pada mode config dalam CLI. Sintaks lengkap yang untuk mengkonfigurasi static routing adalah sebagai berikut :

Keterangan :

- Ipv6 route : perintah ini digunakan untuk menciptakan route statis dengan menggunakan IPv6.

```
Router(config)#ipv6 route ipv6-prefix/ipv6-mask
{ipv6-address | exit-intf}
```

Parameter	Description
ipv6-prefix	Destination to ipv6-prefix (network address) of the remote network to be added to the routing tabel.
ipv6-mask	ipv6-mask of remote network to added the routing table . The subnet mask can be modified to summarize a group of network.
ipv6-address	Commonly referred to as the next-hop router's ipv6 address.
exit-intf	Outgoing interface that is used to forward packets to the destination network.

Fig. 6.4 Konfigurasi IPv6 static routing

- Ipv6-prefix/ipv6-mask : perintah yang digunakan untuk menentukan network tujuan didalam jaringan.
- Ipv6-address / exit interface : IPv6 address adalah alamat dari router di hop berikutnya (next hop) yang akan menerima paket dan meneruskannya ke network tujuan. Alamat netx hop address adalah sebuah interface router yang berada disebuah network yang terhubung secara langsung. Sedangkan exit interface adalah penulisan nama interface router untuk meneruskan paket ke next hop.

6.4 Contoh Konfigurasi IPv4 Static Routing Pada Topology Jaringan

Pada subbab ini akan dikonfigurasi tiga buah router yaitu R1, R2, dan R3 yang ada pada topology diatas dengan menggunakan IPv4 static routing sebagai protokol routingnya.

Skenario :

Pada topology di atas, terdapat tiga buah router yaitu : R1, R2, dan R3. Ketiga router tersebut terhubung dengan menggunakan koneksi WAN dengan kabel Serial yang dihubungkan pada port Serial 0/0/0 pada R1, port Serial 0/0/0 dan 0/0/1 pada R2 dan port Serial 0/0/1 pada R3.

Masing masing router terhung ke switch (SW) yang merupakan koneksi LAN dengan menggunakan port Fastehernet 1/0. Dan masing masin switch (SW) terkoneksi terhadap PC.

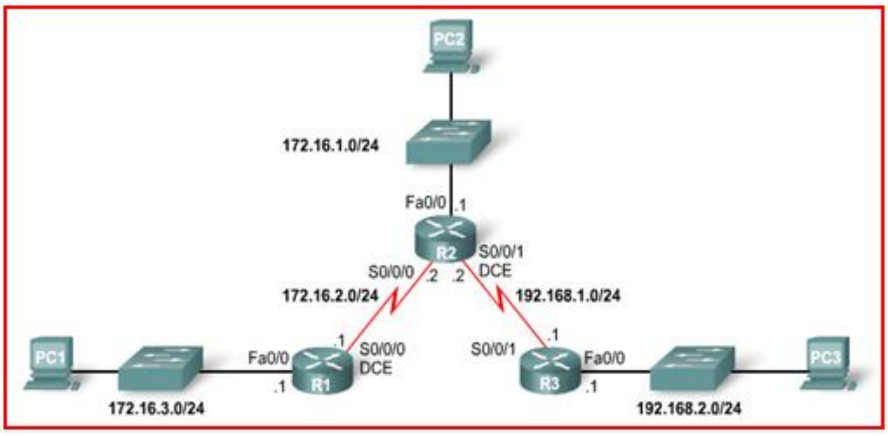


Fig. 6.5 Konfigurasi IPv4 Static Routing Pada Topology Jaringan

Peralatan dan Hardware

Table 6.1 Factors and Willis Deutsch

Hardware	Jumlah	Keterangan
Cisco Router	3	
Cisco Switch	3	
Computer (Host)	3	1 Computer host untuk setiap switch
CAT-5 or better straight-through UTP cables	6	Connects Router to switch, Host1, Host2 and Host3 to switch
Serial cable	2	Connect R1 to R2 to R3

Tabel IP Address

Pada skenarion ini, konfigurasi yang akan dilakukan pada masing masing router adalah :

- Router name
- Priviledge password
- Line console dan Line vty password
- Banner motd
- Konfigurasi interface (Fastehernet dan Serial)
- Konfigurasi Routing menggunakan IPv4 Static Routing

Table 6.2 Factors and Willis Deutsch

Device	Interface	IP Address	Subnet Mask	Default Gateway
R 1	Fa0/0	172.16.3.1	255.255.255.0	N/A
	S0/0/0	172.16.2.1	255.255.255.0	N/A
R 2	Fa0/0	172.16.1.1	255.255.255.0	N/A
	S0/0/0	172.16.2.2	255.255.255.0	N/A
	S0/0/1	172.168.1.2	255.255.255.0	N/A
R 3	Fa0/0	192.168.2.1	255.255.255.0	N/A
	S0/0/1	192.168.1.1	255.255.255.0	N/A
PC	PC 1	172.16.3.2	255.255.255.0	172.16.3.1
	PC 2	172.16.1.2	255.255.255.0	172.16.1.1
	PC 3	192.168.2.2	255.255.255.0	192.168.2.1

6.5 Contoh Konfigurasi IPv6 Static Routing Pada Topology Jaringan

Pada subbab ini akan dikonfigurasi tiga buah router yaitu R1, R2, dan R3 yang ada pada topology diatas dengan menggunakan IPv6 static routing sebagai protokol routingnya.

Skenario :

Pada topology di atas, terdapat tiga buah router yaitu : R1, R2, dan R3. Ketiga router tersebut terhubung dengan menggunakan koneksi WAN dengan kabel Serial yang dihubungkan pada port Serial 0/0/0 pada R1, port Serial 0/0/0 dan 0/0/1 pada R2 dan port Serial 0/0/1 pada R3.

Masing masing router terhung ke switch (SW) yang merupakan koneksi LAN dengan menggunakan port Gigaethernet 0/0. Dan masing masin switch (SW) terkoneksi terhadap PC.

Peralatan dan Hardware

Table 6.3 Factors and Willis Deutsch

Hardware	Jumlah	Keterangan
Cisco Router	3	Cisco Router 2911
Cisco Switch	3	Catalyst 2960
Computer (Host)	3	1 Computer host untuk setiap switch
CAT-5 or better straight-through UTP cables	6	Connects Router to switch, Host1, Host2 and Host3 to switch
Serial cable	2	Connect R1 to R2 to R3

Konfigurasi R1

```
Router>enable
Router#configure terminal
Router(config)#hostname R1
R1(config)#enable secret cisco
R1 (config)#line console 0
R1 (config-line)#password cisco
R1 (config-line)#login
R1 (config-line)#exit
R1 (config)#line vty 0 4
R1 (config-line)#password cisco
R1 (config-line)#login
R1 (config-line)#exit
R1 (config)#banner motd &
Enter TEXT message.  End with the character '&'.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!    AUTORIZED ACCESS ONLY   !!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!  &
R1 (config)#interface serial 0/0/0
R1 (config-if)#ip address 172.16.2.1 255.255.255.0
R1 (config-if)#clock rate 64000
R1 (config-if)#no shutdown
R1 (config-if)#exit
R1 (config)#interface fastethernet 0/0
R1 (config-if)#ip address 172.16.3.1 255.255.255.0
R1 (config-if)#no shutdown
R1 (config-if)#exit
R1 (config)# ip route 172.16.1.0 255.255.255.0 172.16.2.2
R1 (config)# ip route 192.168.2.0 255.255.255.0 172.16.2.2
R1 (config)#exit
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Fig. 6.6 Konfigurasi R1

Tabel IP Address

Pada skenarion ini, konfigurasi yang akan dilakukan pada masing masing router adalah :

- Router name
- Priviledge password
- Line console dan Line vty password
- Banner motd

Konfigurasi R2

```
Router>enable
Router#configure terminal
Router(config)#hostname R2
R2(config)#enable secret cisco
R2 (config)#line console 0
R2 (config-line)#password cisco
R2 (config-line)#login
R2 (config-line)#exit
R2 (config)#line vty 0 4
R2 (config-line)#password cisco
R2 (config-line)#login
R2 (config-line)#exit
R2 (config)#banner motd &
Enter TEXT message.  End with the character '&'.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!    AUTORIZED ACCESS ONLY    !!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! &
R2 (config)#interface serial 0/0/0
R2 (config-if)#ip address 172.16.2.2 255.255.255.0
R2 (config-if)#no shutdown
R2 (config-if)#exit
R2 (config)#interface serial 0/0/1
R2 (config-if)#ip address 192.168.1.2 255.255.255.0
R2 (config-if)# clock rate 64000
R2 (config-if)#no shutdown
R2 (config-if)#exit
R2 (config)#interface fastethernet 0/0
R2 (config-if)#ip address 172.16.1.1 255.255.255.0
R2 (config-if)#no shutdown
R2 (config-if)#exit
R2 (config)# ip route 172.16.3.0 255.255.255.0 172.16.2.1
R2 (config)# ip route 192.168.2.0 255.255.255.0
192.168.1.1
R2 (config)#exit
R2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
```

Fig. 6.7 Konfigurasi R2

- Konfigurasi interface (Fastehernet dan Serial)
- Konfigurasi Routing menggunakan IPV6 Static Routing

Konfigurasi R3

```
Router>enable
Router#configure terminal
Router(config)#hostname R3
R3(config)#enable secret cisco
R3 (config)#line console 0
R3 (config-line)#password cisco
R3 (config-line)#login
R3 (config-line)#exit
R3 (config)#line vty 0 4
R3 (config-line)#password cisco
R3 (config-line)#login
R3 (config-line)#exit
R3 (config)#banner motd &
Enter TEXT message.  End with the character '&'.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!     AUTORIZED ACCESS ONLY    !!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! &
R3 (config)#interface serial 0/0/1
R3 (config-if)#ip address 192.168.1.1  255.255.255.0
R3 (config-if)#no shutdown
R3 (config-if)#exit
R3 (config)#interface fastethernet 0/0
R3 (config-if)#ip address 192.168.2.1  255.255.255.0
R3 (config-if)#no shutdown
R3 (config-if)#exit
R3 (config)# ip route 172.16.1.0 255.255.255.0 192.168.1.2
R3 (config)# ip route 172.16.3.0 255.255.255.0 192.168.1.2
R3 (config)#exit
R3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Fig. 6.8 Konfigurasi R3

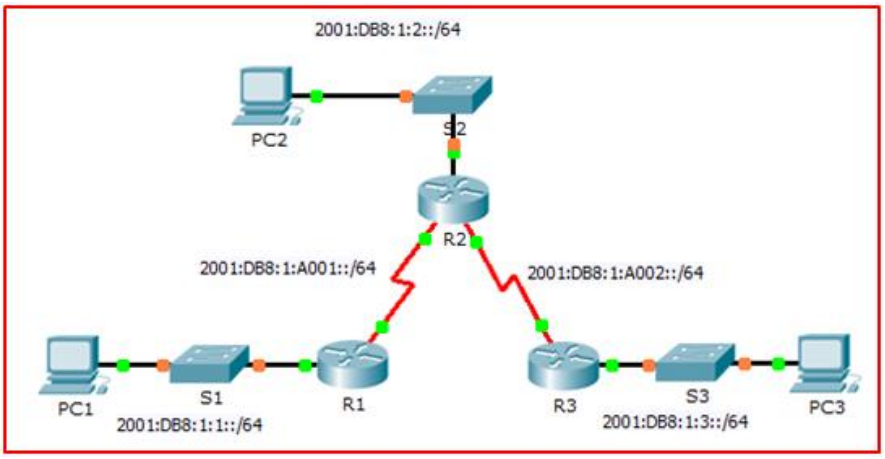


Fig. 6.9 Konfigurasi IPv6 Static Routing Pada Topology Jaringan

Table 6.4 Tabel IP Address

Device	Interface	IPv6 Address/Prefix	Default Gateway
R1	G0/0	2001:DB8:1:1::1/64	N/A
	S0/0/0	2001:DB8:1:A001::1/64	N/A
R2	G0/0	2001:DB8:1:2::1/64	N/A
	S0/0/0	2001:DB8:1:A001::2/64	N/A
	S0/0/1	2001:DB8:1:A002::1/64	N/A
R3	G0/0	2001:DB8:1:3::1/64	N/A
	S0/0/1	2001:DB8:1:A002::2/64	N/A
PC1	NIC	2001:DB8:1:1::F/64	FE80::1
PC2	NIC	2001:DB8:1:2::F/64	FE80::2
PC3	NIC	2001:DB8:1:3::F/64	FE80::3

Konfigurasi R1

```
Router>enable
Router#config terminal
Enter configuration commands, one per line. End with
CNTL/Z.
Router(config)#hostname R1
R1(config)#enable secret cisco
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1 (config)#banner motd &
Enter TEXT message.  End with the character '&'.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!    AUTORIZED ACCESS ONLY   !!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! &
R1(config)#ipv6 unicast-routing
R1(config)#interface gigabitEthernet 0/0
R1(config-if)#ipv6 enable
R1(config-if)#ipv6 address 2001:DB8:1:1::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#int serial 0/0/0
R1(config-if)#ipv6 address 2001:DB8:1:A001::1/64
R1(config-if)#clock rate 128000
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#ipv6 route 2001:DB8:1:2::/64 2001:DB8:1:A001::2
R1(config)#ipv6 route 2001:DB8:1:A002::/64
2001:DB8:1:A001::2
R1(config)#ipv6 route 2001:DB8:1:3::/64 2001:DB8:1:A001::2
R1(config)#exit
R1#copy r s
Destination filename [startup-config]?
Building configuration...
```

Fig. 6.10 Konfigurasi R1

Konfigurasi R2

```
Router>enable
Router#config terminal
Enter configuration commands, one per line. End with
CNTL/Z.
Router(config)#hostname R2
R2(config)#enable secret cisco
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#exit
R2(config)#line vty 0 4
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2 (config)#banner motd &
Enter TEXT message.  End with the character '&'.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!    AUTORIZED ACCESS ONLY    !!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! &
R2(config)#ipv6 unicast-routing
R2(config)#interface gigabitEthernet 0/0
R2(config-if)#ipv6 enable
R2(config-if)#ipv6 address 2001:DB8:1:2::1/64
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#int serial 0/0/0
R2(config-if)#ipv6 address 2001:DB8:1:A001::2/64
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#int serial 0/0/1
R2(config-if)#ipv6 address 2001:DB8:1:A002::1/64
R2(config-if)#clock rate 128000
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#ipv6 route 2001:DB8:1:A002::/64
2001:DB8:1:A001::2
R2(config)# ipv6 route 2001:DB8:1:1::/64 serial0/0/0
R2(config)# ipv6 route 2001:DB8:1:3::/64 serial0/0/0
R2(config)#exit
R2#copy r s
Destination filename [startup-config]?
Building configuration...
[OK]
```

Fig. 6.11 Konfigurasi R2

Konfigurasi R3

```
Router>enable
Router#config terminal
Enter configuration commands, one per line. End with
CNTL/Z.
Router(config)#hostname R1
R3(config)#enable secret cisco
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#exit
R3(config)#line vty 0 4
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3 (config)#banner motd &
Enter TEXT message.  End with the character '&'.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!    AUTORIZED ACCESS ONLY    !!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! &
R3(config)#ipv6 unicast-routing
R3(config)#interface gigabitEthernet 0/0
R3(config-if)#ipv6 enable
R3(config-if)#ipv6 address 2001:DB8:1:3::1/64
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#int serial 0/0/1
R3(config-if)#ipv6 address 2001:DB8:1:A002::2/64
R3(config-if)#clock rate 128000
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#ipv6 route 2001:DB8:1:2::/64
2001:DB8:1:A002::1/64
R3(config)#ipv6 route 2001:DB8:1:A001::/64
2001:DB8:1:A002::1/64
R3(config)#ipv6 route 2001:DB8:1:1::/64
2001:DB8:1:A002::1/64
R3(config)#exit
R3#copy r s
Destination filename [startup-config]?
Building configuration...
[OK]
```

Fig. 6.12 Konfigurasi R3

Chapter 7
Routing Dinamis

7.1 Pendahuluan

Jaringan data yang digunakan dalam kehidupan sehari-hari untuk belajar, bermain, dan dari berbagai pekerjaan kecil, jaringan lokal ke besar, internetwork global. Di rumah, pengguna dapat memiliki router dan dua atau lebih komputer. Di tempat kerja, sebuah organisasi mungkin memiliki beberapa router dan switch melayani kebutuhan komunikasi data ratusan atau bahkan ribuan PC.

Router meneruskan paket dengan menggunakan informasi dalam tabel routing. Rute ke jaringan remote dapat dipelajari oleh router dalam dua cara : rute statis dan rute dinamis. Dalam sebuah jaringan besar dengan banyak jaringan dan subnet, mengkonfigurasi dan memelihara rute statis antara jaringan ini membutuhkan banyak overhead administratif dan operasional. biaya overhead operasional ini terutama rumit ketika perubahan jaringan terjadi, seperti menerapkan subnet baru. Mengimplementasikan protokol routing dinamis dapat meringankan beban konfigurasi dan pemeliharaan tugas dan memberikan skalabilitas jaringan.

