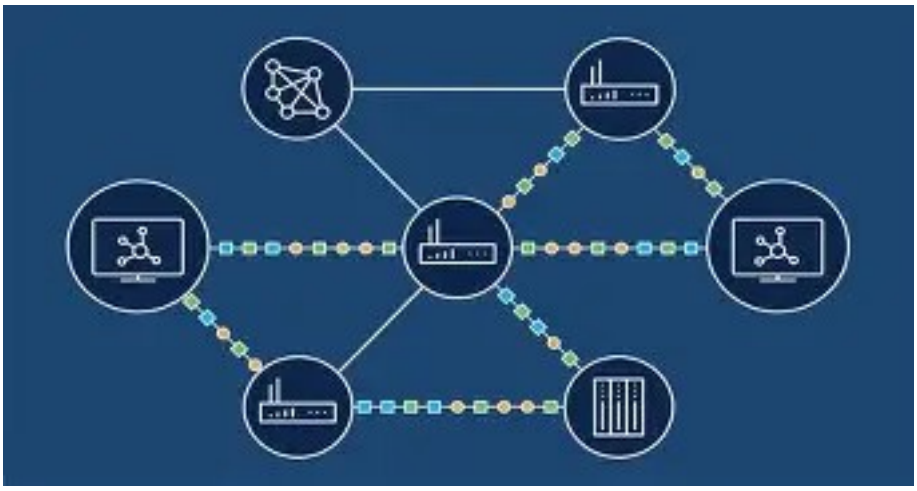
2026

D3-Teknik Komputer
Jurusan Teknologi Informasi
Politeknik Negeri Padang

Ir. H.A. Mooduto, M.Kom.



[SWITCHING, ROUTING & WIRELESS]

Bahan Ajar Berbasis RPS Kurikulum Outcome-Based Education (OBE)

BAHAN AJAR

Mata Kuliah: Switching, Routing, dan Wireless (Teori)
Kode Mata Kuliah: CEN3201
Program Studi: D3-Teknik Komputer, Politeknik Negeri Padang
Dosen Pengampu: Ir. H. A. Mooduto, M.Kom.

MATERI

BAGIAN 1: PENDAHULUAN

- **Bab 1: Pengantar Jaringan Komputer dan Model Referensi**
  - **1.1.** Deskripsi Mata Kuliah dan Kontrak Belajar
  - **1.2.** Konsep Dasar Jaringan Komputer
  - **1.3.** Model Referensi OSI (7 Layer) dan Fungsinya
  - **1.4.** Arsitektur Protokol TCP/IP (Application, Transport, Internet, Network Access)
  - **1.5.** Perangkat Jaringan Dasar: Switch, Router, dan Access Point (Fungsi dan Karakteristik)
  - *(Mendukung Sub-CPMK-1)*

BAGIAN 2: DASAR-DASAR SWITCHING

- **Bab 2: Konsep Collision dan Broadcast Domain**
  - **2.1.** Definisi Collision Domain dan Cara Kerjanya
  - **2.2.** Definisi Broadcast Domain dan Cara Kerjanya
  - **2.3.** Peran Switch dalam Membagi Collision Domain
  - **2.4.** Peran Router dalam Membagi Broadcast Domain
  - *(Mendukung Sub-CPMK-2)*
- **Bab 3: Virtual Local Area Network (VLAN) dan Trunking**
  - **3.1.** Konsep VLAN: Definisi, Manfaat, dan Cara Kerja
  - **3.2.** Jenis-jenis VLAN (Default, Data, Management, Native)
  - **3.3.** Konsep Trunking dan Standar IEEE 802.1Q (Tagging)
  - **3.4.** Konfigurasi VLAN dan Trunking pada Switch Cisco (dengan Simulasi Packet Tracer)
  - *(Mendukung Sub-CPMK-3 & Sub-CPMK-4)*

BAGIAN 3: DASAR-DASAR ROUTING

- **Bab 4: Prinsip Dasar Routing**
  - **4.1.** Konsep Routing: Forwarding Paket antar Jaringan
  - **4.2.** Komponen Tabel Routing (Jaringan Tujuan, Next-Hop, Metric, Interface)
  - **4.3.** Jenis-jenis Routing: Statis vs Dinamis
  - **4.4.** Metrik Routing (Hop Count, Bandwidth, Delay)
  - *(Mendukung Sub-CPMK-5)*
- **Bab 5: Routing Statis**
  - **5.1.** Prinsip dan Karakteristik Routing Statis

    - **5.2.** Konfigurasi Route Statis (dengan Next-Hop dan Exit-Interface)
    - **5.3.** Konfigurasi Default Route
    - **5.4.** Verifikasi Konektivitas dan Tabel Routing (*show ip route, ping, traceroute*)
    - *(Mendukung Sub-CPMK-6)*
- **Bab 6: Routing Dinamis (RIP dan OSPF)**
    - **6.1.** Konsep Routing Dinamis: Kelebihan dan Kekurangan
    - **6.2. Routing Information Protocol (RIP):** Prinsip, Metric (Hop Count), Versi (RIPv1 vs RIPv2)
    - **6.3. Open Shortest Path First (OSPF):** Prinsip, Konsep Area, Metric (Cost), Keunggulan dibanding RIP
    - **6.4.** Perbandingan RIP dan OSPF
    - **6.5.** Konfigurasi Dasar OSPF pada Router Cisco (dengan Simulasi Packet Tracer)
    - *(Mendukung Sub-CPMK-7 & Sub-CPMK-8)*

BAGIAN 4: JARINGAN NIRKABEL (WIRELESS)

- **Bab 7: Teknologi Jaringan Wireless**
    - **7.1.** Pengantar Jaringan Wireless LAN (WLAN)
    - **7.2.** Standar IEEE 802.11 (a/b/g/n/ac/ax) dan Karakteristiknya (Frekuensi, Kecepatan)
    - **7.3.** Topologi Jaringan Wireless: Infrastructure Mode, Ad-Hoc, Mesh
    - **7.4.** Perangkat Wireless: Access Point, Wireless NIC, Antenna
    - *(Mendukung Sub-CPMK-9)*
- **Bab 8: Keamanan Dasar Jaringan Wireless**
    - **8.1.** Ancaman Dasar pada Jaringan Wireless
    - **8.2.** Metode Keamanan Wireless: WEP, WPA, WPA2, WPA3
    - **8.3.** Konfigurasi SSID dan Keamanan WPA2 pada Access Point (dengan Simulasi Packet Tracer)
    - *(Mendukung Sub-CPMK-10)*

BAGIAN 5: TROUBLESHOOTING DAN PROYEK INTEGRASI

- **Bab 9: Troubleshooting Jaringan**
    - **9.1.** Pendekatan Sistematis dalam Troubleshooting
    - **9.2.** Perintah Dasar Troubleshooting: *ping, traceroute, telnet/ssh, show commands* (interface, running-config, ip route, vlan)
    - **9.3.** Studi Kasus Troubleshooting Jaringan *Switched* (VLAN mismatch, trunk error)
    - **9.4.** Studi Kasus Troubleshooting Jaringan *Routed* (routing statis salah, OSPF tidak bertetangga)
    - **9.5.** Studi Kasus Troubleshooting Jaringan *Wireless* (koneksi client, keamanan)
    - *(Mendukung Sub-CPMK-11 & Sub-CPMK-12)*
- **Bab 10: Proyek Terintegrasi: Desain Jaringan Kampus Kecil**
    - **10.1.** Analisis Kebutuhan dan Spesifikasi Jaringan

    - **10.2.** Perancangan Topologi Hierarkis (dengan VLAN, Routing, dan Wireless)
    - **10.3.** Implementasi Konfigurasi Terintegrasi (Switch, Router, Access Point)
    - **10.4.** Verifikasi dan Pengujian Jaringan
    - **10.5.** Panduan Penyusunan Laporan Proyek
    - **10.6.** Panduan Persiapan Presentasi Proyek
    - *(Mendukung Review Sub-CPMK-4,6,8,10 dan Penguatan Sub-CPMK 1-12)*

BAGIAN 6: PENUTUP

- **Bab 11: Review dan Persiapan Ujian Akhir**
    - **11.1.** Ringkasan Materi Perkuliahan (Pertemuan 1-15)
    - **11.2.** Latihan Soal Teori dan Studi Kasus Terintegrasi
    - **11.3.** Simulasi Ujian Praktik (Konfigurasi di Packet Tracer)

LAMPIRAN:

- Lampiran A: Glosarium Istilah Jaringan
- Lampiran B: Daftar Perintah Dasar Cisco IOS
- Lampiran C: Rubrik Penilaian (Tugas, UTS, UAS, Partisipasi) - *sesuai dokumen RPS*
- Lampiran D: Daftar Referensi Lengkap

Bagian 1: PENDAHULUAN

BAB 1
PENGANTAR JARINGAN KOMPUTER DAN MODEL REFERENSI

1.1. Deskripsi Mata Kuliah dan Kontrak Belajar

Selamat datang, mahasiswa sekalian, dalam mata kuliah **Switching, Routing, dan Wireless**. Mata kuliah ini adalah fondasi utama bagi kalian yang bercita-cita menjadi teknisi jaringan komputer atau IT support yang handal.

Apa yang akan kita pelajari?
Kita akan mempelajari bagaimana sebuah jaringan komputer dibangun, mulai dari perangkat kerasnya hingga cara mengkonfigurasinya. Fokus utama kita adalah pada tiga teknologi inti:

1. **Switching:** Bagaimana menghubungkan banyak perangkat dalam satu jaringan lokal (Local Area Network) secara efisien.
2. **Routing:** Bagaimana menghubungkan antar jaringan lokal yang berbeda, termasuk jaringan internet.
3. **Wireless:** Bagaimana membangun jaringan tanpa kabel (nirkabel) yang aman dan andal.

Mengapa mata kuliah ini penting?
Bayangkan sebuah kantor atau kampus tanpa jaringan komputer. Tidak ada internet, tidak bisa berbagi data printer, tidak ada server bersama. Peran kalian sebagai lulusan Teknik Komputer adalah memastikan semua sumber daya tersebut dapat terhubung, berkomunikasi, dan berjalan dengan stabil. Mata kuliah ini akan membekali kalian dengan kemampuan untuk merancang, membangun, dan memecahkan masalah pada jaringan tersebut.

Metode Pembelajaran:
Pembelajaran kita akan menggabungkan teori dan praktik. Di dalam kelas (teori), kita akan membahas konsep-konsep fundamental. Untuk praktik, kita akan menggunakan software simulator bernama **Cisco Packet Tracer**. Software ini memungkinkan kalian merancang topologi jaringan dan mengkonfigurasi perangkat Cisco (switch dan router) secara virtual, persis seperti yang akan kalian lakukan di dunia industri nanti.

Kontrak Belajar:

- **Kehadiran:** Minimal 80% untuk bisa mengikuti UAS.
- **Tugas:** Ada tugas kecil di hampir setiap pertemuan. Kerjakan dengan baik karena bobotnya total 30%.

- **Partisipasi:** Aktif bertanya dan berdiskusi akan menambah nilai partisipasi (10%).
- **Ujian:** UTS (30%) dan UAS (30%) akan menguji pemahaman teori dan kemampuan praktik kalian.

1.2. Konsep Dasar Jaringan Komputer

Sebelum melangkah lebih jauh, mari kita pahami dulu: **Apa itu jaringan komputer?** Secara sederhana, **jaringan komputer adalah dua atau lebih perangkat komputasi (komputer, server, printer, smartphone) yang saling terhubung satu sama lain untuk dapat berbagi data dan sumber daya.**

Tujuan dibangunnya jaringan komputer:

1. **Berbagi Sumber Daya:** Kita bisa menggunakan satu printer untuk banyak komputer (resource sharing). Kita juga bisa menyimpan data di satu server dan mengaksesnya dari mana saja (centralized data).
2. **Komunikasi:** Memungkinkan komunikasi antar pengguna, seperti email, chatting, atau video conference.
3. **Akses Informasi:** Menyediakan akses ke informasi yang berada di komputer lain atau di internet.
4. **Efisiensi dan Reliabilitas:** Dengan jaringan, kita bisa mendistribusikan pekerjaan. Jika satu komputer mati, komputer lain masih bisa mengambil alih tugasnya.

Jenis-jenis Jaringan Berdasarkan Skala:
Kita akan sering mendengar istilah-istilah ini:

- **LAN (Local Area Network):** Jaringan lokal dalam area terbatas, seperti dalam satu ruangan, satu gedung, atau satu kampus. Contoh: Jaringan laboratorium komputer di kampus kita. Kecepatannya tinggi dan biaya relatif murah.
- **MAN (Metropolitan Area Network):** Jaringan yang mencakup satu kota. Biasanya menghubungkan beberapa lokasi LAN. Contoh: Jaringan antar kampus dalam satu kota.
- **WAN (Wide Area Network):** Jaringan dengan cakupan geografis yang luas, bisa antar kota, antar negara, bahkan antar benua. Internet adalah contoh WAN terbesar di dunia.

1.3. Model Referensi OSI (7 Layer) dan Fungsinya

Agar perangkat dari vendor yang berbeda bisa saling berkomunikasi, diperlukan sebuah aturan baku atau **protokol**. Untuk memudahkan pemahaman dan standarisasi, para ahli membuat sebuah model referensi bernama **OSI (Open Systems Interconnection)**.

Model OSI membagi proses komunikasi data menjadi **7 lapisan (layer)**. Bayangkan ini seperti proses pengiriman surat. Setiap lapisan memiliki tugas spesifik dan hanya berkomunikasi dengan lapisan yang sama di perangkat tujuan.

Mari kita bahas dari lapisan paling bawah (fisik) ke lapisan paling atas (aplikasi):

- **Layer 1: Physical (Fisik)**
  - **Fungsi:** Mendefinisikan spesifikasi fisik media transmisi. Ini adalah urusan kabel, konektor, tegangan listrik, dan kecepatan pengiriman bit (0 dan 1).
  - **Perangkat:** Kabel UTP, konektor RJ45, Hub, Repeater, Network Interface Card (NIC).
  - **Protokol/Standar:** Ethernet (spesifikasi fisik), USB, Bluetooth (aspek fisik).
  - *Analogi:* Seperti truk pengangkut surat dan jalan raya yang dilaluinya.
- **Layer 2: Data Link**
  - **Fungsi:** Menyediakan koneksi yang andal antar dua perangkat yang terhubung langsung. Ia bertugas membuat *frame* (paket data yang sudah dibungkus) dan melakukan koreksi kesalahan sederhana. Di sinilah pengalamatan fisik menggunakan **MAC Address** berperan.
  - **Perangkat:** Switch, Bridge. NIC juga bekerja di layer ini.
  - **Protokol/Standar:** Ethernet (bagian MAC), PPP (Point-to-Point Protocol).
  - *Analogi:* Seperti kurir yang menuliskan alamat pengirim dan penerima di amplop (MAC Address) dan memastikan amplop itu sampai ke pos selanjutnya.
- **Layer 3: Network**
  - **Fungsi:** Ini adalah lapisan inti dari routing. Bertugas menentukan jalur terbaik (routing) untuk mengirimkan paket data dari jaringan asal ke jaringan tujuan. Di sinilah pengalamatan logis menggunakan **IP Address** berperan.
  - **Perangkat:** Router.
  - **Protokol:** IP (Internet Protocol), ICMP (ping), OSPF, RIP.
  - *Analogi:* Seperti menentukan rute perjalanan surat dari Padang ke Jakarta, melewati kota-kota mana saja.
- **Layer 4: Transport**
  - **Fungsi:** Bertanggung jawab untuk memastikan pengiriman data yang andal (end-to-end) dari host asal ke host tujuan. Ia memecah data menjadi segmen-segmen, mengatur urutan, dan memastikan tidak ada data yang hilang.
  - **Protokol:** TCP (Transmission Control Protocol) - andal tapi lambat, UDP (User Datagram Protocol) - cepat tapi tidak andal.
  - *Analogi:* Seperti petugas pos yang mencatat semua surat, memastikan tidak ada yang tertinggal, dan memberitahu pengirim jika surat sudah diterima.

- **Layer 5: Session**
  - **Fungsi:** Mengelola sesi komunikasi antar aplikasi. Ia bertugas membuat, memelihara, dan mengakhiri sesi.
  - **Protokol:** NetBIOS, RPC (Remote Procedure Call).
  - *Analogi:* Seperti negosiasi awal: "Halo, saya ingin bicara dengan bagian pemasaran." "Baik, akan saya sambungkan."
- **Layer 6: Presentation**
  - **Fungsi:** Bertugas menerjemahkan data agar bisa dimengerti oleh layer aplikasi. Fungsinya meliputi enkripsi (mengamankan data), dekripsi, dan kompresi (memperkecil ukuran data).
  - **Protokol:** SSL/TLS (untuk enkripsi web), JPEG, GIF (format gambar), MPEG (format video).
  - *Analogi:* Seperti penerjemah bahasa. Surat berbahasa Inggris diterjemahkan ke Bahasa Indonesia agar si penerima mengerti.
- **Layer 7: Application**
  - **Fungsi:** Lapisan yang paling dekat dengan pengguna. Di sinilah aplikasi jaringan beroperasi dan pengguna berinteraksi dengan jaringan.
  - **Protokol:** HTTP/HTTPS (web browsing), FTP (transfer file), SMTP/POP3/IMAP (email), DNS (penerjemah nama domain ke IP).
  - *Analogi:* Pengguna menulis surat di aplikasi email (misal: Outlook). Ini adalah interaksi di layer aplikasi.

Tips Mengingat 7 Layer OSI:

Dari atas ke bawah: **A**ll **P**eople **S**eem **T**o **N**eed **D**ata **P**rocessing
Atau dari bawah ke atas: **P**lease **D**o **N**ot **T**hrow **S**ausage **P**izza **A**way

---

1.4. Arsitektur Protokol TCP/IP (Application, Transport, Internet, Network Access)

Model OSI adalah model teoritis yang sangat bagus untuk pembelajaran. Namun, model yang **benar-benar digunakan di internet dan dunia nyata** adalah model **TCP/IP (Transmission Control Protocol/Internet Protocol)**.

Model TCP/IP menyederhanakan 7 layer OSI menjadi **4 layer**. Perhatikan korelasinya dengan OSI:

Lapisan TCP/IP	Fungsi Utama	Protokol Contoh	Padanan Layer OSI
4. Application	Menyediakan layanan untuk aplikasi pengguna.	HTTP, FTP, DNS, SMTP, DHCP	Layer 5, 6, 7 (Session, Presentation, Application)
3. Transport	Komunikasi end-to-end, pengiriman data andal.	TCP, UDP	Layer 4 (Transport)

Lapisan TCP/IP	Fungsi Utama	Protokol Contoh	Padanan Layer OSI
2. Internet	Menentukan alamat logis (IP) dan jalur routing.	IP, ICMP, ARP, OSPF	Layer 3 (Network)
1. Network Access	Mengirim dan menerima data dari media fisik.	Ethernet, Wi-Fi (802.11), PPP	Layer 1 dan 2 (Physical & Data Link)

Mengapa TCP/IP lebih populer?

1. **Sederhana:** Dengan 4 layer, implementasinya lebih mudah.
2. **Praktis:** Dibangun dan dikembangkan seiring dengan perkembangan internet.
3. **Terbukti Andal:** Model ini sudah menjadi fondasi internet selama puluhan tahun.

Ketika kita browsing, email-an, atau streaming video, data kita diproses melewati layer-layer TCP/IP ini, baik di sisi pengirim maupun penerima.

1.5. Perangkat Jaringan Dasar: Switch, Router, dan Access Point

Sekarang kita akan berkenalan dengan tiga perangkat bintang yang akan kita gunakan sepanjang semester ini. Ingat, setiap perangkat bekerja di layer yang berbeda dalam model OSI/TCP/IP.

A. Switch

- **Layer Kerja:** Layer 2 (Data Link).
- **Fungsi Utama:** Menghubungkan banyak perangkat dalam satu jaringan lokal (LAN).
- **Cara Kerja:** Switch menggunakan **MAC Address** untuk meneruskan data. Ketika sebuah frame data datang, switch membaca MAC Address tujuan, lalu mencari di tabel MAC Address-nya (MAC Address Table) ke port mana perangkat dengan MAC itu terhubung. Setelah ditemukan, frame hanya akan dikirim ke port tujuan tersebut. Ini yang disebut dengan **selective forwarding**.
- **Keunggulan:** Jauh lebih cerdas daripada Hub. Karena hanya mengirim ke port yang tepat, switch mengurangi kemungkinan tabrakan data (collision) dan meningkatkan efisiensi jaringan.
- **Analogi:** Switch seperti resepsionis di kantor kecil yang tahu persis siapa duduk di meja mana. Jika ada surat untuk Budi, resepsionis langsung mengantarkannya ke meja Budi, tidak perlu berteriak ke seluruh ruangan.

B. Router

- **Layer Kerja:** Layer 3 (Network).
- **Fungsi Utama:** Menghubungkan antar jaringan yang berbeda. Inilah gerbang (gateway) menuju jaringan lain, termasuk internet.

- **Cara Kerja:** Router menggunakan **IP Address** untuk menentukan jalur terbaik. Ia memiliki sebuah **tabel routing** (routing table) yang berisi "peta" jaringan. Ketika sebuah paket data datang dengan IP tujuan tertentu, router melihat tabel routing-nya untuk memutuskan ke mana paket itu harus diteruskan selanjutnya (next-hop).
- **Keunggulan:** Router memungkinkan perangkat di jaringan lokal (misal: 192.168.1.0) untuk berkomunikasi dengan perangkat di jaringan internet (misal: 8.8.8.8). Router juga berfungsi memisahkan broadcast domain.
- **Analogi:** Router seperti pos polisi di perbatasan kota. Ia memiliki peta dan tahu jalan mana yang harus ditempuh untuk mencapai kota-kota lain. Jika ada paket yang mau dikirim ke luar kota, paket itu harus melalui pos polisi ini.

C. Access Point

- **Layer Kerja:** Layer 2 (Data Link).
- **Fungsi Utama:** Memancarkan sinyal nirkabel (Wi-Fi) sehingga perangkat seperti laptop dan smartphone dapat terhubung ke jaringan kabel (LAN) secara wireless.
- **Cara Kerja:** Access Point (AP) bertindak sebagai jembatan antara jaringan kabel (switch) dan perangkat nirkabel. AP menerima data dari switch, lalu mengubahnya menjadi sinyal radio (gelombang elektromagnetik) yang dipancarkan ke udara. Sebaliknya, AP menerima sinyal radio dari perangkat nirkabel, mengubahnya kembali menjadi data, dan mengirimkannya ke switch.
- **Keunggulan:** Memberikan mobilitas dan fleksibilitas. Pengguna tidak perlu repot dengan kabel.
- **Analogi:** Access Point seperti menara pemancar sinyal Wi-Fi di rumah atau kantor. Ia mengambil koneksi internet dari kabel (modem/router kabel) dan menyebarkannya ke udara agar bisa dinikmati perangkat lain.

Hubungan Ketiganya dalam Sebuah Jaringan Sederhana:

Bayangkan sebuah kantor kecil.

1. Semua komputer karyawan terhubung ke sebuah **Switch**. Ini membentuk jaringan lokal kantor.
2. Di kantor juga ada sebuah **Access Point** yang terhubung ke switch yang sama, sehingga laptop tamu bisa terhubung ke jaringan kantor via Wi-Fi.
3. Semua perangkat di kantor (komputer via kabel, laptop via Wi-Fi) ingin mengakses internet. Untuk itu, switch terhubung ke sebuah **Router**. Router inilah yang menjadi pintu keluar menuju internet yang disediakan oleh ISP (Internet Service Provider).

Rangkuman Pertemuan 1:
Kita telah belajar tentang definisi jaringan, model OSI 7 layer dengan fungsinya, model TCP/IP 4 layer, dan tiga perangkat penting: Switch, Router, dan Access Point. Pahami betul lapisan kerja masing-masing perangkat dan protokol yang ada di setiap layer, karena ini akan menjadi fondasi untuk materi-materi selanjutnya.

Tugas 1:
Kerjakan kuis singkat yang telah disiapkan untuk menguji pemahaman kalian tentang layer OSI dan fungsi perangkat jaringan.

Bagian 2: DASAR-DASAR SWITCHING

BAB 2
KONSEP COLLISION DAN BROADCAST DOMAIN

2.1. Pengantar: Mengapa Perlu Memahami Domain?

Sebelum kita masuk ke konfigurasi switch, kita perlu memahami "lingkungan kerja" di dalam jaringan ethernet. Dua konsep fundamental yang akan menjelaskan bagaimana data bergerak dan bagaimana perangkat seperti switch dan router meningkatkan kinerja jaringan adalah **Collision Domain** dan **Broadcast Domain**.

