
Modul 1: Advanced Routing 1 (Routing Table Interpretation)

Materi ini membahas cara membaca dan memahami tabel routing pada router Cisco, yang memiliki struktur hierarkis untuk mempercepat proses pencarian rute.

- **Jenis-Jenis Rute Berdasarkan Sumber:**
 - **S (Static):** Rute yang dimasukkan secara manual oleh administrator.
 - **C (Connected):** Rute yang dibuat secara otomatis ketika sebuah interface dikonfigurasi dengan alamat IP dan dalam keadaan aktif.
 - **R (RIP) & O (OSPF):** Rute yang dipelajari secara dinamis melalui protokol routing.
- **Struktur Hierarkis Tabel Routing Cisco:**
 - **Level 1 Route (Induk/Parent):** Rute yang rata kiri. Bisa berupa *Network Route* (sesuai kelas), *Supernet Route* (agregasi beberapa network), atau *Default Route* (0.0.0.0/0). Sebuah Parent Route tidak bisa digunakan untuk meneruskan paket jika ia memiliki turunan (child).
 - **Level 2 Route (Anak/Child):** Rute yang menjorok ke dalam (indentasi). Ini adalah subnet dari sebuah Parent Route.
 - **Ultimate Route:** Rute yang dapat digunakan untuk meneruskan paket karena memiliki *next-hop address* atau *exit interface*. Semua rute Level 2 adalah *ultimate route*. Rute Level 1 juga bisa menjadi *ultimate route* jika tidak memiliki *child*.
- **Proses Pencarian Rute (Routing Lookup):**
 - Router akan mencari rute yang paling spesifik (*the most specific match*) atau yang memiliki prefiks terpanjang (*the longest match*).
 - Contoh: Jika ada rute /18 dan /26 yang cocok untuk sebuah paket tujuan, router akan memilih rute /26 karena lebih spesifik.

Modul 2 & 3: Advanced Routing 2 (OSPF dan Redistribusi Static Route)

Materi ini membahas protokol routing dinamis OSPF (Open Shortest Path First) dan cara mengintegrasikannya dengan rute statis.

- **Konsep Dasar OSPF:**
 - Merupakan protokol *link-state* yang membangun "peta" topologi jaringan.
 - **Administrative Distance (AD):** Nilai kepercayaan sebuah rute. OSPF memiliki AD 110. **Semakin kecil nilai AD, semakin dipercaya.** (Contoh: Static = 1, OSPF = 110, RIP = 120).
 - **Konfigurasi OSPF:**
 - **Process ID:** Angka identifikasi proses OSPF yang hanya berlaku lokal di router tersebut (tidak harus sama antar router).
 - **Area ID:** Semua router dalam satu area **harus memiliki Area ID yang sama** (misal, area 0) agar bisa bertukar informasi routing.
 - **Wildcard Mask:** Kebalikan dari subnet mask (misal, 255.255.255.0 menjadi 0.0.0.255).
- **Redistribusi Rute Statis ke dalam OSPF:**
 - Digunakan agar OSPF dapat "mengiklankan" rute yang dikonfigurasi secara statis.
 - **redistribute static subnets:** **Perintah untuk mendistribusikan rute statis yang spesifik (network-based)** ke dalam domain OSPF.
 - **default-information originate:** **Perintah khusus untuk mendistribusikan default route (0.0.0.0/0) saja** ke dalam domain OSPF. Ini sangat umum digunakan untuk menyediakan jalur ke internet bagi semua router di dalam area OSPF.

Modul 4: IPv6

Materi ini memperkenalkan IPv6 sebagai penerus IPv4 untuk mengatasi keterbatasan jumlah alamat.

- **Fitur dan Perbedaan Utama:**
 - **Ukuran Alamat:** 128-bit (vs 32-bit IPv4).
 - **Format:** Heksadesimal, dipisahkan oleh titik dua (:).
 - **Aturan Penyingkatan:** Nol di depan dapat dihilangkan, dan satu blok nol berurutan dapat diganti dengan ::
 - **Prefix:** Menggunakan notasi prefix (misal, /64) dan tidak ada subnet mask.
- **Jenis Alamat IPv6:**
 - **Global Unicast:** Alamat publik yang dapat dirutekan secara global (misal, 2001:DB8::/32 untuk dokumentasi).
 - **Link-Local:** Alamat yang dimulai dengan FE80::. Dibuat otomatis, hanya berlaku di satu segmen jaringan (link), dan tidak dapat dirutekan. Sering digunakan sebagai alamat *default gateway* pada PC.