Bab ini memperkenalkan protokol routing dinamis. Ini mengeksplorasi manfaat menggunakan protokol routing dinamis, bagaimana yang berbeda protokol routing diklasifikasikan, dan metrik protokol routing digunakan untuk menentukan jalur terbaik untuk lalu lintas jaringan. Topik lain yang dibahas dalam bab ini meliputi karakteristik protokol routing dinamis dan bagaimana berbagai protokol routing berbeda. Jaringan profesional harus memahami protokol routing yang berbeda yang tersedia untuk membuat keputusan tentang kapan harus menggunakan routing statis atau dinamis. Mereka juga perlu mengetahui protokol routing dinamis yang paling tepat dalam lingkungan jaringan tertentu.

7.2 Evolusi Routing Dinamis

Protokol routing dinamis telah digunakan dalam jaringan sejak akhir 1980-an. Salah satu protokol routing pertama adalah Routing Information Protocol (RIP). RIP versi 1 (RIPv1) dirilis pada tahun 1988, tetapi beberapa algoritma dasar dalam protokol yang digunakan pada Advanced Research Projects Agency Network (ARPANET) 1969.

Sebagai jaringan berkembang dan menjadi lebih kompleks, routing protokol baru muncul. Protokol routing RIP yang telah diperbarui untuk mengakomodasi pertumbuhan di lingkungan jaringan, ke RIPv2. Namun, versi yang lebih baru dari RIP masih tidak skala untuk implementasi jaringan yang lebih besar dari saat ini. Untuk mengatasi kebutuhan jaringan yang lebih besar, dua protokol routing maju dikembangkan: Open Shortest Path First (OSPF) dan Intermediate Sistem-to-Intermediate System (IS-IS). Cisco mengembangkan Interior Gateway Routing Protocol (IGRP) dan Ditingkatkan IGRP (EIGRP), yang juga skala baik dalam implementasi jaringan yang lebih besar.

Selain itu, ada kebutuhan untuk menghubungkan internetwork yang berbeda dan menyediakan routing diantara mereka. Border Gateway Protocol (BGP) sekarang digunakan antara penyedia layanan Internet (ISP). BGP juga digunakan antara ISP dan klien pribadi mereka yang lebih besar untuk bertukar informasi routing.

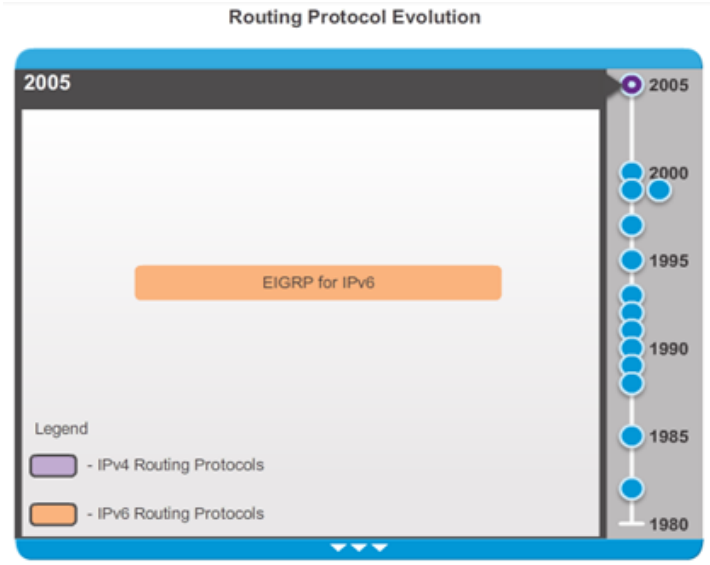


Fig. 7.1 Timeline ketika berbagai protokol diperkenalkan

Dengan munculnya berbagai perangkat pada konsumen yang menggunakan IP, jumlah IPv4 hampir habis; dengan demikian, IPv6 telah muncul. Untuk mendukung

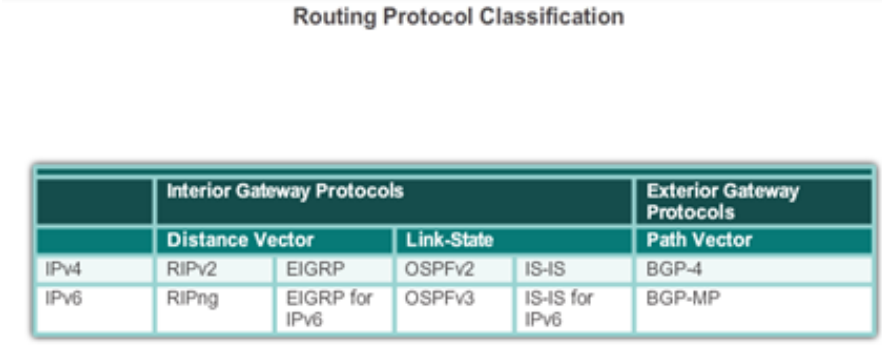


Fig. 7.2 Klasifikasi routing protocol

komunikasi berdasarkan IPv6, versi yang lebih baru dari IP routing protokol telah dikembangkan.

RIP adalah yang paling sederhana dari protokol routing dinamis dan digunakan dalam bagian ini untuk memberikan tingkat dasar pemahaman protokol routing.

7.3 Tujuan Protokol Routing Dinamis

Routing protokol digunakan untuk memfasilitasi pertukaran informasi routing antara router. Sebuah routing protokol adalah seperangkat proses, algoritma, dan pesan yang digunakan untuk bertukar informasi routing dan mengisi tabel routing dengan pilihan routing protokol untuk jalur terbaik.

Tujuan dari protokol routing dinamis meliputi:

- Penemuan jaringan jarak jauh
- Mempertahankan up-to-date informasi routing
- Memilih jalur terbaik ke jaringan tujuan
- Kemampuan untuk menemukan jalan terbaik baru jika jalan saat ini tidak lagi tersedia.

Komponen utama dari protokol routing dinamis meliputi:

- Struktur data : protokol routing biasanya menggunakan tabel atau database untuk operasinya. Informasi ini disimpan dalam RAM.
- Pesan routing protocol : protokol routing menggunakan berbagai jenis pesan untuk menemukan router tetangga, pertukaran informasi routing, dan tugas-tugas lain untuk belajar dan menjaga informasi yang akurat tentang jaringan.
- Algoritma : Algoritma adalah daftar terbatas langkah yang digunakan untuk menyelesaikan tugas. Routing protokol menggunakan algoritma untuk memfasilitasi informasi routing dan penentuan jalur terbaik.

Pada gambar struktur data, pesan routing protokol, dan algoritma routing yang digunakan oleh EIGRP.

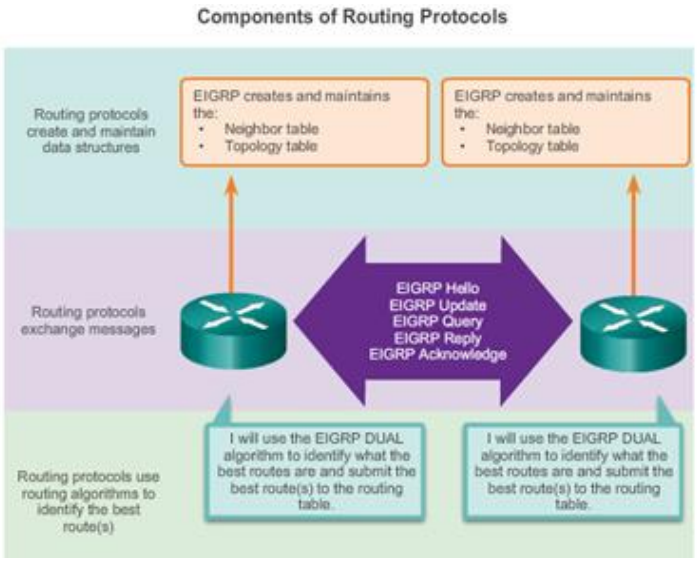


Fig. 7.3 Komponen Routing

7.4 Peranan Protokol Routing Dinamis

Routing protokol memungkinkan router untuk secara dinamis berbagi informasi tentang jaringan jarak jauh dan secara otomatis menambahkan informasi ini ke tabel routing mereka sendiri; melihat animasi pada gambar.

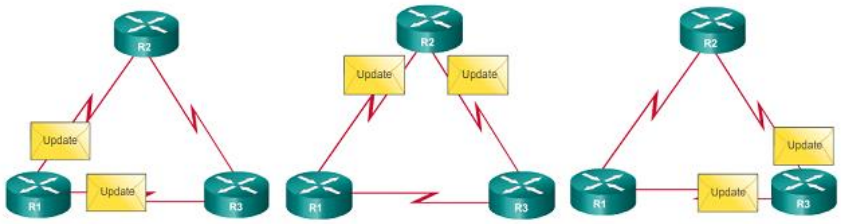


Fig. 7.4 Proses update informasi routing dinamis

Routing protokol menentukan jalur terbaik, atau rute, untuk setiap jaringan. rute yang kemudian ditambahkan ke tabel routing. Manfaat utama dari protokol routing dinamis adalah bahwa router pertukaran informasi routing ketika ada perubahan topologi. pertukaran ini memungkinkan router untuk secara otomatis belajar tentang jaringan baru dan juga untuk menemukan jalur alternatif ketika terjadi kegagalan link ke jaringan saat ini.

Static Routing Advantages and Disadvantages

Advantages	Disadvantages
Easy to implement in a small network.	Suitable only for simple topologies or for special purposes such as a default static route.
Very secure. No advertisements are sent as compared to dynamic routing protocols.	Configuration complexity increases dramatically as network grows.
Route to destination is always the same.	Manual intervention required to re-route traffic.
No routing algorithm or update mechanism required; therefore, extra resources (CPU or RAM) are not required.	

Fig. 7.5 Kelebihan dan Kelemahan Routing Statik

Pada gambar 7.5 terlihat keuntungan dan kerugian dari routing statis. routing statis mudah untuk diterapkan dalam jaringan kecil. Rute statis tetap sama, yang membuat mereka cukup mudah untuk memecahkan masalah. Rute statis tidak mengirim pesan update oleh karena itu, memerlukan sangat sedikit overhead.

Kelemahan routing statis meliputi :

- Mereka tidak mudah diimplementasikan dalam jaringan besar.
- Mengelola konfigurasi statis dapat menjadi memakan waktu.
- Jika link gagal, rute statis tidak dapat mengubah rute lalu lintas.

Pada gambar 7.6. terlihat keuntungan dan kerugian dari routing dinamis. protokol routing dinamis bekerja dengan baik di setiap jenis jaringan yang terdiri dari beberapa router. Mereka terukur dan secara otomatis menentukan rute yang lebih baik jika ada perubahan topologi. Meskipun ada lebih banyak konfigurasi protokol routing dinamis, mereka lebih sederhana untuk mengkonfigurasi di jaringan besar.

Ada kelemahan untuk routing dinamis, routing dinamis membutuhkan pengetahuan tentang perintah tambahan. Hal ini juga kurang aman dari routing statis karena interface yang diidentifikasi oleh protokol routing mengirim routing update keluar. Rute yang diambil mungkin berbeda antara paket. Algoritma routing yang menggunakan CPU tambahan, RAM, dan bandwidth link.

Dynamic Routing Advantages and Disadvantages

Advantages	Disadvantages
Suitable in all topologies where multiple routers are required.	Can be more complex to implement.
Generally independent of the network size.	Less secure. Additional configuration settings are required to secure.
Automatically adapts topology to reroute traffic if possible.	Route depends on the current topology.
	Requires additional CPU, RAM, and link bandwidth.

Fig. 7.6 Kelebihan dan Kekurangan Routing Dinamis

7.5 Klasifikasi Protokol Routing

Protokol routing dapat diklasifikasikan ke dalam kelompok yang berbeda sesuai dengan karakteristik mereka. Secara khusus, protokol routing dapat diklasifikasikan sebagai berikut :

- Purpose (Tujuan) : Interior Gateway Protocol (IGP) atau Exterior Gateway Protocol (EGP)
- Operation (Operasi) : Distance vector, link-state protocol, atau path-vector protocol
- Behavior (Perilaku) : Classful (legacy) atau Classless (protokol tanpa kelas)

Misalnya, IPv4 protokol routing diklasifikasikan sebagai berikut:

- RIPv1 (legacy) : IGP, distance vector, classful protocol
- IGRP (legacy) : IGP, distance vector, classful protokol yang dikembangkan oleh Cisco(deprecated from 12.2 IOS and later)
- RIPv2 : IGP, distance vector, classless protocol
- EIGRP : IGP, distance vector, classless protokol yang dikembangkan oleh Cisco
- OSPF : IGP, link-state, classless protocol
- IS-IS : IGP, link-state, classless protocol
- BGP : EGP, path-vector, classless protocol

7.6 Protokol Routing IGP dan EGP

Autonomous System (AS) adalah kumpulan dari router di bawah administrasi umum seperti perusahaan atau organisasi. Sebuah AS juga dikenal sebagai domain

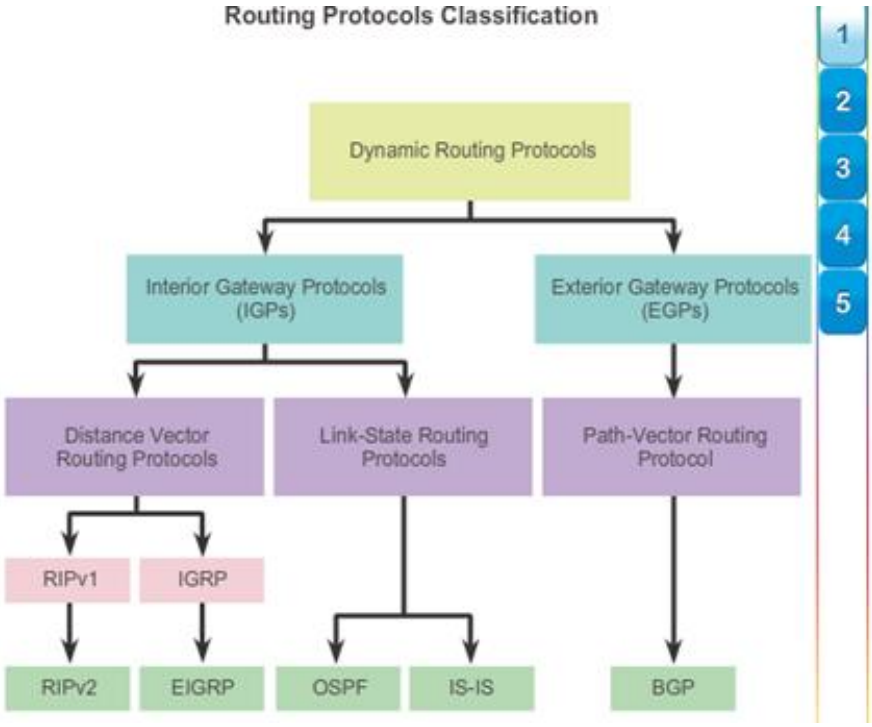


Fig. 7.7 Klasifikasi Protokol Routing

routing. Contoh umum dari AS adalah jaringan internal perusahaan dan jaringan ISP.

Internet didasarkan pada konsep AS, Oleh karena itu dua jenis protokol routing yang diperlukan :

- Interior Gateway Protokol (IGP) : Digunakan untuk routing dalam sebuah AS. Hal ini juga disebut sebagai intra-AS routing. Perusahaan, organisasi, dan bahkan penyedia layanan menggunakan IGP pada jaringan internal mereka. IGP termasuk RIP, EIGRP, OSPF, dan IS-IS.
- Exterior Gateway Protokol (EGP) : Digunakan untuk routing antara AS. Hal ini juga disebut sebagai inter-AS routing. Penyedia layanan dan perusahaan besar mungkin interkoneksi menggunakan EGP. Border Gateway Protocol (BGP) adalah satu-satunya EGP saat ini dan routing protokol resmi yang digunakan oleh Internet.

Catatan: Karena BGP adalah satu-satunya EGP tersedia, istilah EGP jarang digunakan. Sebaliknya, sebagian besar insinyur hanya mengacu pada BGP.