Bayangkan sebuah ruangan besar tempat orang-orang ingin berbicara.

- Jika semua orang berbicara pada waktu yang sama, akan terjadi keributan dan tidak ada yang jelas. Ini adalah **collision**.
- Jika seseorang berteriak memanggil nama "Budi" ke seluruh ruangan, semua orang akan mendengarnya, meskipun hanya Budi yang seharusnya merespon. Ini adalah **broadcast**.

Di jaringan komputer, kita ingin menghindari keributan (collision) dan membatasi teriakan (broadcast) agar jaringan tetap efisien. Mari kita pelajari lebih dalam.

2.2. Konsep Half-Duplex dan Full-Duplex

Untuk memahami collision, kita perlu tahu dua mode komunikasi ini:

- **Half-Duplex:** Perangkat dapat mengirim **ATAU** menerima data, tetapi tidak dapat melakukannya secara bersamaan. Analoginya seperti *walkie-talkie*: kita harus menekan tombol untuk bicara, dan melepasnya untuk mendengar. Jika dua orang menekan tombol bersamaan, suara mereka bertabrakan.
- **Full-Duplex:** Perangkat dapat mengirim **DAN** menerima data secara bersamaan. Analoginya seperti *telepon*: kita bisa bicara sambil mendengar lawan bicara. Di dunia jaringan, kabel UTP dengan koneksi point-to-point (langsung antar dua perangkat) memungkinkan mode ini.

Hub hanya bisa beroperasi di mode **half-duplex**, sedangkan **switch** dan **router** umumnya beroperasi di mode **full-duplex** ketika terhubung langsung ke perangkat lain. Ini adalah kunci utama perbedaannya.

2.3. Collision Domain: Definisi dan Cara Kerja

Apa itu Collision Domain?

Collision Domain adalah bagian dari jaringan di mana *frame* (paket data) dari dua atau lebih perangkat dapat bertabrakan (**collision**) jika mereka mengirim data pada waktu yang bersamaan.

Mengapa Collision Terjadi?
Collision hanya terjadi di lingkungan **half-duplex** atau pada media bersama (shared media), seperti jaringan dengan **Hub**.

Ilustrasi dengan Hub:
- Hub adalah perangkat "bodoh". Ketika sebuah data (dalam bentuk sinyal listrik) masuk ke salah satu port-nya, Hub akan mengkopi dan mengirimkan sinyal tersebut ke **SEMUA port lainnya**.
- Bayangkan Hub seperti corong. Jika dua orang berbicara ke dalam corong yang sama pada saat bersamaan, suara mereka akan campur aduk di dalam corong dan keluar tidak karuan.
- Akibatnya, jika Komputer A dan Komputer B yang terhubung ke Hub yang sama mengirim data secara bersamaan, sinyal mereka akan bertabrakan di dalam Hub. Collision terjadi! Kedua komputer harus berhenti, menunggu waktu acak, lalu mencoba mengirim ulang. Ini mengurangi efisiensi jaringan secara drastis.

Karakteristik Collision Domain:
- **Dibatasi oleh Perangkat Layer 2 (Switch/Bridge) dan Layer 3 (Router).** Perangkat-perangkat ini secara cerdas dapat memisahkan collision domain.
- **Hub dan Repeater** justru *memperluas* collision domain karena mereka hanya meneruskan sinyal listrik tanpa kecerdasan.
- Dalam jaringan **full-duplex** (switch ke perangkat), collision domain secara teoritis menjadi *nol* atau tidak ada, karena jalur kirim dan terima terpisah.

Pertanyaan Kunci: Perangkat mana yang membagi collision domain? **Switch dan Router.** Perangkat mana yang memperluas collision domain? **Hub.**

2.4. Broadcast Domain: Definisi dan Cara Kerja

Apa itu Broadcast Domain?

Broadcast Domain adalah bagian dari jaringan di mana sebuah *frame broadcast* yang dikirim oleh satu perangkat akan diterima oleh **SEMUA perangkat** lainnya di domain yang sama.

Apa itu Frame Broadcast?
- Frame broadcast adalah frame yang dikirim dengan alamat MAC tujuan khusus, yaitu **FF:FF:FF:FF:FF:FF**.
- Ketika sebuah perangkat mengirim frame dengan alamat ini, semua perangkat di jaringan lokal (broadcast domain yang sama) wajib menerima dan memproses frame tersebut.

- **Contoh Protokol yang Menggunakan Broadcast:**
  - **ARP (Address Resolution Protocol):** Ketika komputer A ingin ber-komunikasi dengan komputer B (yang ia ketahui IP-nya, tapi belum tahu MAC Address-nya), ia akan mengirimkan ARP broadcast ke seluruh jaringan: "Siapa yang punya IP 192.168.1.10? Tolong beritahu MAC Address-mu!"
  - **DHCP (Dynamic Host Configuration Protocol):** Ketika komputer baru bergabung ke jaringan dan ingin mendapatkan IP secara otomatis, ia akan mengirim DHCP discover broadcast: "Apakah ada DHCP server di sini? Saya butuh alamat IP!"

Ilustrasi dengan Switch:

- Switch pada dasarnya adalah perangkat cerdas yang meneruskan frame hanya ke port tujuan. Namun, ada satu pengecualian: **frame broadcast**.
- Ketika switch menerima frame dengan MAC tujuan `FF:FF:FF:FF:FF:FF`, ia tidak punya pilihan selain meneruskannya ke **SEMUA port-nya** (kecuali port asal frame datang). Mengapa? Karena tujuan broadcast adalah "semua orang".
- Akibatnya, jika satu perangkat mengirim broadcast, semua perangkat di switch yang sama akan menerimanya. Mereka semua berada dalam satu broadcast domain yang sama.

Masalah dengan Broadcast yang Berlebihan:

Jika broadcast domain terlalu besar (misal, satu switch besar dengan 100 komputer), maka setiap kali satu komputer mengirim ARP, 99 komputer lainnya harus berhenti sejenak untuk memproses broadcast tersebut. Ini membuang CPU cycle dan dapat menyebabkan **broadcast storm** jika ada perangkat yang rusak dan terus-menerus mengirim broadcast. Jaringan bisa menjadi lambat atau bahkan tidak berfungsi.

Pertanyaan Kunci: Perangkat mana yang membagi broadcast domain? **Router.** Switch **tidak** membagi broadcast domain; ia hanya meneruskannya ke semua port.

2.5. Peran Switch dan Router dalam Membagi Domain

Sekarang kita lihat perbedaan mendasar kedua perangkat ini:

Fitur	Switch	Router
Collision Domain	**Membagi** collision domain. Setiap port pada switch adalah sebuah collision domain terpisah (terutama dalam mode full-duplex, collision dihilangkan).	**Membagi** collision domain. Setiap interface router adalah collision domain baru.
Broadcast Domain	**Tidak Membagi** broadcast domain. Semua port dalam satu switch (tanpa VLAN) berada dalam satu broadcast domain yang sama.	**Membagi** broadcast domain. Setiap interface router adalah broadcast domain baru.

Analogi Sederhana:

- **Hub** seperti lorong sempit dalam satu ruangan. Semua orang berdesakan (satu collision domain besar) dan jika satu orang berteriak, semua di lorong itu mendengar (satu broadcast domain).
- **Switch** seperti ruangan besar yang dipartisi menjadi banyak bilik pribadi (banyak collision domain). Namun, ruangan ini masih memiliki satu sistem pengeras suara (public address system). Jika seseorang berteriak melalui pengeras suara, semua orang di semua bilik akan mendengar (satu broadcast domain).
- **Router** seperti bangunan yang terdiri dari banyak ruangan terpisah, masing-masing dengan pintu kedap suara. Jika orang di Ruang A berteriak, hanya orang di Ruang A yang mendengar. Jika ingin bicara dengan orang di Ruang B, ia harus keluar ruangan, melalui pintu, lalu masuk ke Ruang B (berarti ia melewati router). Setiap ruangan adalah broadcast domain sendiri.

2.6. Studi Kasus dan Latihan Analisis Topologi

Mari kita praktikkan pemahaman ini dengan menganalisis beberapa topologi sederhana.

Studi Kasus 1: Topologi dengan Hub dan Switch

Bayangkan sebuah topologi:

- Hub-1 terhubung ke Komputer A, B, dan C.
- Hub-2 terhubung ke Komputer D, E, dan F.
- Switch-1 terhubung ke Hub-1, Hub-2, dan Komputer G.
- Router-1 terhubung ke Switch-1 dan ke jaringan internet.

Pertanyaan:

1. Berapa jumlah collision domain?
2. Berapa jumlah broadcast domain?

Jawaban:

1. **Collision Domain:**
    - Hub-1 dengan 3 komputer adalah 1 collision domain (karena hub).
    - Hub-2 dengan 3 komputer adalah 1 collision domain (karena hub).
    - Koneksi dari Switch-1 ke Komputer G adalah koneksi point-to-point full-duplex. Ini adalah 1 collision domain tersendiri (meski secara teknis collision tidak terjadi).
    - Koneksi dari Switch-1 ke Router-1 adalah 1 collision domain.
    - Koneksi dari Switch-1 ke Hub-1 adalah 1 collision domain (dari sisi switch ke hub).
    - Koneksi dari Switch-1 ke Hub-2 adalah 1 collision domain.
    - **Total Collision Domain = 6.** (Setiap segmen yang dapat terjadi collision dihitung sebagai satu domain)

2. **Broadcast Domain:**
    - Semua perangkat yang terhubung ke Switch-1 (Hub-1, Hub-2, Komputer G, dan interface router) berada di sisi yang sama dari router. Ini berarti mereka semua berada dalam satu broadcast domain yang sama, karena switch akan meneruskan broadcast ke semua port-nya.
    - Interface router di sisi internet berada di broadcast domain yang berbeda (yaitu jaringan ISP).
    - **Total Broadcast Domain = 2.** (Jaringan lokal di sisi kiri router, dan jaringan ISP di sisi kanan router)

Studi Kasus 2: Mengapa Router Penting?

Dari contoh di atas, terlihat bahwa jika jaringan lokal kita semakin besar (dengan menambah banyak switch), broadcast domain-nya tetap satu. Semakin banyak perangkat, semakin banyak lalu lintas broadcast. Jika sampai 1000 perangkat dalam satu broadcast domain, jaringan akan kewalahan.

Solusinya adalah dengan menggunakan **Router** (atau Switch Layer 3 yang memiliki kemampuan routing) untuk **membagi broadcast domain** menjadi beberapa bagian yang lebih kecil. Inilah mengapa dalam jaringan skala besar, kita selalu merancang dengan konsep *subnetting* dan *VLAN* (yang akan kita pelajari di bab selanjutnya) untuk membatasi broadcast domain.

Rangkuman Pertemuan 2:

- **Collision Domain** adalah area di mana tabrakan data bisa terjadi. Dipisahkan oleh switch dan router.
- **Broadcast Domain** adalah area di mana frame broadcast akan menjangkau semua perangkat. Dipisahkan hanya oleh router.
- **Hub** memperluas collision domain dan tidak memisahkan broadcast domain.
- **Switch** memisahkan collision domain per port, tetapi tidak memisahkan broadcast domain.
- **Router** memisahkan collision domain per interface **dan** memisahkan broadcast domain.

Tugas 2:

Kerjakan soal latihan yang telah disiapkan. Analisislah topologi yang diberikan dan tentukan jumlah collision domain serta broadcast domain-nya. Jangan lupa sertakan alasan atau penjelasan singkat.

Bagian 2: DASAR-DASAR SWITCHING (Lanjutan)

BAB 3: VIRTUAL LOCAL AREA NETWORK (VLAN) DAN TRUNKING

3.1. Keterbatasan Switch dan Kebutuhan akan VLAN

Di bab sebelumnya, kita belajar bahwa switch memiliki keterbatasan utama: **switch tidak dapat memisahkan broadcast domain**. Semua port dalam satu switch (atau jaringan switch yang saling terhubung) berada dalam satu broadcast domain yang sama.

Apa implikasinya di dunia nyata?

Bayangkan sebuah perusahaan kecil dengan 3 departemen: **Keuangan (Finance)**, **Sumber Daya Manusia (HRD)**, dan **Teknik (Engineering)**. Mereka semua terhubung ke switch yang sama di ruang server.

- **Masalah Keamanan:** Jika departemen Keuangan mengirim data sensitif (misal: gaji karyawan), data ini sebenarnya hanya boleh dilihat oleh komputer di departemen Keuangan saja. Namun karena semua perangkat berada di satu broadcast domain, secara teknis, komputer di departemen HRD atau Engineering bisa "mendengar" lalu lintas data tersebut (misal dengan software penyadap paket). Data rawan bocor!
- **Masalah Kinerja:** Setiap kali komputer di departemen Teknik melakukan *broadcast ARP*, semua komputer di departemen Keuangan dan HRD harus menerima dan memprosesnya. Lalu lintas *broadcast* yang tidak perlu ini membuang bandwidth dan siklus CPU.

Solusi Fisik (Tradisional):

Kita bisa mengatasi masalah ini dengan membeli switch terpisah untuk setiap departemen. Satu switch untuk Keuangan, satu untuk HRD, satu untuk Teknik. Lalu, kita hubungkan masing-masing switch ke router.

- **Keamanan Terpenuhi:** Lalu lintas data di switch Keuangan tidak akan sampai ke switch lain karena switch tidak terhubung langsung (hanya melalui router jika diizinkan).
- **Broadcast Domain Terbatas:** Setiap switch menjadi broadcast domain-nya sendiri.

Masalah Baru:

Solusi fisik ini membutuhkan biaya besar (membeli banyak switch) dan tidak fleksibel. Bagaimana jika seorang karyawan di departemen Keuangan pindah meja ke ruangan yang dekat dengan departemen Teknik? Kita harus menarik kabel baru ke switch Keuangan yang mungkin lokasinya jauh.

Solusi Virtual (Cerdas): VLAN

Di sinilah **VLAN (Virtual Local Area Network)** menjadi jawabannya. VLAN memungkinkan kita melakukan **segmentasi secara logis (virtual)**, tanpa perlu mengubah fisik jaringan.

3.2. Konsep Dasar VLAN: Definisi, Manfaat, dan Cara Kerja

Apa itu VLAN?

VLAN (Virtual Local Area Network) adalah metode untuk membagi satu jaringan fisik (satu switch atau kumpulan switch) menjadi beberapa jaringan logis yang terpisah.

Dengan VLAN, kita dapat mengelompokkan port-port pada switch berdasarkan fungsi, departemen, atau tim, tanpa mempedulikan lokasi fisik mereka.

Analogi VLAN:

Bayangkan sebuah gedung perkantoran besar (ini adalah **switch fisik**). Di dalam gedung ini, kita bisa membuat sekat-sekat ruangan untuk memisahkan departemen Keuangan, HRD, dan Teknik (**ini adalah VLAN**). Orang-orang di ruangan Keuangan tidak bisa melihat atau mendengar apa yang terjadi di ruangan Teknik, meskipun mereka berada di gedung yang sama. Untuk berkomunikasi antar ruangan, mereka harus keluar melalui pintu utama dan bertemu di ruang resepsionis (**ini adalah router**).

Manfaat Utama VLAN:

1. **Peningkatan Keamanan:** Lalu lintas data di VLAN Keuangan diisolasi dari VLAN lainnya. Komputer di VLAN HRD tidak akan bisa "mendengar" lalu lintas broadcast atau unicast dari VLAN Keuangan secara langsung.
2. **Pengurangan Broadcast Domain:** Broadcast hanya akan menjangkau perangkat dalam VLAN yang sama. Ini meningkatkan kinerja jaringan secara keseluruhan.
3. **Fleksibilitas dan Kemudahan Manajemen:** Jika seorang karyawan pindah ruangan, administrator tidak perlu menarik ulang kabel. Cukup dengan mengubah konfigurasi port switch tempat karyawan tersebut terhubung ke VLAN yang sesuai.
4. **Pengelompokan Berdasarkan Fungsi:** VLAN memungkinkan pengelompokan perangkat berdasarkan perannya, misal: semua telepon IP di VLAN tersendiri, semua server di VLAN tersendiri, semua tamu (guest) di VLAN tersendiri.

Cara Kerja VLAN:

- Switch memberikan label (tag) virtual pada setiap frame data yang menunjukkan dari VLAN mana frame itu berasal.
- Setiap port pada switch dapat dikonfigurasi sebagai:

- **Access Port:** Port ini menjadi anggota dari **satu VLAN tertentu**. Biasanya digunakan untuk menghubungkan perangkat akhir seperti komputer, printer, atau server. Komputer tidak tahu bahwa ia berada di sebuah VLAN; ia hanya mengirim dan menerima data biasa.
- **Trunk Port:** Port ini dapat membawa lalu lintas dari **banyak VLAN sekaligus**. Biasanya digunakan untuk menghubungkan switch dengan switch lain, atau switch dengan router.

3.3. Jenis-jenis VLAN (Default, Data, Management, Native)

Dalam implementasinya, kita mengenal beberapa jenis VLAN berdasarkan fungsinya:

1. **Default VLAN (VLAN 1):**
   - Semua port pada switch Cisco, secara *default*, adalah anggota dari VLAN 1.
   - VLAN 1 tidak bisa dihapus.
   - **Rekomendasi Keamanan:** Jangan gunakan VLAN 1 untuk lalu lintas data pengguna. Biarkan VLAN 1 hanya untuk lalu lintas kontrol tertentu, dan nonaktifkan port-port yang tidak digunakan di VLAN 1.
2. **Data VLAN:**
   - Ini adalah VLAN yang dikonfigurasi khusus untuk membawa lalu lintas data pengguna. Misal: VLAN 10 untuk Keuangan, VLAN 20 untuk HRD. Ini adalah VLAN yang paling sering kita buat dan kelola.
3. **Management VLAN:**
   - VLAN khusus untuk mengelola switch secara remote (misal: melalui telnet atau SSH). Biasanya, alamat IP manajemen switch diberikan di VLAN ini.
   - Memisahkan VLAN manajemen dari VLAN data meningkatkan keamanan, karena akses untuk mengelola switch dipisahkan dari akses pengguna biasa.
4. **Native VLAN:**
   - Konsep ini hanya berlaku di **Trunk Port**. Native VLAN adalah VLAN yang tidak diberi tag (untagged) pada trunk.
   - Secara default, Native VLAN adalah VLAN 1.
   - Fungsinya untuk kompatibilitas dengan perangkat lawas yang mungkin tidak memahami tag VLAN.

3.4. Konsep Trunking dan Standar IEEE 802.1Q

Ketika kita menghubungkan dua switch, dan kita ingin lalu lintas dari VLAN 10 dan VLAN 20 melewati kabel yang sama, kita tidak bisa menggunakan access port. Kita butuh **trunk port**.

Apa itu Trunking?

Trunking adalah mekanisme untuk mengirimkan lalu lintas dari beberapa VLAN melalui satu link fisik yang sama.

Standar IEEE 802.1Q:

Ini adalah standar industri untuk trunking antar switch (terutama switch Cisco dan vendor lain). Cara kerjanya:

1. Ketika sebuah frame data dari VLAN 10 akan dikirim melalui trunk port, switch penyedia (source switch) akan menyisipkan sebuah **header 802.1Q** (sepanjang 4 byte) di dalam frame Ethernet asli.
2. Header ini berisi **VLAN ID (VID)**, yaitu angka 12-bit yang mengidentifikasi VLAN asal frame tersebut (VLAN 10, 20, 30, dst).
3. Frame yang sudah diberi tag ini dikirim melalui kabel trunk.
4. Switch penerima membaca header 802.1Q, melihat VLAN ID-nya, lalu menghapus header tersebut dan meneruskan frame ke port yang sesuai di VLAN tujuan.

Ilustrasi Trunking:

- **Tanpa Trunk (Access Port):** Switch 1 dan Switch 2 dihubungkan dengan dua kabel terpisah. Satu kabel khusus untuk VLAN 10, satu kabel khusus untuk VLAN 20. Ini boros port dan kabel.
- **Dengan Trunk (Trunk Port):** Switch 1 dan Switch 2 dihubungkan dengan **satu kabel**. Di dalam kabel ini, frame-frame dari VLAN 10 dan VLAN 20 berjalan bergantian, masing-masing dengan "stiker" VLAN ID-nya.

3.5. Konfigurasi VLAN dan Trunking di Cisco Switch (Dengan Simulasi Packet Tracer)

Sekarang kita akan mempraktikkan konsep di atas menggunakan Cisco Packet Tracer. Ini adalah panduan langkah demi langkah.

Skenario:

Kita akan membangun jaringan kecil dengan:

- 1 buah Switch (misal: Switch 2960).
- 2 buah PC (PC-A dan PC-B) untuk VLAN 10 (Keuangan).
- 2 buah PC (PC-C dan PC-D) untuk VLAN 20 (HRD).

Tujuan:

- PC-A dan PC-B dapat saling berkomunikasi (ping).
- PC-C dan PC-D dapat saling berkomunikasi.
- PC-A **tidak dapat** berkomunikasi dengan PC-C atau PC-D (karena berbeda VLAN).

Langkah-langkah Konfigurasi:

1. Membuat VLAN di Switch:

Masuk ke mode konfigurasi global pada switch.

```
Switch> enable
Switch# configure terminal
Switch(config)# vlan 10
Switch(config-vlan)# name Keuangan
Switch(config-vlan)# exit
Switch(config)# vlan 20
Switch(config-vlan)# name HRD
Switch(config-vlan)# exit
```

2. Menetapkan Port ke Access Port dan VLAN yang Sesuai:

Asumsikan PC-A terhubung ke port FastEthernet 0/1, PC-B ke F0/2, PC-C ke F0/3, PC-D ke F0/4.

```
! Konfigurasi untuk VLAN 10
Switch(config)# interface fastEthernet 0/1
Switch(config-if)# switchport mode access   ! Menjadikan port sebagai access port
Switch(config-if)# switchport access vlan 10 ! Memasukkan port ke VLAN 10
Switch(config-if)# exit

Switch(config)# interface fastEthernet 0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# exit

! Konfigurasi untuk VLAN 20
Switch(config)# interface fastEthernet 0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 20
Switch(config-if)# exit

Switch(config)# interface fastEthernet 0/4
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 20
Switch(config-if)# exit
```

3. Verifikasi Konfigurasi:

```
Switch# show vlan brief
```

Perintah ini akan menampilkan daftar VLAN yang ada di switch dan port-port mana saja yang menjadi anggotanya.

4. Pengujian Konektivitas:

- Coba `ping` dari PC-A ke PC-B (satu VLAN). Seharusnya **berhasil**.
- Coba `ping` dari PC-A ke PC-C (beda VLAN). Seharusnya **gagal**.
- Jika gagal, maka konfigurasi VLAN kita berhasil!

Studi Kasus Lanjutan (Dua Switch):

Untuk mempraktikkan trunking, tambahkan switch kedua. Hubungkan kedua switch dengan kabel cross (atau straight, tergantung port). Konfigurasikan port yang menghubungkan kedua switch sebagai trunk port.

```
! Pada Switch 1, interface yang terhubung ke Switch 2 (misal G0/1)
Switch1(config)# interface gigabitEthernet 0/1
Switch1(config-if)# switchport mode trunk
Switch1(config-if)# switchport trunk allowed vlan 10,20 ! Opsional, untuk mem-
batasi VLAN yang diizinkan

! Pada Switch 2, interface yang terhubung ke Switch 1 (misal G0/1)
Switch2(config)# interface gigabitEthernet 0/1
Switch2(config-if)# switchport mode trunk
```

Setelah trunk aktif, PC di VLAN 10 di Switch 1 harusnya bisa berkomunikasi dengan PC di VLAN 10 di Switch 2.

Rangkuman Pertemuan 3:

- **VLAN** adalah solusi virtual untuk memisahkan broadcast domain di dalam satu switch fisik, meningkatkan keamanan dan kinerja.
- Ada beberapa jenis VLAN: Default (VLAN 1), Data VLAN, Management VLAN, dan Native VLAN.
- **Trunking** dan standar **IEEE 802.1Q** memungkinkan lalu lintas dari banyak VLAN melewati satu link fisik dengan memberikan tag pada setiap frame.
- Konfigurasi VLAN melibatkan pembuatan VLAN dan penetapan port sebagai access port ke VLAN tertentu.
- Port yang menghubungkan switch harus dikonfigurasi sebagai trunk port.