Modul 5 & 6: VLAN dan Router on a Stick (RoaS)

Materi ini membahas konsep Virtual LAN (VLAN) untuk segmentasi logis dan metode routing antar-VLAN.

- **Konsep Dasar VLAN:**
 - **Tujuan:** Membagi satu switch fisik menjadi beberapa *broadcast domain* virtual yang terpisah, seolah-olah menjadi beberapa switch yang berbeda.
 - **Prinsip Dasar:** **Create** (membuat VLAN) dan **Assign** (menempatkan port ke dalam VLAN).
 - **Mode Port:**
 - **Access Port:** Dikonfigurasi untuk menjadi anggota satu VLAN saja. Biasanya terhubung ke perangkat akhir seperti PC.
 - **Trunk Port:** Dikonfigurasi untuk dapat membawa trafik dari beberapa VLAN sekaligus. Biasanya digunakan untuk menghubungkan antar switch atau switch ke router.

- **Router on a Stick (RoaS):**
 - Metode untuk melakukan *inter-VLAN routing* (routing antar VLAN) menggunakan satu interface fisik router.
 - **Sub-interface:** Pada interface fisik router (misal Gig0/0), dibuat beberapa sub-interface virtual (misal Gig0/0.10, Gig0/0.20).
 - **Konfigurasi:** Setiap sub-interface diberi alamat IP yang akan menjadi *gateway* bagi VLAN-nya masing-masing dan dihubungkan ke VLAN tersebut dengan perintah encapsulation dot1q [vlan_id]. Interface fisik pada router tidak diberi IP, hanya diaktifkan.
-

Modul 7: VLAN Trunking Protocol (VTP)

VTP adalah protokol Cisco-proprietary yang menyederhanakan manajemen VLAN di jaringan dengan banyak switch.

- **Tujuan:** Mengotomatiskan pembuatan, modifikasi, dan penghapusan VLAN di semua switch dalam satu domain, sehingga administrator tidak perlu mengonfigurasinya satu per satu.
- **Penting:** VTP hanya menyinkronkan database VLAN (create/delete), bukan penugasan port (assign). Penugasan port ke VLAN tetap harus dilakukan secara manual di setiap switch.
- **Mode VTP:**
 - **Server:** Dapat membuat/mengubah/menghapus VLAN dan menyebarkan informasi tersebut ke switch lain.
 - **Client:** Menerima informasi VLAN dari server dan tidak dapat membuat VLAN secara lokal.
 - **Transparent:** Meneruskan update VTP dari server, tetapi tidak memprosesnya dan mengelola database VLAN-nya sendiri secara lokal.
- **Syarat:** Semua switch harus berada dalam VTP domain yang sama dan memiliki password VTP yang sama (jika dikonfigurasi).

Modul 8 & 9: Standard & Extended Access Control List (ACL)

ACL digunakan untuk memfilter paket (firewall dasar) berdasarkan aturan yang ditentukan.

- **Prinsip Dasar: Create** (membuat daftar aturan) dan **Assign** (menerapkannya pada interface dengan arah in atau out).
- **Standard ACL (Nomor 1-99):**
 - **Kriteria Filter:** Hanya berdasarkan alamat IP sumber (source).
 - **Aturan Penempatan:** Ditempatkan sedekat mungkin dengan tujuan (destination) untuk menghindari pemblokiran yang tidak diinginkan.
- **Extended ACL (Nomor 100-199):**
 - **Kriteria Filter:** Berdasarkan IP sumber, IP tujuan, protokol (TCP/UDP), dan nomor port.
 - **Aturan Penempatan:** Ditempatkan sedekat mungkin dengan sumber (source) untuk efisiensi, karena paket yang tidak diinginkan dapat segera dibuang.
- **Implicit Deny Any:** Di akhir setiap ACL, terdapat aturan deny any yang tidak terlihat. Jika sebuah paket tidak cocok dengan aturan permit manapun, ia akan ditolak.
- **Tabel Perbandingan Port Number vs Keyword**