Contoh pada gambar 7.9. dibawah ini memberikan skenario sederhana menyoroti penyebaran IGP, BGP, dan routing statis:

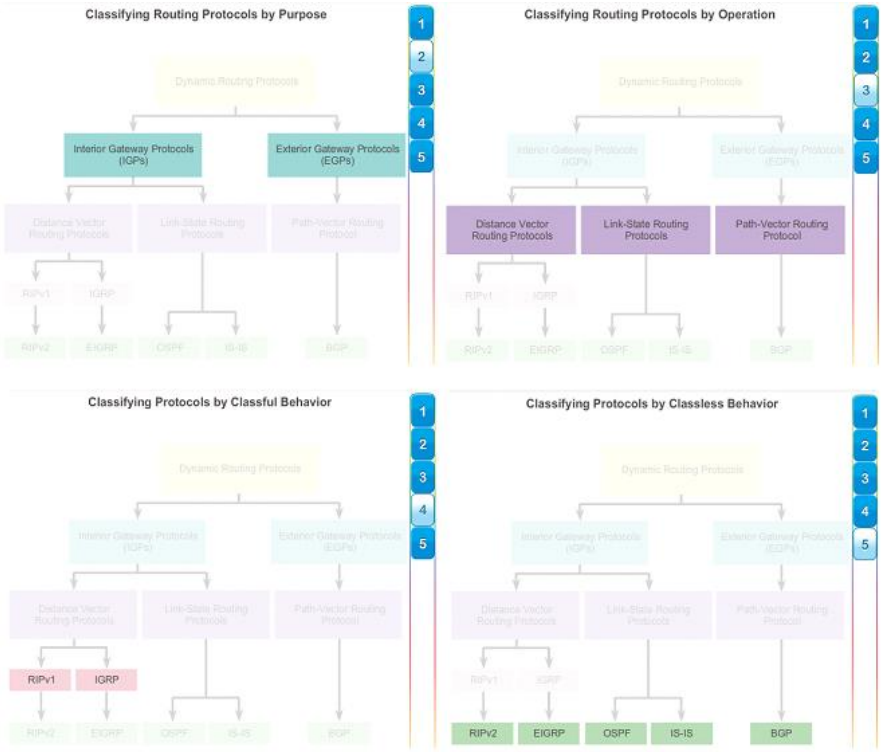


Fig. 7.8 Klasifikasi Protokol Routing

ISP-1 : adalah AS, menggunakan IS-IS sebagai IGP. Interkoneksi dengan autonomous system lainnya dan penyedia layanan menggunakan BGP untuk secara eksplisit mengontrol bagaimana lalu lintas dialihkan.

ISP-2 : adalah AS, menggunakan OSPF sebagai IGP ini. Interkoneksi dengan autonomous system lainnya dan penyedia layanan menggunakan BGP untuk secara eksplisit mengontrol bagaimana lalu lintas dialihkan.

AS-1 : adalah organisasi yang besar dan menggunakan EIGRP sebagai IGP. Karena multihomed (yaitu, menghubungkan ke dua penyedia layanan yang berbeda), menggunakan BGP untuk secara eksplisit mengontrol bagaimana lalu lintas masuk dan meninggalkan AS.

AS-2 : Ini adalah organisasi menengah dan menggunakan OSPF sebagai IGP. Hal ini juga multihomed. Oleh karena itu, ia menggunakan BGP untuk secara eksplisit mengontrol bagaimana lalu lintas masuk dan meninggalkan AS.

AS-3 : adalah sebuah organisasi kecil dengan router yang lebih tua dalam AS, menggunakan RIP sebagai IGP. BGP tidak diperlukan karena single-homed (yaitu, menghubungkan ke salah satu penyedia layanan). Sebaliknya, static routing diimplementasikan antara AS dan penyedia layanan.

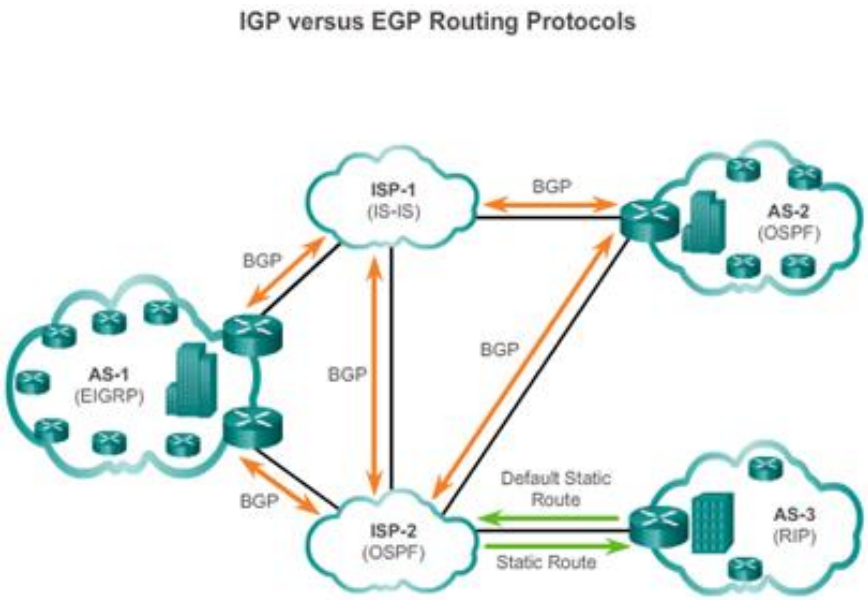


Fig. 7.9 Protokol Routing IGP dan EGP

7.7 Protokol Routing Distance Vector

- Distance (Jarak) : Mengidentifikasi seberapa jauh ke jaringan tujuan dan didasarkan pada metrik seperti hop, biaya, bandwidth, delay, dan banyak lagi.
- Vector : Menentukan arah router atau keluar antarmuka hop berikutnya untuk mencapai tujuan.

Misalnya dalam gambar 7.10 diatas, R1 tahu bahwa jarak untuk mencapai jaringan 172.16.3.0/24 adalah salah satu hop dan arah keluar dari interface S0 / 0/0 menuju R2.

Sebuah router menggunakan distance vector protokol routing tidak memiliki pengetahuan tentang seluruh jalan ke jaringan tujuan. Distance vector protokol menggunakan router sebagai tanda posting di sepanjang jalan ke tujuan akhir. Satu-satunya informasi router tahu tentang jaringan jarak jauh adalah jarak atau metrik untuk mencapai jaringan dan jalur mana atau antarmuka (interface) yang digunakan untuk sampai ke tujuan. Distance vector protokol routing tidak memiliki peta sebenarnya dari topologi jaringan.

Ada empat Distance Vector IGP IPv4:

- RIPv1 - Generasi Pertama protokol
- RIPv2 - Simple Distance Vector protokol routing
- IGRP - Generasi Pertama Cisco proprietary protocol (digantikan oleh EIGRP)
- EIGRP - Versi lanjutan dari Distance Vector protokol routing

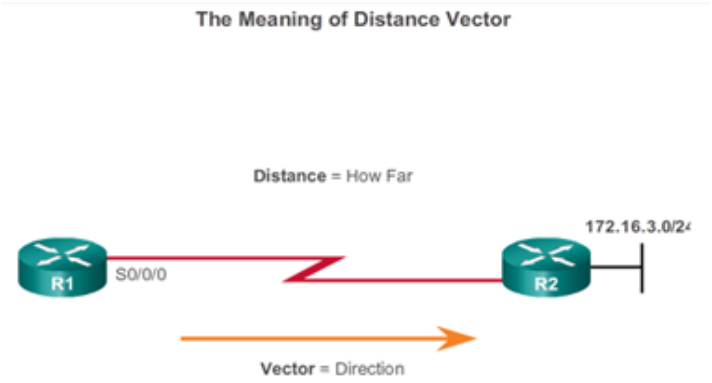


Fig. 7.10 Protokol Routing Distance Vector

7.8 Protokol Routing Link State

Berbeda dengan Distance Vector protokol routing, router dikonfigurasi dengan protokol routing link-state dapat membuat tampilan lengkap atau topologi jaringan dengan mengumpulkan informasi dari semua router lain.

Menggunakan protokol routing link-state adalah seperti memiliki peta lengkap dari topologi jaringan. Sebuah router link-state menggunakan informasi link-state untuk membuat peta topologi dan untuk memilih jalan terbaik untuk semua jaringan tujuan dalam topologi.

Router RIP-enabled mengirim pembaruan berkala informasi routing ke tetangga mereka. Link-state routing protokol tidak menggunakan update periodik. Setelah jaringan telah berkumpul, update link-state hanya dikirim ketika ada perubahan topologi. Misalnya, update link-state dalam animasi tidak dikirim sampai 172.16.3.0 jaringan down.

Pada gambar diatas operasi link-state. Protokol link-state bekerja dengan baik dalam situasi di mana :

- Desain jaringan hirarkis, biasanya terjadi pada jaringan yang besar
- Konvergensi cepat dari jaringan sangat penting
- Administrator memiliki pengetahuan yang baik tentang protokol routing link-state yang dilaksanakan

Ada dua Link-state IPv4 IGP :

- OSPF : Standar Populer berdasarkan routing protokol
- IS-IS : Populer di jaringan penyedia

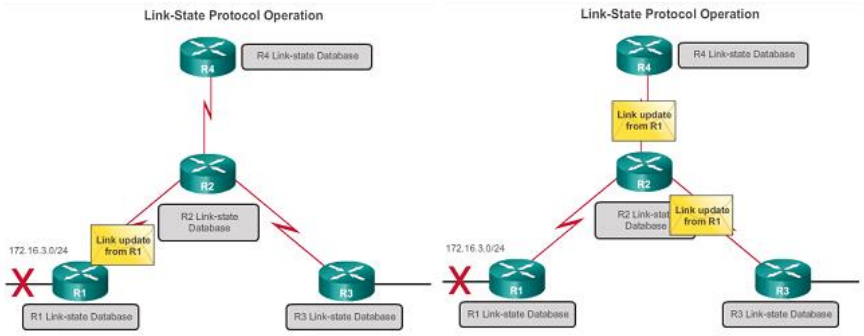


Fig. 7.11 Protokol Routing Link State

7.9 Classful dan Classless

Perbedaan terbesar antara classful dan classless routing protokol adalah bahwa protokol routing classful tidak mengirimkan informasi subnet mask di routing update mereka. protokol routing tanpa kelas meliputi informasi subnet mask dalam routing update.

Catatan: Hanya RIPv1 dan IGRP adalah classful. Semua IPv4 dan IPv6 protokol routing menggunakan classless. pengalamatan classful tidak pernah menjadi bagian dari IPv6 Fakta bahwa RIPv1 dan IGRP tidak mencakup informasi subnet mask di update mereka berarti bahwa mereka tidak dapat memberikan variabel length subnet masks (VLSM) dan classless interdomain routing (CIDR).

Jaringan modern tidak lagi menggunakan IP classful. Classless IPv4 protokol routing (RIPv2, EIGRP, OSPF, dan IS-IS) semua termasuk informasi subnet mask dengan alamat jaringan di update routing. Protokol routing classless mendukung VLSM dan CIDR. IPv6 protokol routing yang tanpa kelas. Perbedaan apakah protokol routing classful atau tanpa kelas biasanya hanya berlaku untuk IPv4 protokol routing. Semua routing protokol IPv6 dianggap tanpa kelas karena mereka termasuk awalan-panjang dengan alamat IPv6.

Classful secara sederhana dapat diartikan ”menggunakan kelas”. Hali ini jika dikaitkan dengan pengalamatan IP Address, maka pengalamatan IP classful dapat diartikan menjadi ”pengalamatan IP Address berdasarkan kelas”. Pengalamatan dengan metode ini ada pada pengalamatan IPv4. Seperti IPv4 dibagi menjadi kelas A, B, C, D, dan E. Dengan pengalamatan IP classful, jaringan yang dapat dibentuk hanya sebatas kapasitas masing-masing kelas dan kapasitas host yang besar yang dimiliki oleh kelas A dan B sering tidak terpakai secara optimum. Selain itu juga telah membuat tabel routing secara global menjadi membengak melebihi kapasitas router. Oleh sebab itu metode ini sudah sering digunakan lagi dan diganti dengan classless.

Classless secara sederhana adalah ”tidak menggunakan kelas”. Jika dikaitkan dengan pengalamatan IP Address, maka pengalamatan IP secara classless dapat diartikan menjadi ”pengalamatan IP Address tanpa mengenal kelas”. Yaitu dengan cara menggunakan Classless-Inter Domain Rouing (CIDR) atau juga dapat dikenal dengan istilah panjang prefiks. Format pengalamatannya adalah dengan memberi tanda slash (/) di belakang alamat IP kemudian diikuti dengan variabel panjang prefiks.

Contoh: 172.26.78.3/28 (172.26.78.3 = alamat IP, /28 = panjang prefiks (CIDR))

Dengan metode classless dapat menyederhanakan tabel routing dengan cara satu tabel routing dapat untuk beberapa jaringan sehingga menghemat penggunaan kapasitas router dalam membuat tabel routing. Selain itu, metode ini memungkinkan untuk menggunakan alamat IP kelas A dan B dengan panjang prefiks tertentu yang belum dipakai.

Dalam rangka menjawab permasalahan menipisnya kapasitas jumlah host IPv4 yang diperkirakan akan habis seluruhnya dalam beberapa tahun lagi, maka dibuatlah protokol atau sistem pengalamatan yang baru yaitu dengan IPv6 dengan panjang 128-bit dan bersifat classless sehingga mampu mendukung jumlah host hingga $3,4 \times 10^{38}$ host.

7.10 Karakteristik Protokol Routing

Karakteristik protokol routing antara lain :

- Kecepatan Konvergensi : Kecepatan konvergensi mendefinisikan seberapa cepat router dalam topologi jaringan berbagi informasi routing. Routing loops dapat terjadi ketika tidak konsisten tabel routing tidak diperbarui karena memperlambat konvergensi dalam perubahan jaringan.
- Skalabilitas : Kemampuan suatu sistem, jaringan, atau proses untuk menangani penambahan beban yang diberikan, atau potensinya untuk ditingkatkan guna menangani penambahan beban tersebut.
- Classful atau Classless (Penggunaan VLSM) : Protokol routing classful tidak menyertakan subnet mask dan tidak dapat mendukung VLSM. Protokol routing classless termasuk subnet mask dalam update. Protokol routing classless mendukung VLSM dan summarization rute yang lebih baik.
- Sumber daya Penggunaan : Penggunaan sumber daya termasuk persyaratan protokol routing seperti ruang memori (RAM), penggunaan CPU, dan pemanfaatan bandwidth link. kebutuhan sumber daya yang lebih tinggi memerlukan hardware yang lebih kuat untuk mendukung operasi routing protocol, di samping proses forwarding paket.
- Implementasi dan Pemeliharaan : Pelaksanaan dan pemeliharaan menggambarkan tingkat pengetahuan yang diperlukan untuk administrator jaringan untuk menerapkan dan memelihara jaringan berdasarkan protokol routing dikerahkan.

Comparing Routing Protocols

	Distance Vector				Link State	
	RIPv1	RIPv2	IGRP	EIGRP	OSPF	IS-IS
Speed Convergence	Slow	Slow	Slow	Fast	Fast	Fast
Scalability - Size of Network	Small	Small	Small	Large	Large	Large
Use of VLSM	No	Yes	No	Yes	Yes	Yes
Resource Usage	Low	Low	Low	Medium	High	High
Implementation and Maintenance	Simple	Simple	Simple	Complex	Complex	Complex

Fig. 7.12 Perbandingan Protokol Routing

7.11 Metrics Protokol Routing

Ada kasus ketika protokol routing belajar lebih dari satu rute ke tujuan yang sama. Untuk memilih jalur terbaik, protokol routing harus mampu mengevaluasi dan membedakan antara jalur yang tersedia. Hal ini dilakukan melalui penggunaan metrik routing.

Sebuah metrik adalah nilai terukur yang ditugaskan oleh protokol routing untuk rute yang berbeda berdasarkan kegunaan dari rute itu. Dalam situasi di mana ada beberapa jalur ke jaringan remote yang sama, metrik routing digunakan untuk menentukan keseluruhan ”biaya” dari jalur dari sumber ke tujuan. Routing protokol menentukan jalur terbaik berdasarkan rute dengan biaya terendah.

Routing protokol yang berbeda menggunakan metrik yang berbeda. Metrik yang digunakan oleh salah satu protokol routing tidak sebanding dengan metrik yang digunakan oleh routing protocol lain. Dua routing protocol yang berbeda mungkin memilih jalan yang berbeda untuk tujuan yang sama.

Pada gambar 7.13 menunjukkan bahwa RIP akan memilih jalur dengan sedikitnya jumlah hop, sedangkan OSPF akan memilih jalur dengan bandwidth tertinggi.

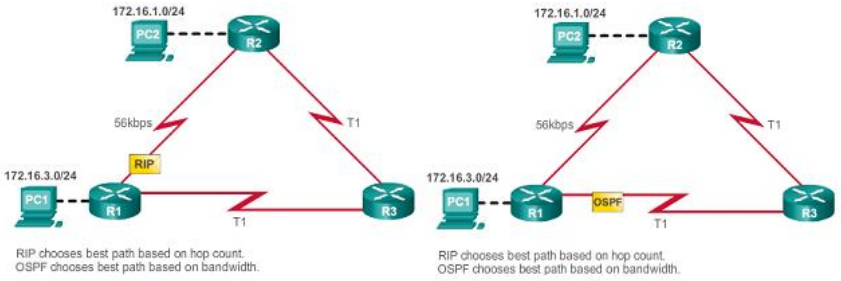


Fig. 7.13 Metrics Protokol Routing

7.12 Routing Information Protocol

Routing Information Protocol (RIP) adalah sebuah protokol generasi routing yang pertama untuk IPv4 awalnya ditetapkan dalam RFC 1058. Sangat mudah untuk mengkonfigurasi, menjadikannya pilihan yang baik untuk jaringan kecil.