Tugas 3 (dan Tugas 4 - Praktik):

1. **Tugas 3 (Teori):** Kerjakan soal latihan tentang perhitungan dan perencanaan VLAN. Misalnya: "Jika Anda memiliki 3 departemen dengan masing-masing 20 karyawan, bagaimana Anda akan merancang VLAN? Berapa banyak subnet IP yang Anda perlukan?"
2. **Tugas 4 (Praktik - Simulasi):** Buka Cisco Packet Tracer. Buat topologi dengan 2 switch dan 4 PC (2 PC di masing-masing switch). Konfigurasikan VLAN 10 dan 20 di kedua switch. Pastikan PC di VLAN yang sama di switch berbeda dapat saling berkomunikasi, dan PC di VLAN berbeda tidak dapat berkomunikasi. Dokumentasikan konfigurasi dan hasil pengujian Anda.

Bagian 3: DASAR-DASAR ROUTING

BAB 4
PRINSIP DASAR ROUTING

4.1. Dari Switching ke Routing: Kebutuhan untuk Menghubungkan Antar Jaringan

Di bagian sebelumnya, kita telah belajar bagaimana **switch** dan **VLAN** dapat menghubungkan banyak perangkat dalam satu jaringan lokal (LAN) dan memisahkan lalu lintas berdasarkan kelompok.

Namun, ada pertanyaan besar: **Bagaimana cara menghubungkan antar VLAN yang berbeda?** Bagaimana cara komputer di VLAN Keuangan (192.168.10.0) dapat berkomunikasi dengan komputer di VLAN HRD (192.168.20.0)? Atau bagaimana mereka dapat mengakses internet?

Jawabannya adalah: **Routing**.

Jika switch adalah "resepsionis" yang mengatur lalu lintas di dalam satu gedung, maka **router adalah "pos polisi" yang menghubungkan antar gedung**. Router memungkinkan data melewati batas-batas jaringan yang berbeda.

4.2. Konsep Dasar Routing: Forwarding Paket Antar Jaringan

Apa itu Routing?

Routing adalah proses memilih dan menentukan jalur terbaik untuk mengirimkan paket data dari satu jaringan ke jaringan lainnya. Perangkat yang melakukan routing disebut **router**.

Prinsip Kerja Router:

1. **Menerima Paket:** Router menerima paket data yang masuk melalui salah satu interface-nya.
2. **Memeriksa Alamat Tujuan:** Router membaca header paket, khususnya **alamat IP tujuan**.
3. **Mencocokkan dengan Tabel Routing:** Router melihat ke dalam **tabel routing** (routing table) yang dimilikinya. Tabel ini berisi "peta jaringan" yang memberi tahu router, ke mana harus meneruskan paket untuk mencapai suatu jaringan tujuan.
4. **Meneruskan Paket:** Berdasarkan informasi di tabel routing, router meneruskan paket ke interface yang sesuai (menuju *next-hop* atau tujuan langsung).

5. **Menjatuhkan Paket:** Jika tidak ada entri yang cocok di tabel routing, router akan menjatuhkan (drop) paket tersebut dan biasanya mengirim pesan "Destination Network Unreachable" kembali ke pengirim.

Ilustrasi Sederhana:
Bayangkan Anda ingin mengirim surat dari Padang ke Jakarta.

1. Anda menulis alamat tujuan di amplop (IP tujuan).
2. Anda membawa surat ke kantor pos terdekat (**router**).
3. Petugas pos melihat tabel tujuan (**tabel routing**). Tabel itu mengatakan: "Untuk mencapai Jakarta, kirim surat ke kantor pos di Palembang terlebih dahulu."
4. Surat Anda dikirim ke Palembang (*next-hop*), dan proses serupa berlanjut hingga surat sampai di Jakarta.

4.3. Komponen Tabel Routing (Jaringan Tujuan, Next-Hop, Metric, Interface)

Tabel routing adalah "otak" dari router. Mari kita bedah komponen-komponen utamanya dengan melihat contoh output perintah `show ip route` pada router Cisco.

```
Router# show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, ...
     10.0.0.0/24 is subnetted, 2 subnets
C       10.0.1.0 is directly connected, FastEthernet0/0
C       10.0.2.0 is directly connected, FastEthernet0/1
S    192.168.1.0/24 [1/0] via 10.0.1.2
O    172.16.0.0/16 [110/20] via 10.0.2.2, 00:12:34, FastEthernet0/1
```

Dari contoh di atas, kita bisa identifikasi komponen-komponennya:

1. **Kode Sumber (Source Code):** Huruf di paling kiri (C, S, O) menunjukkan **bagaimana router mempelajari rute tersebut**.
   - **C (Connected):** Jaringan yang terhubung langsung ke interface router. Ini adalah rute yang otomatis muncul ketika kita memberikan alamat IP pada interface dan mengaktifkannya (no shutdown).
   - **S (Static):** Rute yang dimasukkan secara manual oleh administrator jaringan.
   - **R (RIP) atau O (OSPF):** Rute yang dipelajari secara otomatis dari router lain melalui protokol routing dinamis.
2. **Jaringan Tujuan (Destination Network):** Alamat jaringan yang ingin dituju. Contoh: `10.0.1.0/24`, `192.168.1.0/24`, `172.16.0.0/16`.
3. **Administrative Distance (AD) dan Metric:**
   - Angka dalam kurung siku, misal `[1/0]` atau `[110/20]`.
   - Angka pertama adalah **Administrative Distance (AD)**. Ini adalah "tingkat kepercayaan" terhadap sumber rute. Semakin kecil angkanya, semakin dipercaya. Connected route punya AD 0, Static punya AD 1, OSPF punya AD 110, RIP punya AD 120.

- Angka kedua adalah **Metric**. Ini adalah "nilai/harga" untuk mencapai jaringan tujuan. Metric bisa berupa hop count (RIP), cost (OSPF), atau bandwidth. Router akan memilih rute dengan metric terkecil menuju jaringan yang sama.

4. **Next-Hop dan Interface Keluar:**
   - **via ...:** Menunjukkan alamat IP dari router berikutnya (tetangga) yang harus dituju untuk meneruskan paket.
   - **directly connected ...** atau **FastEthernet0/1** di akhir: Menunjukkan interface mana pada router ini yang harus digunakan untuk mengirim paket.

4.4. Jenis-jenis Routing: Statis vs Dinamis

Secara umum, cara router mendapatkan informasi routing dapat dibagi menjadi dua kategori utama:

Karakteristik	Routing Statis	Routing Dinamis
Cara Konfigurasi	Administrator memasukkan rute secara manual.	Router saling bertukar informasi secara otomatis menggunakan protokol routing.
Skala Jaringan	Cocok untuk jaringan kecil (misal: jaringan SOHO, jaringan dengan 2-3 router).	Cocok untuk jaringan menengah hingga besar (ISP, jaringan kampus, perusahaan besar).
Adaptasi Terhadap Perubahan	Tidak adaptif. Jika ada link yang mati, administrator harus mengubah rute secara manual.	Adaptif. Router akan secara otomatis menghitung ulang jalur jika ada perubahan topologi.
Keamanan	Lebih aman karena tidak ada pertukaran informasi routing.	Perlu konfigurasi keamanan tambahan (misal: autentikasi) untuk mencegah serangan.
Beban Kerja Administrator	Tinggi (terutama jika jaringan besar dan sering berubah).	Rendah (setelah konfigurasi awal).
Beban Kerja Router (CPU)	Rendah.	Tinggi (karena harus menjalankan algoritma routing).

Kesimpulan: Tidak ada yang paling baik. Pilihan tergantung kebutuhan. Di dunia nyata, kombinasi keduanya sering digunakan. Routing statis untuk bagian tepi jaringan (stub network), routing dinamis untuk bagian inti (core network).

4.5. Metrik Routing (Hop Count, Bandwidth, Delay)

Metric adalah nilai yang digunakan oleh protokol routing untuk menentukan jalur terbaik menuju suatu jaringan tujuan. Berikut beberapa metrik yang umum:

1. **Hop Count:**
    - Digunakan oleh **RIP (Routing Information Protocol)**.
    - Sederhana: menghitung berapa banyak router yang harus dilewati untuk mencapai jaringan tujuan.
    - **Kelemahan:** Tidak mempertimbangkan kecepatan link. Jalur dengan 2 hop melalui kabel serat optik 1 Gbps dianggap "lebih buruk" daripada jalur dengan 1 hop melalui kabel tembaga 10 Mbps. Ini tidak akurat.
2. **Cost (OSPF):**
    - Digunakan oleh **OSPF (Open Shortest Path First)**.
    - Cost dihitung berdasarkan **bandwidth** (kecepatan) link. Rumus umum: `Cost = Reference Bandwidth / Interface Bandwidth`.
    - Semakin tinggi bandwidth, semakin rendah cost-nya, dan semakin baik jalur tersebut.
    - **Contoh:** Link FastEthernet (100 Mbps) punya cost lebih kecil daripada link Ethernet (10 Mbps), sehingga lebih dipilih.
3. **Delay:**
    - Waktu yang dibutuhkan untuk mengirimkan paket dari sumber ke tujuan.
    - Bisa dipengaruhi oleh jarak, antrian, dan kecepatan link.
4. **Bandwidth:**
    - Kapasitas maksimum dari sebuah link.
5. **Reliability:**
    - Tingkat keandalan link (berapa sering link mengalami error).
6. **Load:**
    - Seberapa sibuk sebuah link (traffic saat ini).

Protokol routing modern seperti OSPF dan EIGRP menggunakan kombinasi metrik yang lebih kompleks (seperti bandwidth, delay, load, reliability) untuk menentukan jalur terbaik yang lebih akurat.

Rangkuman Pertemuan 4:

- Routing adalah proses meneruskan paket antar jaringan yang berbeda.
- Tabel routing adalah kunci utama, berisi jaringan tujuan, next-hop, metric, dan interface keluar.
- Ada dua jenis routing: **statis** (manual, cocok untuk jaringan kecil) dan **dinamis** (otomatis, cocok untuk jaringan besar).
- **Metric** adalah nilai yang digunakan untuk memilih jalur terbaik. Contoh: hop count (RIP) dan cost/bandwidth (OSPF).

Tugas 5:

Kerjakan soal latihan yang telah disiapkan. Buatlah tabel routing sederhana berdasarkan topologi yang diberikan. Tentukan jalur terbaik dan metrik yang digunakan (gunakan skenario dengan RIP dan OSPF sederhana).

BAB 5: ROUTING STATIS

5.1. Prinsip dan Karakteristik Routing Statis

Setelah memahami konsep dasar routing, kita akan mempraktikkan jenis routing yang paling sederhana: **Routing Statis**.

Apa itu Routing Statis?

Routing statis adalah jenis routing di mana administrator jaringan secara **manual** menambahkan entri ke dalam tabel routing router.

Kapan Routing Statis Digunakan?

- **Jaringan Kecil:** Pada jaringan dengan hanya 2-3 router, routing statis lebih sederhana dan mudah dikonfigurasi.
- **Stub Network:** Jaringan yang hanya memiliki satu jalur keluar menuju dunia luar (misal: jaringan kantor cabang yang hanya terhubung ke kantor pusat).
- **Keamanan:** Untuk tujuan keamanan, rute statis dapat digunakan untuk menentukan jalur yang tetap dan tidak berubah.
- **Backup:** Routing statis dapat digunakan sebagai jalur cadangan jika routing dinamis mengalami kegagalan (floating static route).

Keuntungan Routing Statis:

- Mudah dikonfigurasi untuk jaringan kecil.
- Tidak ada overhead (beban) pada CPU router.
- Tidak ada bandwidth yang terbuang untuk pertukaran informasi routing.
- Lebih aman (karena tidak ada iklan routing).

Kekurangan Routing Statis:

- Konfigurasi manual untuk setiap rute, rawan kesalahan ketik.
- Tidak adaptif terhadap perubahan topologi. Jika link putus, rute statis tetap ada di tabel dan paket akan dikirim ke "jalan buntu".
- Tidak skalabel untuk jaringan besar (akan sangat merepotkan mengkonfigurasi ratusan rute manual).

5.2. Konfigurasi Route Statis (dengan Next-Hop dan Exit-Interface)

Di router Cisco, kita menggunakan perintah `ip route` untuk mengkonfigurasi routing statis. Ada dua cara utama untuk menentukan tujuan:

Sintaks Dasar:

```
ip route <network-tujuan> <subnet-mask> { <next-hop-address> | <exit-interface> }
```

Cara 1: Menggunakan Next-Hop Address

Ini adalah cara yang paling umum. Kita menentukan alamat IP dari router tetangga (next-hop) yang harus dituju.

- **Contoh:** `ip route 192.168.2.0 255.255.255.0 10.0.0.2`
- **Artinya:** Untuk mencapai jaringan `192.168.2.0/24`, kirim paket ke router dengan IP `10.0.0.2`.

Cara 2: Menggunakan Exit-Interface

Kita menentukan interface mana pada router kita yang akan digunakan untuk mengirim paket. Cara ini sering digunakan pada link point-to-point (seperti serial link).

- **Contoh:** `ip route 192.168.2.0 255.255.255.0 serial 0/0/0`
- **Artinya:** Untuk mencapai jaringan `192.168.2.0/24`, kirim paket keluar melalui interface `serial 0/0/0`.

Perbedaan Praktis:

- Jika menggunakan **next-hop**, router akan melakukan rekursif routing (mencari cara untuk mencapai next-hop tersebut). Ini sedikit lebih lambat.
- Jika menggunakan **exit-interface**, router langsung tahu harus keluar dari mana. Ini lebih cepat dan efisien. Biasanya digunakan pada link serial atau point-to-point.

5.3. Konfigurasi Default Route (Rute Default)

Apa itu Default Route?

Default route adalah "rute jalan pintas" untuk semua jaringan yang tidak dikenal. Ini seperti "gerbang terakhir". Jika router menerima paket dengan alamat tujuan yang tidak ada di tabel routing, ia akan mengirim paket tersebut ke default route.

Kapan Digunakan?

Sangat berguna untuk memberikan akses internet ke jaringan lokal. Router tidak perlu tahu semua jaringan di internet. Cukup kirim semua lalu lintas yang tidak dikenal ke router ISP.

Notasi Default Route:

Default route direpresentasikan sebagai `0.0.0.0/0` (network 0.0.0.0 dengan mask 0.0.0.0). Ini berarti "semua jaringan".

Konfigurasi di Cisco:

```
ip route 0.0.0.0 0.0.0.0 <next-hop-ISP>
```

- **Contoh:** `ip route 0.0.0.0 0.0.0.0 203.0.113.1`
- **Artinya:** Untuk semua jaringan yang tidak dikenal (termasuk internet), kirim paket ke router ISP dengan IP `203.0.113.1`.

5.4. Verifikasi Konektivitas dan Tabel Routing

Setelah konfigurasi selesai, kita harus melakukan verifikasi.

Perintah Verifikasi Utama:

1. `show ip route`
   - Menampilkan seluruh tabel routing. Cari entri dengan kode **S** (static) atau **S*** (default route). Pastikan rute yang Anda konfigurasi muncul di sini.
   ```
   Router# show ip route
   ...
   S    192.168.2.0/24 [1/0] via 10.0.0.2
   S*   0.0.0.0/0 [1/0] via 203.0.113.1
   ```

2. `ping`
   - Alat paling dasar untuk menguji konektivitas. Kirim paket ICMP dari satu ujung jaringan ke ujung lainnya.
   - Contoh: `ping 192.168.2.1` dari router atau PC di jaringan 192.168.1.0.

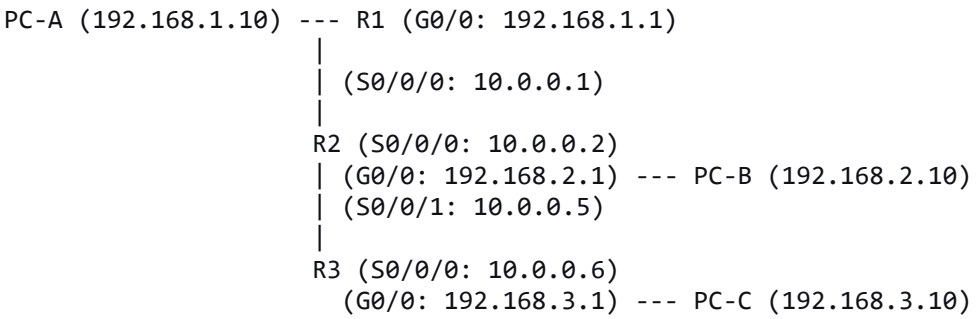
3. `traceroute` **(atau** `tracert` **di Windows)**
   - Melacak jalur yang dilalui paket dari sumber ke tujuan. Ini sangat berguna untuk melihat apakah paket berjalan sesuai jalur yang kita inginkan.
   - Contoh: `traceroute 8.8.8.8` untuk melihat jalur menuju Google DNS.

5.5. Studi Kasus dan Praktik Konfigurasi di Packet Tracer

Skenario:
Kita akan membangun jaringan dengan 3 router (R1, R2, R3) dan 3 jaringan lokal.

- R1 terhubung ke jaringan A: `192.168.1.0/24`
- R2 terhubung ke jaringan B: `192.168.2.0/24`
- R3 terhubung ke jaringan C: `192.168.3.0/24`
- Koneksi antar router menggunakan jaringan `10.0.0.0/30` (subnet mask 255.255.255.252).

Topologi:



Tujuan:
Semua jaringan harus saling terhubung (full connectivity). PC-A harus bisa ping ke PC-C (192.168.3.10).

Langkah Konfigurasi Routing Statis di R1:
R1 tahu tentang jaringan yang terhubung langsung (192.168.1.0/24 dan 10.0.0.0/30 ke R2). R1 perlu tahu cara mencapai:

1. Jaringan B (192.168.2.0/24) di belakang R2.
2. Jaringan C (192.168.3.0/24) di belakang R3.
3. Untuk mencapai R3, paket harus melalui R2 terlebih dahulu.

```
R1> enable
R1# configure terminal
! Route menuju jaringan B (melalui R2)
R1(config)# ip route 192.168.2.0 255.255.255.0 10.0.0.2
! Route menuju jaringan C (melalui R2 juga)
R1(config)# ip route 192.168.3.0 255.255.255.0 10.0.0.2
! (Opsional) Default route jika ada internet
! R1(config)# ip route 0.0.0.0 0.0.0.0 10.0.0.2
R1(config)# end
R1# show ip route
```

Langkah Konfigurasi Routing Statis di R2:
R2 tahu tentang jaringan yang terhubung langsung (192.168.2.0/24, 10.0.0.0/30 ke R1, dan 10.0.0.4/30 ke R3). R2 perlu tahu cara mencapai:

1. Jaringan A (192.168.1.0/24) di belakang R1.
2. Jaringan C (192.168.3.0/24) di belakang R3.

```
R2> enable
R2# configure terminal
! Route menuju jaringan A
R2(config)# ip route 192.168.1.0 255.255.255.0 10.0.0.1
! Route menuju jaringan C
R2(config)# ip route 192.168.3.0 255.255.255.0 10.0.0.6
R2(config)# end
R2# show ip route
```

Langkah Konfigurasi Routing Statis di R3:
R3 tahu tentang jaringan yang terhubung langsung (192.168.3.0/24 dan 10.0.0.4/30 ke R2). R3 perlu tahu cara mencapai:

1. Jaringan A (192.168.1.0/24) di belakang R1 (via R2).
2. Jaringan B (192.168.2.0/24) di belakang R2.

```
R3> enable
R3# configure terminal
! Route menuju jaringan A (melalui R2)
R3(config)# ip route 192.168.1.0 255.255.255.0 10.0.0.5
! Route menuju jaringan B
R3(config)# ip route 192.168.2.0 255.255.255.0 10.0.0.5
R3(config)# end
R3# show ip route
```

Pengujian:

- Dari PC-A, lakukan `ping 192.168.3.10`. Jika berhasil, konfigurasi routing statis kita sudah benar.
- Coba `traceroute` dari R1 ke alamat IP PC-C untuk melihat jalur yang dilalui: R1 -> R2 -> R3.

Rangkuman Pertemuan 5:

- Routing statis dikonfigurasi manual dengan perintah `ip route`.
- Kita bisa menentukan tujuan dengan **next-hop address** atau **exit-interface**.
- **Default route** (`0.0.0.0/0`) adalah rute khusus untuk semua jaringan yang tidak dikenal.
- Verifikasi dengan `show ip route`, `ping`, dan `traceroute` sangat penting untuk memastikan konfigurasi berhasil.

Tugas 6 (Praktik - Simulasi):

Buka Cisco Packet Tracer. Buat topologi seperti studi kasus di atas (3 router, 3 PC). Konfigurasikan routing statis sehingga semua PC dapat saling berkomunikasi. Dokumentasikan langkah-langkah Anda, termasuk:

- Topologi jaringan.
- Konfigurasi IP di setiap interface.
- Perintah routing statis yang digunakan di setiap router.
- Hasil pengujian `ping` dan `traceroute`.

Bagian 3: DASAR-DASAR ROUTING (Lanjutan)

BAB 6
ROUTING DINAMIS (RIP DAN OSPF)

6.1. Keterbatasan Routing Statis dan Kebutuhan akan Routing Dinamis

Pada bab sebelumnya, kita telah mempelajari routing statis. Kita melihat bahwa routing statis sederhana dan mudah dikonfigurasi untuk jaringan kecil. Namun, bayangkan skenario berikut:

Sebuah perusahaan memiliki 10 kantor cabang yang tersebar di seluruh Indonesia. Setiap kantor cabang memiliki 2 router yang saling terhubung. Total ada 20 router. Jaringan ini terus berkembang, dan kadang-kadang ada link yang putus karena kabel putus atau gangguan lainnya.

Jika menggunakan routing statis:

- Administrator harus mengkonfigurasi rute manual di setiap router (bisa puluhan bahkan ratusan rute).
- Jika ada link yang putus di Surabaya, administrator di kantor pusat di Jakarta harus segera mengubah konfigurasi routing di router yang terkena dampak, dan mungkin juga di router lain. Ini sangat lambat dan rawan kesalahan.
- Jaringan akan mati (down) sampai administrator selesai memperbaiki konfigurasi.

Solusi: Routing Dinamis

Di sinilah **routing dinamis** menjadi penyelamat. Dengan routing dinamis, router secara otomatis:

1. **Menemukan** router tetangga.
2. **Bertukar informasi** tentang jaringan yang mereka ketahui.
3. **Menghitung** jalur terbaik secara otomatis.
4. **Beradaptasi** jika ada perubahan topologi (link putus atau link baru).

Routing dinamis memungkinkan jaringan untuk "sembuh sendiri" (self-healing) tanpa campur tangan manual administrator.

6.2. Klasifikasi Protokol Routing Dinamis

Protokol routing dinamis dapat diklasifikasikan berdasarkan cara kerjanya:

A. Berdasarkan Algoritma (Cara Kerja):

1. **Distance Vector:**
   - **Prinsip:** Router hanya tahu "arah" (vector) dan "jarak" (distance) ke suatu jaringan. Mereka secara periodik mengirimkan seluruh tabel routing mereka ke tetangga langsung. Analoginya seperti "petunjuk jalan dari teman": "Jaringan X ada di sebelah timur, berjarak 3 hop dari sini."
   - **Cara Kerja:** "Rumor routing" atau "routing by gossip". Router percaya pada informasi yang diberikan tetangga.
   - **Kelebihan:** Sederhana, mudah dikonfigurasi.
   - **Kekurangan:** Konvergensi lambat (butuh waktu bagi semua router untuk mendapatkan informasi terbaru setelah perubahan), rentan terhadap routing loop.
   - **Contoh: RIP (Routing Information Protocol)** , IGRP.
2. **Link State:**
   - **Prinsip:** Setiap router membuat "peta" lengkap topologi jaringan. Mereka mengirimkan informasi tentang status link mereka (connected, bandwidth, dll) ke **semua router** di area yang sama (flooding). Setiap router kemudian menjalankan algoritma (SPF - Shortest Path First) untuk menghitung jalur terbaik ke setiap jaringan. Analoginya seperti "peta Google Maps": Setiap orang punya peta yang sama dan bisa menghitung rute terpendek sendiri.
   - **Cara Kerja:** Setiap router memiliki database topologi yang identik.
   - **Kelebihan:** Konvergensi cepat, lebih skalabel untuk jaringan besar, tidak mudah terkena routing loop.
   - **Kekurangan:** Lebih kompleks, membutuhkan lebih banyak sumber daya (CPU dan memory) di router.
   - **Contoh: OSPF (Open Shortest Path First)** , IS-IS.