Layanan (Service)	Protokol	Nomor Port	Kata Kunci (Keyword)
FTP (Data)	TCP	20	ftp-data
FTP (Control)	TCP	21	ftp
SSH	TCP	22	ssh
Telnet	TCP	23	telnet
SMTP (Email)	TCP	25	smtp
DNS	TCP/UDP	53	domain
HTTP (Web)	TCP	80	www
POP3 (Email)	TCP	110	pop3
HTTPS (Secure Web)	TCP	443	https

Modul 10: Frame Relay

Frame Relay adalah teknologi WAN Layer 2 yang lebih lawas, dikenal sebagai jaringan **Non-Broadcast Multi-Access (NBMA)**. Artinya, meskipun beberapa perangkat dapat terhubung ke "awan" Frame Relay yang sama, mereka tidak dapat saling mengirimkan broadcast secara default.

- **Konsep dan Cara Kerja:**

- **Alamat Layer 2:** Menggunakan **DLCI (Data-Link Connection Identifier)** sebagai pengenal alamat, bukan MAC address. DLCI ini bersifat signifikan secara lokal (hanya unik pada satu interface).
- **Virtual Circuits:** Service provider membuat koneksi logis yang disebut **Permanent Virtual Circuits (PVCs)** dengan cara **memetakan (pairing) DLCI antara router pelanggan di lokasi yang berbeda**.
- **Konektivitas:** Sebuah router dapat terhubung ke banyak titik (misalnya dalam topologi **Hub-and-Spoke**) melalui beberapa PVC pada satu interface fisik. Ini menciptakan ilusi koneksi pribadi yang langsung melalui jaringan bersama milik provider.

- **Efisiensi dan Model Biaya:**

- **Biaya Lebih Murah:** Frame Relay jauh lebih hemat biaya dibandingkan *leased-line* (saluran sewa) tradisional.
- **Efisiensi Jarak:** Pengguna layanan hanya membayar biaya sewa **local loop** (koneksi fisik dari kantor ke "awan" provider) dan **sewa bandwidth**, tanpa memperhitungkan jarak geografis antar lokasi.
- **Jaminan Bandwidth:** Kapasitas bandwidth dijamin melalui **Committed Information Rate (CIR)**, yaitu jaminan kecepatan minimum yang diatur dan disepakati dengan service provider.

- **Penggunaan dan Aplikasi:**

- Karena efisiensinya, Frame Relay populer digunakan sebagai koneksi **backbone** pada jaringan.
- Banyak diimplementasikan untuk **interkoneksi** antara kantor cabang perusahaan (enterprise), antar ISP (Internet Service Provider), dan untuk jaringan pemerintah.

Modul 11: Spanning Tree Protocol (STP)

STP adalah protokol yang mencegah terjadinya switching loop di jaringan Layer 2 yang memiliki jalur redundan.

- **Tujuan:** Mencegah *broadcast storm* dan ketidakstabilan tabel MAC address dengan cara memblokir port secara logis untuk menciptakan topologi bebas-loop.
- **Proses STP:**
 1. **Pemilihan Root Bridge:** Switch dengan **Bridge ID terendah** akan terpilih sebagai *Root Bridge*. Bridge ID terdiri dari **Priority** (lebih rendah lebih baik) dan **MAC Address** (digunakan sebagai tie-breaker).
 2. **Penentuan Port Roles:**
 - **Root Port:** Di setiap switch non-root, port yang memiliki jalur terpendek (biaya terendah) menuju Root Bridge. Port ini dalam status *forwarding*.
 - **Designated Port:** Di setiap segmen jaringan, port yang menjadi jalur terbaik menuju Root Bridge. Semua port di Root Bridge adalah Designated Port. Port ini dalam status *forwarding*.
 - **Non-Designated / Blocking Port:** Port-port sisanya yang akan diblokir untuk mencegah loop. Jika jalur utama putus, port ini bisa beralih menjadi aktif.