RIPv1 memiliki karakteristik utama sebagai berikut:

- Update routing yang broadcast (255.255.255.255) setiap 30 detik.
- Hop count digunakan sebagai metrik untuk seleksi jalur.
- Sebuah hop lebih besar dari 15 hop dianggap tak terbatas (terlalu jauh). Hop router 15 tidak akan menyebarkan update routing ke router berikutnya.

Pada tahun 1993, RIPv1 telah diperbarui untuk protokol routing tanpa kelas yang dikenal sebagai versi RIP 2 (RIPv2). RIPv2 termasuk perbaikan berikut:

- Classless routing protocol : Mendukung VLSM dan CIDR, karena termasuk subnet mask dalam routing update.
- Peningkatan efisiensi : Ini meneruskan update ke multicast alamat 224.0.0.9, bukan alamat broadcast 255.255.255.255.
- Mengurangi entri routing : Mendukung pengguna summarization rute pada antarmuka apapun.
- Aman : Mendukung mekanisme otentikasi untuk mengamankan update tabel routing antara tetangga.

Pada gambar 7.14 dibawah ini merangkum perbedaan antara RIPv1 dan RIPv2.

Update RIP diringkas menjadi segmen UDP, dengan kedua sumber dan tujuan nomor port diatur ke port UDP 520. Pada tahun 1997, IPv6 versi diaktifkan dari RIP dirilis. RIPng didasarkan pada RIPv2. Ia masih memiliki keterbatasan 15 hop dan jarak administrasi adalah 120.

RIPv1 versus RIPv2

Characteristics and Features	RIPv1	RIPv2
Metric	Both use hop count as a simple metric. The maximum number of hops is 15.	
Updates Forwarded to Address	255.255.255.255	224.0.0.9
Supports VLSM	✗	✓
Supports CIDR	✗	✓
Supports Summarization	✗	✓
Supports Authentication	✗	✓

Fig. 7.14 Perbandingan RIPv1 dan RIPv2

7.13 Enhanced Interior-Gateway Routing Protocol (EIGRP)

Interior Gateway Routing Protocol (IGRP) adalah yang pertama proprietary routing protocol IPv4 yang dikembangkan oleh Cisco pada tahun 1984. Dulu karakteristik desain berikut:

- Bandwidth, delay, beban, dan reliabilitas digunakan untuk membuat metrik komposit.
- Update routing yang disiarkan setiap 90 detik, secara default.

Pada tahun 1992, IGRP digantikan oleh Enhanced IGRP (EIGRP). Seperti RIPv2, EIGRP juga memperkenalkan dukungan untuk VLSM dan CIDR. EIGRP meningkatkan efisiensi, mengurangi routing update, dan mendukung pertukaran pesan aman.

Tabel pada gambar 7.15 merangkum perbedaan antara IGRP dan EIGRP.
EIGRP juga memperkenalkan:

- Bounded triggered updates : Ini tidak mengirim update secara berkala. Hanya perubahan tabel routing yang disebarkan, setiap kali perubahan terjadi. Hal ini akan mengurangi jumlah beban protokol routing pada jaringan. Dibatasi update dipicu berarti bahwa EIGRP hanya mengirim ke tetangga yang membutuhkannya.
- Hello keepalive mechanism : Sebuah pesan Hello kecil secara berkala dipertukarkan untuk menjaga kedekatan dengan router tetangga. Ini berarti penggunaan yang sangat rendah dari sumber daya jaringan selama operasi normal, bukan update periodik.

IGRP versus EIGRP

Characteristics and Features	IGRP	EIGRP
Metric	Both use a composite metric consisting of bandwidth and delay. Reliability and load can also be included in the metric calculation.	
Updates Forwarded to Address	255.255.255.255	224.0.0.10
Supports VLSM	✗	✓
Supports CIDR	✗	✓
Supports Summarization	✗	✓
Supports Authentication	✗	✓

Fig. 7.15 Perbandingan IGRP dan EIGRP

- Maintains a topology table : Memelihara semua yang diterima dari tetangga (tidak hanya jalur terbaik) dalam tabel topologi rute. DUAL dapat memasukkan rute cadangan ke dalam tabel EIGRP topologi.
- Rapid convergence (konvergensi yang cepat) : Jika rute utama gagal, router dapat menggunakan rute alternatif diidentifikasi. Peralihan ke rute alternatif adalah segera dan tidak melibatkan interaksi dengan router lainnya.
- Multiple network layer protocol support : EIGRP menggunakan protokol Modul Dependent (PDM), yang berarti bahwa satu-satunya protokol untuk menyertakan dukungan untuk protokol selain IPv4 dan IPv6, seperti warisan IPX dan AppleTalk.

7.14 Konfigurasi Dasar Protokol RIP

Meskipun RIP jarang digunakan dalam jaringan modern, hal ini berguna sebagai dasar untuk memahami jaringan routing dasar. Untuk alasan ini, bagian ini memberikan gambaran singkat tentang bagaimana mengkonfigurasi pengaturan RIP dasar dan untuk memverifikasi RIPv2.

```
R1>enable
R1#configure terminal
```

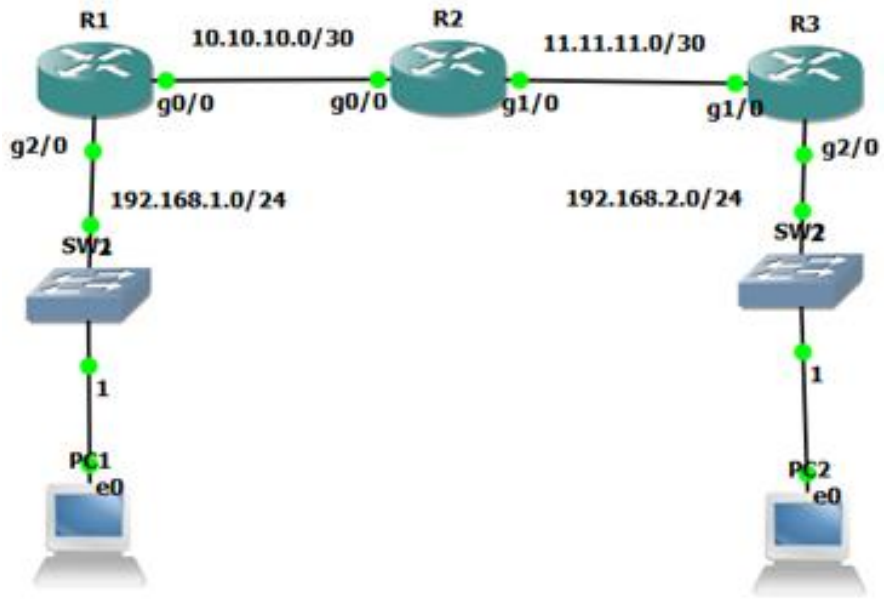


Fig. 7.16 Konfigurasi RIP

```
R1(config)#router rip
R1(config-router)# version 2
R1(config-router)# network 192.168.1.0
R1(config-router)# network 10.10.10.0
```

```
R2>enable R1#configure
terminal R1(config)#router
rip R1(config-router)#
version 2
R1(config-router)# network 11.11.11.0
R1(config-router)# network 10.10.10.0
```

```
R1>enable R1#configure
terminal R1(config)#router
rip R1(config-router)#
version 2
```

```
R1(config-router)# network 192.168.2.0
R1(config-router)# network 11.11.11.0
```

7.15 Shortest Path First Protocols

IPv4 link-state protokol routing ditunjukkan pada gambar 7.17 dibawah ini :

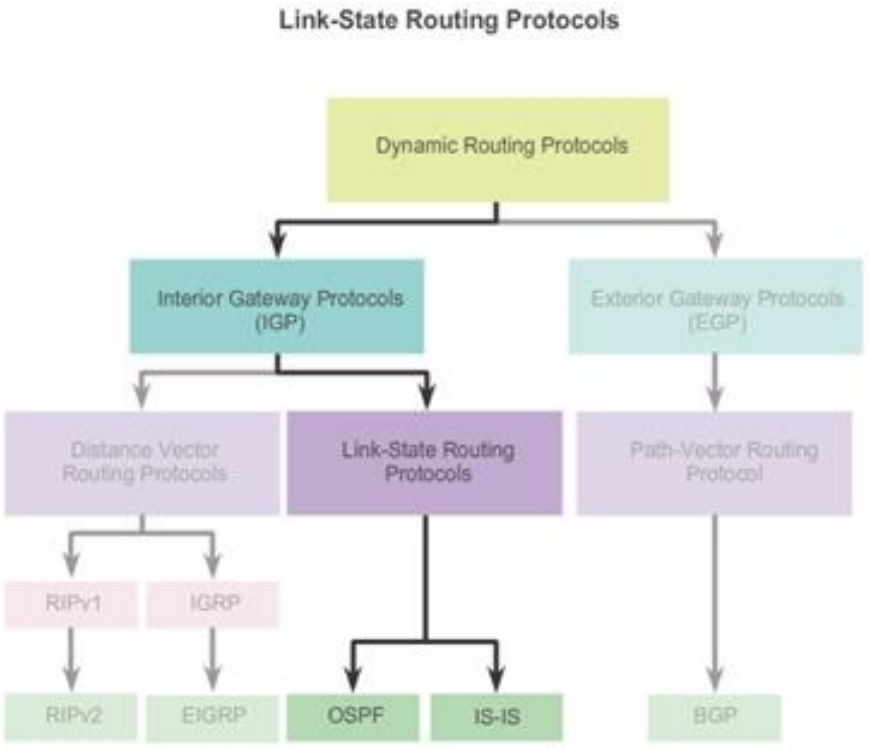


Fig. 7.17 Protokol Routing Link State

- Open Shortest Path First (OSPF)
- Intermediate System-to-Intermediate System (IS-IS)

Link-state routing protokol memiliki reputasi yang jauh lebih kompleks daripada rekan-rekan vektor jarak mereka. Sama seperti RIP dan EIGRP, operasi dasar OSPF dikonfigurasi menggunakan :

- router ospf process-id global configuration command
- network command to advertise networks

7.16 Dijkstra's Algorithm

Semua protokol routing link-state menerapkan algoritma Dijkstra untuk menghitung rute jalan terbaik. algoritma ini sering disebut sebagai jalur terpendek pertama (SPF) algoritma. Algoritma ini menggunakan biaya akumulasi sepanjang setiap jalur, dari sumber ke tujuan, untuk menentukan total biaya rute.

Dalam gambar 7.18, setiap jalur diberi label dengan nilai sewenang-wenang untuk biaya. Biaya jalur terpendek untuk R2 untuk mengirim paket ke LAN melekat R3 adalah 27. Setiap router menentukan biaya sendiri untuk setiap tujuan dalam topologi. Dengan kata lain, setiap router menghitung algoritma SPF dan menentukan biaya dari perspektif sendiri.

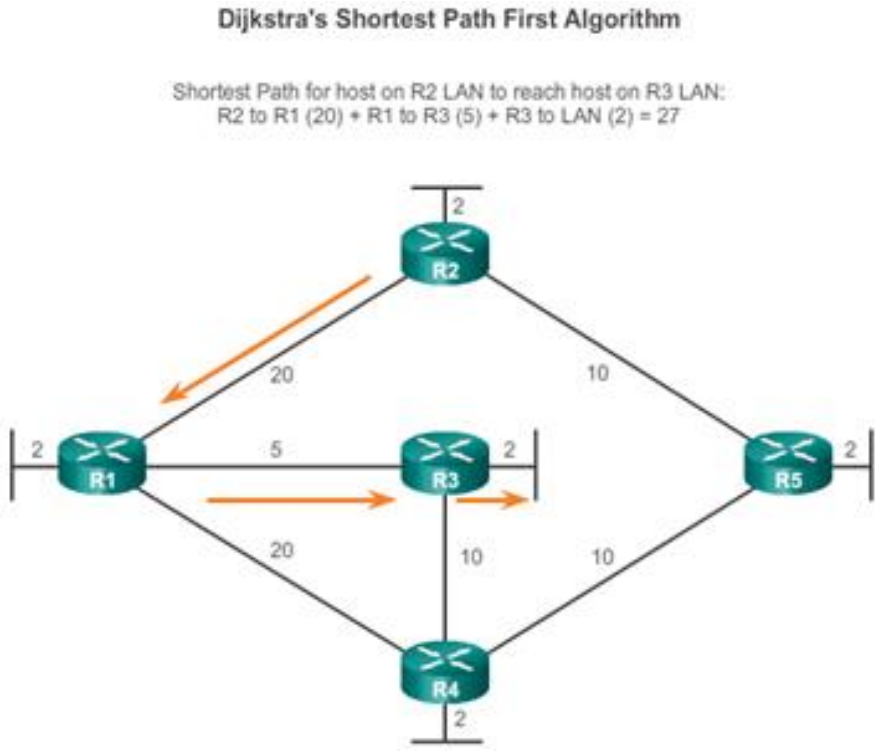


Fig. 7.18 Disjark Algorithm

7.17 Link State Routing Protocol

Open Shortest Path First (OSPF) protokol, yang didefinisikan dalam RFC 2328, adalah Interior Gateway Protocol digunakan untuk mendistribusikan informasi routing dalam Sistem Otonomi tunggal.

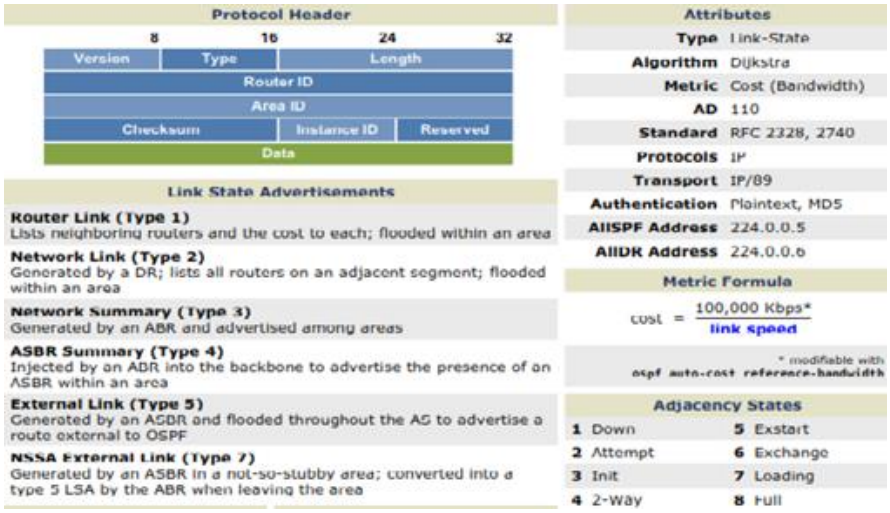


Fig. 7.19 OSPF Header

1. OSPF menggunakan desain jaringan hirarki menggunakan Area;
2. OSPF akan membentuk hubungan tetangga dengan router yang berdekatan di area yang sama;
3. Mengalihkan informasi jarak ke jaringan yang terhubung, OSPF menginformasikan status link yang terhubung langsung menggunakan Link-State Advertisements (LSAs);
4. OSPF mengirimkan update (LSA) bila ada perubahan ke salah satu link nya, dan hanya akan mengirimkan perubahan diupdate. LSA adalah tambahan refresh setiap 30 menit;
5. OSPF menggunakan algorithm Dijkstra Shortest Path First untuk menentukan jalur terpendek;
6. OSPF adalah protokol tanpa kelas, dan dengan demikian mendukung VLSMs.

Karakteristik lain dari OSPF termasuk :

1. OSPF hanya mendukung IP routing;
2. OSPF rute memiliki administrative distance adalah 110;
3. OSPF menggunakan biaya sebagai metrik, yang dihitung berdasarkan bandwidth link. OSPF tidak memiliki batas hop-count;

Proses OSPF membangun dan memelihara tiga tabel terpisah:

- A neighbor table, berisi daftar semua router tetangga;
- A topology table, berisi daftar semua rute yang mungkin untuk semua diketahui jaringan dalam suatu daerah;
- A routing table, berisi rute terbaik untuk masing-masing jaringan yang dikenal.