B. Berdasarkan Area (Skala Jaringan):

1. **Classful (Legacy):** Tidak mengirim informasi subnet mask. Hanya mengenal kelas IP (A, B, C). Sudah usang. Contoh: RIPv1.
2. **Classless (Modern):** Mengirim informasi subnet mask bersama dengan alamat jaringan. Mendukung VLSM (Variable Length Subnet Mask) dan CIDR (Classless Inter-Domain Routing). Contoh: RIPv2, OSPF, EIGRP.

6.3. Routing Information Protocol (RIP)

Apa itu RIP?

RIP adalah salah satu protokol routing tertua dan paling sederhana, termasuk dalam kategori **Distance Vector**.

Karakteristik Utama RIP:

- **Metrik: Hop Count**. Jumlah router yang harus dilewati. Maksimal hop count adalah **15**. Hop count 16 dianggap "tidak terjangkau" (unreachable). Ini membatasi ukuran jaringan yang bisa menggunakan RIP.
- **Versi:**
  - **RIPv1:** Classful (tidak mengirim subnet mask). Tidak mendukung VLSM. Broadcast update.
  - **RIPv2:** Classless (mengirim subnet mask). Mendukung VLSM. Multicast update (ke alamat 224.0.0.9). Mendukung autentikasi sederhana.
- **Update:** Secara default, RIP mengirimkan seluruh tabel routing ke tetangga setiap **30 detik**. Ini menyebabkan lalu lintas broadcast/multicast yang cukup besar di jaringan.
- **Timer RIP:**
  - **Update Timer:** 30 detik (pengiriman update).
  - **Invalid Timer:** 180 detik (jika tidak ada update tentang suatu rute dalam 180 detik, rute dianggap tidak valid).
  - **Hold-down Timer:** 180 detik (periode di mana router tidak menerima informasi baru tentang rute yang sedang down, untuk mencegah routing loop).
  - **Flush Timer:** 240 detik (rute dihapus dari tabel routing).

Kelebihan RIP:

- Sederhana dan mudah dikonfigurasi.
- Mudah dipahami untuk pembelajaran.

Kekurangan RIP:

- **Hop Count Limitation:** Tidak bisa digunakan di jaringan besar (max 15 hop).
- **Konvergensi Lambat:** Butuh waktu beberapa menit untuk stabil setelah perubahan.
- **Metrik Kurang Akurat:** Hanya hop count, tidak mempertimbangkan bandwidth atau delay. Jalur dengan 2 hop melalui kabel 56kbps dial-up akan dipilih daripada jalur dengan 3 hop melalui serat optik 1 Gbps, hanya karena hop count-nya lebih kecil.
- **Boros Bandwidth:** Update setiap 30 detik.

6.4. Open Shortest Path First (OSPF)

Apa itu OSPF?

OSPF adalah protokol routing **Link State** yang modern, sangat populer digunakan di jaringan perusahaan dan ISP. OSPF dirancang untuk mengatasi keterbatasan RIP.

Karakteristik Utama OSPF:

- **Metrik: Cost**. Cost dihitung berdasarkan bandwidth link. Rumus default Cisco: `Cost = 10^8 / Bandwidth (bps)`. Jadi, link FastEthernet (100 Mbps) punya cost = 1, link Ethernet (10 Mbps) punya cost = 10.
- **Konsep Area:** OSPF dapat membagi jaringan besar menjadi area-area yang lebih kecil (hierarkis).
    - **Area 0 (Backbone Area):** Area inti. Semua area lain harus terhubung ke area 0.
    - **Manfaat Area:** Mengurangi ukuran tabel routing, mempercepat konvergensi, mengisolasi masalah dalam satu area.
- **Database Topologi:** Setiap router OSPF membangun **Link State Database (LSDB)** yang berisi peta lengkap jaringan di area-nya.
- **Algoritma SPF (Dijkstra):** Setiap router menjalankan algoritma SPF pada LSDB untuk menghitung jalur terpendek ke setiap jaringan tujuan.
- **Update:** OSPF hanya mengirimkan update ketika ada perubahan (triggered update), bukan secara periodik. Update dikirim secara multicast (ke alamat 224.0.0.5 untuk semua router OSPF, 224.0.0.6 untuk DR/BDR). Ini sangat efisien.
- **Konvergensi Cepat:** Perubahan topologi dapat dideteksi dan dihitung ulang dalam hitungan detik.
- **Autentikasi:** Mendukung autentikasi untuk keamanan pertukaran informasi routing.

Kelebihan OSPF:

- **Skalabel:** Cocok untuk jaringan besar dan sangat besar.
- **Konvergensi Cepat:** Jaringan cepat pulih dari kegagalan.
- **Metrik Akurat:** Menggunakan bandwidth, sehingga memilih jalur yang benar-benar terbaik.
- **Efisien:** Tidak ada update periodik, hanya triggered update.
- **Mendukung VLSM dan CIDR.**

Kekurangan OSPF:

- **Lebih Kompleks:** Konfigurasi dan troubleshooting lebih sulit daripada RIP.
- **Membutuhkan Sumber Daya Lebih:** Router perlu CPU dan memory yang lebih besar untuk menjalankan algoritma SPF dan menyimpan LSDB.

6.5. Perbandingan RIP dan OSPF

Fitur	RIP	OSPF
Kategori	Distance Vector	Link State
Metrik	Hop Count (max 15)	Cost (berdasarkan bandwidth)
Konvergensi	Lambat (menit)	Cepat (detik)
Update	Periodik (30 detik)	Triggered (saat ada perubahan)
Skalabilitas	Kecil (max 15 hop)	Besar hingga sangat besar (dengan area)
Kompleksitas	Rendah	Tinggi
Sumber Daya Router	Rendah	Tinggi
VLSM/CIDR	RIPv1: Tidak, RIPv2: Ya	Ya
Penggunaan	Jaringan kecil, pembelajaran	Jaringan enterprise, ISP

6.6. Konfigurasi Routing Dinamis di Cisco Packet Tracer

Kita akan mempraktikkan konfigurasi RIP dan OSPF menggunakan topologi yang sama seperti di bab routing statis (3 router R1, R2, R3).

Topologi (sama seperti sebelumnya):

```
PC-A (192.168.1.10/24) --- R1 (G0/0: 192.168.1.1/24)
                           | (S0/0/0: 10.0.0.1/30)
                           |
                           R2 (S0/0/0: 10.0.0.2/30)
                           | (G0/0: 192.168.2.1/24) --- PC-B (192.168.2.10/24)
                           | (S0/0/1: 10.0.0.5/30)
                           |
                           R3 (S0/0/0: 10.0.0.6/30)
                             (G0/0: 192.168.3.1/24) --- PC-C (192.168.3.10/24)
```

A. Konfigurasi RIPv2

Langkah 1: Konfigurasi IP di Semua Interface (sama seperti routing statis)

Pastikan semua interface router sudah memiliki IP yang benar dan dalam status `up` (`no shutdown`).

Langkah 2: Aktifkan RIP dan Tentukan Jaringan yang Dipublikasikan

Di setiap router, kita masuk ke mode konfigurasi router RIP dan mendeklarasikan jaringan yang **terhubung langsung** ke router tersebut (bukan jaringan tujuan).

Di R1:

```
R1> enable
R1# configure terminal
R1(config)# router rip
R1(config-router)# version 2           ! Menggunakan RIPv2 (classless)
R1(config-router)# no auto-summary     ! Mematikan auto-summary agar subnet mask d
ipertahankan
R1(config-router)# network 192.168.1.0 ! Jaringan yang terhubung ke R1 (LAN)
R1(config-router)# network 10.0.0.0    ! Jaringan serial yang terhubung ke R2
R1(config-router)# end
R1# show ip route
```

Perhatikan bahwa kita tidak perlu mendeklarasikan `192.168.2.0` atau `192.168.3.0` di R1. RIP akan belajar jaringan tersebut secara otomatis dari R2 dan R3.

Di R2:

```
R2> enable
R2# configure terminal
R2(config)# router rip
R2(config-router)# version 2
R2(config-router)# no auto-summary
R2(config-router)# network 192.168.2.0
R2(config-router)# network 10.0.0.0    ! Mencakup subnet 10.0.0.0/30 dan 10.0.0.4/
30
R2(config-router)# end
R2# show ip route
```

Di R3:

```
R3> enable
R3# configure terminal
R3(config)# router rip
R3(config-router)# version 2
R3(config-router)# no auto-summary
R3(config-router)# network 192.168.3.0
R3(config-router)# network 10.0.0.0
R3(config-router)# end
R3# show ip route
```

Langkah 3: Verifikasi

- Gunakan `show ip route` di setiap router. Anda akan melihat rute dengan kode **R** (RIP) yang menunjuk ke jaringan yang tidak terhubung langsung.
- Gunakan `show ip protocols` untuk melihat detail konfigurasi routing yang aktif.
- Lakukan `ping` dari PC-A ke PC-C (192.168.3.10) untuk memastikan konektivitas.

B. Konfigurasi OSPF (Single Area)

Sebelum mengkonfigurasi OSPF, **hapus konfigurasi RIP** terlebih dahulu di semua router dengan perintah `no router rip`.

Langkah 1: Konfigurasi IP (sama, pastikan sudah benar)
Langkah 2: Aktifkan OSPF dan Tentukan Jaringan serta Area

Di setiap router, kita masuk ke mode konfigurasi router OSPF (dengan nomor process ID, misal 1) dan mendeklarasikan jaringan yang terhubung langsung beserta **wildcard mask** dan **area** (kita gunakan area 0 untuk semua).

Apa itu Wildcard Mask?

Wildcard mask adalah kebalikan dari subnet mask.
Cara menghitungnya: `Wildcard = 255.255.255.255 - Subnet Mask`.

- Untuk subnet mask `255.255.255.0` (/24), wildcard-nya adalah `0.0.0.255`.
- Untuk subnet mask `255.255.255.252` (/30), wildcard-nya adalah `0.0.0.3`.

Di R1:

```
R1> enable
R1# configure terminal
R1(config)# router ospf 1              ! Process ID 1 (hanya lokal, bisa 1-65535)
R1(config-router)# network 192.168.1.0 0.0.0.255 area 0
R1(config-router)# network 10.0.0.0 0.0.0.3 area 0   ! Wildcard untuk /30
R1(config-router)# end
R1# show ip route
```

Di R2:

```
R2> enable
R2# configure terminal
R2(config)# router ospf 1
R2(config-router)# network 192.168.2.0 0.0.0.255 area 0
R2(config-router)# network 10.0.0.0 0.0.0.3 area 0   ! Jaringan ke R1
R2(config-router)# network 10.0.0.4 0.0.0.3 area 0   ! Jaringan ke R3
R2(config-router)# end
R2# show ip route
```

Di R3:

```
R3> enable
R3# configure terminal
R3(config)# router ospf 1
R3(config-router)# network 192.168.3.0 0.0.0.255 area 0
R3(config-router)# network 10.0.0.4 0.0.0.3 area 0   ! Jaringan ke R2
R3(config-router)# end
R3# show ip route
```

Langkah 3: Verifikasi OSPF

- Gunakan `show ip route`. Anda akan melihat rute dengan kode **O** (OSPF) menuju jaringan lain.
- Gunakan `show ip ospf neighbor` untuk melihat router tetangga yang telah ditemukan oleh OSPF. Ini adalah perintah penting untuk troubleshooting OSPF.
- Gunakan `show ip ospf interface` untuk melihat detail OSPF pada setiap interface.
- Lakukan `ping` dari PC-A ke PC-C untuk memastikan konektivitas.

6.7. Troubleshooting Routing Dinamis

Masalah Umum pada RIP:

1. **Tidak ada rute RIP di tabel routing:** Periksa apakah `network` statement sudah benar dan mencakup semua interface yang relevan. Pastikan tidak ada ACL yang memblokir port RIP (UDP 520).
2. **Hop count melebihi 15:** RIP tidak akan menggunakan rute dengan hop count 16.
3. **Versi mismatch:** Pastikan semua router menggunakan `version 2` atau kompatibel.

Masalah Umum pada OSPF:

1. **Tidak ada tetangga (neighbor):**
   - Periksa koneksi fisik dan IP.
   - Pastikan interface dalam status `up/up`.
   - Pastikan kedua router berada di **area yang sama** pada subnet tersebut.
   - Periksa **wildcard mask**. Jika salah, jaringan mungkin tidak diikutsertakan dalam proses OSPF.
   - Pastikan tidak ada firewall atau ACL yang memblokir multicast OSPF (224.0.0.5, 224.0.0.6).
2. **Tabel routing tidak lengkap:**
   - Periksa LSDB dengan `show ip ospf database`. Apakah semua link diketahui?
   - Pastikan semua jaringan dideklarasikan dengan benar di semua router.

Rangkuman Pertemuan 6:

- Routing dinamis memungkinkan router belajar jaringan secara otomatis dan beradaptasi dengan perubahan.
- **RIP** adalah distance vector sederhana dengan metrik hop count (max 15). Cocok untuk pembelajaran dan jaringan kecil.
- **OSPF** adalah link state modern dengan metrik cost (bandwidth), konvergensi cepat, dan skalabel untuk jaringan besar.
- Konfigurasi RIP menggunakan `router rip` dan `network`.
- Konfigurasi OSPF menggunakan `router ospf [process-id]` dan `network [network] [wildcard] area [area-id]`.
- Verifikasi dengan `show ip route`, `show ip protocols`, `show ip ospf neighbor`, dan `ping`.

Tugas 7 (Praktik - Simulasi):

1. Buka Cisco Packet Tracer. Gunakan topologi yang sama (3 router, 3 PC).
2. **Pertama,** hapus semua konfigurasi routing statis (gunakan `no ip route ...`).
3. **Kedua,** konfigurasikan RIPv2 di semua router. Pastikan semua PC dapat saling ping. Dokumentasikan hasil `show ip route` di setiap router.

4. **Ketiga,** hapus konfigurasi RIP, lalu konfigurasikan OSPF single area (area 0) di semua router. Pastikan semua PC dapat saling ping. Dokumentasikan hasil `show ip route` dan `show ip ospf neighbor` di setiap router.
5. Buat laporan singkat yang membandingkan tabel routing RIP dan OSPF. Apakah ada perbedaan dalam pemilihan jalur? Mengapa?

Bagian 4: JARINGAN NIRKABEL (WIRELESS)

BAB 7
TEKNOLOGI JARINGAN WIRELESS

7.1. Pengantar Jaringan Wireless LAN (WLAN)

Selama ini kita membahas jaringan yang menggunakan kabel (wired network). Kabel UTP menjadi media transmisi data. Namun, perkembangan teknologi dan tuntutan mobilitas membuat **jaringan nirkabel (wireless)** menjadi sangat populer.

Apa itu Jaringan Wireless?

Jaringan wireless adalah jaringan yang menggunakan **gelombang elektromagnetik (radio frekuensi)** sebagai media transmisi data, menggantikan fungsi kabel.

Mengapa Wireless Penting?

- **Mobilitas:** Pengguna dapat bergerak bebas (di area coverage) sambil tetap terhubung ke jaringan. Bayangkan jika di kafe atau kampus kita harus duduk di dekat colokan kabel untuk bisa internetan.
- **Kemudahan Instalasi:** Tidak perlu menarik kabel ke setiap sudut ruangan. Sangat cocok untuk gedung bersejarah atau area di mana instalasi kabel sulit dilakukan.
- **Skalabilitas:** Menambah pengguna baru cukup mudah, tidak perlu mencari port kabel yang kosong.
- **Estetika:** Ruangan terlihat lebih rapi tanpa kabel yang berserakan.

Tantangan Jaringan Wireless:

- **Keamanan:** Sinyal radio menyebar ke udara, bisa "didengar" oleh siapa saja yang berada dalam jangkauan.
- **Interferensi:** Sinyal radio bisa terganggu oleh perangkat lain (microwave, bluetooth, telepon nirkabel) atau bahkan oleh dinding dan benda logam.
- **Kecepatan:** Umumnya lebih lambat dan kurang stabil dibandingkan kabel.
- **Media Bersama (Shared Medium):** Semua perangkat berbagi frekuensi yang sama. Semakin banyak perangkat, kecepatan yang didapat masing-masing perangkat bisa menurun.

7.2. Standar IEEE 802.11 (a/b/g/n/ac/ax) dan Karakteristiknya

Standar yang mengatur jaringan wireless LAN (Wi-Fi) dikeluarkan oleh institut IEEE (Institute of Electrical and Electronics Engineers) dengan kode **802.11**. Seiring waktu, muncul berbagai amendemen (tambahan huruf) yang meningkatkan kecepatan dan fitur.

Berikut adalah standar utama yang perlu diketahui:

Standar	Frekuensi	Kecepatan Maks (Teoritis)	Karakteristik
802.11a	5 GHz	54 Mbps	Cepat pada masanya, tapi jarak pendek. Kurang populer karena frekuensi 5 GHz saat itu mahal.
802.11b	2.4 GHz	11 Mbps	Populer pertama kali. Jangkauan luas, tapi lambat dan mudah interferensi.
802.11g	2.4 GHz	54 Mbps	Menggabungkan jangkauan 2.4 GHz dengan kecepatan 54 Mbps. Kompatibel dengan 802.11b.
802.11n	2.4 GHz & 5 GHz	600 Mbps	**(Wi-Fi 4)** . Memperkenalkan teknologi **MIMO (Multiple-Input Multiple-Output)** , yaitu menggunakan beberapa antena untuk mengirim dan menerima data sekaligus.
802.11ac	5 GHz	6.93 Gbps	**(Wi-Fi 5)** . Peningkatan besar-besaran. Hanya bekerja di 5 GHz (lebih bersih, sedikit interferensi). Mendukung MIMO yang lebih canggih (MU-MIMO).
802.11ax	2.4 GHz & 5 GHz	9.6 Gbps	**(Wi-Fi 6)** . Standar terbaru (saat ini). Lebih efisien, lebih cepat, lebih baik dalam menangani banyak perangkat sekaligus di area padat seperti stadion atau mall.

Catatan Penting:

- **2.4 GHz:** Jangkauan lebih jauh, lebih baik menembus dinding, tapi lebih padat dan mudah interferensi (banyak perangkat lain menggunakan frekuensi ini: bluetooth, microwave, dll).
- **5 GHz:** Jangkauan lebih pendek, kurang bisa menembus dinding, tapi lebih sedikit interferensi dan menyediakan lebih banyak kanal (channel) yang tidak saling tumpang tindih. Ideal untuk kecepatan tinggi di area terbatas.

7.3. Topologi Jaringan Wireless: Infrastructure Mode, Ad-Hoc, Mesh

Dalam membangun jaringan wireless, kita mengenal beberapa mode atau topologi dasar:

A. Infrastructure Mode

Ini adalah mode yang paling umum digunakan di rumah, kantor, kampus, dan tempat umum.

- **Komponen:** Ada perangkat sentral yang disebut **Access Point (AP)**. AP bertindak sebagai jembatan antara jaringan kabel (switch/router) dan perangkat nirkabel (client/station).
- **Cara Kerja:** Semua komunikasi antar perangkat wireless harus melalui AP. Jika Laptop A ingin berbicara dengan Laptop B, data harus naik ke AP dulu, lalu diturunkan ke Laptop B.
- **Keuntungan:** Mudah dikelola, AP dapat mengatur akses dan keamanan. Client bisa roaming (berpindah) antar AP jika area coverage luas.

B. Ad-Hoc Mode (Independent Basic Service Set - IBSS)

Mode ini adalah koneksi langsung antar perangkat wireless, tanpa menggunakan Access Point.

- **Komponen:** Hanya dua atau lebih perangkat wireless yang saling terhubung langsung.
- **Cara Kerja:** Perangkat saling mencari dan terhubung secara peer-to-peer.
- **Penggunaan:** Jarang digunakan untuk akses internet. Biasanya untuk berbagi file sementara antar dua laptop, atau untuk game multiplayer langsung.
- **Kelemahan:** Tidak terpusat, keamanan sulit diatur, jangkauan terbatas.

C. Mesh Mode

Ini adalah topologi di mana setiap perangkat (biasanya AP Mesh) saling terhubung satu sama lain, membentuk jaring (mesh).

- **Komponen:** Banyak AP Mesh yang masing-masing bisa bertindak sebagai router untuk AP lain. Biasanya ada satu AP yang terhubung ke jaringan kabel (internet), disebut RAP (Root Access Point).
- **Cara Kerja:** Data dapat melompat dari satu AP Mesh ke AP Mesh lainnya hingga mencapai tujuan. Ini sangat cocok untuk area luas di mana sulit menarik kabel ke setiap AP, seperti di halaman kampus, taman kota, atau pelabuhan.
- **Keuntungan:** Self-healing (jika satu AP mati, data bisa mencari jalur lain melalui AP lain), coverage luas.

7.4. Perangkat Wireless: Access Point, Wireless NIC, Antenna

Untuk membangun jaringan wireless, kita membutuhkan beberapa perangkat keras:

1. Access Point (AP)

- **Fungsi:** Menjadi pusat koneksi bagi perangkat wireless (infrastructure mode). Mengubah data dari jaringan kabel menjadi sinyal radio, dan sebaliknya.
- **Mode Operasi AP (di Packet Tracer):**
  - **Access Point (Standalone):** Mode default. AP berdiri sendiri, perlu dikonfigurasi satu per satu.
  - **Repeater:** Menerima sinyal dari AP utama dan memancarkannya kembali untuk memperluas jangkauan. (Mengurangi bandwidth hingga 50%).
  - **Bridge:** Menghubungkan dua jaringan kabel secara wireless.
  - **Root Bridge:** AP yang terhubung langsung ke jaringan kabel.

2. Wireless Network Interface Card (NIC)

- **Fungsi:** Perangkat keras di komputer/laptop/smartphone yang memungkinkan perangkat tersebut terhubung ke jaringan wireless. Bisa berupa chip internal di motherboard, atau USB dongle.

3. Antenna

- **Fungsi:** Memancarkan dan menerima sinyal radio. Jenis antena mempengaruhi pola pancaran sinyal.
- **Jenis Antena:**
  - **Omnidirectional:** Menyebarkan sinyal ke segala arah (360 derajat). Cocok untuk coverage area di dalam ruangan.
  - **Directional (Yagi, Parabolic):** Memfokuskan sinyal ke satu arah tertentu. Cocok untuk koneksi point-to-point jarak jauh (antar gedung).

7.5. Studi Kasus dan Latihan Analisis Kebutuhan Wireless

Skenario 1: Kafe Kecil

Sebuah kafe ingin menyediakan Wi-Fi gratis untuk pengunjung. Area sekitar 100 m^2, dengan satu router dari ISP di sudut ruangan.

- **Kebutuhan:** Coverage merata di seluruh area kafe.
- **Solusi:** Satu Access Point dengan antena omnidirectional ditempatkan di tengah ruangan, terhubung ke router ISP. Konfigurasi SSID yang mudah diingat (nama kafe). Gunakan enkripsi WPA2 untuk keamanan.

Skenario 2: Kampus Luas

Kampus ingin menyediakan Wi-Fi di area lapangan dan taman, tanpa menarik kabel ke tengah lapangan.

- **Kebutuhan:** Coverage di area terbuka luas, tanpa infrastruktur kabel di tengah.
- **Solusi:** Gunakan topologi **Mesh**. Pasang beberapa AP Mesh di tiang-tiang lampu di sekitar lapangan. Satu AP Mesh (RAP) terhubung ke jaringan kabel gedung, AP lainnya (MAP) akan saling terhubung secara wireless dan menyebarkan sinyal ke seluruh area.

Skenario 3: Kantor dengan Banyak Perangkat

Kantor dengan 50 karyawan, masing-masing membawa laptop dan smartphone. Sering terjadi lemot saat jam istirahat.

- **Kebutuhan:** Kapasitas untuk menangani banyak perangkat sekaligus.
- **Solusi:** Gunakan Access Point dengan standar terbaru **802.11ax (Wi-Fi 6)** yang dirancang untuk lingkungan padat. Bisa juga menggunakan beberapa AP dengan kanal yang tidak saling tumpang tindih (misal: kanal 1, 6, dan 11 di 2.4 GHz) untuk mendistribusikan beban.