7.18 Intermediate System to Intermediate System (IS-IS)

Intermediate System to Intermediate System (IS-IS), merupakan routing protocol yang diciptakan oleh International Standarization Organization (ISO). Tujuan diciptakan IS-IS oleh ISO adalah agar protokol routing ini menjadi sebuah standar terbuka yang dapat digunakan oleh semua perangkat jaringan. Namun Kenyataannya yang lebih banyak digunakan adalah semua protokol dan sistem pengalamatan yang diciptakan berdasarkan organisasi standar Open System Interconnection (OSI). Sistem pengalamatan Internet Protocol (IP) yang selama ini dikenal luas di seluruh dunia dan protokol routing lain seperti OSPF diciptakan berdasarkan standar dari OSI. Dibawah ini merupakan atribut dari protokol routing IS-IS :

Attributes	
Type	Link-State
Algorithm	Dijkstra
Metric	Default (10)
AD	115
Standard	ISO 10589
Protocols	IP, CLNS
Transport	CLNP
Authentication	Plaintext, MD5

Fig. 7.20 Atribut Protokol IS-IS

Pada umumnya IS-IS sama seperti routing protocol lain yang menggunakan metode link state dalam penentuan rutenya, biasanya metode link state akan menghasilkan rute yang terbaik dari segi kecepatan. Dibawah ini merupakan gambar perbedaan metode antara Distance Vector dan Link State.

Distance vector akan menggunakan jalur A langsung ke B karena dianggap paling dekat walaupun koneksi menggunakan serial interface yang kecepatannya jauh lebih lambat dari gigabyte port. Sedangkan Link State akan menggukanan jalur A-C-D-B, walaupun hop count nya jauh lebih besar tapi bandwitdh yang digunakan lebih besar dan lebih cepat.

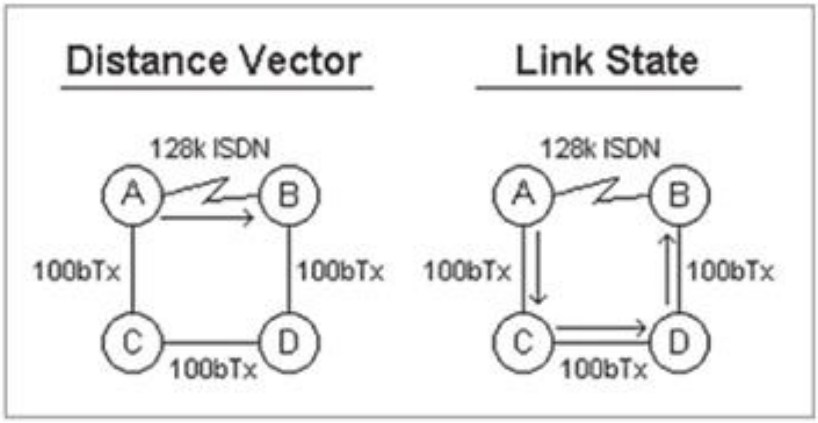


Fig. 7.21 Perbandingan Distance Vector dan Link State

NSAP Addressing

Relevance	Interdomain Part		Domain Specific Part		
NSAP	AFI	IDI	HODSP	System ID	SEL
Example	47	0005.80ff.f800.0000	0001	0000.0c00.1234	00
Condensed	Area			System ID	SEL

Interdomain Part (IDP) · Portion of the address used in routing between autonomous systems; assigned by ISO

Domain Specific Part (DSP) · Portion of the address relevant only within the local AS

Authority and Format Identifier (AFI) · Identifies the authority which dictates the format of the address

Initial Domain Identifier (IDI) · An organization belonging to the AFI

High Order DSP (HODSP) · The area within the AS

System ID · Unique router identifier; six bytes for Cisco devices; often taken from a MAC address

NSAP Selector (SEL) · Identifies a network layer service; always 0x00 in a NET address

Routing Levels

Level 0 Used to locate end systems

Level 1 Routing within an area

Level 2 Backbone between areas

Level 3 Inter-AS routing

Terminology

Type-Length-Value (TLV) · Variable length modular datasets

Link State PDU (LSP) · Carry TLVs describing link state information

Sequence Number Packet (SNP) · Used to request and advertise LSPs; can be complete (CSNP) or partial (PSNP)

Hello Packet · Establish and maintain neighbor adjacencies

Designated Intermediate System (DIS) · A pseudonode responsible for emulating point-to-point links across a multiaccess segment

Fig. 7.22 IS-IS Header

Pengalamatan IS-IS terdiri dari tiga bagian :

- Identifier Area : tiga byte pertama adalah ID daerah. Byte pertama dari gambar dibawah ini 47 adalah identifier alamat keluarga (AFI) dari otoritas;
- Dua byte ID daerah 0005 mewakili IS-IS area nomor;
- Identifier sistem : Enam byte berikutnya mengidentifier node router pada jaringan. Identifier sistem setara dengan host atau alamat pada jaringan IP.

7.19 Kesimpulan

Protokol routing dinamis yang digunakan oleh router untuk memfasilitasi pertukaran informasi routing antara router. Tujuan dari protokol routing dinamis meliputi:

- Penemuan jaringan jarak jauh
- Mempertahankan up-to-date informasi routing
- Memilih jalur terbaik ke jaringan tujuan
- Kemampuan untuk menemukan jalan terbaik baru jika jalan saat ini tidak lagi tersedia.

Sementara protokol routing dinamis memerlukan overhead administrasi kurang dari routing statis, mereka memerlukan mendedikasikan bagian dari sumber daya router untuk operasi protokol, termasuk waktu CPU dan jaringan link bandwidth.

Jaringan biasanya menggunakan kombinasi keduanya routing statis dan dinamis. routing dinamis adalah pilihan terbaik untuk jaringan besar dan routing statis lebih baik untuk jaringan stub. Protokol routing dapat diklasifikasikan sebagai classful atau classless, distance-vector atau link-state, dan interior gateway protocol atau exterior gateway protocol.

Chapter 8
Single-Area OSPF

8.1 Pendahuluan

Menurut Teare (2010), pengembangan dari routing protokol OSPF dimulai pada tahun 1987. OSPF adalah protokol pertama yang dikembangkan keseluruhan oleh Internet Engineering Task Force (IETF). Sepuluh tahun kemudian OSPF working group milik IETF masih ada, dan protokol OSPF berlanjut dikembangkan, meskipun dasar protokol OSPF telah ditentukan dengan publikasi spesifikasi OSPF versi 2 pertama kali ditahun 1991. OSPF dibuat pada pertengahan tahun 1980an, OSPF menutup kelemanhan - kelemahan dari RIP pada jaringan di perusahaan yang berskala besar. Karena OSPF berdasar open standard (user yang menggunakan tidak dikenakan biaya), maka sangat popular digunakan dijaringan sebuah perusahaan dan juga memiliki banyak kelebihan, antara lain:

- Bisa berjalan pada kebanyakan router, karena berdasar open standard.
- Menggunakan algoritma SPF (Shortest Path First), dikembangkan oleh Edsger Djikstra.
- Menyediakan konvergensi yang cepat, dengan dipicu dan update kea rah atas melalui Link State Advertisements (LSAs).
- Menggunakan Classless Protokol dan memungkinkan desain hirarki dengan VLSM dan route summarization.
- Memiliki fitur Intelegence Metric, yang mana merupakan kebalikan dari bandwidth interface.

Ketika router pertama kali hidup, router mengirimkan hello message pada semua jalur point to - point dan pesan tersebut dikirim secara multicast di jaringan LAN kepada grup yang terdiri dari semua router lainnya. Dari balasannya setiap router mempelajari siapa tetangganya. Router pada jaringan yang sama merupakan sesama tetangga.

OSPF bekerja dengan cara menukar informasi antara router - router yang berdampingan, yang mana tidak sama dengan antara router yang saling bertetangga. Sederhananya adalah tidak efektif untuk setiap router pada LAN berbicara ke setiap router

	Interior Gateway Protocols				Exterior Gateway Protocols
	Distance Vector		Link-State		Path Vector
IPv4	RIPv2	EIGRP	OSPFv2	IS-IS	BGP-4
IPv6	RIPng	EIGRP for IPv6	OSPFv3	IS-IS for IPv6	BGP-MP

Fig. 8.1 Perkembangan OSPF

juga pada LAN. Untuk menghindari situasi ini satu router dipilih sebagai Designated Router (DR). Router tersebut diibaratkan sebagai adjacent router ke semua router lainnya pada jaringan LAN dan pertukaran informasi dengan mereka. Router tetangga yang tidak berdampingan langsung tidak saling bertukar informasi dengan satu sama lain. Sebuah cadangan untuk DR yang dinamakan Backup Designated Router (BDR) selalu dijaga agar informasi up to - date untuk menghilangkan transisi jika router DR rusak dan perlu diganti. Pada kondisi biasa setiap router secara periodik mengirim pesan LINK STATE UPDATE ke setiap router di sebelahnya. Setiap pesan memiliki nomor yang berurutan sehingga router dapat melihat apakah pesan LINK STATE UPDATE yang masuk lebih lama atau lebih baru daripada yang sudah dimiliki. Router juga mengirim pesan ini ketika ada jalur hidup atau mati atau cost - nya berubah.

Message Type	Description
Hello	Digunakan untuk menemukan siapa *router* tetangganya.
Link state update	Menyediakan cost *router* pengirim ke *router* tetangganya.
Link state ack	Membenarkan update pada link state.
Database description	Memberitahukan update yang mana yang *router* pengirim miliki.
Link state request	Meminta informasi dari *router* pasangan.

Fig. 8.2 Jenis - Jenis pesan OSPF

Area OSPF terdiri atas 2 jenis, yaitu single area dan multiple area. Pada modul ini lebih fokus pada Single-Area OSPF. Single area network merupakan routing OSPF yang memiliki satu area network saja dan biasanya digunakan untuk area yang kecil hal ini disebabkan karena jumlah router yang ada pada area network tersebut terbatas atau sedikit. Ketika menggunakan single area ini maka seluruh in-

formasi routing akan disebar ke tiap - tiap router pada area tersebut. Single area ini dapat diidentifikasikan dengan angka antara 0 sampai 4.294.967.295. hal ini dimaksudkan untuk memudahkan pengenalan terhadap suatu area. OSPFsingle area tidak memakai system summarization.

Sedangkan pada multiple area OSPF system summarization normalnya digunakan. Jika OSPF mempunyai lebih dari 1 area makan area 0 harus ada. Menerapkan multiple area OSPF area harus diterapkan pada area tersebut serta harus terkoneksi dengan area lainnya. Area 0 akan berperan sebagai jembatan penyeberangan informasi - informasi routing ke area lainnya.

8.2 Konfigurasi OSPF

Perintah perintah yang digunakan untuk konfigurasi OSPF mirip dengan EIGRP. Hanya saja kita perlu menentukan dari awal akan seperti apakah bentuk topologi network yang hendak dibangun. Akan sangat baik sekali jika kita sudah bisa memprediksinya untuk beberapa tahun ke depan.

1. Mengaktifkan proses OSPF

   router ospf <process-id>
   misal : R1(config)# router ospf 1

   Process-id adalah sembarang bilangan bulat positif dari 1 sampai 65535. Process-id ini bersifat local (bagi masing masing router), pada sebuah area nilainya tidak perlu sama, boleh berbeda beda. Namun penulis lebih suka menggunakan process-id yang sama agar memudahkan menghapalkannya.
   Pada sebuah router, mungkin saja menjalankan beberapa buah process-id OSPF sekaligus. Setiap proses haruslah menggunakan process-id yang berbeda beda. Namun sebaiknya hal ini dihindari sebab dapat menguras resource router.

2. Menentukan area pada network interface router

   network <network address> <wild mask> area <area-id>
   misal :
   R1(config-router)# network 192.168.10.0 0.0.255.255 area 0

   Area-id adalah bilangan bulat positif dari 0 sampai 4294967295 atau bilangan dalam format IP address xxxx.xxxx.xxx.xxx. Area-id adalah nomor area yang terkait dengan subnet. Lazimnya router router yang satu subnet akan dikelompokkan dalam satu area juga. Penulis lebih menyukai menggunakan area-id berupa bilangan bulat.

3. Menentukan router-id (RID)

router-id <router-id>
misal : R1(config-router)# router-id 1.1.1.1

Router-id (RID) merupakan identitas bagi router router OSPF. RID akan berperan langsung dalam penentuan topologi, DR, dan BDR. RID harus unik atau tidak boleh sama pada sebuah OSPF domain.
Biasanya secara default RID akan ditentukan berdasarkan nilai IP address tertinggi pada interface loopback atau interface pisik. Namun kita bisa menentukan nilai RID sesuai dengan kebutuhan.

8.3 Contoh Konfigurasi OSPF

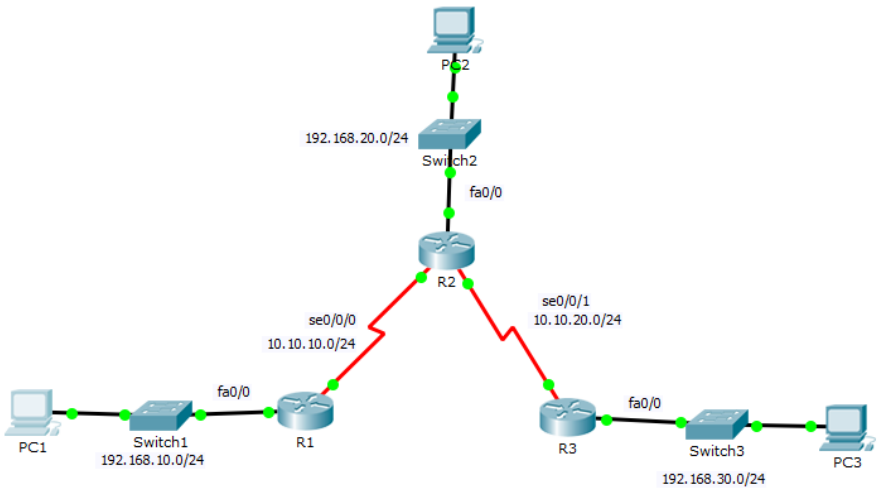


Fig. 8.3 Topologi OSPFv2

8.4 Tugas Lab

Buatlah topologi dan teruskan konfigurasi OSPFv3 sesuai dengan contoh yang telah dijabarkan sebelumnya. *untuk alamat IP dibebaskan. Lakukan konfigurasi dengan benar dan kumpulkan file PKA pada dosen.

Konfigurasi R1

```
Router>enable
Router#configure terminal
Router(config)#hostname R1
R1(config)#enable secret cisco
R1 (config)#line console 0
R1 (config-line)#password cisco
R1 (config-line)#login
R1 (config-line)#exit
R1 (config)#line vty 0 4
R1 (config-line)#password cisco
R1 (config-line)#login
R1 (config-line)#exit
R1 (config)#banner motd &
Enter TEXT message.  End with the character '&'.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!    AUTORIZED ACCESS ONLY   !!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! &
R1 (config)#interface serial 0/0/0
R1 (config-if)#ip address 10.10.10.1 255.255.255.0
R1 (config-if)#clock rate 64000
R1 (config-if)#no shutdown
R1 (config-if)#exit
R1 (config)#interface fastethernet 0/0
R1 (config-if)#ip address 192.168.10.1 255.255.255.0
R1 (config-if)#no shutdown
R1 (config-if)#exit
R1(config)#router ospf 10
R1(config-router)#router-id 1.1.1.1
R1(config-router)#net 192.168.10.0 0.0.0.255 area 11
R1(config-router)#net 10.10.10.0 0.0.0.255 area 11
R1 (config)#exit
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Fig. 8.4 Konfigurasi R1

Konfigurasi R2

```
Router>enable
Router#configure terminal
Router(config)#hostname R2
R2(config)#enable secret cisco
R2 (config)#line console 0
R2 (config-line)#password cisco
R2 (config-line)#login
R2 (config-line)#exit
R2 (config)#line vty 0 4
R2 (config-line)#password cisco
R2 (config-line)#login
R2 (config-line)#exit
R2 (config)#banner motd &
Enter TEXT message.  End with the character '&'.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!    AUTORIZED ACCESS ONLY   !!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! &
R2 (config)#interface serial 0/0/0
R2 (config-if)#ip address 10.10.10.2 255.255.255.0
R2 (config-if)#no shutdown
R2 (config-if)#exit
R2 (config)#interface serial 0/0/1
R2 (config-if)#ip address 10.10.20.1 255.255.255.0
R2 (config-if)#no shutdown
R2 (config-if)#exit
R2 (config)#interface fastethernet 0/0
R2 (config-if)#ip address 192.168.20.1 255.255.255.0
R2 (config-if)#no shutdown
R2 (config-if)#exit
R2(config)#router ospf 10
R2(config-router)#router-id 2.2.2.2
R2(config-router)#net 192.168.20.0 0.0.0.255 area 11
R2(config-router)#net 10.10.20.0 0.0.0.255 area 11
R2(config-router)#net 10.10.10.0 0.0.0.255 area 11
R2(config-router)#exit
R2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
```

Fig. 8.5 Konfigurasi R2

Konfigurasi R3

```
Router>enable
Router#configure terminal
Router(config)#hostname R3
R3(config)#enable secret cisco
R3 (config)#line console 0
R3 (config-line)#password cisco
R3 (config-line)#login
R3 (config-line)#exit
R3 (config)#line vty 0 4
R3 (config-line)#password cisco
R3 (config-line)#login
R3 (config-line)#exit
R3 (config)#banner motd &
Enter TEXT message.  End with the character '&'.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!    AUTORIZED ACCESS ONLY   !!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! &
R3 (config)#interface serial 0/0/1
R3 (config-if)#ip address 10.10.20.2 255.255.255.0
R3(config-if)#clock rate 64000
R3 (config-if)#no shutdown
R3 (config-if)#exit
R3 (config)#interface fastethernet 0/0
R3 (config-if)#ip address 192.168.30.1 255.255.255.0
R3 (config-if)#no shutdown
R3 (config-if)#exit
R3(config)#router ospf 10
R3(config-router)#router-id 3.3.3.3
R3(config-router)#net 192.168.30.0 0.0.0.255 area 11
R3(config-router)#net 10.10.20.0 0.0.0.255 area 11
R3(config-router)#exit
R3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Fig. 8.6 Konfigurasi R3

Configuring Global-Unicast Addresses on R1

```
R1(config)# ipv6 unicast-routing
R1(config)#
R1(config)# interface GigabitEthernet 0/0
R1(config-if)# description R1 LAN
R1(config-if)# ipv6 address 2001:DB8:CAFE:1::1/64
R1(config-if)# no shut
R1(config-if)#
R1(config-if)# interface Serial0/0/0
R1(config-if)# description Link to R2
R1(config-if)# ipv6 address 2001:DB8:CAFE:A001::1/64
R1(config-if)# clock rate 128000
R1(config-if)# no shut
R1(config-if)#
R1(config-if)# interface Serial0/0/1
R1(config-if)# description Link to R3
R1(config-if)# ipv6 address 2001:DB8:CAFE:A003::1/64
R1(config-if)# no shut
R1(config-if)# end
R1#
```

Fig. 8.7 Input IPv6

```
R1(config)# ipv6 router ospf 10
R1(config-rtr)# router-id 1.1.1.1
R1(config-rtr)# end
R1#
```

Fig. 8.8 Enable Router-Id OSPFv3

```
R1(config)# interface GigabitEthernet 0/0
R1(config-if)# ipv6 ospf 10 area 0
R1(config-if)#
R1(config-if)# interface Serial0/0/0
R1(config-if)# ipv6 ospf 10 area 0
R1(config-if)#
R1(config-if)# interface Serial0/0/1
R1(config-if)# ipv6 ospf 10 area 0
R1(config-if)#
R1(config-if)# end
R1#
R1# show ipv6 ospf interfaces brief
Interface  PID   Area      Intf ID  Cost   State  Nbrs F/C
Se0/0/1    10      0         7      15625  P2P    0/0
Se0/0/0    10      0         6      647    P2P    0/0
Gi0/0      10      0         3       1     WAIT   0/0
R1#
```

Fig. 8.9 Enable OSPFv3 pada Interface

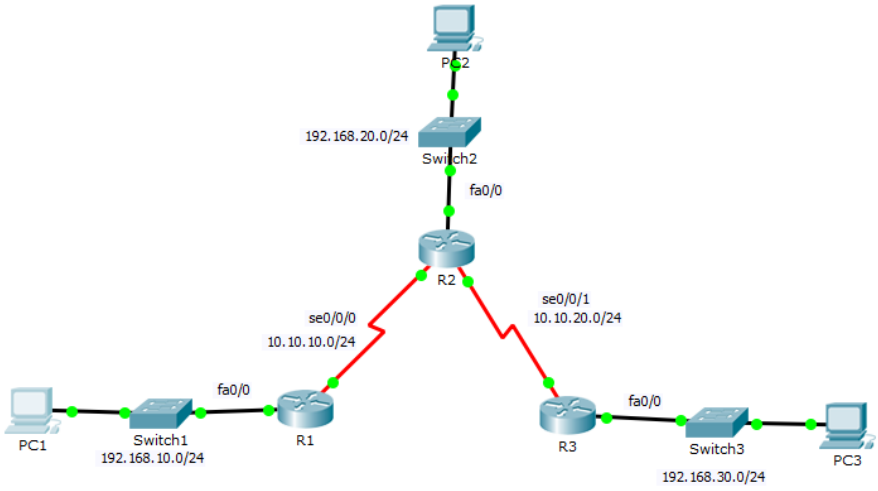


Fig. 8.10 Tugas Lab

Chapter 9
Access Control List (ACL)

9.1 Pendahuluan

ACL sederhananya digunakan untuk mengijinkan atau tidak paket dari host menuju ke tujuan tertentu. ACL terdiri atas aturan - aturan dan kondisi yang menentukan trafik jaringan dan menentukan proses di router apakah nantinya paket akan dilewatkan atau tidak. Modul ini akan menerangkan standar dan extended ACL, penempatan ACL dan beberapa aplikasi dari penggunaan ACL. ACL adalah daftar kondisi yang digunakan untuk mengetes trfaik jaringan yang mencoba melewati interface router. Daftar ini memberitahu router paket - paket mana yang akan diterima atau ditolak. Penerimaan dan penolakan berdasarkan kondisi tertentu.

Untuk mem-filter trafik jaringa, ACL menentukan jika paket itu dilewatkan atau diblok pada interface router. Router ACL membuat keputusan berdasarkan alamat asal, alamat tujuan, protokol, dan nomor port. ACL harus didefinisikan berdasarkan protokol, arah atau port. Untuk mengontrol aliran trafik pada interface, ACL harus didefinisikan setiap protokol pada interface. ACL kontrol trafik pada satu arah dalam interface. Dua ACL terpisah harus dibuat untuk mengontrol trafik inbound dan outbound.

Berikut ini adalah fungsi dari ACL:

1. Membatasi trafik jaringan dan meningkatkan unjuk kerja jaringan. Misalnya, ACL memblok trafik video, sehingga dapat menurunkan beban jaringan dan meningkatkan unjuk kerja jaringan.
2. Mengatur aliran trafik. ACL mampu memblok update routing. Jika update tidak dibutuhkan karena kondisi jaringan, maka bandwidth dapat dihemat.
3. Mampu membrikan dasar keamanan untuk akses ke jaringan. Misalnya, host A tidak diijinkan akses ke jaringan HRD dan host B diijinkan.
4. Memutuskan jenis trafik mana yang akan dilewatkan atau diblok melalui interface router. Misalnya, trafik email dilayani, trafik telnet diblok.
5. Mengontrol daerah-daerah dimana klien dapat mengakses jaringan.
6. Memilih host-hots yang diijinkan atau diblok akses ke segmen jaringan. Misal, ACL mengijinkan atau memblok FTP atau HTTP.

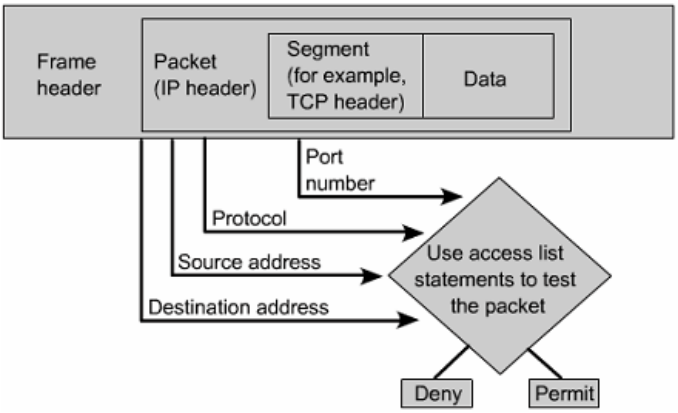


Fig. 9.1 Ilustrasi ACL

9.2 Cara Kerja ACL

Keputusan dibuat berdasarkan pernyataan/statement cocok dalam daftar akses dan kemudian menerima atau menolak sesuai apa yang didefinisikan di daftar pernyataan. Perintah dalam pernyataan ACL adalah sangat penting, kalau ditemukan pernyataan yang cocok dengan daftar akses, maka router akan melakukan perintah menerima atau menolak akses. Berikut ini gambar cara kerja ACL.

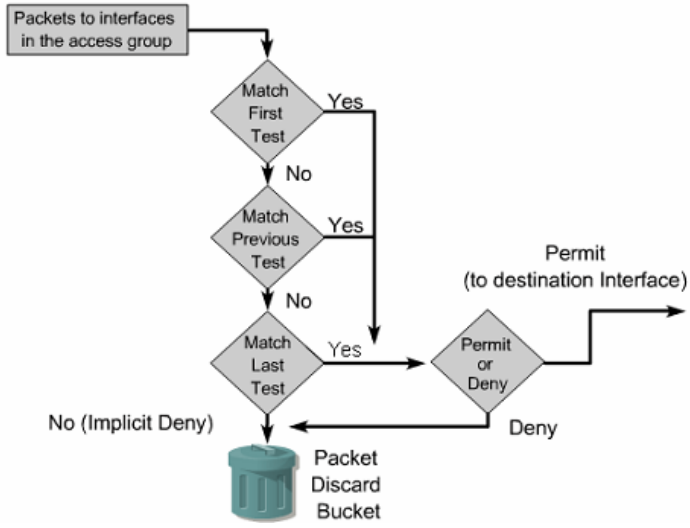


Fig. 9.2 Cara Kerja ACL

Pada saat frame masuk ke interface, router memeriksa apakah alamat layer 2 cocok atau apakah frame broadcast. Jikaalamat frame diterima, maka informasi frame ditandai dan router memeriksa ACL pada interface inbound. Jika ada ACL, paket diperiksa lagi sesuai dengan daftar akses. Jika paket cocok dengan pernyataan, paket akan diterima atau ditolak. Jika paket diterima di interface, ia akan diperiksa sesuai dengan table routing untuk menentukan interface tujuan dan di-switch keinterface itu. Selanjutnya router memriksa apakah interface tujuan mempunyaiACL. Jika ya, paket diperiksa sesuai dengan daftar akses. Jika paketcocok dengan daftar akses, ia akan diterima atau ditolak. Tapi jika tidak ada ACL paket diterima dan paket dienkapsulasi di layer 2 dan di-forwardkeluar interface device berikutnya.

9.3 Jenis ACL

9.3.1 Standard ACL

Standard ACL hanya menggunakan alamat sumber IP di dalam paket IP sebagai kondisi yang ditest. Semua keputusan dibuat berdasarkan alamat IP sumber. Ini artinya, standard ACL pada dasarnya melewatkan atau menolak seluruh paket protocol. ACL ini tidak membedakan tipe dari lalu lintas IP seperti WWW, telnet, UDP, DSP.

Standar ACL memeriksa alamat sumber dari paket IP yang routed. Perbandingan akan menghasilkan berbagai akses diijinkan atau ditolak untuk seluruh deretan protokol, berdasarkan pada jaringan, subnet, dan alamat host. Sebagai contoh, paket datang dalam Fa0/0 diperiksa untuk alamat sumber dan protocol. Jika paket diijinkan, paket routed melalui router untuk interface output. Jika paket tidak diijinkan, paket dihentikan pada interface yang datang. Versi standar perintah global configuration access - list digunakan untuk menetapkan standar ACL dengan angka dari 1 sampai 99 (juga dari 1300 sampai 1999 pada IOS terbaru).

Perintah lengkap standar ACL adalah:

```
Router(config)# access-list access-list-number deny —permit source [source-
wildcard ] [log]
```

Untuk menghapus ACL digunakan penambahan kata no diawal kalimat ACL, seperti contoh:

```
Router(config)# no access-list access-list-number
```

9.3.2 Extended ACL

Extended ACL bisa mengevalusai banyak field lain pada header layer 3 dan layer 4 pada paket IP. ACL ini bisa mengevaluasi alamat IP sumber dan tujuan, field protocol pada header network layer dan nomor port pada header transport layer. Ini memberikan extended ACL kemampuan untuk membuat keputusan-keputusan lebih spesifik ketika mengontrol lalu lintas.

Extended ACL lebih sering digunakan dari pada standard ACL sebab memberikan nilai range control yang besar. Extended ACL memeriksa sumber dan tujuan alamat paket dan mampu memeriksa protocol dan nomor port.

Perintah ip access - group menghubungkan extended ACL yang ada ke interface. Ingat hanya satu ACL per interface, per tujuan, per protocol diberikan.

Format perintahnya adalah:

```
Router(config-if)# ip access-group access-list-number in — out
```

9.4 Jenis Lalu Lintas ACL

9.4.1 Inbound ACL

Ketika sebuah ACL diterapkan pada paket inbound di sebuah interface, paket tersebut diproses melalui ACL sebelum di-route ke outbound interface. Setiap paket yang ditolak tidak bisa di-route karena paket ini diabaikan sebelum proses routing diabaikan.

9.4.2 Outbond ACL

Ketika sebuah ACL diterapkan pada paket outbound pada sebuah interface, paket tersebut di-route ke outbound interface dan diproses melalui ACL malalui antrian.

9.5 Verifikasi ACL

Untuk menampilkan informasi interface IP dan apakah terdapat ACL di interface itu gunakan perintah show ip interface. Perintah show access-lists untuk menampilkan isi dari ACL dalam router. Sedangkan perintah show running-config untuk melihat konfigurasi access list.

```
Router#show ip interface
FastEthernet0/0 is up, line protocol is down
  Internet address is 192.168.1.1/24
  Broadcast address is 255.255.255.255
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is 2
Serial0/0 is down, line protocol is down
  Internet address is 200.200.2.1/24
  Broadcast address is 255.255.255.255
  MTU is 1500 bytes
```

Fig. 9.3 Perintah show ip interface

```
Router#show access-lists
Standard IP access list 2
 deny   172.16.1.1
 permit 172.16.1.0, wildcard bits 0.0.0.255
 deny   172.16.0.0, wildcard bits 0.0.255.255
 permit 172.0.0.0, wildcard bits 0.255.255.255
Extended IP access list 101
 permit tcp 192.168.6.0 0.0.0.255 any eq telnet
 permit tcp 192.168.6.0 0.0.0.255 any eq ftp
 permit tcp 192.168.0.0 0.0.0.255 any eq ftp-data
Router#
```

Fig. 9.4 Perintah show access-lists

Terdapat hal yang perlu diperhatikan dalam perintah ACL yang seharusnya diikuti ketika membuat dan mengimplementasikan ACL pada router :

- Hanya bisa menerapkan satu ACL untuk setiap interface, setiap protocol dan setiap arah. Artinya bahwa ketika membuat ACL IP, hanya bisa membuat sebuah inbound ACL dan satu Outbound ACL untuk setiap interface.
- ACL adalah daftar urutan pernyataan penerimaan atau penolakan yang dijalankan untuk pengalamatan atau protokol layer atas.
- Penempatan dan urutan pernyataan ACL adalah hal yang sangat penting untuk unjuk kerja jaringan.
- Standar ACL digunakan untuk memeriksa alamat asal dari paket yang akan dirutekan.
- Sedangkan extended ACL digunakan lebih spesifik daripada standar ACL yang menyediakan lebih banyak parameter dan argumen.

9.6 Tugas Lab

Buatlah topologi dibawah ini pada Packet Tracer sesuaikan dengan IP yang telah ditentukan dan konfigurasi ACL. Lakukan konfigurasi dengan benar dan kumpulkan file PKA pada dosen.

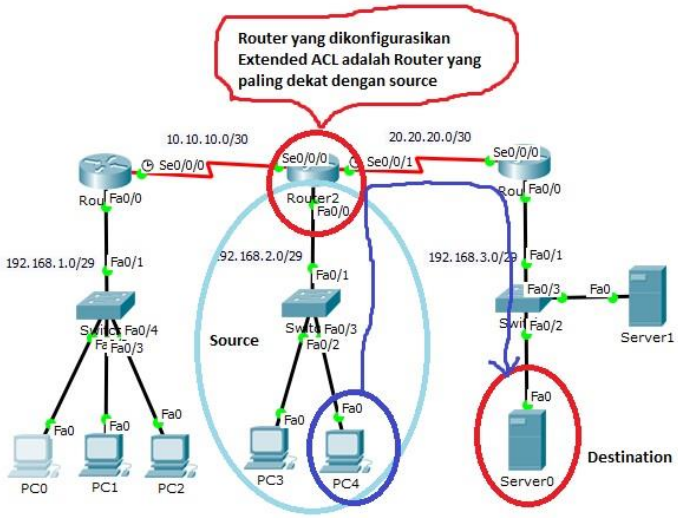


Fig. 9.5 Tugas Lab

Chapter 10
DHCP

10.1 Pendahuluan

Setiap perangkat yang terhubung ke jaringan membutuhkan alamat IP yang unik. Administrator jaringan memberikan alamat IP statis untuk router, server, printer, dan perangkat jaringan lainnya yang lokasi (fisik dan logis) tidak mungkin untuk berubah. Ini biasanya perangkat yang memberikan layanan kepada pengguna dan perangkat pada jaringan. Oleh karena itu, alamat yang ditugaskan kepada mereka harus tetap konstan. Selain itu, alamat statis memungkinkan administrator untuk mengelola perangkat ini dari jarak jauh. Hal ini lebih mudah bagi administrator jaringan untuk mengakses perangkat ketika mereka dapat dengan mudah menentukan alamat IP-nya.