Rangkuman Pertemuan 7:

- Jaringan wireless menggunakan gelombang radio, menawarkan mobilitas dan kemudahan instalasi.
- Standar IEEE 802.11 terus berkembang: a/b/g (legacy), n (Wi-Fi 4), ac (Wi-Fi 5), ax (Wi-Fi 6).
- Topologi utama: **Infrastructure** (dengan AP), **Ad-Hoc** (langsung antar perangkat), **Mesh** (jaring antar AP untuk coverage luas).
- Perangkat utama: Access Point, Wireless NIC, dan Antenna.

Tugas 8:

Kerjakan soal latihan yang telah disiapkan. Identifikasi tipe topologi wireless yang tepat untuk skenario-skenario yang diberikan (misal: rumah tinggal, kantor bertingkat, area parkir luas, koneksi antar gedung). Jelaskan alasan pemilihan Anda.

BAB 8: KEAMANAN DASAR JARINGAN WIRELESS

8.1. Ancaman Dasar pada Jaringan Wireless

Sifat wireless yang menyiarkan sinyal ke udara membuatnya rentan terhadap berbagai ancaman keamanan. Beberapa ancaman umum:

1. **Eavesdropping (Penyadapan):**
    - Karena sinyal menyebar ke udara, siapa pun yang berada dalam jangkauan dengan perangkat yang sesuai (misal: laptop dengan software Wireshark) dapat "mendengar" lalu lintas data yang tidak terenkripsi. Mereka bisa menangkap password, email, atau data sensitif lainnya.
2. **Unauthorized Access (Akses Tidak Sah):**
    - Jika jaringan wireless tidak diamankan dengan baik, orang asing (war driver) dapat terhubung ke jaringan kita. Mereka bisa menggunakan internet kita untuk aktivitas ilegal, atau mengakses file dan resource di jaringan lokal kita.
3. **Rogue Access Point (AP Palsu):**
    - Penyerang memasang Access Point palsu dengan SSID yang mirip dengan SSID resmi (misal: "Wifi Kampus Gratis" palsu). Pengguna yang tidak curiga terhubung ke AP palsu tersebut. Penyerang kemudian bisa menyadap semua data yang dikirim pengguna (man-in-the-middle attack).
4. **Denial of Service (DoS):**
    - Penyerang membanjiri frekuensi radio dengan sinyal gangguan (interferensi) sehingga jaringan wireless resmi tidak dapat berfungsi dengan baik.

8.2. Metode Keamanan Wireless: WEP, WPA, WPA2, WPA3

Untuk mengatasi ancaman tersebut, berbagai protokol keamanan dikembangkan. Urutan perkembangannya dari yang paling lemah ke paling kuat:

1. WEP (Wired Equivalent Privacy)

- **Status: TIDAK AMAN. JANGAN DIGUNAKAN.**
- **Cara Kerja:** Menggunakan kunci statis (sama untuk semua pengguna) dan enkripsi RC4 yang lemah.
- **Kelemahan:** Kunci dapat dipecahkan dalam hitungan menit dengan tools yang mudah didapat. Sangat rentan.

2. WPA (Wi-Fi Protected Access)

- **Status: Sementara, sudah usang.**
- **Cara Kerja:** Dibuat sebagai solusi darurat untuk menambal kelemahan WEP. Masih menggunakan enkripsi RC4, tapi dengan TKIP (Temporal Key Integrity Protocol) yang mengubah kunci secara dinamis setiap kali mengirim paket.
- **Kelemahan:** TKIP juga akhirnya ditemukan kelemahannya. Tidak direkomendasikan lagi.

3. WPA2 (Wi-Fi Protected Access 2)

- **Status: STANDAR KEAMANAN MINIMAL SAAT INI.**
- **Cara Kerja:** Menggunakan enkripsi **AES (Advanced Encryption Standard)** yang sangat kuat, dengan protokol CCMP. Jauh lebih aman daripada WEP dan WPA.
- **Mode:**
    - **WPA2-Personal (PSK - Pre-Shared Key):** Menggunakan satu password (kunci) yang sama untuk semua pengguna. Cocok untuk rumah dan kantor kecil.
    - **WPA2-Enterprise (802.1X):** Menggunakan server autentikasi terpisah (RADIUS) di mana setiap pengguna memiliki username dan password sendiri. Jauh lebih aman dan terkelola, cocok untuk perusahaan dan kampus.

4. WPA3 (Wi-Fi Protected Access 3)

- **Status: STANDAR TERBARU DAN PALING AMAN.**
- **Peningkatan:**
    - **SAE (Simultaneous Authentication of Equals):** Pengganti PSK yang lebih aman, mencegah serangan brute-force password secara offline.
    - **Enkripsi yang Lebih Kuat:** Menggunakan enkripsi 192-bit untuk mode Enterprise.
    - **Forward Secrecy:** Jika password berhasil dipecahkan di masa depan, data lama yang disadap sebelumnya tetap tidak bisa didekripsi.

- **Mudah Digunakan:** Memudahkan konfigurasi untuk perangkat tanpa layar (seperti IoT).

8.3. Konfigurasi SSID dan Keamanan WPA2 pada Access Point (Dengan Simulasi Packet Tracer)

Sekarang kita akan mempraktikkan konfigurasi dasar wireless menggunakan Cisco Packet Tracer.

Skenario:
Kita akan membangun jaringan wireless sederhana:
- 1 buah Access Point (misal: Access Point-PT).
- 2 buah Laptop (Laptop-PT) yang akan terhubung secara wireless.
- 1 buah Server (opsional) untuk DHCP, atau kita bisa menggunakan DHCP di AP.

Tujuan:
- Mengatur SSID menjadi "Kampus_Wifi".
- Mengamankan jaringan dengan WPA2-PSK, password "Polinepad123".
- Laptop dapat terhubung dan mendapatkan IP address secara otomatis.

Langkah-langkah Konfigurasi:

1. Konfigurasi Access Point:
- Klik dua kali pada Access Point.
- Buka tab **Config**.
- Di sisi kiri, pilih **Port 0** (ini adalah port ethernet/kabel). Setel ke mode **Trunk** jika akan dihubungkan ke switch dengan VLAN, atau biarkan di **Access** untuk jaringan sederhana. (Untuk latihan ini, biarkan default).
- Di sisi kiri, pilih **Port 1** (ini adalah interface wireless).
  - **SSID:** Isi dengan "Kampus_Wifi".
  - **Authentication:** Pilih **WPA2-PSK**.
  - **PSK Pass Phrase:** Isi dengan "Polinepad123" (atau password lain yang kuat).
  - **Encryption:** Biarkan **AES**.
  - Pastikan **Radio Status** dalam keadaan **On**.
- (Opsional) Jika AP tidak terhubung ke router/DHCP server, kita bisa aktifkan DHCP Server di AP.
  - Pilih menu **Services** -> **DHCP**.
  - **Pool Name:** "wifi-pool"
  - **Default Gateway:** isikan IP AP (misal 192.168.1.1)
  - **DNS Server:** 8.8.8.8 (Google DNS)
  - **Start IP Address:** 192.168.1.100
  - **Subnet Mask:** 255.255.255.0
  - **Maximum Number of Users:** 50

    - Klik **Add** lalu **Save**.
    - **Aktifkan** DHCP dengan mengklik tombol **On** di pojok kanan atas.

2. Konfigurasi Laptop:

- Klik dua kali pada Laptop.
- Pastikan Laptop dalam keadaan **Off** (matikan dulu dengan mengklik tombol power).
- Di panel kiri, ganti modul dari **PT-LAPTOP-NM-1CFE** (modul ethernet kabel) menjadi **PT-LAPTOP-NM-1W** (modul wireless). Caranya: seret modul wireless ke slot kosong, lalu kembalikan modul ethernet ke pojok kanan bawah.
- Nyalakan kembali Laptop (klik tombol power).
- Buka tab **Desktop** -> **PC Wireless**.
- Di tab **Connect**, Anda akan melihat daftar SSID yang terdeteksi. Pilih **Kampus_Wifi**.
- Klik **Connect**. Akan muncul prompt untuk memasukkan password. Isi dengan "Polinepad123".
- Setelah terhubung, buka tab **Link Status**. Anda akan melihat bahwa Laptop sudah mendapatkan IP address (jika DHCP diaktifkan).
- Untuk verifikasi, buka **Command Prompt** di Desktop, lalu `ipconfig` untuk melihat IP, dan `ping` ke IP AP atau ke server lain jika ada.

3. Verifikasi Keamanan:

- Coba lakukan hal yang sama di Laptop lain. Pastikan bisa terhubung.
- Coba salah satu Laptop untuk melakukan `ping` ke Laptop lainnya. Seharusnya berhasil karena mereka berada di jaringan wireless yang sama.
- (Untuk pengujian keamanan sederhana): Coba matikan keamanan di AP (set Authentication ke Disabled). Laptop lain dengan modul wireless (yang belum dikonfigurasi) akan langsung bisa melihat dan terhubung ke jaringan tanpa password. Ini menunjukkan pentingnya WPA2.

Rangkuman Pertemuan 8:

- Jaringan wireless rentan terhadap penyadapan, akses tidak sah, dan serangan lainnya.
- Keamanan wireless berkembang dari WEP (tidak aman), WPA (sementara), menjadi **WPA2 (standar minimal saat ini)** dan WPA3 (standar terbaru).
- WPA2-Personal menggunakan pre-shared key (password) dan enkripsi AES, cukup aman untuk rumah dan kantor kecil.
- Konfigurasi dasar di Packet Tracer meliputi pengaturan SSID, pemilihan metode autentikasi (WPA2-PSK), dan pengaturan DHCP.

Tugas 9 (Praktik - Simulasi):

Buka Cisco Packet Tracer. Buat topologi dengan:

- 1 Access Point.
- 3 Laptop dengan modul wireless.
- (Opsional) 1 Switch dan 1 Server jika ingin jaringan lebih kompleks.

1. Konfigurasikan Access Point dengan SSID "Lab_TI_2026" dan keamanan WPA2-PSK dengan password "JaringanAman".
2. Konfigurasikan DHCP di Access Point agar memberikan IP otomatis ke client.
3. Hubungkan ketiga Laptop ke jaringan wireless tersebut.
4. Verifikasi bahwa semua Laptop mendapatkan IP dan dapat saling `ping`.
5. Dokumentasikan langkah-langkah Anda, termasuk screenshot konfigurasi AP dan hasil pengujian.

Bagian 5: TROUBLESHOOTING DAN PROYEK INTEGRASI

BAB 9
TROUBLESHOOTING JARINGAN

9.1. Pendekatan Sistematis dalam Troubleshooting

Troubleshooting adalah seni dan ilmu dalam memecahkan masalah jaringan. Kemampuan ini sangat penting bagi seorang teknisi jaringan. Ketika jaringan bermasalah, jangan panik dan jangan mencoba-coba secara acak. Gunakan pendekatan sistematis.

Model OSI sebagai Panduan Troubleshooting:
Salah satu pendekatan terbaik adalah dengan menggunakan model OSI 7 layer. Kita bisa memeriksa dari layer terbawah (Physical) hingga ke layer atas (Application).

Dua Pendekatan Utama:

1. **Top-Down Approach (Dari Atas ke Bawah):**
   - **Cara:** Mulai dari layer Application (7), lalu turun ke bawah.
   - **Kapan Digunakan:** Jika masalah diduga terkait dengan aplikasi tertentu. Misal: Browser error, tapi aplikasi lain (Zoom, Email) berjalan lancar.
   - **Contoh:** Cek apakah web server merespon (Application), cek firewall (Presentation/Session), cek koneksi TCP (Transport), dll.
2. **Bottom-Up Approach (Dari Bawah ke Atas):**
   - **Cara:** Mulai dari layer Physical (1), lalu naik ke atas.
   - **Kapan Digunakan:** Jika masalah bersifat umum (tidak ada koneksi sama sekali), atau jika kita mencurigai masalah fisik.
   - **Contoh:** Cek kabel (Physical), cek link LED (Physical), cek konfigurasi IP (Network), dll. Ini adalah pendekatan yang paling umum dan direkomendasikan untuk pemula.

Langkah-Langkah Sistematis Troubleshooting:

1. **Identifikasi Masalah:** Tanyakan pada pengguna: "Apa yang tidak bisa dilakukan? Kapan mulai terjadi? Apakah ada yang berubah?" Kumpulkan gejala selengkap mungkin.
2. **Kumpulkan Informasi:** Gunakan perintah-perintah troubleshooting (ping, traceroute, show commands) untuk mengumpulkan data dari perangkat jaringan.
3. **Analisis dan Bentuk Hipotesis:** Berdasarkan data, buat dugaan sementara tentang penyebab masalah.
4. **Uji Hipotesis:** Coba perbaiki berdasarkan dugaan. Jika masalah selesai, bagus. Jika tidak, ulangi dari langkah 2 dengan informasi baru.

5. **Dokumentasikan:** Catat masalah, penyebab, dan solusinya untuk referensi di masa depan.

9.2. Perintah Dasar Troubleshooting (ping, traceroute, show commands)

Berikut adalah senjata utama kita untuk troubleshooting di perangkat Cisco dan PC:

A. Perintah di PC/Command Prompt:

- `ping [IP atau hostname]`
  - Alat paling dasar untuk menguji konektivitas layer 3 (Network).
  - Mengirim paket ICMP Echo Request dan menunggu Echo Reply.
  - **Analisis Hasil:**
    - `Reply from ...`: Sukses.
    - `Request timed out`: Tidak ada balasan. Bisa karena firewall memblokir, router tidak memiliki rute balik, atau perangkat mati.
    - `Destination host unreachable`: Router tidak tahu cara mencapai tujuan.
- `tracert [IP atau hostname]` **(Windows) /** `traceroute` **(Linux/Router)**
  - Melacak jalur yang dilalui paket menuju tujuan.
  - Sangat berguna untuk melihat di hop ke berapa paket berhenti.
- `ipconfig` **(Windows) /** `ifconfig` **(Linux)**
  - Melihat konfigurasi IP perangkat kita sendiri: IP address, subnet mask, default gateway.
- `arp -a`
  - Melihat tabel ARP (hubungan IP address dengan MAC address) di perangkat kita.

B. Perintah di Router/Switch Cisco:

- `show ip interface brief` **(atau** `show ip int br`**)**
  - **Perintah PALING PERTAMA yang harus dijalankan.**
  - Menampilkan semua interface, IP address, dan statusnya.
  - **Status:**
    - `up/up`: Interface hidup dan bekerja (layer 1 dan 2 OK).
    - `administratively down/down`: Interface dimatikan secara manual dengan perintah `shutdown`. Nyalakan dengan `no shutdown`.
    - `down/down`: Masalah fisik (kabel tidak terhubung, perangkat lawan mati).
    - `up/down`: Masalah layer 2 (misal: protokol tidak jalan, biasanya di interface serial).
- `show running-config` **(atau** `show run`**)**
  - Melihat konfigurasi yang sedang berjalan di router/switch.
- `show startup-config`
  - Melihat konfigurasi yang akan dimuat saat reboot.
- `show vlan brief`

    - (Di switch) Melihat daftar VLAN dan port apa saja yang menjadi anggotanya.
- `show interfaces trunk`
    - (Di switch) Melihat port mana saja yang menjadi trunk, dan VLAN apa saja yang diizinkan.
- `show ip route`
    - Melihat tabel routing. Apakah rute ke jaringan tujuan ada? Apakah menggunakan next-hop yang benar?
- `show ip protocols`
    - Melihat detail protokol routing yang berjalan (RIP, OSPF).
- `show ip ospf neighbor`
    - (Untuk OSPF) Melihat apakah router sudah bertetangga dengan router lain. Jika kosong, ada masalah di layer 2 atau konfigurasi OSPF.
- `debug` **commands (HATI-HATI!)**
    - Perintah untuk melihat proses secara real-time. Bisa membebani CPU router. Gunakan hanya untuk troubleshooting spesifik, dan segera nonaktifkan dengan `undebug all`.

9.3. Studi Kasus Troubleshooting Jaringan Switched (VLAN mismatch, trunk error)

Skenario 1: VLAN Mismatch (Access Port)

- **Gejala:** PC di VLAN 10 tidak bisa berkomunikasi dengan PC lain di VLAN 10 yang sama, tapi terhubung ke switch berbeda.
- **Penyebab:** Port switch tempat PC terhubung (access port) mungkin berada di VLAN yang salah.
- **Troubleshooting:**
    1. `show vlan brief` di kedua switch. Periksa di VLAN 10, port mana saja yang menjadi anggota.
    2. `show running-config interface fastEthernet 0/1` (pada port yang dimaksud). Periksa perintah `switchport access vlan ...`.
    3. **Solusi:** Jika salah, masuk ke interface config dan setel ke VLAN yang benar: `switchport access vlan 10`.

Skenario 2: Trink Port Error (Trunk Mismatch)

- **Gejala:** PC di VLAN yang sama di dua switch berbeda tidak bisa berkomunikasi.
- **Penyebab:** Port trunk antara kedua switch mungkin tidak dikonfigurasi dengan benar, atau ada ketidaksesuaian native VLAN.
- **Troubleshooting:**
    1. `show interfaces trunk` di kedua switch. Apakah port yang dimaksud muncul sebagai trunk? VLAN apa saja yang diizinkan?
    2. `show interfaces fastEthernet 0/24 switchport` (atau port trunk). Periksa mode (trunk) dan native VLAN.
    3. **Solusi:**

- Jika port tidak menjadi trunk: `switchport mode trunk`.
- Jika ada perbedaan native VLAN: Setel native VLAN yang sama di kedua sisi: `switchport trunk native vlan <number>` (biasanya dibiarkan VLAN 1, atau diubah ke VLAN khusus untuk keamanan). Native VLAN HARUS sama di kedua sisi.

9.4. Studi Kasus Troubleshooting Jaringan Routed (Routing statis salah, OSPF tidak bertetangga)

Skenario 1: Routing Statis Salah

- **Gejala:** PC di jaringan A tidak bisa ping ke PC di jaringan C, tapi bisa ke jaringan B.
- **Penyebab:** Rute statis di salah satu router mungkin salah (salah next-hop, salah subnet mask, atau salah interface).
- **Troubleshooting:**
  1. `ping` dari R1 ke R2 (10.0.0.2) dan ke R3 (10.0.0.6). Apakah koneksi antar router hidup?
  2. `show ip route` di R1. Apakah ada rute ke jaringan C (192.168.3.0/24)? Jika ada, apakah next-hop-nya benar (10.0.0.2)?
  3. `traceroute` dari R1 ke IP PC-C (192.168.3.10). Lihat di mana paket berhenti.
  4. **Solusi:** Jika rute salah atau tidak ada, tambahkan atau perbaiki dengan `ip route 192.168.3.0 255.255.255.0 10.0.0.2` (di R1).

Skenario 2: OSPF Tidak Bertetangga (Neighbor)

- **Gejala:** Tidak ada rute OSPF di tabel routing.
- **Penyebab:** Router tidak menemukan tetangga OSPF.
- **Troubleshooting:**
  1. `show ip interface brief`. Pastikan interface yang menghubungkan kedua router dalam status `up/up`.
  2. `show ip ospf neighbor`. Apakah ada output? Jika kosong, lanjutkan.
  3. `show running-config | section router ospf`. Periksa `network` statement. Apakah jaringan yang menghubungkan kedua router (misal: 10.0.0.0/30) sudah diikutsertakan dalam OSPF? Apakah wildcard mask-nya benar?
  4. `show ip ospf interface fastEthernet 0/0` (pada interface yang relevan). Apakah interface tersebut termasuk dalam OSPF? Di area berapa?
  5. **Solusi:** Jika network statement salah atau kurang, perbaiki: `network 10.0.0.0 0.0.0.3 area 0`. Pastikan kedua router berada di area yang sama pada subnet yang menghubungkan mereka.

9.5. Studi Kasus Troubleshooting Jaringan Wireless (Koneksi client, keamanan)

Skenario: Client Tidak Bisa Terhubung ke Wi-Fi

- **Gejala:** Laptop melihat SSID, tapi gagal terhubung.
- **Penyebab:** Bisa karena salah password, filter MAC address, atau DHCP tidak berfungsi.
- **Troubleshooting:**
    1. **Cek Password:** Pastikan password yang dimasukkan benar. Perhatikan huruf besar/kecil.
    2. **Cek DHCP:** Di laptop, buka command prompt, ketik `ipconfig`. Apakah mendapat IP? Jika dapat IP APIPA (169.254.x.x), berarti DHCP gagal.
        - Periksa apakah DHCP server di AP aktif.
        - Coba set IP statis di laptop (sesuai subnet AP) untuk menguji konektivitas.
    3. **Cek Filter MAC Address:** Di konfigurasi AP, apakah ada fitur MAC filtering yang diaktifkan? Jika ya, pastikan MAC address laptop sudah terdaftar.
    4. **Cek Koneksi AP ke Jaringan Kabel:** Jika AP terhubung ke switch/router, pastikan kabel ethernet di port AP dan switch berfungsi dengan baik. Cek LED indikator.

Rangkuman Pertemuan 9:

- Troubleshooting memerlukan pendekatan sistematis, seperti model OSI (bottom-up atau top-down).
- Perintah dasar di PC: `ping`, `tracert`, `ipconfig`.
- Perintah dasar di Cisco: `show ip int brief`, `show running-config`, `show vlan brief`, `show ip route`, `show ip ospf neighbor`.
- Masalah umum di jaringan switched: VLAN mismatch, trunk error.
- Masalah umum di jaringan routed: routing statis salah, OSPF tidak bertetangga.
- Masalah umum di wireless: salah password, DHCP gagal, MAC filtering.

Tugas 10 (Praktik - Simulasi):

Buka Cisco Packet Tracer. Buat topologi kecil dengan 2 switch, 2 router, dan beberapa PC yang sudah dikonfigurasi dengan VLAN dan routing statis/OSPF (gunakan konfigurasi dari tugas sebelumnya).

1. Perkenalkan **satu kesalahan** ke dalam jaringan (misal: ubah access port ke VLAN yang salah di satu switch, atau hapus satu rute statis di router).
2. Dokumentasikan gejala yang muncul (misal: PC mana yang tidak bisa saling ping).
3. Lakukan troubleshooting menggunakan perintah-perintah yang telah dipelajari. Catat setiap langkah dan perintah yang Anda gunakan.
4. Perbaiki kesalahan tersebut.
5. Buat laporan singkat tentang proses troubleshooting Anda.

Tugas 11 (Lanjutan):
Lakukan hal yang sama dengan skenario yang berbeda, misal: matikan interface trunk, atau ubah network statement OSPF.

BAB 10
PROYEK TERINTEGRASI: DESAIN JARINGAN KAMPUS KECIL

10.1. Tujuan Proyek

Setelah mempelajari semua konsep dari switching, routing, hingga wireless, saatnya kita menggabungkan semuanya dalam sebuah proyek terintegrasi. Tujuan dari proyek ini adalah:

1. Mahasiswa mampu **menganalisis kebutuhan** jaringan untuk sebuah organisasi.
2. Mahasiswa mampu **merancang topologi** jaringan yang efisien dan sesuai kebutuhan.
3. Mahasiswa mampu **mengimplementasikan konfigurasi** VLAN, routing (statis/dinamis), dan wireless.
4. Mahasiswa mampu **melakukan verifikasi dan troubleshooting** terhadap jaringan yang dibangun.
5. Mahasiswa mampu **mendokumentasikan** dan **mempresentasikan** hasil pekerjaannya.

10.2. Skenario dan Spesifikasi Kebutuhan

Skenario:
Anda adalah seorang teknisi jaringan yang ditugaskan untuk merancang dan membangun jaringan untuk sebuah kampus kecil bernama "Politeknik Maju". Kampus ini memiliki 3 gedung utama:

1. **Gedung A (Rektorat & Administrasi):**
    - 30 komputer untuk staf administrasi dan keuangan.
    - 5 printer jaringan.
    - 1 server internal (untuk data pegawai dan keuangan).
2. **Gedung B (Fakultas Teknik):**
    - 2 laboratorium komputer, masing-masing 20 komputer (total 40 komputer untuk mahasiswa).
    - 10 komputer untuk dosen dan staf laboratorium.
    - 2 server untuk laboratorium (server praktikum).
3. **Gedung C (Ruang Kelas & Perpustakaan):**
    - 10 komputer di perpustakaan untuk akses katalog dan internet.

    - Area hotspot Wi-Fi untuk mahasiswa di lorong dan taman sekitar gedung (diperkirakan 50-100 perangkat nirkabel aktif bersamaan).
    - 2 access point diperlukan untuk coverage yang merata.

Kebutuhan Fungsional:

- Setiap kelompok pengguna (Administrasi, Dosen Teknik, Mahasiswa Teknik, Perpustakaan, dan Wi-Fi) harus berada di jaringan yang terpisah (VLAN berbeda) demi keamanan dan manajemen.
- Semua jaringan harus tetap bisa mengakses internet dan server-server yang diizinkan (misal: server administrasi hanya bisa diakses dari VLAN Administrasi, server praktikum bisa diakses dari VLAN Dosen Teknik dan VLAN Mahasiswa Teknik).
- Jaringan harus andal. Jika salah satu link antar gedung putus, komunikasi antar gedung tidak boleh terputus total (redundansi).
- Jaringan wireless harus aman dengan enkripsi WPA2-PSK atau WPA2-Enterprise (untuk mahasiswa, bisa menggunakan voucher/username).

10.3. Perancangan Topologi Hierarkis

Berdasarkan kebutuhan di atas, kita perlu merancang topologi yang efisien. Kita akan menggunakan pendekatan **hierarkis 3 layer** (meskipun dalam skala kecil bisa disederhanakan):

1. **Access Layer:** Switch yang terhubung langsung ke pengguna (komputer, printer, AP). Di layer ini, kita akan menerapkan VLAN (access port).
2. **Distribution Layer:** Switch yang mengagregasi koneksi dari access layer. Di layer ini, kita akan menerapkan routing antar VLAN (menggunakan Switch Layer 3 atau Router-on-a-stick). Kita juga akan menerapkan kebijakan keamanan (misal: ACL).
3. **Core Layer:** (Opsional untuk skala kecil). Router utama yang menghubungkan jaringan kampus ke internet (ISP). Di sini kita akan menerapkan routing statis default atau routing dinamis ke ISP.

Rencana VLAN:

VLAN ID	Nama VLAN	Network IP	Keterangan
10	Admin	192.168.10.0/24	Staf administrasi & keuangan
20	Dosen_Teknik	192.168.20.0/24	Dosen Fakultas Teknik
30	Mahasiswa_Teknik	192.168.30.0/24	Mahasiswa di lab Teknik
40	Perpustakaan	192.168.40.0/24	Komputer di perpustakaan
50	Wi-Fi	192.168.50.0/24	Hotspot mahasiswa & tamu

VLAN ID	Nama VLAN	Network IP	Keterangan
99	Management	172.16.99.0/24	VLAN untuk manajemen switch (akses SSH)
100	Server	172.16.100.0/24	VLAN khusus untuk server-server

Rencana Routing:

- Antar VLAN di dalam kampus akan menggunakan **Router-on-a-stick** di Distribution Layer, atau menggunakan **Switch Layer 3** (jika tersedia di Packet Tracer, gunakan switch 3560).
- Koneksi ke internet akan menggunakan **routing statis default** dari router kampus ke router ISP.
- Untuk redundansi, kita bisa membuat dua link antara switch distribution di gedung A dan B, dan menggunakan **Spanning Tree Protocol (STP)** untuk mencegah loop, atau menggunakan **EtherChannel** untuk menggabungkan link.

10.4. Implementasi Konfigurasi Terintegrasi (Panduan Langkah demi Langkah)

Berikut adalah langkah-langkah umum implementasi di Cisco Packet Tracer. (Detail perintah diserahkan kepada mahasiswa untuk dieksplorasi berdasarkan materi sebelumnya).

Langkah 1: Bangun Topologi Fisik

- Tempatkan switch, router, server, dan PC sesuai dengan denah gedung.
- Hubungkan perangkat dengan kabel yang sesuai (UTP straight/cross).

Langkah 2: Konfigurasi Dasar Perangkat

- Beri hostname yang sesuai pada setiap switch dan router (misal: Switch_Acc_A1, Router_Dist_A).
- Setel password enable dan vty untuk akses remote (SSH jika bisa).
- Setel VLAN Manajemen (VLAN 99) dan beri IP pada interface VLAN 99 di setiap switch untuk manajemen.

Langkah 3: Konfigurasi VLAN dan Trunking

- Buat semua VLAN yang direncanakan di switch distribution (atau semua switch).
- Konfigurasi port yang terhubung ke PC/server/AP sebagai **access port** dan masukkan ke VLAN yang sesuai.
- Konfigurasi port yang menghubungkan switch satu sama lain, dan switch ke router, sebagai **trunk port**. Izinkan semua VLAN yang relevan.

Langkah 4: Konfigurasi Routing Antar VLAN

- **Opsi A (Router-on-a-Stick):** Di router distribution, buat sub-interface untuk setiap VLAN di interface yang terhubung ke switch distribution. Beri IP address

sesuai dengan network masing-masing VLAN (IP ini akan menjadi default gateway untuk perangkat di VLAN tersebut). Aktifkan encapsulation dot1Q.
- **Opsi B (Switch Layer 3):** Jika menggunakan switch 3560, aktifkan routing dengan perintah `ip routing`. Buat interface VLAN untuk setiap VLAN dan beri IP address. Pastikan port yang terhubung ke switch lain adalah trunk, dan port yang terhubung ke router core adalah routed port (atau trunk juga).

Langkah 5: Konfigurasi Routing ke Internet

- Di router kampus (core), konfigurasi IP untuk interface yang terhubung ke router ISP (misal: 203.0.113.2/30).
- Konfigurasi **default route** menuju router ISP: `ip route 0.0.0.0 0.0.0.0 203.0.113.1`.
- Di router ISP, konfigurasi IP untuk interface yang terhubung ke kampus, dan buat rute statis kembali ke jaringan internal kampus (misal: `ip route 192.168.0.0 255.255.0.0 203.0.113.2`). Atau, di router kampus, kita bisa melakukan **redistribusi** jika menggunakan routing dinamis.

Langkah 6: Konfigurasi Wireless

- Tempatkan Access Point di Gedung C (dan area luar).
- Hubungkan AP ke switch access layer di Gedung C melalui port trunk (atau access port di VLAN Wi-Fi).
- Konfigurasi AP dengan SSID "Kampus_Wifi", keamanan WPA2-PSK dengan password yang kuat.
- Pastikan AP mendapatkan IP dari DHCP server di VLAN Wi-Fi (bisa dari router atau server).

Langkah 7: Konfigurasi DHCP Server

- Di router atau server, konfigurasi DHCP pool untuk setiap VLAN (kecuali VLAN yang menggunakan IP statis, seperti server dan manajemen).
- Contoh DHCP pool untuk VLAN 10: network 192.168.10.0/24, default-gateway 192.168.10.1, DNS 8.8.8.8.

Langkah 8: Verifikasi dan Pengujian

- Lakukan `ping` dari PC di satu VLAN ke PC di VLAN yang sama (uji di dalam VLAN).
- Lakukan `ping` dari PC di satu VLAN ke PC di VLAN lain (uji routing antar VLAN). Seharusnya berhasil.
- Lakukan `ping` dari PC ke server di VLAN 100. Seharusnya berhasil.
- Lakukan `ping` dari PC ke internet (misal: 8.8.8.8). Seharusnya berhasil.
- Uji koneksi wireless: laptop harus bisa terhubung ke SSID, mendapatkan IP, dan bisa `ping` ke PC di jaringan kampus dan ke internet.

10.5. Dokumentasi dan Laporan Proyek

Laporan proyek harus mencakup:

1. **Halaman Judul:** Nama proyek, nama mahasiswa, NIM, kelas.
2. **Pendahuluan:** Latar belakang dan tujuan proyek.
3. **Analisis Kebutuhan:** Penjelasan singkat tentang skenario dan kebutuhan pengguna.
4. **Desain Topologi:**
    - Diagram topologi fisik dan logis (gunakan alat bantu seperti draw.io atau fitur Packet Tracer).
    - Tabel perangkat (nama, peran, model, interface yang digunakan).
    - Tabel IP Addressing dan VLAN.
5. **Konfigurasi:**
    - Cuplikan (screenshot) konfigurasi penting dari setiap perangkat (VLAN, trunk, routing, DHCP, wireless).
    - Jangan copy seluruh running-config, cukup bagian yang relevan.
6. **Hasil Pengujian:**
    - Hasil `ping` dan `traceroute` untuk membuktikan konektivitas (screenshot).
    - Penjelasan tentang hasil pengujian.
7. **Kesimpulan dan Saran:** Apa yang dipelajari, kesulitan yang dihadapi, dan saran untuk pengembangan.
8. **Lampiran:** (Opsional) File Packet Tracer (.pkt).

10.6. Panduan Persiapan Presentasi Proyek

Pada pertemuan 14, setiap kelompok akan mempresentasikan hasil proyek mereka. Berikut panduannya:

- **Durasi:** 10-15 menit per kelompok.
- **Konten Presentasi (Slide):**
    - Slide 1: Judul dan Anggota Kelompok.
    - Slide 2: Gambaran Umum Proyek (skenario dan kebutuhan).
    - Slide 3: Topologi Jaringan (tampilkan diagram yang jelas).
    - Slide 4: Skema IP dan VLAN.
    - Slide 5: Sorotan Konfigurasi (misal: routing antar VLAN, wireless).
    - Slide 6: Hasil Pengujian (tampilkan screenshot ping yang berhasil).
    - Slide 7: Kendala dan Solusi.
    - Slide 8: Kesimpulan.
- **Demonstrasi:** Siapkan file Packet Tracer yang sudah jadi. Tunjukkan live (atau screenshot) beberapa pengujian konektivitas.
- **Sesi Tanya Jawab:** Setiap anggota harus siap menjawab pertanyaan tentang proyek mereka, terutama bagian yang mereka kerjakan.

Rangkuman Pertemuan 10 (Proyek Mini):

- Proyek ini mengintegrasikan semua materi: switching (VLAN, trunking), routing (antar VLAN, default route), wireless, dan DHCP.
- Perancangan topologi yang baik adalah kunci keberhasilan.
- Dokumentasi yang rapi memudahkan verifikasi dan troubleshooting.
- Presentasi melatih kemampuan komunikasi dan argumentasi.

Tugas 12 (Proyek Mini - Kelompok):

Bentuk kelompok (3-4 orang). Kerjakan proyek sesuai skenario "Jaringan Kampus Kecil" di atas. Kumpulkan laporan dan file Packet Tracer sebelum pertemuan 14. Siapkan presentasi untuk dipaparkan di pertemuan 14.

Tugas 13 (Presentasi):

Presentasikan hasil proyek kelompok Anda di depan kelas.

Bagian 6: PENUTUP

BAB 11
REVIEW DAN PERSIAPAN UJIAN AKHIR

11.1. Tujuan Review

Pertemuan ini adalah pertemuan terakhir sebelum kalian menghadapi Ujian Akhir Semester (UAS). Tujuan dari review ini adalah:

1. **Menyegarkan kembali** seluruh materi yang telah dipelajari dari Pertemuan 1 hingga 15.
2. **Mengidentifikasi** bagian-bagian mana yang masih perlu dipelajari lebih lanjut.
3. **Mempraktikkan** soal-soal latihan dan studi kasus yang mirip dengan UAS.
4. **Membangun kepercayaan diri** sebelum menghadapi ujian.

UAS akan terdiri dari dua bagian:

- **Bagian Teori (40%):** Soal essay dan pilihan ganda yang menguji pemahaman konsep.
- **Bagian Praktik Simulasi (60%):** Studi kasus di Cisco Packet Tracer di mana kalian harus mengkonfigurasi jaringan dari awal atau memperbaiki jaringan yang bermasalah.

11.2. Ringkasan Materi Perkuliahan (Pertemuan 1-15)

Mari kita kilas balik semua materi yang telah kita lewati bersama.

Bagian 1: Pendahuluan (Pertemuan 1-2)

- **Model OSI & TCP/IP:** 7 layer OSI (Physical, Data Link, Network, Transport, Session, Presentation, Application) dan 4 layer TCP/IP (Network Access, Internet, Transport, Application). Pahami fungsi setiap layer.
- **Perangkat Jaringan:** Switch (Layer 2, forwarding berdasarkan MAC), Router (Layer 3, forwarding berdasarkan IP, memisahkan broadcast domain), Access Point (jembatan kabel ke wireless).
- **Collision vs Broadcast Domain:** Collision domain dipisahkan oleh switch dan router. Broadcast domain **hanya** dipisahkan oleh router. Hub memperluas collision domain.

Bagian 2: Dasar-Dasar Switching (Pertemuan 3-4)

- **VLAN (Virtual LAN):** Memisahkan satu switch fisik menjadi beberapa jaringan logis. Manfaat: keamanan, pengurangan broadcast, fleksibilitas.
- **Jenis VLAN:** Default VLAN (VLAN 1), Data VLAN, Management VLAN, Native VLAN.

- **Trunking (802.1Q):** Mengirim lalu lintas banyak VLAN melalui satu link dengan menambahkan tag VLAN ID pada frame.
- **Access Port vs Trunk Port:** Access port untuk perangkat akhir (satu VLAN). Trunk port untuk koneksi antar switch atau switch-ke-router (banyak VLAN).
- **Konfigurasi Dasar VLAN:**
  - Membuat VLAN: `vlan <id>` `name <nama>`
  - Assign access port: `switchport mode access`, `switchport access vlan <id>`
  - Konfigurasi trunk: `switchport mode trunk`, `switchport trunk allowed vlan <list>`

Bagian 3: Dasar-Dasar Routing (Pertemuan 5-7)

- **Prinsip Routing:** Meneruskan paket antar jaringan berdasarkan tabel routing.
- **Komponen Tabel Routing:** Kode sumber (C, S, R, O), jaringan tujuan, next-hop, metric, interface.
- **Routing Statis:**
  - Konfigurasi manual: `ip route <network> <mask> {next-hop | exit-interface}`
  - Default route: `ip route 0.0.0.0 0.0.0.0 <next-hop>`
  - Verifikasi: `show ip route`, `ping`, `traceroute`
- **Routing Dinamis:**
  - **RIP (Routing Information Protocol):** Distance vector, metrik hop count (max 15). Konfigurasi: `router rip`, `version 2`, `no auto-summary`, `network <network>`.
  - **OSPF (Open Shortest Path First):** Link state, metrik cost (bandwidth), konvergensi cepat, skalabel. Konfigurasi: `router ospf <process-id>`, `network <network> <wildcard> area <area-id>`.
  - Verifikasi OSPF: `show ip route`, `show ip ospf neighbor`, `show ip ospf interface`.

Bagian 4: Jaringan Nirkabel (Pertemuan 9-10)

- **Standar 802.11:** a/b/g/n/ac/ax. Pahami perbedaan frekuensi (2.4 GHz vs 5 GHz) dan kecepatan.
- **Topologi Wireless:** Infrastructure (dengan AP), Ad-Hoc (langsung), Mesh (jaring antar AP).
- **Keamanan Wireless:** WEP (tidak aman), WPA (sementara), **WPA2 (standar minimal)** , WPA3 (terbaru). WPA2-PSK untuk rumah/kantor kecil.
- **Konfigurasi Dasar AP:** Set SSID, pilih autentikasi (WPA2-PSK), set password, aktifkan DHCP.

Bagian 5: Troubleshooting dan Proyek (Pertemuan 11-14)

- **Pendekatan Troubleshooting:** Bottom-up (mulai dari layer fisik) paling direkomendasikan.
- **Perintah Penting:**
  - PC: `ping`, `tracert`, `ipconfig`

    - Cisco: `show ip int brief`, `show running-config`, `show vlan brief`, `show interfaces trunk`, `show ip route`, `show ip ospf neighbor`
- **Masalah Umum:** VLAN mismatch, trunk error, routing statis salah, OSPF tidak bertetangga, salah password Wi-Fi, DHCP gagal.
- **Proyek Terintegrasi:** Merancang jaringan kampus kecil dengan VLAN, routing antar VLAN, routing ke internet, dan wireless.

11.3. Latihan Soal Teori dan Studi Kasus Terintegrasi

Mari kita coba beberapa soal latihan untuk menguji pemahaman kalian.

A. Soal Teori (Essay Singkat):

1. **Soal:** Jelaskan perbedaan fungsi utama antara Switch, Router, dan Access Point. Pada layer OSI berapa masing-masing perangkat tersebut bekerja?
    - **Jawaban:** Switch (Layer 2) menghubungkan perangkat dalam satu jaringan lokal berdasarkan MAC Address. Router (Layer 3) menghubungkan antar jaringan yang berbeda berdasarkan IP Address. Access Point (Layer 2) bertindak sebagai jembatan antara jaringan kabel dan perangkat nirkabel.
2. **Soal:** Apa yang dimaksud dengan Collision Domain dan Broadcast Domain? Perangkat apa yang memisahkan masing-masing domain tersebut?
    - **Jawaban:** Collision domain adalah area di mana tabrakan data bisa terjadi. Dipisahkan oleh Switch dan Router. Broadcast domain adalah area di mana frame broadcast akan menjangkau semua perangkat. Hanya Router yang dapat memisahkan broadcast domain.
3. **Soal:** Sebutkan 3 manfaat utama penggunaan VLAN dalam sebuah jaringan.
    - **Jawaban:** (1) Meningkatkan keamanan dengan mengisolasi lalu lintas antar kelompok. (2) Mengurangi lalu lintas broadcast. (3) Fleksibilitas dan kemudahan manajemen (karyawan pindah ruangan tidak perlu mengubah kabel).
4. **Soal:** Jelaskan perbedaan utama antara protokol routing RIP dan OSPF dari segi metrik, cara kerja, dan skalabilitas.
    - **Jawaban:**
        - **RIP:** Metrik hop count (max 15), cara kerja distance vector (mengandalkan info tetangga), skalabilitas rendah (cocok untuk jaringan kecil).
        - **OSPF:** Metrik cost (berdasarkan bandwidth), cara kerja link state (membangun peta topologi), skalabilitas tinggi (cocok untuk jaringan besar dengan area).
5. **Soal:** Sebutkan 3 perintah troubleshooting di Cisco router/switch beserta fungsinya.
    - **Jawaban:**
        - `show ip interface brief`: Melihat status dan IP semua interface.
        - `show ip route`: Melihat tabel routing.

- `show vlan brief`: (di switch) Melihat daftar VLAN dan port anggotanya.

B. Studi Kasus Terintegrasi (Soal Praktik Simulasi - Skenario UAS):

Skenario:
Anda diberikan file Packet Tracer yang berisi topologi jaringan perusahaan "PT. Maju Jaya" yang sudah setengah jadi. Topologi terdiri dari:

- 2 buah switch (Switch1 dan Switch2) yang terhubung via trunk.
- 1 buah router (Router1) yang terhubung ke Switch1.
- 4 buah PC: PC-A dan PC-B terhubung ke Switch1, PC-C dan PC-D terhubung ke Switch2.
- 1 buah server (Server1) terhubung ke Router1.

Kondisi Awal (Yang sudah terkonfigurasi):

- Semua perangkat sudah diberi alamat IP sesuai tabel di bawah, namun **konektivitas belum berjalan sempurna**.
- VLAN 10 (Finance) dan VLAN 20 (HR) sudah dibuat di kedua switch.
- Interface router sudah diberi IP (G0/0: 192.168.1.1/24).

Perangkat	IP Address	Gateway	VLAN
PC-A	192.168.10.10/24	192.168.10.1	10
PC-B	192.168.10.11/24	192.168.10.1	10
PC-C	192.168.20.10/24	192.168.20.1	20
PC-D	192.168.20.11/24	192.168.20.1	20
Server1	192.168.1.10/24	192.168.1.1	-

Tugas Anda (Apa yang harus dilakukan/diperbaiki):

1. **Identifikasi Masalah Konektivitas:**
    - Dari PC-A, coba `ping` ke PC-B (satu VLAN, satu switch). Apakah berhasil? Jika tidak, apa kemungkinan penyebabnya? (Petunjuk: Periksa access port di Switch1).
    - Dari PC-A, coba `ping` ke PC-C (beda VLAN, beda switch). Apakah berhasil? Jika tidak, apa kemungkinan penyebabnya? (Petunjuk: Perlu routing antar VLAN dan trunk yang benar).
    - Dari PC-A, coba `ping` ke Server1 (192.168.1.10). Apakah berhasil? Jika tidak, apa kemungkinan penyebabnya? (Petunjuk: Periksa default gateway di PC, dan routing di router).

2. **Perbaiki Konfigurasi:**
    - Pastikan semua access port untuk PC berada di VLAN yang benar.
    - Pastikan port trunk antara Switch1 dan Switch2 sudah dikonfigurasi dengan benar dan mengizinkan semua VLAN yang diperlukan (VLAN 10 dan 20).
    - Konfigurasikan **router-on-a-stick** di Router1 agar dapat merutekan lalu lintas antar VLAN 10 dan 20, serta ke Server1. Buat sub-interface untuk VLAN 10 dan 20 di interface G0/0 dengan encapsulation dot1Q.
    - Pastikan default gateway di setiap PC sudah diisi dengan IP sub-interface yang sesuai (192.168.10.1 untuk VLAN 10, 192.168.20.1 untuk VLAN 20).
3. **Verifikasi:**
    - Setelah semua konfigurasi diperbaiki, pastikan:
        - PC-A bisa `ping` ke PC-B.
        - PC-A bisa `ping` ke PC-C.
        - PC-A bisa `ping` ke Server1.
        - Semua konektivitas berjalan dua arah.
4. **Dokumentasikan** perintah-perintah yang Anda gunakan untuk memperbaiki masalah dan hasil pengujiannya.

(Soal ini adalah contoh tipikal soal UAS praktik. Mahasiswa harus mampu menganalisis dan memperbaiki konfigurasi yang salah.)

11.4. Simulasi Ujian Praktik (Tips dan Trik)

Untuk mempersiapkan UAS praktik, berikut beberapa tips:

1. **Kenali Topologi Awal:** Saat membuka file ujian, luangkan 2-3 menit pertama untuk mempelajari topologi. Perangkat apa saja yang ada? Bagaimana koneksinya? IP address sudah diberikan atau belum?
2. **Baca Soal dengan Teliti:** Pahami apa yang diminta. Apakah diminta mengkonfigurasi dari awal, atau memperbaiki konfigurasi yang salah? Perhatikan detail IP, VLAN ID, dan nama interface.
3. **Kerjakan Secara Sistematis (Bottom-Up):**
    - **Layer 1 & 2:** Pastikan semua kabel terhubung dengan benar. Periksa status interface dengan `show ip int brief`. Semua interface yang digunakan harus `up/up`. Nyalakan interface yang `administratively down` dengan `no shutdown`.
    - **Layer 2 (Switching):** Periksa VLAN (`show vlan brief`). Pastikan access port di VLAN yang benar. Periksa trunk (`show interfaces trunk`). Pastikan trunk mengizinkan VLAN yang diperlukan.
    - **Layer 3 (Routing & IP):** Periksa IP address di PC dan router. Periksa tabel routing (`show ip route`). Apakah ada rute ke semua jaringan? Jika tidak, tambahkan routing statis atau perbaiki konfigurasi routing dinamis.

    - **Layer 3 (Default Gateway):** Pastikan setiap PC memiliki default gateway yang benar (biasanya IP router di VLAN tersebut).
4. **Gunakan Perintah Verifikasi Secara Rutin:** Setelah setiap langkah konfigurasi, gunakan `show running-config | section ...` atau `show ip route` untuk memastikan perintah Anda diterapkan dengan benar.
5. **Uji dengan `ping` Secara Bertahap:**
    - Uji koneksi ke gateway terlebih dahulu (dari PC `ping` ke IP router).
    - Uji koneksi ke perangkat di VLAN yang sama.
    - Uji koneksi ke perangkat di VLAN yang berbeda (pastikan routing antar VLAN berfungsi).
    - Uji koneksi ke internet jika ada.
6. **Jangan Panik Jika Ada Error:** Troubleshooting adalah bagian dari ujian. Baca pesan error, periksa kembali konfigurasi Anda.
7. **Simpan Konfigurasi:** Di akhir ujian, pastikan Anda mengetik `copy running-config startup-config` atau `write memory` di setiap router dan switch agar konfigurasi tersimpan.

11.5. Sesi Tanya Jawab

(Gunakan sesi ini untuk menjawab pertanyaan mahasiswa tentang materi yang masih kurang dipahami. Dorong mahasiswa untuk bertanya tentang topik-topik yang mereka rasa sulit, terutama yang berkaitan dengan konfigurasi praktik.)

Penutup:

Selamat, kalian telah menyelesaikan seluruh rangkaian materi mata kuliah Switching, Routing, dan Wireless. Kalian sekarang memiliki fondasi yang kuat untuk menjadi seorang teknisi jaringan yang handal. Ingatlah bahwa teori adalah dasar, tetapi praktik dan pengalaman langsung adalah kunci untuk menguasai bidang ini. Teruslah bereksperimen dengan Packet Tracer di rumah, dan jangan ragu untuk mengeksplorasi teknologi-teknologi baru di dunia jaringan.