Namun, komputer dan pengguna dalam suatu organisasi sering berubah lokasi, fisik dan logis. Ini bisa sulit dan memakan waktu untuk administrator untuk menetapkan alamat IP baru setiap kali bergerak karyawan. Selain itu, untuk karyawan mobile bekerja dari lokasi terpencil, manual pengaturan parameter jaringan yang benar dapat menantang. Bahkan untuk klien desktop, tugas manual alamat IP dan informasi pengalamatan lainnya menyajikan beban administrasi, terutama seiring berkembangnya jaringan.

Memperkenalkan Dynamic Host Configuration Protocol (DHCP) server untuk jaringan lokal menyederhanakan alamat IP tugas untuk desktop dan perangkat mobile. Menggunakan DHCP server terpusat memungkinkan organisasi untuk mengelola semua tugas alamat IP dinamis dari server tunggal. Praktek ini membuat manajemen alamat IP yang lebih efektif dan menjamin konsistensi di seluruh organisasi, termasuk kantor cabang.

- Memudahkan dalam transfer data kepada PC client lain atau PC server.
- DHCP menyediakan alamat-alamat IP secara dinamis dan konfigurasi lain. DHCP ini didesain untuk melayani network yang besar dan konfigurasi TCP/IP yang kompleks.

- DHCP memungkinkan suatu client menggunakan alamat IP yang reusable, artinya alamat IP tersebut bisa dipakai oleh client yang lain jika client tersebut tidak sedang menggunakannya (off).
- DHCP memungkinkan suatu client menggunakan satu alamat IP untuk jangka waktu tertentu dari server.
- DHCP akan memberikan satu alamat IP dan parameter-parameter kofigurasi lainnya kepada client.

10.2 Pengenalan DHCPv4

DHCPv4 memberikan alamat IPv4 dan informasi konfigurasi jaringan lainnya secara dinamis. Karena klien desktop biasanya membuat sebagian besar node jaringan, DHCPv4 adalah alat yang sangat berguna dan hemat waktu untuk administrator jaringan.

Sebuah dedicated server DHCPv4 adalah scalable dan relatif mudah untuk mengelola. Namun, dalam sebuah cabang kecil atau lokasi SOHO, router Cisco dapat dikonfigurasi untuk menyediakan layanan DHCPv4 tanpa perlu untuk dedicated server. Sebuah set fitur Cisco IOS (disebut ”IP Easy)” menawarkan opsional, fitur lengkap server yang DHCPv4.

DHCPv4 mencakup tiga mekanisme alokasi alamat yang berbeda untuk memberikan fleksibilitas ketika menetapkan alamat IP:

- Manual Allocation : Administrator memberikan alamat pra-dialokasikan IPv4 ke klien, dan DHCPv4 berkomunikasi hanya alamat IPv4 ke perangkat.
- Automatic Allocation : DHCPv4 secara otomatis memberikan alamat IPv4 statis permanen ke perangkat, memilih dari kolam yang tersedia alamat. Tidak ada sewa dan alamat secara permanen ditugaskan ke perangkat.
- Dinamis Alokasi : DHCPv4 dinamis memberikan, atau sewa, alamat IPv4 dari kolam alamat untuk jangka waktu terbatas yang dipilih oleh server, atau sampai klien tidak lagi membutuhkan alamat.

10.3 Konfigurasi Dasar DHCPv4

10.4 Stateless Address Autoconfiguration (SLAAC)

Mirip dengan IPv4, IPv6 alamat unicast global dapat dikonfigurasi secara manual atau secara dinamis. Namun, ada dua metode di mana alamat IPv6 unicast global dapat diberikan secara dinamis:

- Stateless Address Autoconfiguration (SLAAC)
- Dynamic Host Configuration Protocol untuk IPv6 (Stateful DHCPv6)

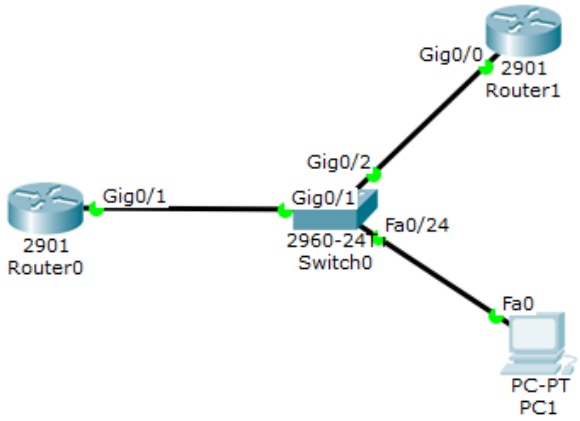


Fig. 10.1 Topologi

ROUTER DHCP-SERVER

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname DHCP-SERVER
DHCP-SERVER(config)#interface gigabitEthernet0/1
DHCP-SERVER(config-if)#ip address 192.168.0.1 255.255.255.0
DHCP-SERVER(config-if)#description Gateway-LAN
DHCP-SERVER(config-if)#no shutdown


DHCP-SERVER(config)#ip dhcp pool belajar-dhcp
DHCP-SERVER(dhcp-config)#default-router 192.168.0.1
DHCP-SERVER(dhcp-config)#network 192.168.0.0 255.255.255.0
```

Fig. 10.2 Konfigurasi Router DHCP-Server

SLAAC adalah metode di mana perangkat dapat memperoleh alamat IPv6 unicast global tanpa jasa server DHCPv6. Pada inti dari SLAAC adalah ICMPv6. ICMPv6 mirip dengan ICMPv4 tetapi mencakup fungsi tambahan dan merupakan protokol yang jauh lebih kuat. SLAAC menggunakan ICMPv6 Router Solicitation dan Router Advertisement pesan untuk memberikan pengalamatan dan informasi konfigurasi lainnya yang biasanya akan diberikan oleh server DHCP:

- Router Solicitation (RS) Message : Ketika klien dikonfigurasi untuk mendapatkan informasi yang menangani secara otomatis menggunakan SLAAC, klien

ROUTER-CLIENT

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname ROUTER-CLIENT
ROUTER-CLIENT(config)#interface gigabitEthernet0/0
ROUTER-CLIENT(config-if)#ip address dhcp
ROUTER-CLIENT(config-if)#no shutdown
```

Router#**sh interfaces gigabitEthernet0/0** (perintah untuk melihat "ROUTER-ONE" mendapatkan IP berapa dari "ROUTER DHCP-SERVER" ?

Pada kasus ini router mendapatkan IP :

```
ROUTER-CLIENT#sh interfaces gigabitEthernet0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
  Hardware is CN Gigabit Ethernet, address is 00d0.976d.3d01 (bia
00d0.976d.3d01)
  Internet address is 192.168.0.2/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

Fig. 10.3 Konfigurasi Router Client

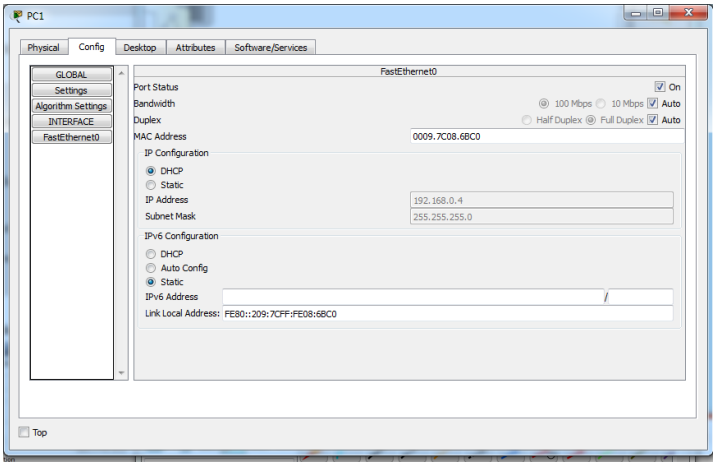


Fig. 10.4 Konfigurasi PC Client

mengirimkan pesan RS ke router. Pesan RS dikirim ke IPv6 semua-router alamat multicast FF02 :: 2.

- Router Advertisement (RA) Message : Pesan RA dikirim oleh router untuk memberikan informasi pengalamatan kepada klien dikonfigurasi untuk mendapatkan alamat IPv6 secara otomatis. Seorang klien menggunakan informasi ini untuk membuat alamat IPv6 unicast global sendiri. Sebuah router mengirimkan pesan RA berkala, atau dalam menanggapi pesan RS. Secara default, router Cisco men-

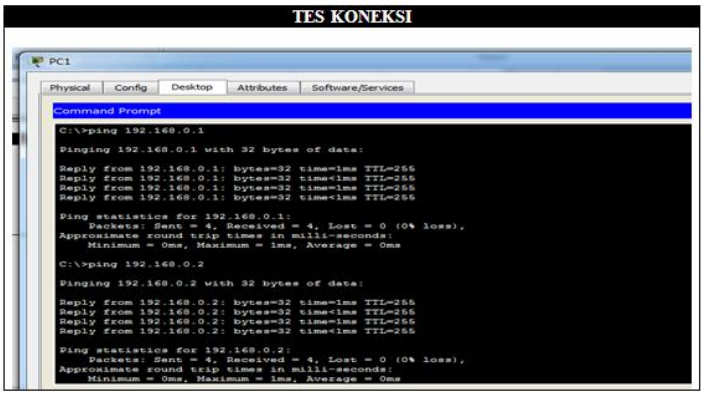


Fig. 10.5 Tes Koneksi

girim pesan RA setiap 200 detik. Pesan RA selalu dikirim ke IPv6 semua-node address multicast FF02 :: 1.

Chapter 11
Network Address Translation untuk IPv4

11.1 Pendahuluan

NAT (Network Address Translation) atau dalam bahasa Indonesia disebut dengan Penafsiran Alamat Jaringan adalah suatu metode untuk menghubungkan lebih dari 1 (satu) komputer ke dalam jaringan internet dengan menggunakan 1 (satu) alamat IP Address. Banyak yang menggunakan metode ini dikarenakan ketersediaan Alamat IP Address yang memang terbatas, kebutuhan akan keamanan (security), dan kemudahan serta fleksibilitas di dalam suatu administrasi jaringan. NAT menjadi salah satu protokol di dalam suatu sistem jaringan. NAT ini memungkinkan suatu jaringan dengan IP Address atau Internet Protocol yang bersifat Private atau Private IP yang sifatnya belum ter-registrasi di dalam jaringan internet dalam mengakses jalur internet.

Hal ini berarti bahwa suatu alamat IP bisa mengakses internet menggunakan IP Private atau bahkan menggunakan IP Publik, NAT biasanya ditempatkan di dalam suatu router. NAT ini juga sering digunakan dalam menggabungkan atau menghubungkan 2 (dua) buah jaringan yang saling berbeda, dan menafsirkan atau menerjemahkan IP Private atau bukan IP Public di dalam jaringan internal ke dalam jaringan yang legal network sehingga memiliki hak dalam melakukan akses data di sebuah jaringan.

Internet merupakan sebuah jaringan yang menghubungkan seluruh pengguna komputer di seluruh dunia. Untuk menghubungkan setiap komputer tersebut digunakan sebuah pengenal komputer yang disebut dengan IP Address. Satu IP Address hanya dapat digunakan oleh satu komputer, dalam satu jaringan tidak diperbolehkan adanya IP Address yang sama. Sedangkan jumlah IP Address yang tersedia tidak sebanding dengan jumlah pengguna yang akan terhubung dengan jaringan internet. Untuk mengatasi semua itu, disiasatilah dengan diciptakanya protocol bernama NAT (Network Address Translation).

Fungsi NAT (Network Address Translation :

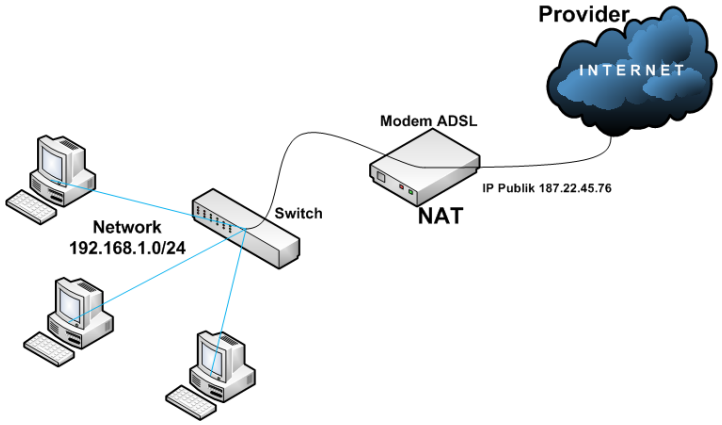


Fig. 11.1 Ilustrasi NAT

- Menerjemahkan IP Address komputer menjadi IP Public yang memiliki hak akses ke jaringan Internet
- Menghemat IP Legal yang dibutuhkan oleh Internet Service Provider
- Menghindari pengulangan pengalamatan ketika jaringan berubah
- Mengurangi duplikat IP Address
- Meningkatkan fleksibilitas jaringan

Kekurangan NAT :

- Ada aplikasi Internet yang tidak dapat berjalan menggunakan NAT
- Proses translasi dapat menimbulkan delay switching
- Menghilangkan kemampuan traceability end-to-end IP.

11.2 Jenis-Jenis NAT (Network Address Translation)

11.2.1 NAT Statis

NAT Statis adalah yang menggunakan tabel routing tetap, alokasi yang diberikan ditetapkan sesuai dengan alamat asal ke alamat tujuan. Jadi komputer tidak dapat melakukan transaksi data apabila belum didaftarkan dalam tabel NAT. Penerjemahan dilakukan ketika sebuah IP Address lokal dipetakan dalam IP Public, alamat tersebut dipetakan satu lawan satu secara static. NAT akan melakukan data request dan data sent sesuai dengan aturan yang telah ditetapkan dalam tabel NAT.

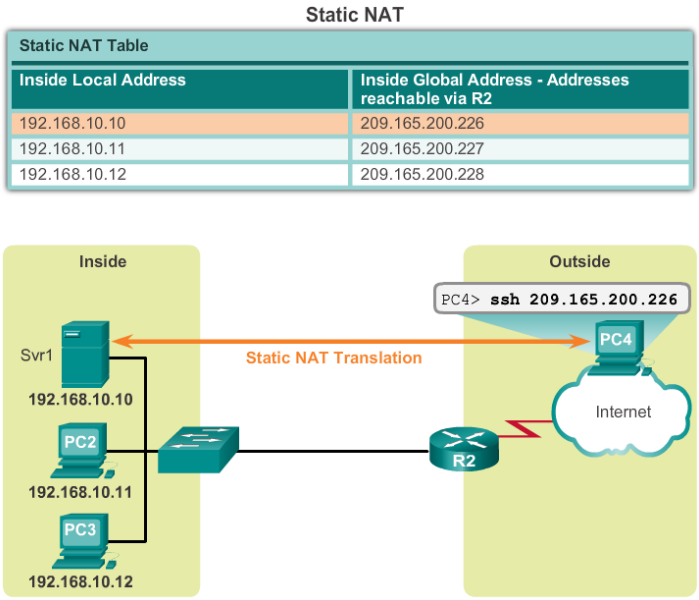


Fig. 11.2 Ilustrasi Statik NAT

11.2.2 NAT Dinamis

NAT dinamis menggunakan logika balancing, yaitu dimana pada tabel NAT ditanamkan logika kemungkinan dan pemecahan dari suatu alamat. Ada 2 jenis NAT dinamis, yaitu NAT System Pool dan NAT System Overload.

11.2.3 NAT Sistem Overload

NAT dengan sistem Overloading menggunakan logika request atau permintaan dari banyak client atau banyak alamat dioperkan atau diberikan ke satu alamat IP distribusi. Sejumlah IP lokal/internal dapat ditranslasikan ke satu alamat IP global (outside). Sejumlah IP Lokal /internal dapat ditranslasikan ke satu alamat IP global (outside). Hal ini sangat menghemat penggunakan alokasi IP dari ISP. Sharing/pemakaian bersama satu alamat IP ini menggunakan metoda port multiplexing, atau perubahan port ke packet outbound. Sehingga ada yang menyebut NAT sistem overload dengan istilah PAT (Port Address Translation) atau NAT Dynamic Over-Load.

Penggabungan sistem overloading dan sistem pool telah dilakukan oleh banyak produsen router dan menghasilkan logika yang banyak digunakan untuk load balancing saat ini yaitu Round Robbin Load Balancing, dimana logika ini melakukan

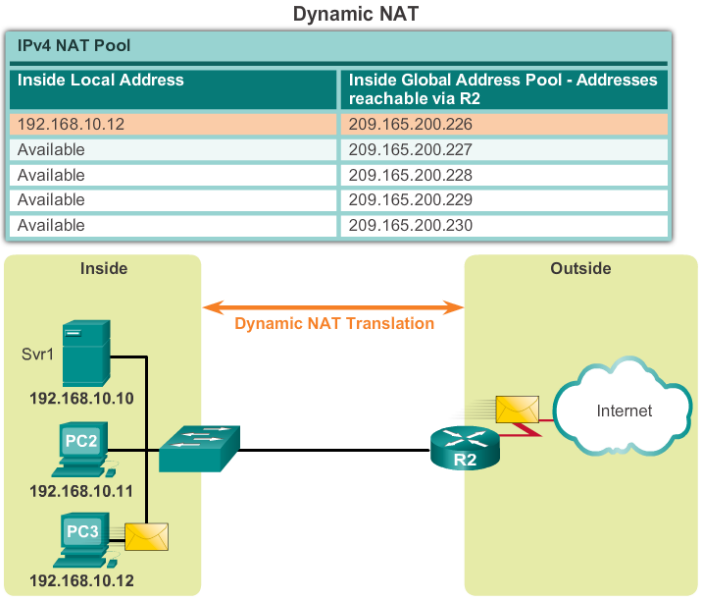


Fig. 11.3 Ilustrasi NAT Dinamis

pengiriman request secara berurutan, secara bergantian ke alamat gateway yang telah ditanamkan dalam tabel NAT sebelumnya, sehingga suatu multirequest dari sebuah alamat IP dapat melalui lebih dari satu alamat distribusi, penerapan ini dapat dilakukan dalam penggunaan Dual Wan Router, selain itu logika ini juga memiliki logika Fail Over, dimana bila suatu alamat distribusi tidak dapat lagi mengirimkan paket maka paket akan dialihkan ke alamat distribusi yang lain.

11.3 Konfigurasi NAT

11.3.1 Konfigurasi NAT Static

Kenapa di namakan Static seperti pembagian IP Address saja, karena di dalam NAT Static termasuk one to one NAT atau satu IP Private untuk satu IP Public dan tidak akan pernah berubah ubah IP Publicnya, berikut ini contoh NAT Static.

Setelah memahami sedikit tentang NAT Static biar tidak lama lama, Gambar 11.4 merupakan Topology dari NAT Static.

Keterangan:
N=Network
Background BIRU (Public)
Background HIJAU (Private)

Table 11.1 IP NAT Static

No.	IP Local/Private	IP Public
1	192.168.32.10	213.18.123.110
2	192.168.32.12	213.18.123.111
3	192.168.32.15	213.18.123.112

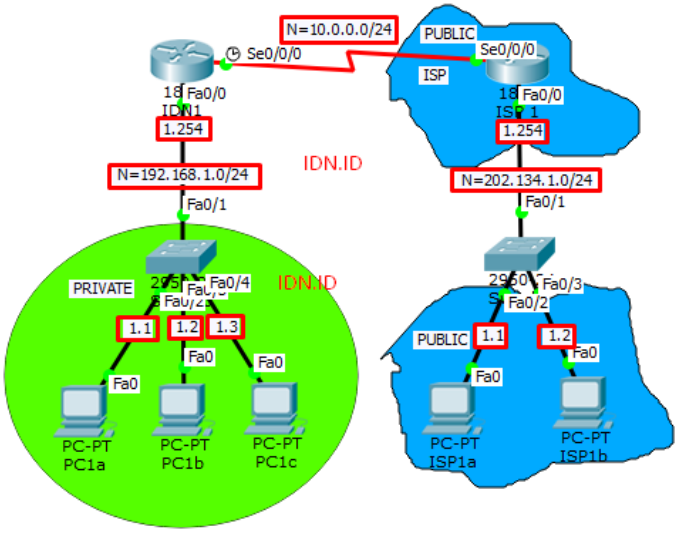


Fig. 11.4 NAT Static

1.1 / 1.254 dll.= IP belakang dari Network-nya.

Table 11.2 IP Static NAT:

No.	IP Local/Private	IP Public
1	192.168.1.1	50.1.1.1
2	192.168.1.2	50.1.1.2
3	192.168.1.3	50.1.1.3

Lakukan input IP dan konfigurasi seperti biasa, kemudian masukkan perintah berikut ini dalam langkah mengaktifkan NAT Static.

Setelah ke dua sisi router telah kita konfigurasi seperti contoh diatas, kemudian cek PING antar PC atau Router namun ada baiknya cek kembali konfigurasi di Router IDN1 yang telah dilakukan seperti contoh berikut.

Konfigurasi Router IDN 1

Membuat IP