Selamat belajar dan semoga sukses dalam Ujian Akhir Semester!

LAMPIRAN A
GLOSARIUM ISTILAH JARINGAN

Istilah	Singkatan	Penjelasan Singkat
Access Point	AP	Perangkat yang memancarkan sinyal Wi-Fi, menghubungkan perangkat nirkabel ke jaringan kabel.
Access Port	-	Port pada switch yang menjadi anggota hanya satu VLAN, digunakan untuk perangkat akhir (PC, printer).
Administrative Distance	AD	Nilai kepercayaan terhadap sumber rute. Semakin kecil nilainya, semakin dipercaya. Connected=0, Static=1, OSPF=110, RIP=120.
Address Resolution Protocol	ARP	Protokol untuk mendapatkan MAC address dari suatu IP address dalam jaringan lokal.
Bandwidth	BW	Kapasitas maksimum transfer data pada suatu link, biasanya diukur dalam bps (bit per second).
Broadcast	-	Frame atau paket yang dikirim ke semua perangkat dalam satu jaringan (broadcast domain).
Broadcast Domain	-	Kumpulan perangkat yang akan menerima frame broadcast yang dikirim oleh salah satu anggotanya. Dipisahkan oleh router.
Cisco Packet Tracer	CPT	Software simulator jaringan dari Cisco untuk keperluan pembelajaran dan praktik konfigurasi.
Classless Inter-Domain Routing	CIDR	Metode alokasi IP address yang memungkinkan penggunaan subnet mask yang tidak baku (VLSM).
Collision	-	Tabrakan data yang terjadi ketika dua perangkat mengirim data secara bersamaan dalam media bersama (half-duplex).
Collision Domain	-	Bagian jaringan di mana collision dapat terjadi. Dipisahkan oleh switch dan router.
Cost	-	Metrik yang digunakan OSPF, dihitung berdasarkan bandwidth link.
Default Gateway	-	IP address dari router yang menjadi pintu keluar menuju jaringan lain (biasanya internet).
Default Route	-	Rute khusus untuk menjangkau semua jaringan yang tidak dikenal (0.0.0.0/0).

Istilah	Singkatan	Penjelasan Singkat
Distance Vector	-	Jenis protokol routing di mana router mengirimkan tabel routing ke tetangga (contoh: RIP).
Domain Name System	DNS	Sistem yang menerjemahkan nama domain (google.com) ke IP address (142.250.185.46).
Dynamic Host Configuration Protocol	DHCP	Protokol yang memberikan konfigurasi IP secara otomatis kepada perangkat dalam jaringan.
Encapsulation	-	Proses membungkus data dari layer atas dengan header dari layer di bawahnya sebelum dikirim.
EtherChannel	-	Teknologi untuk menggabungkan beberapa link fisik menjadi satu link logis untuk meningkatkan bandwidth dan redundansi.
Fast Ethernet	FE	Standar Ethernet dengan kecepatan 100 Mbps.
Gigabit Ethernet	GE	Standar Ethernet dengan kecepatan 1000 Mbps (1 Gbps).
Hop Count	-	Metrik yang digunakan RIP, yaitu jumlah router yang harus dilewati untuk mencapai jaringan tujuan.
Hub	-	Perangkat layer 1 yang meneruskan sinyal ke semua port (memperluas collision domain).
Institute of Electrical and Electronics Engineers	IEEE	Organisasi internasional yang menetapkan standar teknologi, termasuk standar jaringan (802.3 untuk Ethernet, 802.11 untuk Wi-Fi).
Internet Protocol	IP	Protokol layer 3 yang menangani pengalamatan dan routing paket data.
Internet Service Provider	ISP	Perusahaan penyedia layanan internet.
Local Area Network	LAN	Jaringan lokal dengan cakupan terbatas (satu gedung, satu kampus).
Link State	-	Jenis protokol routing di mana router mengirimkan informasi status link ke semua router (contoh: OSPF).
MAC Address	-	Alamat fisik perangkat jaringan (48-bit), ditanamkan di NIC.
Metric	-	Nilai yang digunakan protokol routing untuk menentukan jalur terbaik ke suatu jaringan.

Istilah	Singkatan	Penjelasan Singkat
Multiple-Input Multiple-Output	MIMO	Teknologi yang menggunakan banyak antena untuk mengirim dan menerima data sekaligus, meningkatkan throughput.
Network Interface Card	NIC	Kartu antarmuka jaringan (kabel atau wireless) yang memungkinkan perangkat terhubung ke jaringan.
Next-Hop	-	Alamat IP dari router berikutnya yang harus dituju untuk mencapai suatu jaringan.
Open Shortest Path First	OSPF	Protokol routing link state yang modern, menggunakan metrik cost, dan cocok untuk jaringan besar.
Open Systems Interconnection	OSI	Model referensi 7 layer untuk komunikasi jaringan (Physical, Data Link, Network, Transport, Session, Presentation, Application).
Pre-Shared Key	PSK	Metode autentikasi di WPA2-Personal di mana semua pengguna menggunakan password yang sama.
Ping	-	Perintah untuk menguji konektivitas layer 3 dengan mengirim paket ICMP Echo Request.
RIP	RIP	Routing Information Protocol, protokol routing distance vector dengan metrik hop count (max 15).
Router	-	Perangkat layer 3 yang menghubungkan antar jaringan, melakukan routing, dan memisahkan broadcast domain.
Routing Table	-	Tabel di router yang berisi informasi tentang jaringan tujuan, next-hop, metric, dan interface.
Spanning Tree Protocol	STP	Protokol di switch untuk mencegah loop dengan cara memblokir port redundan secara logis.
Service Set Identifier	SSID	Nama jaringan Wi-Fi yang terlihat oleh pengguna.
Subnet Mask	-	Angka 32-bit yang membedakan bagian network dan host dari sebuah IP address.
Switch	-	Perangkat layer 2 yang meneruskan frame berdasarkan MAC address, memisahkan collision domain per port.
Transmission Control Protocol	TCP	Protokol layer 4 yang andal (connection-oriented), menjamin pengiriman data urut dan tanpa error.
Traceroute	-	Perintah untuk melacak jalur yang dilalui paket menuju

Istilah	Singkatan	Penjelasan Singkat
		tujuan.
Trunk Port	-	Port pada switch yang dapat membawa lalu lintas dari banyak VLAN (dengan tag 802.1Q).
User Datagram Protocol	UDP	Protokol layer 4 yang cepat (connectionless), tidak menjamin pengiriman data, cocok untuk streaming.
Variable Length Subnet Mask	VLSM	Kemampuan menggunakan subnet mask yang berbeda-beda dalam satu jaringan utama, menghemat IP.
Virtual LAN	VLAN	Metode membagi satu switch fisik menjadi beberapa jaringan logis yang terpisah.
VLAN ID	VID	Angka 12-bit (1-4094) yang mengidentifikasi sebuah VLAN.
Wide Area Network	WAN	Jaringan dengan cakupan geografis luas, menghubungkan beberapa LAN. Internet adalah WAN terbesar.
Wi-Fi	-	Merek dagang untuk teknologi jaringan nirkabel berdasarkan standar IEEE 802.11.
Wildcard Mask	-	Kebalikan dari subnet mask, digunakan dalam konfigurasi OSPF (dan ACL) untuk mencocokkan rentang IP.
Wired Equivalent Privacy	WEP	Protokol keamanan wireless lawas yang sudah tidak aman.
Wi-Fi Protected Access	WPA/WPA2 /WPA3	Protokol keamanan wireless. WPA2 adalah standar minimal saat ini, WPA3 adalah yang terbaru.

LAMPIRAN B
DAFTAR PERINTAH DASAR CISCO IOS (CHEAT SHEET)

Mode-Mode di Cisco IOS:

Perintah	Fungsi	Prompt
`enable`	Masuk ke mode privileged EXEC	`Router#`
`configure terminal`	Masuk ke mode konfigurasi global	`Router(config)#`
`interface fastEthernet 0/0`	Masuk ke mode konfigurasi interface	`Router(config-if)#`
`line console 0`	Masuk ke mode konfigurasi line console	`Router(config-line)#`
`router rip`	Masuk ke mode konfigurasi router RIP	`Router(config-router)#`
`router ospf 1`	Masuk ke mode konfigurasi router OSPF	`Router(config-router)#`
`vlan 10`	Masuk ke mode konfigurasi VLAN	`Switch(config-vlan)#`
`exit`	Keluar satu level	-
`end`	Keluar langsung ke privileged EXEC	-

Perintah Dasar dan Konfigurasi Awal:

Perintah	Fungsi
`hostname [nama]`	Memberi nama pada perangkat.
`enable secret [password]`	Mengatur password untuk masuk ke mode enable (terenkripsi).
`line console 0` `password [pass]` `login`	Mengatur password untuk akses console.
`line vty 0 4` `password [pass]` `login`	Mengatur password untuk akses remote (Telnet/SSH).
`service password-encryption`	Mengenkripsi semua password di running-config.
`banner motd #[pesan]#`	Membuat pesan selamat datang (Message of The Day).
`show running-config`	Melihat konfigurasi yang sedang berjalan.
`show startup-config`	Melihat konfigurasi yang tersimpan di NVRAM.

Perintah	Fungsi
`copy running-config startup-config` atau `write memory`	Menyimpan konfigurasi.
`reload`	Merestart perangkat.
`erase startup-config`	Menghapus konfigurasi yang tersimpan.

Konfigurasi Interface dan IP Address:

Perintah	Fungsi
`interface [tipe nomor]`	Memilih interface untuk dikonfigurasi.
`ip address [IP] [mask]`	Memberi IP address pada interface.
`no shutdown`	Mengaktifkan interface (menyalakan).
`shutdown`	Mematikan interface.
`show ip interface brief`	Menampilkan ringkasan status dan IP semua interface.
`show interfaces [tipe nomor]`	Menampilkan detail interface tertentu.
`description [teks]`	Memberi deskripsi pada interface.

Konfigurasi VLAN dan Trunking:

Perintah	Fungsi
`vlan [id]`	Membuat VLAN dengan ID tertentu.
`name [nama]`	Memberi nama pada VLAN.
`show vlan brief`	Menampilkan daftar VLAN dan port anggotanya.
`interface [tipe nomor]`	Memilih port yang akan dikonfigurasi.
`switchport mode access`	Menjadikan port sebagai access port.
`switchport access vlan [id]`	Memasukkan access port ke dalam VLAN tertentu.
`switchport mode trunk`	Menjadikan port sebagai trunk port.
`switchport trunk allowed vlan [list]`	Mengatur VLAN apa saja yang diizinkan melewati trunk.

Perintah	Fungsi
`switchport trunk native vlan [id]`	Mengubah native VLAN (default=1).
`show interfaces trunk`	Menampilkan port-port trunk dan VLAN yang diizinkan.
`show interfaces [tipe nomor] switchport`	Menampilkan detail konfigurasi switchport pada suatu interface.

Konfigurasi Routing Statis:

Perintah	Fungsi
`ip route [network] [mask] [next-hop/exit-interface]`	Menambahkan rute statis.
`ip route 0.0.0.0 0.0.0.0 [next-hop]`	Menambahkan default route.
`show ip route`	Menampilkan tabel routing.
`show ip route [network]`	Menampilkan rute spesifik ke suatu jaringan.

Konfigurasi RIP:

Perintah	Fungsi
`router rip`	Memasuki mode konfigurasi router RIP.
`version 2`	Menggunakan RIPv2.
`no auto-summary`	Mematikan auto-summary (penting untuk VLSM).
`network [network-address]`	Mendeklarasikan jaringan yang terhubung langsung.
`show ip protocols`	Menampilkan detail protokol routing yang berjalan.

Konfigurasi OSPF:

Perintah	Fungsi
`router ospf [process-id]`	Memasuki mode konfigurasi router OSPF.
`network [network] [wildcard] area [area-id]`	Mendeklarasikan jaringan yang akan diikutsertakan dalam OSPF.
`show ip ospf neighbor`	Menampilkan daftar tetangga OSPF.

Perintah	Fungsi
`show ip ospf interface`	Menampilkan detail OSPF pada setiap interface.
`show ip ospf database`	Menampilkan link-state database OSPF.

Perintah Troubleshooting dan Verifikasi:

Perintah	Fungsi
`ping [IP]`	Menguji konektivitas dasar.
`traceroute [IP]`	Melacak jalur yang dilalui paket.
`show arp`	Menampilkan tabel ARP.
`debug [opsi]`	Menampilkan proses secara real-time (gunakan hati-hati!).
`undebug all`	Mematikan semua proses debug.
`show history`	Menampilkan perintah-perintah yang pernah diketik.
`terminal history size [ukuran]`	Mengatur ukuran buffer history.

LAMPIRAN C
RUBRIK PENILAIAN (Sesuai Dokumen RPS)

(Ini adalah ringkasan rubrik penilaian yang sudah ada di halaman 10-20 dokumen RPS. Disajikan ulang di sini untuk kelengkapan bahan ajar.)

C.1 Rekapitulasi Bobot Penilaian

No	Jenis Penilaian	Jumlah	Total Bobot
1	Tugas per pertemuan	13 tugas	30%
2	Partisipasi	-	10%
3	Ujian Tengah Semester (UTS)	1	30%
4	Ujian Akhir Semester (UAS)	1	30%
	TOTAL		**100%**

C.2 Rubrik Penilaian Tugas (Contoh untuk Pertemuan 4: Konfigurasi VLAN)

Komponen Penilaian	Bobot	Skor 86-100 (Sangat Baik)	Skor 71-85 (Baik)	Skor 56-70 (Cukup)	Skor 0-55 (Kurang)
Kebenaran konfigurasi VLAN	40%	Konfigurasi VLAN sesuai skenario, semua perintah tepat, tidak ada error	Konfigurasi VLAN benar, ada 1-2 kesalahan minor	Konfigurasi VLAN kurang tepat, ada beberapa kesalahan	Konfigurasi VLAN salah/tidak berfungsi
Kebenaran konfigurasi trunking	30%	Konfigurasi trunking tepat, mode trunk aktif, semua VLAN diizinkan	Konfigurasi trunking benar, ada 1 kesalahan minor	Konfigurasi trunking kurang tepat	Konfigurasi trunking salah
Konektivitas antar VLAN	20%	Semua host dalam VLAN yang sama dapat berkomunikasi, antar VLAN berbeda tidak dapat	Sebagian besar host dapat berkomunikasi (≥80%)	Komunikasi hanya berhasil pada 60-79% host	Komunikasi tidak berjalan

Komponen Penilaian	Bobot	Skor 86-100 (Sangat Baik)	Skor 71-85 (Baik)	Skor 56-70 (Cukup)	Skor 0-55 (Kurang)
		berkomunikasi			
Dokumentasi dan pelaporan	10%	Laporan lengkap, rapi, mencakup topologi, konfigurasi, dan hasil pengujian	Laporan cukup lengkap, kurang 1-2 komponen	Laporan kurang lengkap atau kurang rapi	Laporan tidak lengkap/tidak dikumpulkan

(Rubrik lengkap untuk setiap pertemuan dapat dilihat di dokumen RPS halaman 10-20)

LAMPIRAN D:
DAFTAR REFERENSI

1. **Buku Utama (CCNA):**
   - Odom, W. (2020). *CCNA 200-301 Official Cert Guide, Volume 1 & 2*. Cisco Press.
   - Lammle, T. (2020). *CCNA Certification Study Guide: Exam 200-301*. Sybex.
2. **Buku Teori Jaringan:**
   - Forouzan, B. A. (2019). *TCP/IP Protocol Suite* (5th ed.). McGraw-Hill Education.
   - Stallings, W. (2021). *Data and Computer Communications* (11th ed.). Pearson.
   - Tanenbaum, A. S., & Wetherall, D. J. (2021). *Computer Networks* (6th ed.). Pearson.
3. **Buku Protokol dan Praktik:**
   - Hartpence, B. (2021). *Packet Guide to Core Network Protocols* (2nd ed.). O'Reilly Media.
   - Doyle, J., & Carroll, J. (2016). *Routing TCP/IP, Volume I & II* (2nd ed.). Cisco Press. (Referensi lanjutan).
4. **Sumber Online:**
   - **Cisco Networking Academy:** www.netacad.com (Materi resmi Cisco, sangat direkomendasikan).
   - **Cisco Documentation:** www.cisco.com (Dokumentasi resmi semua perintah Cisco).
   - **Packet Tracer Tutorials:** Banyak tersedia di YouTube dan blog-blog teknologi.

JURUSAN TEKNOLOGI INFORMASI

RENCANA PEMBELAJARAN SEMESTER (RPS)
PROGRAM STUDI D3-TEKNIK KOMPUTER
POLITEKNIK NEGERI PADANG

Nama Mata Kuliah	**Switching, Routing, dan Wireless (Teori)**
Kode Mata Kuliah	**CEN3201**
Semester	**2 (Dua)**
SKS	**2 SKS**
Dosen Pengampu	**Ir. H. A. Mooduto, M.Kom.**

---

1. DESKRIPSI MATA KULIAH

Mata kuliah ini membekali mahasiswa dengan pengetahuan dan keterampilan dasar dalam merancang, mengkonfigurasi, dan mengelola jaringan komputer, dengan fokus pada teknologi switching, routing (statis dan dinamis), serta jaringan nirkabel (wireless). Pembelajaran dilakukan secara teoritis dan dilengkapi dengan simulasi menggunakan perangkat lunak simulator jaringan (Cisco Packet Tracer) untuk mempersiapkan mahasiswa menghadapi kebutuhan industri di bidang jaringan. Mata kuliah ini merupakan fondasi penting bagi profil lulusan sebagai Teknisi Jaringan Komputer dan IT Support.

2. CAPAIAN PEMBELAJARAN LULUSAN (CPL) YANG DIBEBANKAN PADA MATA KULIAH

Berdasarkan kurikulum Program Studi D3-Teknik Komputer, CPL yang relevan dengan mata kuliah ini adalah:

Kode CPL	Deskripsi Capaian Pembelajaran Lulusan
CPL-5	Mampu menganalisis kebutuhan jaringan, merancang topologi sederhana, serta melakukan instalasi, konfigurasi, dan *troubleshooting* perangkat jaringan (router, switch, *access point*) untuk memastikan konektivitas yang stabil dan aman.

3. CAPAIAN PEMBELAJARAN MATA KULIAH (CPMK)

Setelah mengikuti mata kuliah ini, **mahasiswa mampu**:

Kode CPMK	Deskripsi Capaian Pembelajaran Mata Kuliah
CPMK-1	Menjelaskan konsep dasar switching, routing, dan jaringan wireless serta arsitektur protokol TCP/IP. (C2)
CPMK-2	Mengkonfigurasi switch untuk implementasi VLAN dan spanning-tree protocol. (C3)
CPMK-3	Mengkonfigurasi routing statis dan dinamis (RIP, OSPF) pada router. (C3)
CPMK-4	Mengimplementasikan jaringan wireless dengan keamanan dasar. (C3)
CPMK-5	Melakukan *troubleshooting* terhadap permasalahan umum pada jaringan switched, routed, dan wireless. (C4)

4. KEMAMPUAN AKHIR YANG DIHARAPKAN (SUB-CPMK)

Kode Sub-CPMK	Deskripsi Kemampuan Akhir (Sub-CPMK)	Keterkaitan dengan CPMK
Sub-CPMK-1	Menjelaskan model OSI dan TCP/IP, fungsi perangkat jaringan (switch, router, access point).	CPMK-1
Sub-CPMK-2	Membedakan konsep collision domain dan broadcast domain.	CPMK-1
Sub-CPMK-3	Menjelaskan konsep VLAN dan trunking.	CPMK-2
Sub-CPMK-4	Mengkonfigurasi VLAN dan trunking pada switch.	CPMK-2
Sub-CPMK-5	Menjelaskan konsep routing dan tabel routing.	CPMK-3
Sub-CPMK-6	Mengkonfigurasi routing statis.	CPMK-3
Sub-CPMK-7	Menjelaskan prinsip routing dinamis (RIP, OSPF).	CPMK-3
Sub-CPMK-8	Mengkonfigurasi routing dinamis (RIP, OSPF) pada router.	CPMK-3
Sub-CPMK-9	Menjelaskan standar dan topologi jaringan wireless.	CPMK-4
Sub-CPMK-10	Mengkonfigurasi access point dan keamanan dasar wireless (WPA2).	CPMK-4
Sub-CPMK-11	Melakukan verifikasi dan troubleshooting koneksi jaringan.	CPMK-5
Sub-CPMK-12	Menganalisis dan memperbaiki kesalahan konfigurasi pada jaringan.	CPMK-5

5. TABEL KORELASI CPL – CPMK

CPL	CPMK-1	CPMK-2	CPMK-3	CPMK-4	CPMK-5	Bobot CPL (%)
CPL-5	√	√	√	√	√	100%

Catatan: Bobot CPL-5 pada mata kuliah ini adalah 100% karena seluruh CPMK mendukung pencapaian CPL-5.

6. TABEL KORELASI CPL - SUB-CPMK

CPL	Sub-CPMK-1	Sub-CPMK-2	Sub-CPMK-3	Sub-CPMK-4	Sub-CPMK-5	Sub-CPMK-6	Sub-CPMK-7	Sub-CPMK-8	Sub-CPMK-9	Sub-CPMK-10	Sub-CPMK-11	Sub-CPMK-12
CPL-5	√	√	√	√	√	√	√	√	√	√	√	√

7. DAFTAR REFERENSI

1. Odom, W. (2020). *CCNA 200-301 Official Cert Guide, Volume 1 & 2*. Cisco Press.
2. Lammle, T. (2020). *CCNA Certification Study Guide: Exam 200-301*. Sybex.
3. Forouzan, B. A. (2019). *TCP/IP Protocol Suite* (5th ed.). McGraw-Hill Education.
4. Stallings, W. (2021). *Data and Computer Communications* (11th ed.). Pearson.
5. Hartpence, B. (2021). *Packet Guide to Core Network Protocols* (2nd ed.). O'Reilly Media.

8. BAHAN KAJIAN (POKOK BAHASAN)

- Model OSI dan TCP/IP
- Perangkat Jaringan (Switch, Router, Access Point)
- Konsep VLAN dan Trunking
- Routing Statis dan Dinamis (RIP, OSPF)
- Jaringan Nirkabel (Wireless LAN) dan Keamanannya
- Troubleshooting Jaringan

9. RENCANA PEMBELAJARAN

Pertemuan Ke-	Kemampuan Akhir (Sub-CPMK)	Topik Bahasan	Metode Pembelajaran	Pengalaman Belajar Mahasiswa	Waktu (Menit)	Kriteria & Indikator Penilaian	Bobot (%) Penilaian	CPL yang Dikaitkan
1	**Sub-CPMK-1:** Menjelaskan model OSI dan TCP/IP, fungsi perangkat jaringan (switch, router, access point).	Pengantar Jaringan: Model OSI & TCP/IP, Perangkat Jaringan	Ceramah, Diskusi	Membaca referensi, mengerjakan kuis singkat tentang layer OSI.	100	Ketepatan menjelaskan fungsi masing-masing layer dan perangkat.	2% (Tugas 1)	CPL-5
2	**Sub-CPMK-2:** Membedakan konsep collision domain dan broadcast domain.	Konsep Domain: Collision vs Broadcast, Peran Switch dan Router	Ceramah, Studi Kasus	Menganalisis topologi sederhana untuk menentukan collision dan broadcast domain.	100	Kemampuan mengidentifikasi domain pada topologi.	2% (Tugas 2)	CPL-5

Pertemuan Ke-	Kemampuan Akhir (Sub-CPMK)	Topik Bahasan	Metode Pembelajaran	Pengalaman Belajar Mahasiswa	Waktu (Menit)	Kriteria & Indikator Penilaian	Bobot (%) Penilaian	CPL yang Dikaitkan
3	**Sub-CPMK-3:** Menjelaskan konsep VLAN dan trunking.	VLAN dan Trunking: Konsep, Manfaat, Standar 802.1Q	Ceramah, Diskusi	Menyelesaikan soal latihan tentang perhitungan VLAN dan trunk.	100	Ketepatan menjelaskan cara kerja VLAN dan trunk.	2% (Tugas 3)	CPL-5
4	**Sub-CPMK-4:** Mengkonfigurasi VLAN dan trunking pada switch.	Konfigurasi VLAN dan Trunking di Cisco Switch	Workshop Simulasi (Packet Tracer)	Melakukan konfigurasi VLAN dan trunking di simulator.	100	Kebenaran konfigurasi dan konektivitas antar VLAN.	3% (Tugas 4)	CPL-5
5	**Sub-CPMK-5:** Menjelaskan konsep routing dan tabel routing.	Dasar Routing: Prinsip, Tabel Routing, Metrik	Ceramah, Studi Kasus	Membuat tabel routing sederhana berdasarkan topologi yang diberikan.	100	Ketepatan menentukan jalur dan metrik.	2% (Tugas 5)	CPL-5
6	**Sub-CPMK-6:** Mengkonfigurasi routing statis.	Konfigurasi Routing Statis	Workshop Simulasi (Packet Tracer)	Melakukan konfigurasi routing statis antar router.	100	Kebenaran konfigurasi dan konektivitas antar jaringan.	3% (Tugas 6)	CPL-5
7	**Sub-CPMK-7 & 8:** Menjelaskan dan mengkonfigurasi routing dinamis (RIP, OSPF).	Routing Dinamis: RIP, OSPF (Konsep dan Konfigurasi Dasar)	Workshop Simulasi, Diskusi	Membandingkan RIP dan OSPF, melakukan konfigurasi dasar OSPF.	100	Ketepatan menjelaskan perbedaan dan kebenaran konfigurasi.	3% (Tugas 7)	CPL-5

Pertemuan Ke-	Kemampuan Akhir (Sub-CPMK)	Topik Bahasan	Metode Pembelajaran	Pengalaman Belajar Mahasiswa	Waktu (Menit)	Kriteria & Indikator Penilaian	Bobot (%) Penilaian	CPL yang Dikaitkan
8	**UJIAN TENGAH SEMESTER (UTS)**	Materi Pertemuan 1-7	Ujian Tertulis	Menjawab soal essay dan studi kasus	100	Ketepatan jawaban sesuai kunci	30%	CPL-5
9	**Sub-CPMK-9:** Menjelaskan standar dan topologi jaringan wireless.	Pengantar Jaringan Wireless: Standar IEEE 802.11, Topologi	Ceramah, Studi Kasus	Mengidentifikasi tipe topologi wireless berdasarkan skenario.	100	Kemampuan memilih topologi yang tepat.	2% (Tugas 8)	CPL-5
10	**Sub-CPMK-10:** Mengkonfigurasi access point dan keamanan dasar wireless (WPA2).	Konfigurasi Access Point dan Keamanan Wireless	Workshop Simulasi	Melakukan konfigurasi SSID, enkripsi WPA2 pada access point.	100	Kebenaran konfigurasi keamanan.	3% (Tugas 9)	CPL-5
11	**Sub-CPMK-11:** Melakukan verifikasi dan troubleshooting koneksi jaringan.	Troubleshooting Jaringan: Perintah Dasar (ping, traceroute, show commands)	Workshop Simulasi, Studi Kasus	Menggunakan perintah troubleshooting untuk mendiagnosis masalah.	100	Ketepatan mengidentifikasi masalah dan solusi.	3% (Tugas 10)	CPL-5
12	**Sub-CPMK-12:** Menganalisis dan memperbaiki kesalahan konfigurasi pada jaringan.	Studi Kasus Troubleshooting Lanjutan	Studi Kasus, Diskusi Kelompok	Menganalisis topologi bermasalah dan memperbaikinya.	100	Kemampuan memperbaiki konfigurasi yang salah.	3% (Tugas 11)	CPL-5

Pertemuan Ke-	Kemampuan Akhir (Sub-CPMK)	Topik Bahasan	Metode Pembelajaran	Pengalaman Belajar Mahasiswa	Waktu (Menit)	Kriteria & Indikator Penilaian	Bobot (%) Penilaian	CPL yang Dikaitkan
13	**Sub-CPMK-4,6,8,10 (Review dan Praktik Terintegrasi)**	Proyek Mini: Merancang Jaringan Kampus Kecil	Workshop Proyek	Mendesain dan mengkonfigurasi jaringan yang menggabungkan VLAN, routing, dan wireless.	100	Kebenaran desain dan konfigurasi, serta laporan.	3% (Tugas 12)	CPL-5
14	**Sub-CPMK-1 s.d 12 (Penguatan)**	Presentasi Proyek dan Diskusi	Presentasi, Diskusi	Mempresentasikan hasil proyek dan menjawab pertanyaan.	100	Kejelasan presentasi, kemampuan argumentasi.	2% (Tugas 13)	CPL-5
15	**Review Materi**	Review seluruh materi dan persiapan UAS	Ceramah, Tanya Jawab	Mengikuti review dan bertanya.	100	Partisipasi aktif	0% (Bonus)	CPL-5
16	**UJIAN AKHIR SEMESTER (UAS)**	Materi Pertemuan 1-15	Ujian Tertulis & Praktik Simulasi	Menjawab soal essay dan menyelesaikan studi kasus konfigurasi di simulator.	100	Ketepatan jawaban dan konfigurasi	30%	CPL-5

Total Bobot Penilaian:

- Tugas per pertemuan (13 tugas): 2% x 5 + 3% x 8 = 10% + 24% = **34%** (disesuaikan menjadi 30% dengan merata-rata, namun di atas sudah dihitung 30% tepat jika beberapa tugas 2% dan beberapa 3%, total 30%. Dalam tabel di atas total tugas = 30%).
- Partisipasi: 10% (dinilai dari keaktifan selama diskusi, bertanya, dan presentasi).
- UTS: 30%
- UAS: 30%

  Total: 100%

Mengetahui,
Ketua Program Studi D3-Teknik Komputer

(Andre Febrian Kasmar, S.T., M.T)

Padang, 23 Februari 2026
Dosen Pengampu,

(Ir. H. A. Mooduto, M.Kom.)

RUBRIK PENILAIAN

MATA KULIAH: CEN3201-SWITCHING, ROUTING, DAN WIRELESS (2 SKS Teori)

PROGRAM STUDI D3-TEKNIK KOMPUTER POLITEKNIK NEGERI PADANG

A. RUBRIK PENILAIAN TUGAS PER PERTEMUAN

Pertemuan 1: Sub-CPMK-1 (Model OSI dan TCP/IP)

Komponen Penilaian	Bobot	Skor 86-100 (Sangat Baik)	Skor 71-85 (Baik)	Skor 56-70 (Cukup)	Skor 0-55 (Kurang)
Ketepatan menjelaskan fungsi layer OSI	50%	Menjelaskan semua 7 layer dengan fungsi yang tepat dan contoh protokol yang akurat	Menjelaskan 5-6 layer dengan fungsi tepat, kurang contoh	Menjelaskan 3-4 layer dengan fungsi cukup tepat	Menjelaskan <3 layer atau fungsi keliru
Ketepatan menjelaskan fungsi perangkat jaringan	30%	Menjelaskan fungsi switch, router, access point dengan detail dan perbedaannya jelas	Menjelaskan fungsi ketiga perangkat dengan baik, kurang detail perbedaan	Menjelaskan 2 perangkat dengan tepat, 1 perangkat kurang tepat	Menjelaskan <2 perangkat atau fungsi keliru
Ketepatan menjawab kuis	20%	Menjawab semua soal dengan benar (>90%)	Menjawab 70-89% soal dengan benar	Menjawab 50-69% soal dengan benar	Menjawab <50% soal dengan benar

Pertemuan 2: Sub-CPMK-2 (Collision vs Broadcast Domain)

Komponen Penilaian	Bobot	Skor 86-100	Skor 71-85	Skor 56-70	Skor 0-55
Kemampuan mengidentifikasi collision domain	40%	Mengidentifikasi semua collision domain pada topologi kompleks dengan tepat	Mengidentifikasi sebagian besar collision domain (≥80%)	Mengidentifikasi 60-79% collision domain	Mengidentifikasi <60% collision domain
Kemampuan mengidentifikasi broadcast domain	40%	Mengidentifikasi semua broadcast domain pada topologi kompleks dengan tepat	Mengidentifikasi sebagian besar broadcast domain (≥80%)	Mengidentifikasi 60-79% broadcast domain	Mengidentifikasi <60% broadcast domain
Ketepatan analisis peran perangkat	20%	Menjelaskan dengan tepat peran switch dalam membagi collision domain dan router dalam membagi broadcast domain	Menjelaskan dengan baik namun kurang detail	Penjelasan kurang tepat atau hanya sebagian	Penjelasan keliru

Pertemuan 3: Sub-CPMK-3 (Konsep VLAN dan Trunking)

Komponen Penilaian	Bobot	Skor 86-100	Skor 71-85	Skor 56-70	Skor 0-55
Ketepatan menjelaskan konsep VLAN	40%	Menjelaskan definisi, manfaat, dan cara kerja VLAN dengan sangat jelas dan sistematis	Menjelaskan dengan baik namun kurang 1-2 aspek	Penjelasan kurang lengkap atau kurang tepat	Penjelasan keliru atau tidak relevan
Ketepatan menjelaskan konsep trunking	30%	Menjelaskan fungsi trunk, standar 802.1Q, dan cara kerja tagging dengan detail	Menjelaskan dengan baik namun kurang detail	Penjelasan kurang tepat atau hanya sebagian	Penjelasan keliru
Kemampuan menyelesaikan soal latihan	30%	Menyelesaikan semua soal dengan benar dan menunjukkan langkah perhitungan yang sistematis	Menyelesaikan ≥80% soal dengan benar	Menyelesaikan 60-79% soal dengan benar	Menyelesaikan <60% soal dengan benar

Pertemuan 4: Sub-CPMK-4 (Konfigurasi VLAN dan Trunking)

Komponen Penilaian	Bobot	Skor 86-100	Skor 71-85	Skor 56-70	Skor 0-55
Kebenaran konfigurasi VLAN	40%	Konfigurasi VLAN sesuai skenario, semua perintah tepat, tidak ada error	Konfigurasi VLAN benar, ada 1-2 kesalahan minor	Konfigurasi VLAN kurang tepat, ada beberapa kesalahan	Konfigurasi VLAN salah/tidak berfungsi
Kebenaran konfigurasi trunking	30%	Konfigurasi trunking tepat, mode trunk aktif, semua VLAN diizinkan	Konfigurasi trunking benar, ada 1 kesalahan minor	Konfigurasi trunking kurang tepat	Konfigurasi trunking salah
Konektivitas antar VLAN	20%	Semua host dalam VLAN yang sama dapat berkomunikasi, antar VLAN berbeda tidak dapat berkomunikasi	Sebagian besar host dapat berkomunikasi (≥80%)	Komunikasi hanya berhasil pada 60-79% host	Komunikasi tidak berjalan
Dokumentasi dan pelaporan	10%	Laporan lengkap, rapi, mencakup topologi, konfigurasi, dan hasil pengujian	Laporan cukup lengkap, kurang 1-2 komponen	Laporan kurang lengkap atau kurang rapi	Laporan tidak lengkap/tidak dikumpulkan

Pertemuan 5: Sub-CPMK-5 (Konsep Routing dan Tabel Routing)

Komponen Penilaian	Bobot	Skor 86-100	Skor 71-85	Skor 56-70	Skor 0-55
Ketepatan menjelaskan prinsip routing	40%	Menjelaskan prinsip routing, fungsi tabel routing, dan metrik dengan sangat jelas dan contoh	Menjelaskan dengan baik namun kurang 1-2 aspek	Penjelasan kurang lengkap	Penjelasan keliru
Kemampuan membuat tabel routing	40%	Membuat tabel routing lengkap dan tepat untuk semua router berdasarkan topologi	Membuat tabel routing benar untuk ≥80% router	Membuat tabel routing benar untuk 60-79% router	Membuat tabel routing salah untuk >40% router
Ketepatan menentukan jalur dan metrik	20%	Menentukan jalur terbaik dan nilai metrik dengan tepat untuk semua skenario	Menentukan dengan tepat untuk sebagian besar skenario (≥80%)	Menentukan dengan tepat untuk 60-79% skenario	Menentukan dengan keliru

Pertemuan 6: Sub-CPMK-6 (Konfigurasi Routing Statis)

Komponen Penilaian	Bobot	Skor 86-100	Skor 71-85	Skor 56-70	Skor 0-55
Kebenaran konfigurasi routing statis	50%	Konfigurasi route statis pada semua router dengan tepat, menggunakan next-hop atau exit-interface yang benar	Konfigurasi benar pada ≥80% router, ada 1-2 kesalahan minor	Konfigurasi benar pada 60-79% router, ada beberapa kesalahan	Konfigurasi salah pada >40% router
Konektivitas antar jaringan	30%	Semua jaringan dapat saling terhubung (full connectivity)	Sebagian besar jaringan terhubung (≥80%)	60-79% jaringan terhubung	<60% jaringan terhubung
Verifikasi konfigurasi	20%	Menggunakan perintah show ip route, ping, traceroute dengan tepat untuk memverifikasi	Menggunakan perintah verifikasi dengan baik namun kurang 1-2 aspek	Menggunakan perintah verifikasi kurang tepat	Tidak melakukan verifikasi atau keliru

Pertemuan 7: Sub-CPMK-7 & 8 (Routing Dinamis RIP/OSPF)

Komponen Penilaian	Bobot	Skor 86-100	Skor 71-85	Skor 56-70	Skor 0-55
Ketepatan menjelaskan perbedaan RIP dan OSPF	30%	Menjelaskan perbedaan RIP dan OSPF secara komprehensif (metrik, konvergensi, skalabilitas, classful/classless)	Menjelaskan dengan baik namun kurang 1-2 aspek	Penjelasan kurang lengkap atau kurang tepat	Penjelasan keliru
Kebenaran konfigurasi OSPF	40%	Konfigurasi OSPF pada semua router dengan tepat (network statements, router-id, area)	Konfigurasi benar pada ≥80% router, ada 1-2 kesalahan minor	Konfigurasi benar pada 60-79% router	Konfigurasi salah pada >40% router
Verifikasi dan konektivitas	30%	Semua jaringan terhubung, tabel routing OSPF lengkap, verifikasi dengan show ip ospf, show ip route	Sebagian besar jaringan terhubung (≥80%)	60-79% jaringan terhubung	<60% jaringan terhubung

Pertemuan 8: UJIAN TENGAH SEMESTER (UTS)

Komponen Penilaian	Bobot	Skor 86-100	Skor 71-85	Skor 56-70	Skor 0-55
Soal teori (50%)	50%	Menjawab semua soal teori dengan benar, lengkap, dan sistematis	Menjawab ≥80% soal dengan benar	Menjawab 60-79% soal dengan benar	Menjawab <60% soal dengan benar
Studi kasus (50%)	50%	Menganalisis studi kasus dengan tepat, memberikan solusi lengkap dan terstruktur	Analisis tepat, solusi cukup lengkap (≥80%)	Analisis kurang tepat, solusi kurang lengkap	Analisis keliru, solusi tidak relevan

Pertemuan 9: Sub-CPMK-9 (Standar dan Topologi Wireless)

Komponen Penilaian	Bobot	Skor 86-100	Skor 71-85	Skor 56-70	Skor 0-55
Ketepatan menjelaskan standar IEEE 802.11	40%	Menjelaskan berbagai standar 802.11 (a/b/g/n/ac/ax) dengan frekuensi, kecepatan, dan karakteristiknya	Menjelaskan sebagian besar standar (≥80%) dengan tepat	Menjelaskan 60-79% standar dengan tepat	Menjelaskan <60% standar atau keliru
Kemampuan memilih topologi wireless	40%	Memilih topologi (infrastructure, ad-hoc, mesh) yang tepat untuk berbagai skenario dengan alasan jelas	Memilih topologi tepat untuk ≥80% skenario	Memilih topologi tepat untuk 60-79% skenario	Memilih topologi keliru untuk >40% skenario
Analisis kebutuhan	20%	Menganalisis kebutuhan jaringan wireless untuk studi kasus dengan sangat tepat	Analisis cukup tepat	Analisis kurang tepat	Analisis keliru

Pertemuan 10: Sub-CPMK-10 (Konfigurasi Access Point dan Keamanan Wireless)

Komponen Penilaian	Bobot	Skor 86-100	Skor 71-85	Skor 56-70	Skor 0-55
Kebenaran konfigurasi SSID	30%	Konfigurasi SSID tepat, broadcast SSID sesuai kebutuhan	Konfigurasi SSID benar, ada 1 kesalahan minor	Konfigurasi SSID kurang tepat	Konfigurasi SSID salah
Kebenaran konfigurasi keamanan WPA2	40%	Konfigurasi WPA2 dengan enkripsi AES, password kuat, semua parameter tepat	Konfigurasi WPA2 benar, ada 1-2 kesalahan minor	Konfigurasi keamanan kurang tepat (WEP/WPA)	Konfigurasi keamanan salah/tidak ada
Konektivitas client wireless	30%	Semua client dapat terhubung dengan aman dan mendapatkan IP	Sebagian besar client (≥80%) terhubung	60-79% client terhubung	<60% client terhubung

Pertemuan 11: Sub-CPMK-11 (Verifikasi dan Troubleshooting)

Komponen Penilaian	Bobot	Skor 86-100	Skor 71-85	Skor 56-70	Skor 0-55
Penggunaan perintah troubleshooting	30%	Menggunakan perintah ping, traceroute, show commands dengan tepat dan efisien	Menggunakan perintah dengan baik namun kurang 1-2 perintah	Penggunaan perintah kurang tepat	Tidak dapat menggunakan perintah dengan benar
Kemampuan mengidentifikasi masalah	40%	Mengidentifikasi sumber masalah dengan tepat berdasarkan gejala dan data yang ada	Mengidentifikasi sebagian besar masalah (≥80%)	Mengidentifikasi 60-79% masalah	Mengidentifikasi <60% masalah atau keliru
Kemampuan memberikan solusi	30%	Memberikan solusi yang tepat, terstruktur, dan dapat diimplementasikan	Solusi tepat namun kurang detail	Solusi kurang tepat	Solusi keliru

Pertemuan 12: Sub-CPMK-12 (Analisis dan Perbaikan Kesalahan Konfigurasi)

Komponen Penilaian	Bobot	Skor 86-100	Skor 71-85	Skor 56-70	Skor 0-55
Kemampuan menganalisis konfigurasi yang salah	40%	Menganalisis konfigurasi dan menemukan semua kesalahan dengan tepat dan cepat	Menemukan ≥80% kesalahan	Menemukan 60-79% kesalahan	Menemukan <60% kesalahan
Kemampuan memperbaiki konfigurasi	40%	Memperbaiki semua kesalahan dengan konfigurasi yang tepat, jaringan kembali normal	Memperbaiki ≥80% kesalahan	Memperbaiki 60-79% kesalahan	Memperbaiki <60% kesalahan
Dokumentasi proses troubleshooting	20%	Mendokumentasikan langkah-langkah troubleshooting dengan jelas, sistematis, dan lengkap	Dokumentasi cukup lengkap	Dokumentasi kurang lengkap	Dokumentasi tidak ada/tidak rapi

Pertemuan 13: Proyek Mini (Jaringan Kampus Kecil)

Komponen Penilaian	Bobot	Skor 86-100	Skor 71-85	Skor 56-70	Skor 0-55
Kebenaran desain topologi	25%	Mendesain topologi yang efisien, sesuai kebutuhan, dan mengikuti prinsip hierarkis	Desain baik, ada 1-2 kekurangan	Desain cukup, ada beberapa kekurangan	Desain tidak sesuai/tidak efisien
Kebenaran konfigurasi VLAN	20%	Konfigurasi VLAN dan trunking tepat sesuai desain	Konfigurasi benar, ada 1-2 kesalahan minor	Konfigurasi kurang tepat	Konfigurasi salah
Kebenaran konfigurasi routing	20%	Konfigurasi routing (statis/dinamis) tepat, semua jaringan terhubung	Konfigurasi benar, ada 1-2 kesalahan minor	Konfigurasi kurang tepat	Konfigurasi salah
Kebenaran konfigurasi wireless	15%	Konfigurasi access point dan keamanan tepat	Konfigurasi benar, ada 1 kesalahan minor	Konfigurasi kurang tepat	Konfigurasi salah
Dokumentasi dan laporan	20%	Laporan lengkap (topologi, konfigurasi, pengujian, analisis), rapi, dan sistematis	Laporan cukup lengkap	Laporan kurang lengkap	Laporan tidak lengkap/tidak ada

Pertemuan 14: Presentasi Proyek

Komponen Penilaian	Bobot	Skor 86-100	Skor 71-85	Skor 56-70	Skor 0-55
Kejelasan presentasi	30%	Presentasi jelas, terstruktur, mudah dipahami, menggunakan alat bantu yang efektif	Presentasi cukup jelas	Presentasi kurang jelas	Presentasi tidak jelas
Kemampuan menjelaskan desain dan konfigurasi	30%	Menjelaskan desain dan konfigurasi dengan rinci, logis, dan tepat	Menjelaskan dengan baik, kurang 1-2 aspek	Penjelasan kurang rinci atau kurang tepat	Penjelasan keliru
Kemampuan menjawab pertanyaan	30%	Menjawab pertanyaan dengan tepat, logis, dan percaya diri	Menjawab dengan baik untuk sebagian besar pertanyaan	Menjawab kurang tepat untuk beberapa pertanyaan	Tidak dapat menjawab pertanyaan
Kerjasama tim	10%	Semua anggota tim berpartisipasi aktif dan saling mendukung	Sebagian besar anggota aktif	Hanya beberapa anggota yang aktif	Tidak ada kerjasama tim

Pertemuan 15: Review Materi (Bonus Partisipasi)

Komponen Penilaian	Bobot	Skor 86-100	Skor 71-85	Skor 56-70	Skor 0-55
Partisipasi aktif dalam review	100% (Bonus)	Aktif bertanya, menjawab pertanyaan dosen, memberikan kontribusi positif	Cukup aktif	Kurang aktif	Tidak berpartisipasi

Pertemuan 16: UJIAN AKHIR SEMESTER (UAS)

Komponen Penilaian	Bobot	Skor 86-100	Skor 71-85	Skor 56-70	Skor 0-55
Soal teori (40%)	40%	Menjawab semua soal teori dengan benar, lengkap, dan sistematis	Menjawab ≥80% soal dengan benar	Menjawab 60-79% soal dengan benar	Menjawab <60% soal dengan benar
Soal praktik simulasi (60%)	60%	Menyelesaikan studi kasus konfigurasi di simulator dengan tepat, semua fitur berfungsi, troubleshooting berhasil	Menyelesaikan ≥80% konfigurasi dengan benar	Menyelesaikan 60-79% konfigurasi dengan benar	Menyelesaikan <60% konfigurasi dengan benar

---

B. RUBRIK PENILAIAN PARTISIPASI (10%)

Kriteria	Skor 86-100 (Sangat Baik)	Skor 71-85 (Baik)	Skor 56-70 (Cukup)	Skor 0-55 (Kurang)
Keaktifan bertanya/menjawab (50%)	Aktif bertanya dan/atau menjawab di setiap pertemuan, pertanyaan berkualitas	Aktif di sebagian besar pertemuan (≥80%)	Aktif di 60-79% pertemuan	Aktif di <60% pertemuan
Kualitas kontribusi diskusi (50%)	Kontribusi relevan, menunjukkan pemahaman mendalam, membantu teman	Kontribusi cukup relevan dan membantu	Kontribusi kurang relevan atau hanya sekedar pendapat	Tidak memberikan kontribusi berarti

---

C. REKAPITULASI BOBOT PENILAIAN

No	Jenis Penilaian	Jumlah	Total Bobot
1	Tugas per pertemuan	13 tugas	30%
2	Partisipasi	-	10%
3	Ujian Tengah Semester (UTS)	1	30%
4	Ujian Akhir Semester (UAS)	1	30%
	TOTAL		**100%**

Catatan Implementasi:

1. Dosen mengisi skor untuk setiap komponen penilaian pada setiap pertemuan.
2. Nilai akhir tugas per pertemuan adalah rata-rata dari seluruh komponen penilaian pada pertemuan tersebut.
3. Nilai partisipasi diakumulasi dari seluruh pertemuan.
4. Nilai akhir mahasiswa = (Rata-rata nilai tugas × 30%) + (Nilai partisipasi × 10%) + (Nilai UTS × 30%) + (Nilai UAS × 30%).

Mengetahui,
Ketua Program Studi D3-Teknik Komputer

(Andre Febrian Kasmar, S.T., M.T)

Padang, 23 Februari 2026
Dosen Pengampu,

(Ir. H. A. Mooduto, M.Kom.)