```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
Router(config)#hostname idn1
idn1(config)#int se0/0/0
idn1(config-if)#ip add 10.0.0.1 255.255.0.0
idn1(config-if)#clock rate 64000
idn1(config-if)#no shut
idn1(config-if)#exit
idn1(config)#int fa 0/0
idn1(config-if)#ip add 192.168.1.254 255.255.255.0
idn1(config-if)#no shut
idn1(config-if)#int se0/0/0
idn1(config-if)#exit
```

Membuat NAT

```
idn1(config)#ip nat inside source static 192.168.1.1
50.1.1.1
idn1(config)#ip nat inside source static 192.168.1.2
50.1.1.2
idn1(config)#ip nat inside source static 192.168.1.3
50.1.1.3
```

Implementasi NAT

```
idn1(config)#int fa0/0
idn1(config-if)#ip nat inside
idn1(config-if)#exit
idn1(config)#int se0/0/0
idn1(config-if)#ip nat outside
idn1(config-if)#exit
```

Membuat Default Route (Routing)

```
idn1(config)#ip route 0.0.0.0 0.0.0.0 10.0.0.2
```

Fig. 11.5 Konfigurasi Router IDN 1

11.3.2 Konfigurasi NAT Dinamis

NAT Dynamic seperti halnya IP DHCP kita tidak perlu konfigurasi IP satu per satu demikian juga NAT Dynamic kita tidak perlu konfigurasi IP Public satu persatu

Konfigurasi Router ISP 1

Membuat IP

```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
Router(config)#int se 0/0/0
Router(config-if)#ip add 10.0.0.2 255.255.0.0
Router(config-if)#clock rate 64000
Router(config-if)#no shut
Router(config-if)#int fa0/0
Router(config-if)#ip add 202.134.1.254 255.255.255.0
Router(config-if)#no shut
Router(config-if)#exit
```

Membuat Default Route (Routing)

```
Router(config)#ip route 50.0.0.0 255.0.0.0 10.0.0.1
```

Fig. 11.6 Konfigurasi Router ISP 1

Router IDN 1

idn1(config)#do sh ip nat trans

Pro	Inside global	Inside local	Outside local	Outside global
icmp	50.1.1.1:1	192.168.1.1:1	202.134.1.1:1	202.134.1.1:1
icmp	50.1.1.1:2	192.168.1.1:2	202.134.1.1:2	202.134.1.1:2
icmp	50.1.1.1:3	192.168.1.1:3	202.134.1.1:3	202.134.1.1:3
icmp	50.1.1.1:4	192.168.1.1:4	202.134.1.1:4	202.134.1.1:4
icmp	50.1.1.1:5	192.168.1.1:5	202.134.1.1:5	202.134.1.1:5
icmp	50.1.1.1:6	192.168.1.1:6	202.134.1.1:6	202.134.1.1:6
icmp	50.1.1.1:7	192.168.1.1:7	202.134.1.1:7	202.134.1.1:7
icmp	50.1.1.1:8	192.168.1.1:8	202.134.1.1:8	202.134.1.1:8
---	50.1.1.1	192.168.1.1	---	---
---	50.1.1.2	192.168.1.2	---	---
---	50.1.1.3	192.168.1.3	---	---

Fig. 11.7 Router IDN 1

semuanya otomatis atau dynamic, ini biasanya di gunakan pada IP Private yang banyak, jadi Translate ke IP Publicnya (NAT) sekaligus sesuai dengan jmlah IP

Private nya dan hanya dengan memasukkan IP Pool Public dengan jumlah yang di tentukan, jadi jangan berharap untuk satu IP Private pada satu IP Public yang sama karena nanti akan berubah - ubah IP Publicnya, ini termasuk type many to many NAT, seperti contoh di bawah ini.

Table 11.3 Tabel IP NAT Dinamis

No.	IP Local/Private	IP Public	Dinamis
1	192.168.32.10	213.18.123.116	213.18.123.112 (192.168.32.12)
2	192.168.32.12	213.18.123.112	213.18.123.113 (192.168.32.31)
3	192.168.32.11	213.18.123.115	213.18.123.114 (192.168.32.7)
4	192.168.32.31	213.18.123.114	213.18.123.115 (192.168.32.11)
5	192.168.32.7	213.18.123.113	213.18.123.116 (192.168.32.10)

Oke langsung saja masuk ke LAB NAT Dynamic, masih sama Topolgy seperti LAB Static tinggal di rubah saja dengan menghapus konfigurasi NAT Static yang sebelumnya dengan Command berikut ini:

kemudian membuat NAT Dynamic dengan Syntax berikut ini:

```
idn1(config)# access-list <ACL-Nomer> permit <Network ID>
<WildcardMask>
idn1(config)# ip nat pool <Name> <Starting Publc IP> <End Public IP>
netmask <Mask>
idn1(config)# ip nat inside source list <ACL-Nomer> pool <Name>
```

Verifikasikan seperti halnya pada NAT Static yaitu dengan melakukan PING terlebih dahulu pada semua PC1 (IDN) ke PC ISP, kemudian ketik command berikut ini pada Router IDN.

Itu daftar IP yang di translasikan ke IP Public oleh Router IDN pada konfigurasi NAT Dynamic, bisa melakukan pengecekan yang lainnya, misal: sh ip route, sh ip int br, dll.

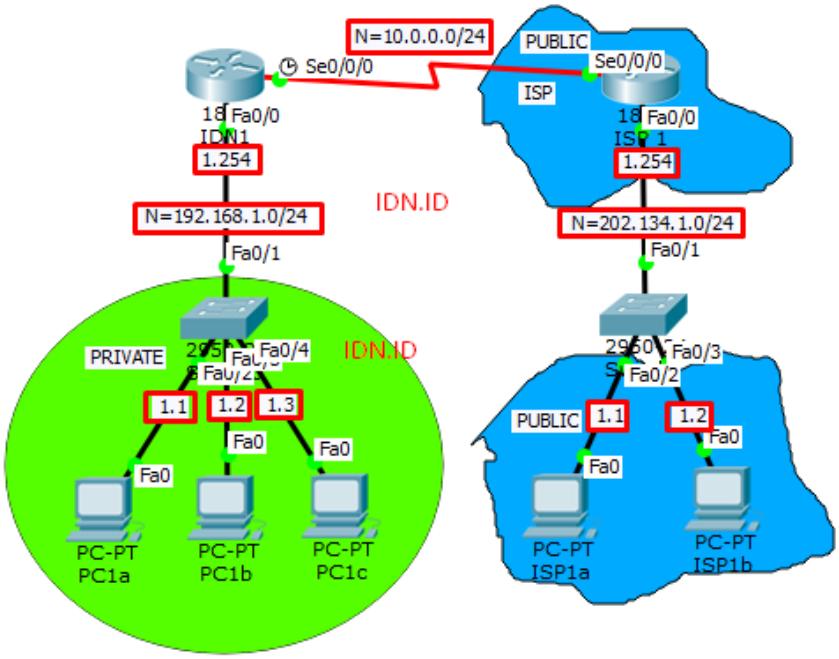


Fig. 11.8 NAT Dinamis

Konfigurasi Router IDN 1

Membuat IP

```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
Router(config)#hostname idn1
idn1(config)#int se0/0/0
idn1(config-if)#ip add 10.0.0.1 255.255.0.0
idn1(config-if)#clock rate 64000
idn1(config-if)#no shut
idn1(config-if)#exit
idn1(config)#int fa 0/0
idn1(config-if)#ip add 192.168.1.254 255.255.255.0
idn1(config-if)#no shut
idn1(config-if)#int se0/0/0
idn1(config-if)#exit
```

Membuat NAT

```
idn1(config)#access-list 50 permit 192.168.1.0 0.0.0.255
idn1(config)#ip nat pool IDN 50.1.1.1 50.1.1.200 netmask
255.255.255.0
idn1(config)#ip nat inside source list 50 pool IDN
```

Implementasi NAT

```
idn1(config)#int se0/0/0
idn1(config-if)#ip nat outside
idn1(config-if)#exit
idn1(config)#int fa0/0
idn1(config-if)#ip nat inside
idn1(config-if)#exit
```

Membuat Default Route (Routing)

```
idn1(config)#ip route 0.0.0.0 0.0.0.0 10.0.0.2
```

Fig. 11.9 Konfigurasi Router IDN 1

Konfigurasi Router ISP 1

Membuat IP

```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
Router(config)#int se 0/0/0
Router(config-if)#ip add 10.0.0.2 255.255.0.0
Router(config-if)#clock rate 64000
Router(config-if)#no shut
Router(config-if)#int fa0/0
Router(config-if)#ip add 202.134.1.254 255.255.255.0
Router(config-if)#no shut
Router(config-if)#exit
```

Membuat Default Route (Routing)

```
Router(config)#ip route 50.0.0.0 255.0.0.0 10.0.0.1
```

Fig. 11.10 Konfigurasi Router ISP 1

Router IDN 1

idn1#sh ip nat trans

Pro	Inside global	Inside local	Outside local	Outside global
icmp	50.1.1.1:5	192.168.1.2:5	202.134.1.2:5	202.134.1.2:5
icmp	50.1.1.1:6	192.168.1.2:6	202.134.1.2:6	202.134.1.2:6
icmp	50.1.1.1:7	192.168.1.2:7	202.134.1.2:7	202.134.1.2:7
icmp	50.1.1.1:8	192.168.1.2:8	202.134.1.2:8	202.134.1.2:8
icmp	50.1.1.2:1	192.168.1.3:1	202.134.1.2:1	202.134.1.2:1
icmp	50.1.1.2:2	192.168.1.3:2	202.134.1.2:2	202.134.1.2:2
icmp	50.1.1.2:3	192.168.1.3:3	202.134.1.2:3	202.134.1.2:3
icmp	50.1.1.2:4	192.168.1.3:4	202.134.1.2:4	202.134.1.2:4
icmp	50.1.1.2:5	192.168.1.3:5	202.134.1.2:5	202.134.1.2:5
icmp	50.1.1.2:6	192.168.1.3:6	202.134.1.2:6	202.134.1.2:6
icmp	50.1.1.2:7	192.168.1.3:7	202.134.1.2:7	202.134.1.2:7
icmp	50.1.1.2:8	192.168.1.3:8	202.134.1.2:8	202.134.1.2:8
icmp	50.1.1.3:10	192.168.1.1:10	202.134.1.2:10	202.134.1.2:10
icmp	50.1.1.3:11	192.168.1.1:11	202.134.1.2:11	202.134.1.2:11
icmp	50.1.1.3:12	192.168.1.1:12	202.134.1.2:12	202.134.1.2:12
icmp	50.1.1.3:9	192.168.1.1:9	202.134.1.2:9	202.134.1.2:9

Fig. 11.11 Router IDN 1

Daftar Pustaka

1. Kurose, James F., and Keith W. Ross. *Computer networking: a top-down approach*. Vol. 5. Reading: Addison-Wesley, 2010.
2. Lin, Ying-Dar. *Computer networks: an open source approach*. McGraw-Hill, 2012.
3. Sofana, Iwan. *Cisco CCNA & Jaringan Komputer*. Informatika. Bandung (2010).
4. Lammle, Todd. *CCNA Cisco Certified Network Associate Deluxe Study Guide*. John Wiley & Sons, 2011.
5. Odom, Wendell. *Cisco CCNA Routing and Switching ICND 200-101: Official Cert Guide*. Pearson Education, 2013.
6. Odom, Wendell. *CCNP Route 642-902 official certification guide*. Cisco Press, 2010.
7. Odom, Wendell, Rus Healy, and Denise Donohue. *CCIE routing and switching certification guide*. Pearson Education, 2010.
8. McQuerry, Stephen, and M. Thomas. *Interconnecting Cisco Network Devices*. Cisco Press, 2000.
9. Sofana, Iwan. *CISCO CCNP dan Jaringan Komputer (Materi Route, Switch, & Troubleshooting)*. Bandung: Informatika (2012).
10. Rafiudin, Rahmat. *Mengupas Tuntas Cisco Router*. Elexmedia Komputindo, Jakarta (2003).
11. Clark, Kennedy, and Kevin Hamilton. *Cisco LAN Switching (CCIE Professional Development series)*. (2001).